



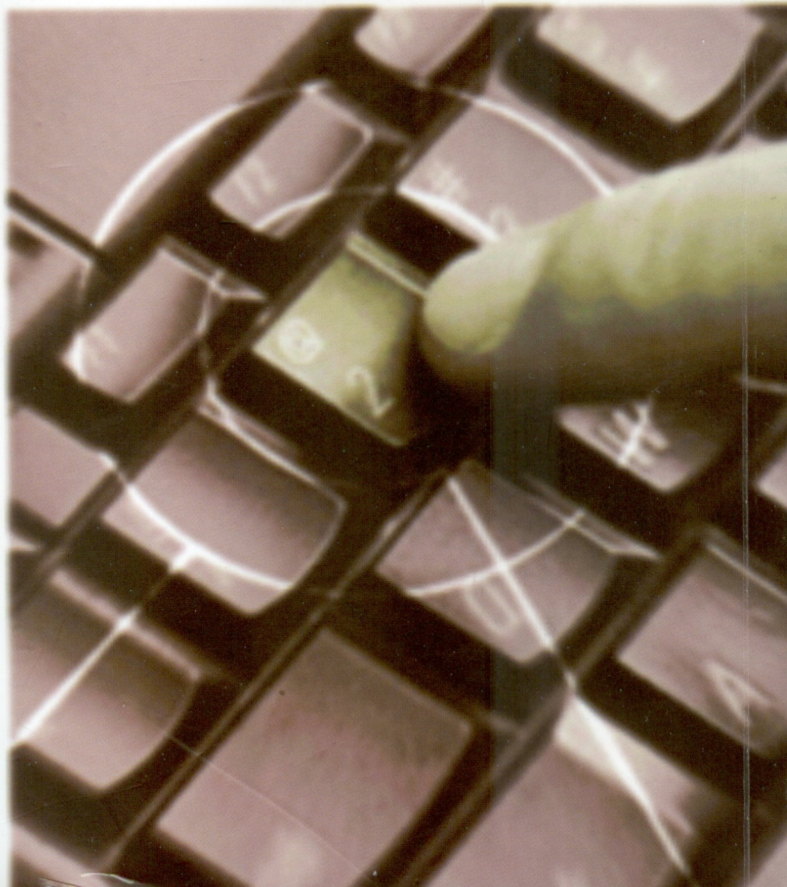
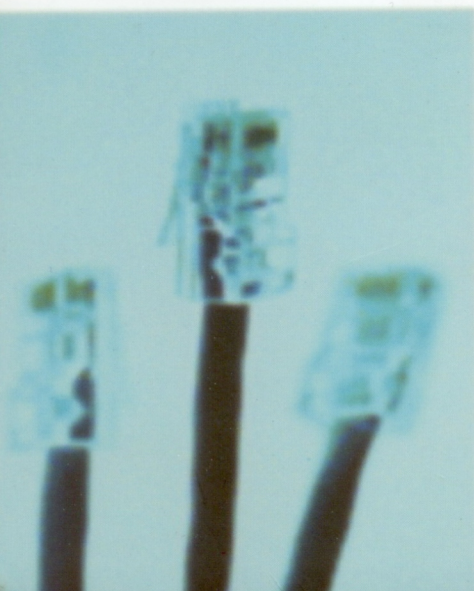
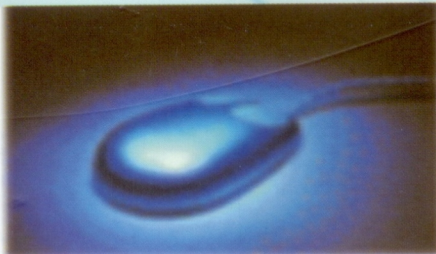
وزارت ارتباطات و فناوری اطلاعات
معاونت فناوری اطلاعات

جلد اول

دستورالعمل‌های اجرایی مدیریت امنیت اطلاعات

طرح تدوین طرح جامع فناوری اطلاعات کشور

کد پروژه : 40812001-04-3-4 ITMP



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



وزارت ارتباطات و فناوری اطلاعات
معاونت فناوری اطلاعات

دستورالعمل‌های اجرایی مدیریت امنیت اطلاعات

جلد اول

طرح تدوین طرح جامع فناوری اطلاعات کشور

(کد پروژه: ITMP-40812001-04-3-4)

مجری طرح:

مهندس عبدالمجید ریاضی

معاون فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات

گروه تدوین:

مهندس بهنام ولی‌زاده

دکتر علی ناصری

مهندس سید علیرضا میرمعینی

مهندس محمد مهدی نظام‌آبادی

مهندس حمید خوانساری

مهندس علی ثاقب

مهندس مرتضی انصاری

مهندس بیژن مولایی

سال ۱۳۸۸

سرشناسه	: ریاضی، عبدالمجید، ۱۳۳۰
عنوان و نام پدیدآور	: دستورالعمل‌های اجرایی مدیریت امنیت اطلاعات (جلد اول): طرح تدوین طرح جامع فناوری اطلاعات کشور (کد پروژه 4-3-4-40812001-TMP) / مجری طرح عبدالمجید ریاضی؛
	: گروه تدوین: علی ناصری، بهنام ولی‌زاده [و دیگران]
مشخصات نشر	: تهران: نص: ۱۳۸۸
مشخصات ظاهری	: ۷۷۶ ص جدول نمودار
شابک	: 976-964-410-201-1
وضعیت فهرست نویسی	: فیا.
یادداشت	: گروه تدوین: علی ناصری، بهنام ولی‌زاده، محمد مهدی نظام‌آبادی، سیدعلی‌رضا میرمعینی، حمیدخوانساری، علی ثاقب موفق و بیژن مولایی
موضوع	: کامپیوترها -- ایمنی اطلاعات -- مدیریت -- دستنامه‌ها
شناسه افزوده	: ناصری، علی، ۱۳۴۸ -
شناسه افزوده	: ولی‌زاده، بهنام، ۱۳۵۵ -
رده بندی کنگره	: ۱۳۸۸ ۹۲۹/۷۶ QA
رده بندی دیویی	: ۶۵۸/۴۷۸
شماره کتابشناسی ملی	: ۱۷۷۲۳۰۵

دستورالعمل‌های اجرایی مدیریت امنیت اطلاعات – جلد اول

گروه تدوین: ناصری / ولی‌زاده / نظام‌آبادی / میرمعینی / خوانساری / ثاقب موفق / انصاری / مولایی

ویراستار: عاطفه قوامی فر

چاپ اول: تابستان ۸۸

تیراژ: ۲۰۰۰

ناشر: «نص»

چاپ و صحافی: سازمان چاپ و انتشارات وزارت فرهنگ و ارشاد اسلامی

طراحی و آماده‌سازی: موسسه علمی و فرهنگی «نص»

دفتر:

تلفن:

وب سایت:

ISBN: 976-964-410-201-1

شابک: ۹۷۶-۹۶۴-۴۱۰-۲۰۱-۱

پیشگفتار

زندگی بشر از عصر تولید انبوه به عصر ارتباطات و اطلاعات ارتقاء یافته و حرکت تکاملی کشورهای جهان به سوی جوامع اطلاعاتی و دانش بنیان، کلیه فرایندها و فعالیت‌های اقتصادی، فرهنگی، صنعتی، سیاسی و روابط اجتماعی را تحت تاثیر قرار داده است.

چارچوب ساختاری تشکیل دهنده این عصر را تولید، پردازش، انتقال و مدیریت اطلاعات و ارتباطات به منظور ایجاد پایگاه‌های دانش و معرفت فردی، گروهی، سازمانی و کشور تشکیل می‌دهد و لذا فناوری اطلاعات را که شامل فناوری‌های به کارگرفته شده در فرایند مذکور می‌باشد برای جوامع بشری به عنوان عامل حیاتی و تعیین کننده مطرح ساخته است.

در دنیای امروز اطلاعات نه تنها به عنوان یکی از منابع و دارایی‌های اصلی سازمان‌ها شناخته می‌شود بلکه در حکم وسیله و ابزاری برای مدیریت اثر بخش بر سایر منابع و دارایی‌های سازمان (منابع مالی، نیروی انسانی و غیره) نیز محسوب می‌شود و لذا از اهمیت و ارزش ویژه‌ای برخوردار گشته است. اما این ارزش تنها در صورتی محقق و دست یافتنی خواهد بود که اطلاعات بتوانند در زمان مناسب، با کیفیت مطلوب و امنیت قابل قبول در اختیار افراد مناسب قرارگیرد و ارتباطات به صورت مطلوب و بهینه در سازمان برقرار گردد. از این رو است که فناوری اطلاعات که زمینه‌ساز انتقال، جابجایی، به کارگیری و مدیریت موثر اطلاعات در کشورها می‌باشد، از اهمیتی حیاتی برخوردار گشته است. لذا در راستای چشم‌انداز بیست ساله جمهوری اسلامی ایران مبنی بر تحقق جامعه‌ای توسعه یافته، متناسب با مقتضیات فرهنگی، متکی بر اصول اخلاقی و ارزش‌های اسلامی، حفظ هویت ایرانی اسلامی با تاکید بر مردم سالاری دینی و عدالت اجتماعی، آزادی‌های مشروع، حفظ کرامت و حقوق انسان‌ها و برخوردار از دانش پیشرفته از یک طرف، و تاثیر عمیق فناوری اطلاعات و ارتباطات بر ابعاد مختلف زندگی بشر و بالاخص نقش حیاتی و حساس آن در جنبه‌های فرهنگی، اقتصادی، امنیتی، اجتماعی و سیاسی از طرف دیگر وزارت ارتباطات و فناوری اطلاعات را برآن داشت که جهت برنامه‌ریزی کلان توسعه فناوری اطلاعات اقدام به پیشنهاد طرح تدوین طرح جامع فناوری اطلاعات کشور به سازمان مدیریت و برنامه‌ریزی نماید

که بعد از بررسی کارشناسی طی موافقت‌نامه‌ای به امضاء طرفین (وزارت ارتباطات و فناوری اطلاعات و سازمان مدیریت و برنامه‌ریزی) رسید این موافقت‌نامه شامل ۵ پروژه اصلی؛ تدوین طرح کلان فناوری اطلاعات، تدوین برنامه اجرایی وظایف وزارت در حوزه امنیت (افتا)، ایجاد بانک اطلاعاتی وضعیت فناوری اطلاعات، تدوین چارچوب کاربردهای فناوری اطلاعات در کشور، تهیه و پیش‌نویس لوایح و مقررات حقوقی است که هر کدام حاوی زیر بخش‌های مختلف می‌باشند.

امید است انجام فعالیت‌های مندرج در این طرح بتواند زمینه توسعه و ارتقاء صنعت و خدمات فناوری اطلاعات در کشور را مهیا سازد. این کتاب نتیجه حاصل یکی از فعالیت‌های طرح می‌باشد که با همت کارشناسان فناوری اطلاعات به سرانجام رسیده است.

عبدالمجید ریاضی

مجری طرح تدوین طرح جامع فناوری اطلاعات

پیشگفتار.....	۱
مقدمه.....	۱
۱- دیباچه.....	۱
۲- ساختار گزارش.....	۲
۳- ساختار دستورالعمل ها.....	۳
۴- مبانی راهبردی و مستندات قانونی تأمین امنیت در حوزه فناوری اطلاعات.....	۴
۱- ماهیت و ملاحظات اجرایی نظام مدیریت امنیت اطلاعات.....	۷
۱-۱- ماهیت و نوع دستورالعمل های اجرایی نظام مدیریت امنیت اطلاعات.....	۷
۲-۱- سلسله مراتب سازمانی در ایجاد و به کارگیری نظام مدیریت امنیت اطلاعات.....	۱۲
۳-۱- سلسله مراتب سیاست گذاری و اجرا در نظام مدیریت امنیت اطلاعات.....	۱۲
۴-۱- ترتیب اجرای دستورالعمل های نظام مدیریت امنیت اطلاعات.....	۱۴
۵-۱- ملاحظات هزینه یی در ایجاد و پیاده سازی نظام مدیریت امنیت اطلاعات.....	۱۶
۲- مبانی مدیریت امنیت اطلاعات.....	۲۱
۱-۲- مدیریت امنیت اطلاعات (مقدمه ای بر انتخاب روش و تعریف نهادها و مکانیزم های حفظ امنیت اطلاعات).....	۲۱
۱-۲-۱- ترسیم وضعیت مطلوب.....	۲۳
۱-۲-۲- سیاست گذاری امنیتی، سازماندهی براساس روش استاندارد انتخاب شده.....	۲۴
۱-۲-۳- تهیه لیست دارایی های اطلاعاتی.....	۲۸
۱-۲-۴- تحلیل ریسک و انتخاب ابزار.....	۳۰
۱-۲-۵- انتخاب محدوده عملیاتی، زمانبندی عملیات و مدیریت ریسک.....	۳۱
۱-۲-۶- ممیزی.....	۳۲
۱-۲-۷- عملیات تصحیحی.....	۳۳
۱-۲-۸- به هنگام سازی چرخه فعالیت و بازنگری روش انجام کار.....	۳۳
۱-۲-۹- آموزش و کسب گواهینامه های معتبر داخلی یا بین المللی.....	۳۳
۲-۲- راهنمای استفاده.....	۳۴
۳-۲- مثال برای اختصاصی سازی.....	۳۷
۴-۲- دستورالعمل تولید و کنترل اسناد.....	۳۸
۳- دستورالعمل ها.....	۴۷
۱-۳- سیاست گذاری امنیتی.....	۵۲
۲-۳- سازمان (دهی) امنیت اطلاعات.....	۹۵
۳-۳- مدیریت دارایی های اطلاعاتی.....	۱۹۵
۴-۳- کنترل دسترسی.....	۳۵۱
تعریف ها و اصطلاحات.....	۸۱۷

مقدمه

۱- دیباچه

هدف از اجرای این طرح تدوین دستورالعمل‌های اجرایی مدیریت امنیت اطلاعات بر اساس استاندارد بین‌المللی ISO-27001 می‌باشد. این دستورالعمل‌ها در سه مرحله بر اساس جدول پیشنهادی BS-7799 برای تدوین بیانیه کاربردپذیری (SOA) تدوین خواهند شد. به عبارت دیگر تدوین دستورالعمل‌ها به نحوی خواهد بود که بتوان بر اساس آن‌ها به اسناد مورد نیاز برای پیاده‌سازی بیانیه کاربردپذیری سامانه مدیریت امنیت اطلاعات دست یافت. از آن‌جا که استاندارد BS-7799 به عنوان یکی از منابع اصلی استاندارد ملی "مدیریت حفاظت اطلاعات - قسمت ۲، ویژگی‌های سیستم مدیریت حفاظت اطلاعات" مورد استفاده واقع شده است، این دستورالعمل‌ها نیز به طور کامل منطبق بر آموزه‌های استاندارد ملی مدیریت حفاظت اطلاعات مصوب کمیته ملی استاندارد رایانه و فراوری داده‌ها مورخ ۱۳۸۲/۷/۲۹ خواهد بود.

در تدوین این دستورالعمل‌ها اصول زیر مورد توجه قرار خواهند گرفت:

- توجه به ساختارهای اداری و سازمانی نهادهای بهره‌بردار.
- راهنمایی نهادهای بهره‌بردار برای ایجاد واحدهای متصدی مدیریت و حفظ امنیت اطلاعات
- اولویت بندی مراحل انجام طرح به‌طوری‌که در اولین مرحله به دستورالعمل‌هایی پرداخته خواهد شد که حتی‌الامکان برای پیاده‌سازی آن‌ها نیاز به تخصیص بودجه‌های کلان نباشد (البته بدیهی است که دستیابی به سطح قابل قبول امنیت مستلزم صرف بودجه‌های مرتبط خواهد بود).
- ارائه فرآیند قدم به قدم جهت پیاده‌سازی دستورالعمل‌ها از طریق روندنماهای اجرایی.

۲- ساختار گزارش

گزارش حاضر در سه بخش جداگانه تدوین شده است که عبارت‌اند از:

- الف- ماهیت و ملاحظات اجرایی نظام مدیریت امنیت اطلاعات
- ب- مبانی نظام مدیریت امنیت اطلاعات، روش تولید و استفاده از مستندات
- ج- دستورالعمل‌های نظام مدیریت امنیت اطلاعات

لازم به توضیح است که طی این پروژه بخش اول دستورالعمل‌های مرتبط با امنیت اطلاعات برای تأمین اهداف کنترلی زیر تدوین و ارائه شده‌اند و متعاقباً بخش‌های دوم و سوم تدوین و منتشر خواهند شد. دستورالعمل‌های بخش اول متعلق به چهار سرفصل اصلی مدیریت امنیت (بر اساس استاندارد ISO/IEC-27001) به شرح زیر می‌باشند:

- الف- سیاست گذاری امنیت اطلاعات
- ب- سازماندهی امنیت اطلاعات
- ج- مدیریت دارایی‌ها و تحلیل ریسک امنیتی
- د- کنترل دسترسی
- سایر سرفصل‌های امنیت اطلاعات به شرح زیر می‌باشد:
- امنیت منابع (نیروی انسانی)
- امنیت فیزیکی و محیطی
- مدیریت ارتباطات و عملیات
- برپایی، توسعه و نگهداری سیستم‌های اطلاعاتی
- مدیریت وقایع امنیت اطلاعات
- مدیریت پیوستگی (تداوم) عملیات
- انطباق

البته همان‌طور که می‌توان حدس زد پیاده‌سازی فصل‌های اخیر مستلزم صرف هزینه‌های بیشتر و قابل توجه می‌باشد و دستورالعمل‌های مربوط در قالب دو مرحله جداگانه دیگر منتشر خواهد شد.

۳- ساختار دستورالعمل‌ها

دستورالعمل‌های تدوین شده حاوی مطالب زیر خواهد بود:

- هدف از اجرای دستورالعمل
- مسئولیت‌های اجرایی و افراد مجری
- فرآیند اجرایی
- ابزار، تجهیزات و نرم‌افزارها و سخت‌افزارهای مورد نیاز
- روند نما (فلوچارت اجرایی)

ساختار فوق در کلیه دستورالعمل‌ها رعایت خواهد گردید. به علاوه هر دستورالعمل دارای سطوح مختلف اجرایی خواهد بود که با توجه به نوع سازمان، نوع داده‌ها و سیستم‌های اطلاعاتی ذخیره شده در سازمان، نحوه و حجم تعامل سازمان با ارباب رجوع یا سازمان‌های دیگر و پارامترهای زیربط اضافی تعیین خواهد گردید. (این پارامترها تحت عنوان شناسه اهمیت نهاد بهره‌بردار و شناسه طبقه‌بندی امنیتی اطلاعات در نهاد بهره‌بردار لحاظ خواهند شد که نحوه تعیین آن‌ها و تخصیص شناسه‌ها در دستورالعمل‌های طبقه‌بندی تشریح خواهد شد).

بدیهی است دستورالعمل‌های مربوط به سازمان‌های مهمتر پیچیدگی بیشتری نسبت به سازمان‌های عادی خواهند داشت. مبنای طبقه‌بندی سازمان‌ها از لحاظ امنیت و درجه حساسیت، معیارهای ارائه شده از طرف سازمان‌های مرجع مانند سازمان پدافند غیرعامل و نهادهای زیربط در دولت جمهوری اسلامی ایران می‌باشد.

انتشار دستورالعمل‌های مدیریت امنیت اطلاعات با هدف ارائه راه حل‌هایی عملی برای تأمین امنیت اطلاعات الکترونیکی شهروندان جمهوری اسلامی ایران انجام می‌پذیرد. قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران وظایف زیر را برای دولت جمهوری اسلامی ایران بر شمرده است:

- ماده ۴۴ (بند ج): تهیه و تصویب سند راهبردی برقراری امنیت در فضای تولید و تبادل اطلاعات کشور در محیط‌های رایانه‌ای
- ماده ۱۰۰ (بند و): حفظ و صیانت از حریم خصوصی افراد

- ماده ۱۰۰ (بند ز): ارتقای احساس امنیت اجتماعی در مردم و جامعه

علاوه بر آن ایجاد ساختارهای دفاعی در سطوح مختلف جامعه و کشور از وظایف ذاتی دولت‌ها می‌باشد. بنابراین از کلیه نهادهای وابسته به نظام جمهوری اسلامی ایران انتظار می‌رود حداکثر سعی خود را در نیل به اهداف مندرج در میثاق‌های ملی مانند قانون اساسی و قوانین توسعه‌ای و سندهای راهبردی مصوب از سوی نهادهای مسئول به انجام رسانند. در تدوین دستورالعمل‌های حاضر ارائه الگویی قابل پیاده‌سازی، قابل ارزیابی و پاسخگو جهت نیل به اهداف فوق مد نظر قرار گرفته است.

۴- مبانی راهبردی و مستندات قانونی تأمین امنیت در حوزه فناوری اطلاعات

"زندگی بشر از عصر تولید انبوه به عصر ارتباط و اطلاعات ارتقاء یافته و حرکت تکاملی کشورهای جهان به سوی جوامع اطلاعاتی و دانش بنیان، کلیه فرآیندها و فعالیت‌های اقتصادی، فرهنگی، صنعتی، سیاسی و روابط اجتماعی را تحت تأثیر قرار داده است.

چهارچوب ساختاری تشکیل دهنده این عصر را تولید، پردازش، انتقال و مدیریت اطلاعات و ارتباطات به منظور ایجاد پایگاه‌های دانش و معرفت فردی، گروهی، سازمانی و کشوری تشکیل می‌دهد و لذا فناوری اطلاعات را که شامل فناوری‌های به‌کار گرفته شده در فرآیند مذکور می‌باشد برای جوامع بشری به عنوان عامل حیاتی و تعیین کننده مطرح ساخته است".

مطالب فوق که عیناً از پیشگفتار سند راهبردی "نظام جامع فناوری اطلاعات کشور" نقل شده است گویای توجه به اهمیت و تأثیر فناوری‌های اطلاعات در سطوح عالی راهبری و مدیریت کشور می‌باشد. در بخش دیگری از سند مذکور گفته شده است:

"در دنیای امروز اطلاعات نه تنها به عنوان یکی از منابع و دارایی‌های اصلی سازمان شناخته می‌شوند، بلکه در حکم وسیله و ابزاری برای مدیریت اثر بخش بر سایر منابع و دارایی‌های سازمان (منابع مالی، نیروی انسانی و غیره) نیز محسوب می‌شود و لذا از اهمیت و ارزش ویژه‌ای برخوردار گشته است. اما این ارزش تنها در صورتی محقق و دست یافتنی خواهد بود که اطلاعات بتواند در زمان مناسب، با کیفیت مطلوب و امنیت قابل قبول در اختیار افراد مناسب قرار گیرد و ارتباطات به صورت مطلوب و بهینه در سازمان برقرار گردد".

معاونت فناوری اطلاعات بر اساس وظایف ذاتی و مأموریت سازمانی خود اقدام به تدوین پیش نویس سند راهبردی نظام جامع فناوری اطلاعات در قالب ۷ حوزه راهبردی، ۲۹ راهبرد و ۱۳۳ راهکار نمود که این سند در جلسه مورخ ۸۶/۸/۱۹ کمیسیون راهبرد شورای عالی فناوری اطلاعات به تصویب اعضای کمیسیون رسیده و نهایتاً در تاریخ ۸۶/۱۰/۵ مورد تصویب هیأت محترم وزیران قرار گرفت. این سند به عنوان مستند اصلی طرح تدوین دستورالعمل‌های مدیریت امنیت اطلاعات تلقی شده و مورد مراجعه قرار خواهد گرفت.

علاوه بر آن اسناد و راهبردهای مرتبط با متون زیر به عنوان سایر مبانی تدوین دستورالعمل‌های مدیریت امنیت اطلاعات مورد مراجعه قرار خواهد گرفت و سعی بر آن بوده است که الزامات مطرح شده در آن‌ها نیز رعایت شوند:

- سند امنیت فضای تبادل اطلاعات کشور- افتا (شورای عالی افتا-۱۳۸۴)
- مطالعات تجارت الکترونیک- متا (وزارت بازرگانی- ۱۳۸۴)
- قانون تجارت الکترونیک
- قانون حفاظت از حقوق پدید آورندگان نرم‌افزار

دلیل اصلی اجرای طرح تدوین دستورالعمل‌های مدیریت امنیت اطلاعات انجام حرکتی بنیادی در جهت استانداردسازی فعالیت‌های جاری در حوزه فناوری اطلاعات و ارتباطات می‌باشد و مبتنی بر سند چشم انداز بیست ساله جمهوری اسلامی ایران است که بیان می‌دارد:

"ایران کشوری است توسعه یافته با جایگاه اول اقتصادی، علمی و فناوری در سطح منطقه، با هویت اسلامی و انقلابی، الهام بخش در جهان اسلام و با تعامل سازنده و مؤثر در روابط بین الملل".

استانداردسازی مدل مدیریت امنیت اطلاعات فعالیت‌هایی است که می‌توان از طریق آن و بر اساس تعریف مدل‌های قابل ارزیابی ایجاد و حفظ محرمانگی، جامعیت (صحت) و دسترسی پذیری، دستیابی امن، کارا و به موقع به اطلاعات و دارایی‌های اطلاعاتی را تضمین نمود و در نتیجه به اهداف زیر دست یافت

- اطمینان بخشی به کاربران و طرف‌های اداری، تجاری و بین المللی
- پاسخگویی در مقابل افراد ذینفع، کاربران، مراجع حکومتی و مردم

- رعایت قابل اثبات قرارها و قراردادهای دو یا چند جانبه، مقررات و قوانین موضوعه
 - دستیابی به سیستمی قابل بهبود و تصحیح پذیر
- نتایج اجرای این طرح در ارتباط مستقیم با راهکارهای زیر مندرج در سند "نظام جامع فناوری اطلاعات کشور" می‌باشد:
- بند و-۴-۶-۱- استقرار نظام مدیریت و راهبری امنیت فضای تبادل اطلاعات کشور
 - بند و-۴-۶-۲- استانداردسازی محصولات و ساز و کار امنیت حوزه فناوری اطلاعات
 - بند و-۴-۶-۴- ایجاد نظام پیشگیری و مقابله با تهدیدات مختلف در حوزه فناوری اطلاعات
- همچنین از زحمات و کوشش‌های افراد زیر که در طول اجرای این طرح با اعلام نظرات اصلاحی خود موجب افزایش کیفیت خروجی‌ها شده‌اند قدردانی می‌شود:
- آقای مهندس محمد مهدی نظام آبادی، کارشناس مسئول طرح، دفتر امور زیربنایی فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات
 - آقای مهندس سید علیرضا میرمعینی، مدیرعامل موسسه پژوهش‌های راهبردی امن رای
 - آقای مهندس حمید خوانساری، کارشناس امنیت اطلاعات حوزه ستادی وزارت ارتباطات و فناوری اطلاعات
 - آقای مهندس علی ثاقب، اداره حفاظت شبکه شرکت ارتباطات زیرساخت
 - آقای مهندس مرتضی انصاری، کارشناس ارشد امنیت اطلاعات در وزارت آموزش و پرورش
 - آقای مهندس بیژن مولایی، کارشناس ارشد امنیت اطلاعات بانک سپه
- همچنین دفتر امور زیربنایی فناوری اطلاعات ضمن پذیرفتن مسئولیت خطاهای احتمالی موجود در اسناد، از متخصصان و افراد صاحب نظر تقاضا دارد نظرات اصلاحی خود را به این دفتر ارسال نمایند.

مهندس بهنام ولی‌زاده	دکتر علی ناصری
معاون دفتر امور زیر بنایی فناوری اطلاعات	عضو هیأت علمی دانشگاه امام حسین (ع)
وزارت ارتباطات و فناوری اطلاعات	و مدیر کل امور زیر بنایی فناوری اطلاعات

۱- ماهیت و ملاحظات اجرایی نظام مدیریت امنیت اطلاعات

۱-۱- ماهیت و نوع دستورالعمل‌های اجرایی نظام مدیریت امنیت اطلاعات

هدف از تدوین دستورالعمل‌های اجرایی نظام مدیریت امنیت اطلاعات معرفی روشی کارا و سازمان‌یافته و قدم به قدم جهت برپاسازی یک نظام مدیریتی می‌باشد، به‌طوری‌که بتوان با استفاده از رهنمودهای ارائه شده و در دسترس، مبادرت به ایجاد یک مرجع یا مرکز و یا به‌طور کلی نهاد جهت تصدی‌گری امور مربوط به امنیت اطلاعات نمود. البته اندازه این نهاد و روابط آن با سایر اجزای سازمان بستگی به نیازها و سیاست‌گذاری‌های کلی نهاد مادر دارد. به عنوان مثال ایجاد این نهاد در ستاد مرکزی یک وزارتخانه باید با توجه به مأموریت‌های آن وزارتخانه انجام پذیرد و متناسب با گستردگی حوزه فعالیت آن وزارتخانه در سطح کشور و یا سطح اهمیت فعالیت‌های آن وزارتخانه باشد.

از طرف دیگر ممکن است متقاضی ایجاد این نهاد یک واحد تولیدی متوسط در یکی از شهرک‌های صنعتی باشد. بدیهی است که در سطح وزارتخانه مذکور لازم است هماهنگی‌های بیشتری به عمل آمده و افراد مؤثر در تصمیم‌سازی و تصمیم‌گیری‌ها به کمک فرا خوانده شوند، اما در سطح واحد تولیدی می‌توان وظائف این نهاد را به یک نفر از کارشناسان رایانه که آموزش کافی دیده است واگذار نمود.

صرف‌نظر از اندازه نهاد یا سازمان، در هنگام تشکیل هر نهاد یا سازمان لازم است ابزار و امکانات زیر فراهم شود یا به عبارت دیگر هر نهاد یا سازمان متشکل از فعالیت‌ها و اجزای زیر است:

- الف- تعیین حوزه فعالیت، سیاست‌گذاری و انتخاب خط مشی عملیاتی
- ب- طراحی زیر مجموعه‌های عملیاتی، نمودار سازمانی و سازماندهی
- ج- تهیه مقررات، دستورالعمل‌های اجرایی و رویه‌ها
- د- تأمین نیروی انسانی مجرب یا آموزش نیروی انسانی موجود بر اساس مقررات و

دستورالعمل‌های اجرایی و رویه‌ها

در طرح حاضر نیز به الزامات فوق توجه شده است و دستورالعمل‌های ایجاد نظام مدیریت امنیت اطلاعات به‌طوری تدوین شده‌اند که پاسخگوی نیازهای ایجاد یک سازمان یا نهاد جهت ایجاد نهاد

متصدی امنیت اطلاعات سازمان (با هر اندازه یا سطح) باشند. به طور کلی دستورالعمل‌های اجرایی نظام مدیریت امنیت اطلاعات از دیدگاه اجرایی قابل تقسیم به سه دسته کلی می‌باشند که عبارت‌اند از:

- دستورالعمل‌های مربوط به سیاست‌گذاری کلان و انتخاب خط مشی عملیاتی
- دستورالعمل‌های سازمان‌دهی و تنظیم روابط داخلی یا خارجی
- دستورالعمل‌های اجرایی

جدول‌های زیر حاوی فهرست تفکیک شده دستورالعمل‌های اجرایی نظام مدیریت امنیت اطلاعات از دیدگاه اجرایی می‌باشند.

أ- دستورالعمل‌های سیاست‌گذاری کلان و انتخاب خط مشی

شماره مرجع	موضوع
۱-۱	راهنمای سیاست‌گذاری امنیت اطلاعات
۱-۱-۱	سند سیاست‌گذاری امنیت اطلاعات
۲-۱-۱	بازنگری سند سیاست‌گذاری امنیت اطلاعات
۳-۱-۱	سند تعیین قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات
۱-۱-۲	تعهد و اهتمام مدیریت ارشد سازمان به امنیت اطلاعات
۸-۱-۲	بازنگری مستقل سامانه امنیت اطلاعات

ب- دستورالعمل‌های سازمان‌دهی و تنظیم روابط داخلی یا خارجی

شماره مرجع	موضوع
۲-۱-۲	هماهنگی امنیت اطلاعات
۳-۱-۲	تعیین مسئولیت در حوزه امنیت اطلاعات
۵-۱-۲	توافقنامه‌های حفظ محرمانگی
۶-۱-۲	برقراری ارتباط با مراجع حکومتی
۷-۱-۲	ارتباط با سایر مراجع یا سازمان‌ها یا نهادها (ی دارای اشتراک منافع)
۱-۲-۲	شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری
۲-۲-۲	رعایت نکات امنیتی هنگام تعامل با مشتریان یا ارباب رجوع

شماره مرجع	موضوع
۳-۲-۲	رعایت معیارهای امنیتی در قراردادهای اشخاص ثالث
۱-۱-۳	فهرست موجودی دارایی‌های اطلاعاتی
۱-۲-۳	دستورالعمل طبقه‌بندی اطلاعات
۴-۳-۳	بیانیه کاربرپذیری (SOA) اختصاصی

ج-دستورالعمل‌های اجرایی

شماره مرجع	موضوع
۴-۱-۲	صدور مجوز استفاده از تجهیزات پردازش اطلاعات
۲-۱-۳	تعیین متصدی و یا مالکیت دارایی‌های اطلاعاتی
۳-۱-۳	نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی
۲-۲-۳	برچسب‌گذاری دارایی‌های اطلاعاتی و نگهداری
۱-۳-۳	گزارش مرحله شناخت سیستم
۲-۳-۳	ارزیابی ریسک
۳-۳-۳	مدیریت و مقابله با ریسک
۱-۱-۷	سیاست‌گذاری کنترل دسترسی
۱-۲-۷	ثبت کاربر
۲-۲-۷	مدیریت دسترسی‌های ممتاز
۳-۲-۷	مدیریت کلمه عبور کاربر
۴-۲-۷	بازنگری حقوق دسترسی کاربران
۱-۳-۷	استفاده از کلمه عبور
۲-۳-۷	تجهیزات کاربری بدون مراقب
۳-۳-۷	روش مانیتور پاک و میز پاکیزه
۱-۴-۷	سیاست‌گذاری در استفاده از سرویس‌های شبکه
۲-۴-۷	احراز صلاحیت کاربر برای اتصال به شبکه‌های خارج از سازمان

شماره مرجع	موضوع
۳-۴-۷	شناسایی تجهیزات در شبکه
۴-۴-۷	حفاظت از سرویس‌های رفع اشکال از راه دور و پیکربندی درگاه‌ها
۵-۴-۷	جداسازی شبکه‌ها
۶-۴-۷	کنترل اتصال‌های شبکه
۷-۴-۷	کنترل مسیریابی شبکه
۱-۵-۷	رویه‌های امن آغاز به کار
۲-۵-۷	شناسایی و احراز صلاحیت (تائید اعتبار) کاربر
۳-۵-۷	سیستم مدیریت کلمه عبور
۴-۵-۷	استفاده از ابزارهای سیستم
۵-۵-۷	محدودیت مدت نشست
۶-۵-۷	محدودیت زمان اتصال
۱-۶-۷	محدودسازی دسترسی به اطلاعات
۲-۶-۷	جداسازی سامانه (سیستم)‌های حساس
۱-۷-۷	پردازش همراه و مخابرات سیار
۲-۷-۷	کار از راه دور

تأمین نیروی انسانی و مجرب یا آموزش نیروی انسانی موجود بر اساس مقررات و دستورالعمل‌های فوق مکمل فعالیت‌های ایجاد نظام مدیریت امنیت اطلاعات می‌باشد. مشاغل لازم در حوزه امنیت اطلاعات و شرایط احراز آن و مهارت‌های لازم جهت تصدی هر یک از مشاغل به طور کامل در دستورالعمل هماهنگی اطلاعات (دستورالعمل ۲-۱-۲) شرح داده شده است.

بنابراین و بر فرض عدم وجود نهادی برای تصدی‌گری مدیریت امنیت اطلاعات در یک سازمان و برای ایجاد آن لازم است مقدمات آن بر اساس دستورالعمل‌های مندرج در دو جدول اول و دوم فوق آماده شود. پس از تشکیل نهاد بر اساس دستورالعمل‌های مندرج در آن دو جدول لازم است نیروی انسانی بر اساس مندرجات دستورالعمل هماهنگی اطلاعات (دستورالعمل ۲-۱-۲) آموزش داده شده و به

کار گرفته شود. در مرحله بعدی که مرحله اجرایی پیاده‌سازی نظام مدیریت امنیت اطلاعات است لازم است دستورالعمل‌های مندرج در جدول سوم فوق در اختیار نهاد ایجاد شده قرار گیرد و به مورد اجراء گذاشته شوند.

مراحل فوق را می‌توان در قالب فلوچارت اجرایی زیر نمایش داد :



۱-۲- سلسله مراتب سازمانی در ایجاد و به کارگیری نظام مدیریت امنیت اطلاعات

رعایت نظم در انجام امور، سازماندهی، مستندسازی و رعایت الزامات قانونی، شالوده اصلی نظام مدیریت امنیت اطلاعات را تشکیل می‌دهد. بنابراین نباید به هیچ وجه اجازه داده شود ایجاد یا به کارگیری نظام مدیریت امنیت به عنوان بهانه‌یی برای نادیده گرفتن مقررات یا دور زدن قوانین یا عدم رعایت سلسله مراتب سازمانی به کار گرفته شود.

بنابراین لازم است در تدوین یا اجرای کلیه دستورالعمل‌های نظام مدیریت امنیت اطلاعات رعایت سلسله مراتب سازمانی به عنوان یک الزام اصیل در نظر گرفته شود. جهت اجرای این اصل لازم است: هنگام اقدام به سیاست‌گذاری در حوزه امنیت اطلاعات ابتدا سیاست‌گذاری‌های موجود در این زمینه از نهاد بالادستی استعلام شود. سیاست‌گذاری جدید در مورد هر موضوع فقط وقتی پذیرفتنی است که نهاد بالادست در این خصوص سیاست‌گذاری خاصی نداشته باشد.

هر گونه تغییر در سیاست‌گذاری نهادهای متبوع بلافاصله باید در سیاست‌گذاری‌های نهاد تابع لحاظ گردد. طبقه‌بندی‌های حفاظتی دارای‌های اطلاعاتی باید حداقل معادل طبقه‌بندی‌های حفاظتی تعیین شده توسط نهاد بالادستی باشد.

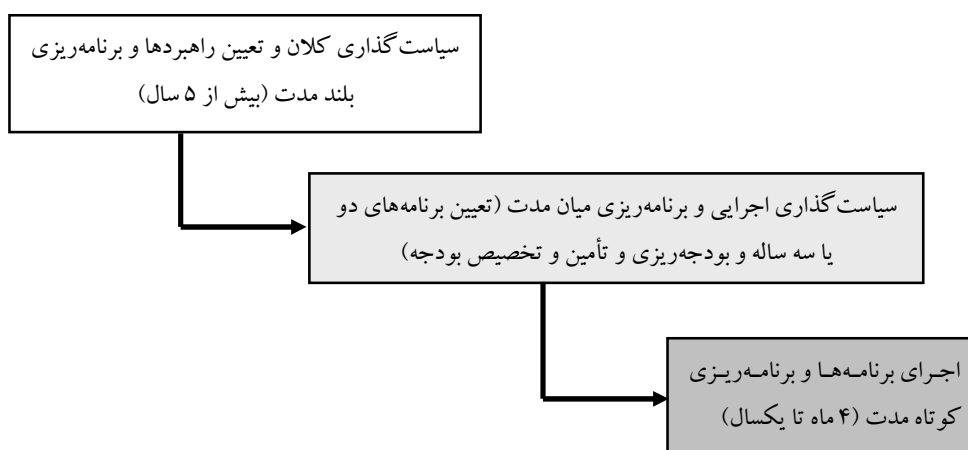
در صورت صدور دستورالعمل جدید امنیت اطلاعات توسط نهاد بالادستی دستورالعمل‌های مغایر با آن از درجه اعتبار ساقط بوده و لازم است دستورالعمل صادر شده جدید به مورد اجراء گذاشته شود.

۱-۳- سلسله مراتب سیاست‌گذاری و اجرا در نظام مدیریت امنیت اطلاعات

سلسله مراتب سیاست‌گذاری و اجرای نظام مدیریت امنیت اطلاعات به شرح زیر خواهد بود:

- الف- سیاست‌گذاری کلان در سطح راهبردی (به عنوان مثال در سطح وزارتی یا کشوری و یا مدیریت ارشد سازمانی)
- ب- برنامه‌ریزی، سازمان‌دهی، بودجه‌بندی و هماهنگی در سطح مدیریتی میانی (به عنوان مثال در سطح اداره کل / سازمان / شرکت...)
- ج- اجرا در واحدهای مختلف سازمانی یا شرکتی (توسط مدیران اجرایی یا کارشناسان فنی)

بنابراین سلسله مراتب سیاست‌گذاری و اجراء را می‌توان در قالب نمودار زیر نمایش داد:



مسئولیت ایجاد نظام مدیریت امنیت به عهده مدیریت ارشد سازمان و مسئولیت راهبری آن به عهده مدیریت میانی سازمان می‌باشد. به عنوان مثال مسئولیت ایجاد مرکز حراست امنیت اطلاعات در یک وزارتخانه به عهده وزیر می‌باشد. پس از تشکیل این مرکز لازم است بودجه و نیروی انسانی لازم برای آن تخمین زده شده و تأمین گردد. مسئولیت این کار به عهده معاونت‌های مختلف (اعم از معاونت پشتیبانی، معاونت فنی، ...) در حوزه وظایف خود می‌باشد. پس از تشکیل این مرکز مسئولیت ایجاد و حفظ امنیت اطلاعات به عهده همان مرکز خواهد بود که بر اساس نظام سلسله مراتبی تعریف شده برای آن به فعالیت خواهد پرداخت. پشتیبانی از این مرکز و یا تغییر و تصحیح برنامه‌ها و نوع فعالیت آن مشابه سایر نهادهای دیگر موجود در سازمان می‌باشد.

البته بدیهی است که این مرکز نیز ممکن است در خصوص اجرای برنامه‌های اجرایی خود نیاز به سیاست‌گذاری‌های مقطعی داشته باشد. این کار در حد سیاست‌های خرد و با رعایت سلسله مراتب سازمانی ایجاد و به کارگیری نظام مدیریت امنیت اطلاعات که قبلاً شرح داده شد بلامانع می‌باشد.

۴-۱- ترتیب اجرای دستورالعمل‌های نظام مدیریت امنیت اطلاعات

همان‌گونه که قبلاً گفته شد فعالیت‌های مربوط به ایجاد و اجرای نظام مدیریت امنیت اطلاعات دارای ماهیت‌های گوناگونی اعم از سیاست‌گذاری، سازماندهی و اجرایی می‌باشند. ممکن است استفاده کننده از این دستورالعمل‌ها در خصوص ترتیب اجرای این دستورالعمل‌ها ایده خاصی نداشته باشد. بنابراین جهت تسهیل در پیاده‌سازی این دستورالعمل‌ها سطوح راهنمای زیر ارائه می‌شود. ترتیب اجرای سطوح از بالا به پایین می‌باشد و می‌توان دستورالعمل‌هایی که در یک سطح قرار گرفته‌اند را به صورت موازی و یا تقریباً هم‌زمان به اجرا گذاشت.

سطح ۱:

- اجرای سند سیاست‌گذاری امنیت اطلاعات - دستورالعمل ۱-۱-۱

سطح ۲:

- اجرای سند تعیین قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات - دستورالعمل ۳-۱-۱

سطح ۳:

- اعلام تعهد و اهتمام مدیریت ارشد سازمان به حفظ امنیت اطلاعات - دستورالعمل ۱-۱-۲

سطح ۴:

- اجرای دستورالعمل هماهنگی امنیت اطلاعات - دستورالعمل ۲-۱-۲

- تعیین مسئولیت در حوزه امنیت اطلاعات - دستورالعمل ۳-۱-۲

سطح ۵:

- تهیه توافقتنامه‌های حفظ محرمانگی - دستورالعمل ۵-۱-۲

- برقراری ارتباط با مراجع حکومتی - دستورالعمل ۶-۱-۲

- ارتباط با سایر مراجع یا سازمان‌ها یا نهادها (ی دارای اشتراک منافع) - دستورالعمل ۷-۱-۲

سطح ۶:

- تهیه فهرست موجودی دارایی‌های اطلاعاتی - دستورالعمل ۱-۱-۳
- اجرای دستورالعمل طبقه‌بندی اطلاعات - دستورالعمل ۱-۲-۳

سطح ۷:

- تعیین متصدی یا مالکیت دارایی‌های اطلاعاتی - دستورالعمل ۲-۱-۳
- تعیین نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی - دستورالعمل ۳-۱-۳
- برچسب‌گذاری دارایی‌های اطلاعاتی - دستورالعمل ۲-۲-۳

سطح ۸:

- تهیه گزارش شناخت سیستم - دستورالعمل ۱-۳-۳
- شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری - دستورالعمل ۱-۲-۲
- ارزیابی ریسک - دستورالعمل ۲-۳-۳
- مدیریت و مقابله با ریسک - دستورالعمل ۳-۳-۳

سطح ۹:

- تعیین و رعایت نکات امنیتی هنگام تعامل با مشتریان یا ارباب رجوع - دستورالعمل ۲-۲-۲
- تعیین و رعایت معیارهای امنیتی در قراردادهای اشخاص ثالث - دستورالعمل ۳-۲-۲
- تدوین بیانیه کاربردپذیری (SOA) اختصاصی سازمان - دستورالعمل ۴-۳-۳

سطح ۱۰:

- بازنگری سند سیاست‌گذاری امنیت اطلاعات - دستورالعمل ۲-۱-۱

سطح ۱۱:

- به کارگیری سایر دستورالعمل‌های باقیمانده که در سطوح فوق به آن‌ها اشاره نشده است.
- به کارگیری و مراجعه دوره‌ای دستورالعمل‌های سطوح فوق مانند:
 - بازنگری منظم سند سیاست‌گذاری امنیت اطلاعات - دستورالعمل ۲-۱-۱
 - شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری - دستورالعمل ۱-۲-۲
 - مدیریت و مقابله با ریسک - دستورالعمل ۳-۳-۳

ممکن است در هر سازمان و با توجه به حوزه عملکرد و نیازهای سازمان نیاز به تدوین دستورالعمل‌های جدید و یا حذف برخی از دستورالعمل‌های سطح بندی شده فوق باشد. این کار با رعایت سیاست‌گذاری‌های کلان امنیت اطلاعات سازمان و کسب موافقت رده‌های بالاتر که هماهنگی فعالیت‌های امنیت اطلاعات را به عهده دارند بلامانع است.

۱-۵- ملاحظات هزینه‌ی در ایجاد و پیاده‌سازی نظام مدیریت امنیت اطلاعات

ایجاد هر گونه نظام جدید به‌خصوص در سطح رسمی، مستلزم صرف هزینه‌های متناسب با مأموریت و حوزه پیاده‌سازی آن نظام می‌باشد.

بنابر اصل هزینه/فایده لازم است قبل از ایجاد هر نظام جدید در خصوص ضرورت ایجاد آن نظام بررسی لازم انجام شود. این بررسی به عهده برنامه‌ریزان کلان و مدیران ارشد سازمان می‌باشد که با آگاهی از چالش‌ها و فرصت‌های فراروی سازمان در خصوص ضرورت ایجاد نظام تصمیم‌گیری می‌نمایند. پس از اثبات ضرورت ایجاد نظام، مرحله بعدی تخصیص بودجه لازم جهت اجرای آن و تعیین زمانبندی‌های صرف بودجه می‌باشد.

مراحل پیاده‌سازی و اجرای نظام مدیریت امنیت اطلاعات از لحاظ صرف بودجه را می‌توان به چهار مرحله تقسیم کرد که عبارت‌اند از:

- مرحله اول: سیاست‌گذاری کلان و تدوین برنامه‌های راهبردی
- مرحله دوم: سازماندهی و ایجاد زیرساخت‌های سازمانی
- مرحله سوم: ایجاد زیرساخت‌های امنیتی و امن‌سازی اولیه
- مرحله چهارم: حفاظت از امنیت و تداوم آن

مرحله اول ناظر بر فعالیت‌های سیاست‌گذاری کلان و تدوین برنامه‌های راهبردی می‌باشد که هر چند از لحاظ صرف وقت مدیران ارشد و برنامه‌ریزان خبره مستلزم صرف وقت نسبتاً قابل توجه می‌باشد، اما معمولاً نیازی به تخصیص بودجه خاصی برای آن نمی‌باشد و می‌توان آن را در محدوده فعالیت‌های جاری مدیران ارشد قرار داد.

مرحله دوم که عبارت است از سازمان‌دهی و ایجاد زیرساخت‌های سازمانی، مشابه مراحل لازم در هر ساختار سازمانی دیگر می‌باشد که سازمان‌ها و شرکت‌ها دارای تجربه‌های متعدد در این زمینه بوده و به ازای تعداد نفراتی که لازم است در آن سازمان به کار گرفته شوند به آن بودجه تخصیص می‌دهند و می‌توان بودجه لازم برای آن را بودجه‌ای متعارف در نظر گرفت.

مرحله سوم یعنی ایجاد زیرساخت‌های امنیتی و امن‌سازی اولیه از لحاظ صرف هزینه نسبت به سایر مراحل متمایز می‌باشد. بودجه لازم برای این مرحله صرف‌نظر از کوچک یا بزرگ بودن سازمان و یا نوع فعالیت‌های آن نسبت به بودجه کل لازم برای ایجاد نظام مدیریت امنیت اطلاعات رقم قابل توجهی را تشکیل می‌دهد.

زیرساخت‌های امنیتی را می‌توان به صورت زیر دسته‌بندی کرد:

- زیرساخت امنیت محیطی و فیزیکی
 - زیرساخت کلید عمومی
 - زیرساخت امنیت ارتباطات و شبکه
 - زیرساخت امنیت انرژی و نیازهای حیاتی
 - زیرساخت پشتیبان‌گیری و مقابله با شرایط اضطراری
- زیرساخت‌های فوق عموماً زیرساخت‌های گران‌قیمت و پر هزینه می‌باشند و امن‌سازی اولیه نیز مستلزم صرف هزینه قابل توجه می‌باشد. این فعالیت شامل فعالیت‌های زیر می‌باشد:
- تدوین روال‌ها و دستورالعمل‌های امنیت اطلاعات
 - نصب آنتی ویروس و نرم‌افزارهای حفاظتی
 - امن‌سازی نرم‌افزارها و سخت‌افزارها
 - امن‌سازی اتاق‌ها و مکان‌های نگهداری اطلاعات
 - بازآرایی شبکه
 - تنظیم پیکربندی تجهیزات
 - آموزش نیروی انسانی

عملیات امن‌سازی اولیه را می‌توان جزو عملیات پر هزینه تلقی نمود. البته بدیهی است که امن‌سازی اولیه هزینه بسیار کمتری نسبت به ایجاد زیرساخت‌های امنیتی دارد و به علاوه می‌توان آن را به‌صورت مستقل نیز انجام داد.

مرحله چهارم یا حفاظت از امنیت اطلاعات و تداوم آن نیز را می‌توان به‌صورت فعالیتی مستمر در نظر گرفت و هزینه‌های مربوط به آن نیز متناسب با سایر فعالیت‌های مستمر سازمان می‌باشد. این هزینه‌ها قابل تقسیم به دو دسته هزینه نیروی انسانی و پشتیبانی از ایشان (هزینه مستمر) و هزینه‌های بهبود با به هنگام‌سازی روش‌ها یا زیرساخت‌های امنیتی (هزینه‌های موردی) می‌باشند.

ملاحظات هزینه‌ای ایجاد و پیاده‌سازی نظام مدیریت امنیت اطلاعات را می‌توان به‌صورت زیر خلاصه و دسته‌بندی کرد:

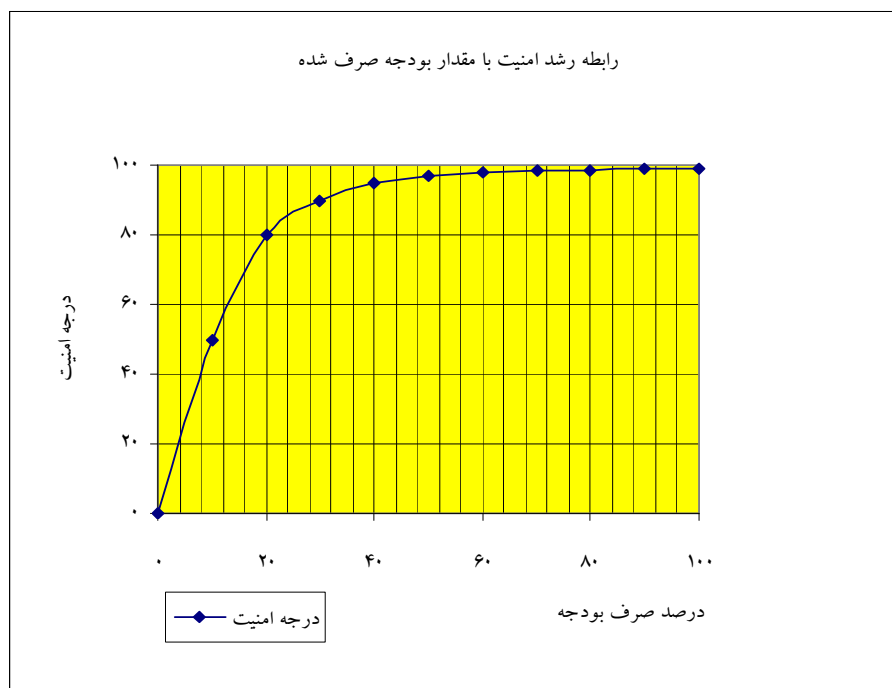
مراحل صرف بودجه در برپایی نظام مدیریت امنیت اطلاعات

مقطع صرف هزینه	نوع فعالیت	شرح فعالیت	نوع بودجه مورد نیاز و نسبت آن به کل بودجه استقرار
مرحله اول	ایجاد نظام	سیاست‌گذاری کلان و تدوین برنامه‌های راهبردی	بودجه متعارف برنامه‌ریزی - (۰.۵٪)
مرحله دوم	ایجاد نظام	سازماندهی	بودجه متعارف سازماندهی - (۰.۵٪)
مرحله سوم	پیاده‌سازی	امن‌سازی اولیه	بودجه عملیات زود بازده امن‌سازی - (۰.۵٪)
	پیاده‌سازی	ایجاد زیرساخت امنیتی	بودجه عملیات ایجاد زیرساخت امنیتی - (۸۵٪)

توضیح: بودجه استقرار عبارت است از مجموع بودجه ایجاد نظام و پیاده‌سازی نظام مدیریت امنیت اطلاعات و یا به عبارت دیگر مجموع بودجه تخصیص داده شده به مرحله‌های اول تا سوم جدول فوق

موضوع قابل توجه در این‌جا لزوم صرف بودجه‌های کلان‌تر جهت رسیدن به درجه امنیت بالاتر می‌باشد. باید توجه داشت که طبق نظر کلیه کارشناسان خبره امنیت اطلاعات دستیابی به امنیت کامل (یا امنیت ۱۰۰٪) غیرممکن است. این به آن معنی است که صرف بودجه بیشتر لزوماً منجر به درجه امنیت بالاتر نمی‌شود. به عبارت دیگر صرف هر واحد بودجه در مراحل اولیه امن‌سازی تأثیر بسیار بیشتری در

افزایش درجه امنیت نسبت به صرف همان مقدار بودجه در مراحل بعدی خواهد داشت. برای درک بهتر موضوع توجه به نمودار زیر ضروری است:



توجه: مقادیر نمودار به صورت فرضی و برای درک بهتر موضوع تنظیم شده‌اند.

همان‌طور که در این نمودار دیده می‌شود اثر بخشی صرف بودجه‌های اولیه در مراحل ابتدایی ایجاد نظام مدیریت امنیت اطلاعات بسیار بیشتر از مراحل تحکیم امنیت و ایجاد زیرساخت‌های امنیتی می‌باشد. بنابراین ضروری است مراحل اولیه ایجاد نظام مدیریت امنیت اطلاعات شامل سیاست‌گذاری کلان، سازمان‌دهی و امن‌سازی اولیه در اولویت اجرایی قرار گیرند تا امنیت نسبی ایجاد شده و به دنبال آن و با دقت بیشتر به انتخاب زیرساخت‌های امنیتی و استقرار آن‌ها پرداخت.

نتایج حاصل از مطالعه حمله‌های انجام شده نیز در پیش گرفتن روش فوق را تأیید می‌کند. بیشتر حمله‌های موفق علیه اهداف اطلاعاتی با سوءاستفاده از ضعف‌های ساده بر اساس متدهای آسان مثل

حدس زدن کلمه عبور، دسترسی به تجهیزاتی که اصولاً فاقد رویه کنترل دسترسی بوده‌اند، تخلیه تلفنی، جازدن خود به عنوان تعمیرکار یا نیروی خدماتی و یا ضعف در پیکربندی تجهیزات (عدم تغییر در پیکربندی پیش فرض و یا اشکال در فرمان‌های پیکربندی) برنامه‌ریزی و اجرا شده‌اند.

هر چند تخصیص بودجه و صرف هزینه باید بر اساس نتایج حاصل از ارزیابی ریسک (موضوع دستورالعمل ۳-۳-۲) انجام پذیرد، اما به‌طور کلی باید به سه موضوع مهم در امن‌سازی توجه کرد:

- الف- در امن‌سازی فرآیندهای عادی لازم است به کارآیی روش‌های امن‌سازی و بودجه تخصیص داده شده به آن توجه کرد. در صورتی‌که روش امن‌سازی بیش از حد پیچیده باشد ممکن است خود به عامل تهدید تبدیل شود (به علت علاقه افراد به دور زدن آن یا عدم اعتقاد به اجرای کامل آن).
- ب- در امن‌سازی فرآیندهایی که نقص در آن‌ها منجر به تهدید جان یا آبروی افراد و یا امنیت ملی می‌شود، فقط باید کارآیی روش امن‌سازی مورد توجه قرار گرفته و از ایجاد محدودیت بودجه‌ای خودداری شود.
- پ- اگر در هر مرحله از عملیات امن‌سازی تحت شرایط بند ب فوق تشخیص داده شود که تامین بودجه خارج از توان سازمان می‌باشد لازم است مراتب کتبی به کمیته امنیت اطلاعات اعلام شود.

۲- مبانی مدیریت امنیت اطلاعات

۲-۱- مدیریت امنیت اطلاعات (مقدمه‌ای بر انتخاب روش و تعریف نهادها و مکانیزم‌های حفظ امنیت اطلاعات)

پرداختن به امنیت اطلاعات به معنی توجه به حفظ دارایی‌های اطلاعاتی سازمان است. اطلاعات و تجهیزات و تاسیسات مربوط به آن همانند سایر دارایی‌های مهم موسسه، از جمله دارایی‌هایی است که برای دارنده آن دارای ارزش بوده و لازم است به صورت مناسبی حفاظت شود. این نوع دارایی در شکل‌های مختلف ظاهر می‌شود. برخی از دارایی‌های اطلاعاتی عبارت‌اند از:

- سخت‌افزار
- نرم‌افزار (سیستم عامل، ابزارها و برنامه‌های کاربردی)
- بانک‌های اطلاعاتی
- خدمات (پردازشی، ارتباطی و پشتیبانی) و سطح کیفی ارائه آن

مدیریت امنیت اطلاعات فرآیندی است که براساس آن از اطلاعات در مقابل تهدیدات مختلف حفاظت خواهد شد، به نحوی که از ادامه فعالیت با حداکثر حفاظت، کارایی و بهره‌وری و بهره‌برداری از فرصت‌های عملیاتی، اطمینان حاصل شود.

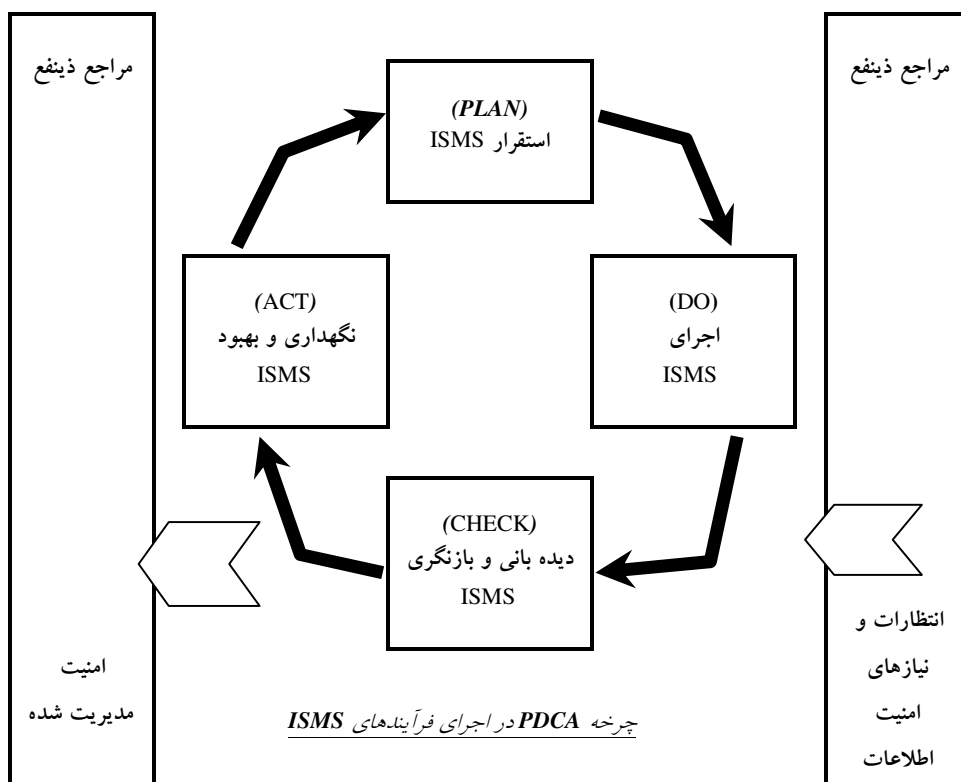
مفاهیم مربوط به حفظ امنیت اطلاعات در زمینه فناوری اطلاعات طیف گسترده‌ای را تشکیل می‌دهد. از آن‌جا که فناوری‌های اطلاعاتی گسترش بسیار یافته و تقریباً در حال تاثیرگذار شدن بر کلیه امور روزمره سازمان‌های مختلف است، انتخاب نوع نگرش، محدوده‌ی فعالیت و روش انجام کار در زمینه‌های مربوط به آن اهمیت بسیار داشته و از پیچیدگی خاصی نیز برخوردار است. در این شرایط لازم است روش مدیریتی سازمان یافته‌ای انتخاب و در پیش گرفته شود و براساس آن، جنبه‌های مختلف حفاظت از دارایی‌های اطلاعاتی مورد توجه قرار گرفته و اجرا شود.

به عبارت دیگر می‌توان گفت انتخاب مدل مدیریتی حفظ امنیت اطلاعات و فراهم آوردن شرایط اجرای آن مدل، مهمترین گام در ایجاد یک سیستم حفاظت از امنیت اطلاعات و پیوستگی ارائه خدمات می‌باشد.

مدل‌های مدیریتی مختلفی در زمینه حفظ امنیت و حفاظت اطلاعات وجود دارد. هر یک از این مدل‌ها از دیدگاه‌های مختلف نظامی، اجتماعی، اقتصادی و تکنولوژیکی به موضوع پرداخته و راه حل خود را ارائه می‌کنند. مدل‌های دیگری نیز وجود دارند که ترکیبی از عوامل اخیر را در نظر گرفته و به ارائه راه حل می‌پردازند. به عنوان مثال می‌توان از مدل‌های ارائه شده توسط وزارت دفاع ایالات متحده (DoD)، سازمان همکاری‌های اقتصادی آسیا پاسیفیک (APEC) و اتحادیه اروپایی نام برد. برخی از این مدل‌ها (مدل‌های نظامی) بسیار جزئی نگر بوده و رویه‌های مختلفی را برای هر رشته از اطلاعات ثبت کرده و اجرای این رویه‌ها را الزامی می‌دانند.

با توجه به ساختار سازمانی، نوع فعالیت و گستره جغرافیایی شبکه‌های تجاری، مدلی مورد نیاز است که بتوان اولاً "براساس آن روشی کارآمد و قابل ارزیابی برای شناسایی تهدیدات و میزان زیان ناشی از آسیب‌های احتمالی تعریف نمود، ثانياً "براساس ماهیت، اصول و روش‌های پردازش و انتقال اطلاعات، مکانیزم‌های کنترلی مورد نیاز را طراحی کرد و ثالثاً" با شناسایی نیازهای امنیتی بستر قانونی مورد نیاز برای فعالیت را فراهم آورد.

مدل مدیریتی پیشنهاد شده در استاندارد سری ISO-27001 واجد کلیه شروط فوق می‌باشد. این مدل با تعریف امنیت و سیاست‌گذاری‌های مربوط به آن، بحث در مورد ساختار سازمانی و نهاد امنیت و موارد دیگر از قبیل روش‌های ارزیابی ریسک، ایجاد امنیت در نیروی انسانی، امنیت فیزیکی، کنترل دسترسی، امنیت شبکه‌ها و انطباق با قوانین موضوعه و ممیزی امنیت، مدل مدیریتی کارایی را پیشنهاد می‌کند.



چگونگی پیاده‌سازی این مدل مدیریتی به فضای عملیاتی، توان تاثیرگذاری و عزم سازمانی نهاد استفاده کننده بستگی دارد.

۲-۱-۱- ترسیم وضعیت مطلوب

امنیت اطلاعات از طریق به‌کارگیری مجموعه‌ای از فرآیندهای کنترلی به دست می‌آید که در سیاست‌ها، روش‌های عملیاتی، ساختار سازمانی و نرم‌افزارهای عملیاتی تعبیه می‌شود. این فرآیندها دسترسی به اهداف زیر را امکان پذیر می‌سازد:

- محرمانه بودن (اطمینان از این‌که اطلاعات فقط در دسترس افراد مجاز است)
- جامعیت و صحت (تامین دقت و کامل بودن اطلاعات و روش‌های پردازش آن)

- در دسترس بودن (اطمینان از این که افراد مجاز بتوانند در مواقع نیاز به اطلاعات جامع و صحیح و سایر منابع مرتبط با آن دسترسی داشته باشند).
- پیاده‌سازی فرآیندهای گفته شده در بالا و دسترسی به اهداف سه گانه محرمانگی، جامعیت و در دسترس بودن، با در نظر داشتن روش‌ها و هدف‌های فرعی زیر امکان پذیر خواهد شد:
- سیاست‌گذاری امنیتی یا تعیین اهداف فرعی و فعالیت‌هایی که باعث دسترسی به اهداف اصلی می‌شوند.
- روش امن‌سازی که با در نظر گرفتن فرهنگ سازمانی هدف طراحی شده باشد.
- پشتیبانی قابل لمس و همکاری مدیریت ارشد سازمان
- تشخیص صحیح نیازهای امنیتی، ارزیابی ریسک و مدیریت آن
- توجیه مدیران و نیروی انسانی در زمینه نیاز به امنیت
- آموزش و به هنگام سازی دانسته‌ها
- برپایی سیستم قابل درک و قابل ارزیابی برای تعیین میزان کارایی روش‌های مدیریت امنیت اطلاعات و جمع‌آوری پیشنهادات مختلف برای بهبود عملکرد آن.

۲-۱-ب- سیاست‌گذاری امنیتی، سازماندهی براساس روش استاندارد انتخاب شده

۲-۱-ب-۱- تعیین خط مشی

سیاست‌گذاری عبارت است از تعیین طرح یا فعالیتی که بتوان با استفاده از آن بر نحوه فعالیت سازمان یا مجموعه اثر گذارد. این اثرگذاری از طریق تعیین نحوه تصمیم سازی و نوع اقدامات لازم اعمال می‌شود.

سیاست‌گذاری براساس مندرجات موجود در متن سند سیاست‌گذاری که به تصویب مدیریت عالی سازمان می‌رسد، انجام می‌پذیرد.

لازم است در سند سیاست‌گذاری چهارچوب سازمانی، استراتژی و سیاست‌ها به موازات محرمانگی، جامعیت و در دسترس بودن اطلاعات، مورد توجه قرار گیرد. طبق مکانیزم تهیه سند سیاست‌گذاری لازم است اجزاء زیر تشریح شوند:

- چهارچوب امنیتی (خط مشی): چتر وسیعی که کلیه مکانیزم‌های امنیتی را تحت پوشش قرار می‌دهد و علاوه بر پاسخگویی به نیازهای فعلی، نیازهای آتی سازمان را نیز در نظر گرفته و برآورده می‌سازد.
 - استراتژی: براساس چهارچوب امنیتی تهیه می‌شود و چگونگی دسترسی به اهداف سازمانی را معین می‌کند. استراتژی براساس اهداف صریح یا ضمنی معرفی شده در چهارچوب امنیتی سازمان تعریف می‌گردد.
 - سیاست‌ها: قواعد ساده‌ای است که باید و نبایدهای امنیت اطلاعاتی را تعیین می‌کند و لازم است در چهارچوب امنیتی سازمان تعریف شده باشند.
 - دستورالعمل‌ها و رویه‌ها: توضیحی ساده از سیاست‌های سازمان است که به صورت قدم به قدم و عملی، نوع کار و چگونگی انجام آن را بیان می‌کند.
- از آن‌جا که حفظ امنیت موضوعی عام است و تک تک اعضاء سازمان باید به عنوان بخشی از وظائف سازمانی خود به آن بپردازند، لازم است تدابیری اندیشیده شود که اولاً "به عنوان یک وظیفه سازمانی، مسؤول خاصی برای آن تعیین شود تا بر اجرای فرآیندهای مربوط نظارت کند و ثانیاً" باید سیاست‌گذاری امنیتی تحت حمایت کامل و آشکار مدیریت سازمان و مرجع مشروعیت دهنده به فعالیت‌های مربوطه قرار داشته باشد.

۲-۱-ب-۲- ایجاد کمیته امنیت اطلاعات

حفظ امنیت اطلاعات مسئولیتی مشترک بین همه اعضاء تیم مدیریت سازمان می‌باشد. لازم است کمیته‌ای خاص برای راهبری فعالیت‌های امنیتی و با تاکید بر ارائه تعاریف روشن و گویا و پشتیبانی واضح از روش‌های اجرای فعالیت‌های تعریف شده، ایجاد شود. وظیفه این کمیته ترویج آموزه‌های امنیتی در حیطه سازمان از طریق ایجاد التزام و تعهد اعضاء و تدارک منابع کافی برای آن می‌باشد.

اعضاء این کمیته از بین بدنه مدیریتی سازمان انتخاب می‌شوند. برخی از وظائف این کمیته عبارت است از:

- سیاست‌گذاری و بازنگری سیاست‌های امنیتی اطلاعات و تعیین مسؤولیت‌های کلی
- زیرنظر داشتن تغییرات مشخص در وضعیت امنیتی تجهیزات و آسیب پذیری‌های عمده

- شناسایی و زیرنظر داشتن رویدادهای امنیتی اطلاعات
- طراحی روش‌های جدید برای بهبود وضعیت امنیت اطلاعات

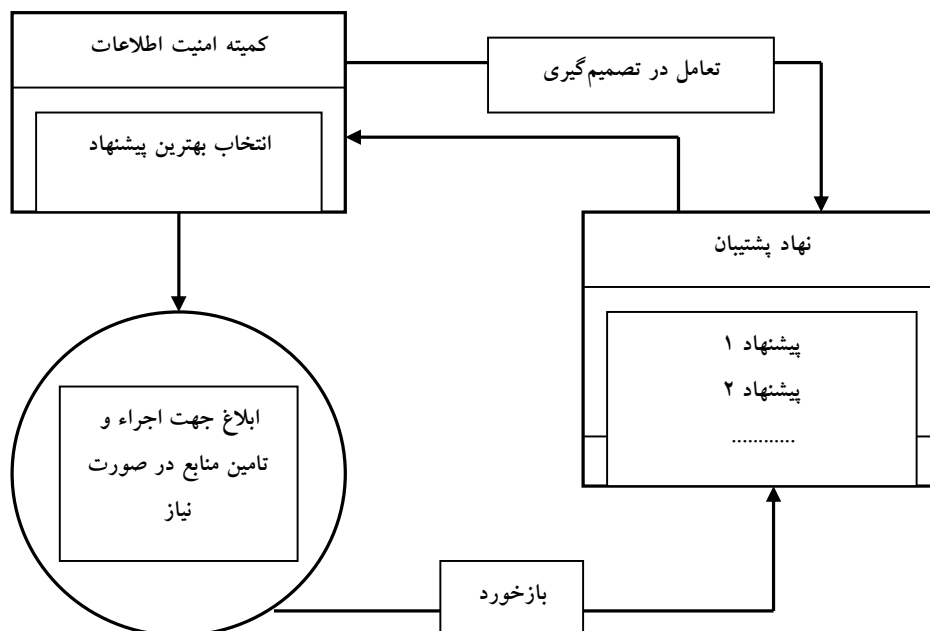
هر یک از مدیران عضو این کمیته در مقابل کلیه اهداف امنیتی مسؤولیت کامل خواهند داشت. البته باید توجه داشت که کمیته نهادی تصمیم‌گیرنده است و لازم است از طرق واحدهای تصمیم ساز (مانند کارگروه و یا واحد امنیت اطلاعات و یا گروه‌های CERT¹ یا BCP²) پشتیبانی شود. مکانیزم‌های تشکیل کمیته و نهادهای پشتیبان آن در بخش دستورالعمل‌ها تشریح خواهد شد.

۲-۱-ب-۳- ایجاد نهاد امنیت اطلاعات

هریک از سازمان‌های استفاده کننده از دارایی‌های اطلاعاتی باید جایگاه نهاد مسؤول امنیت اطلاعات را تعریف کرده و نقش‌ها، مسؤولیت‌ها و حوزه فعالیت آن را تعیین نمایند. در سازمان‌هایی که درصدد ایجاد این نهاد هستند، می‌توان ابتداء یک کارگروه امنیت تشکیل داد. وظیفه این کارگروه تعریف استراتژی‌ها، شرح ماموریت و افق عملیاتی، تعیین ممیزان اولیه و تصویب ساختار سازمانی و کسب اختیار برای این واحد می‌باشد. این نهاد به عنوان بازوی اجرایی مدیریت سازمان در حفظ امنیت اطلاعات عمل می‌کند و اندازه آن متأثر از اندازه سازمان متبوع می‌باشد. در سازمان‌های کوچک می‌توان این نهاد را به صورت مجازی تشکیل داد، اما تشکیل این نهاد در سازمان‌های متوسط، بزرگ و یا مهم ضروری است. دستورالعمل چگونگی تشخیص اندازه سازمان و تشکیل این نهاد در بخش بعد آمده است.

¹ - Computer Emergency Response Team

² - Business Continuity Plan



چرخه تصمیم سازی و تصمیم‌گیری

ارکان این نهاد عبارت است از:

- مدیریت عالی سازمان
 - اسناد و طرح‌های مستند و مصوب سازمان (مانند سندهای خط و مشی و دستورالعمل‌های مدیریت امنیت اطلاعات)
 - ساختار پشتیبان (کمیته امنیت اطلاعات و گروه احیاء سیستم)
 - واحد امنیت اطلاعات
- ساختار سازمانی و نمودار مربوط به آن براساس اسناد و طرح‌های مستند و مصوب سازمان و با تفویض اختیار از طرف مدیریت عالی سازمان، طراحی و تصویب خواهد شد.

۲-۱-۱-۴- طرح احیاء سیستم و گروه پاسخ اضطراری

وظایف مربوط به مدیریت حوادث از طریق تعیین رویه‌های خاص دوره‌ای و اضطراری قابل تعریف‌اند. این مسئولیت‌ها براساس طرح‌های پاسخ اضطراری و احیاء سیستم تعریف خواهند شد. گروه پاسخ اضطراری (CERT) براساس طرح مقابله با حوادث رایان‌های تشکیل می‌شود و وظیفه مقابله با حوادث روزمره را به عهده دارد.

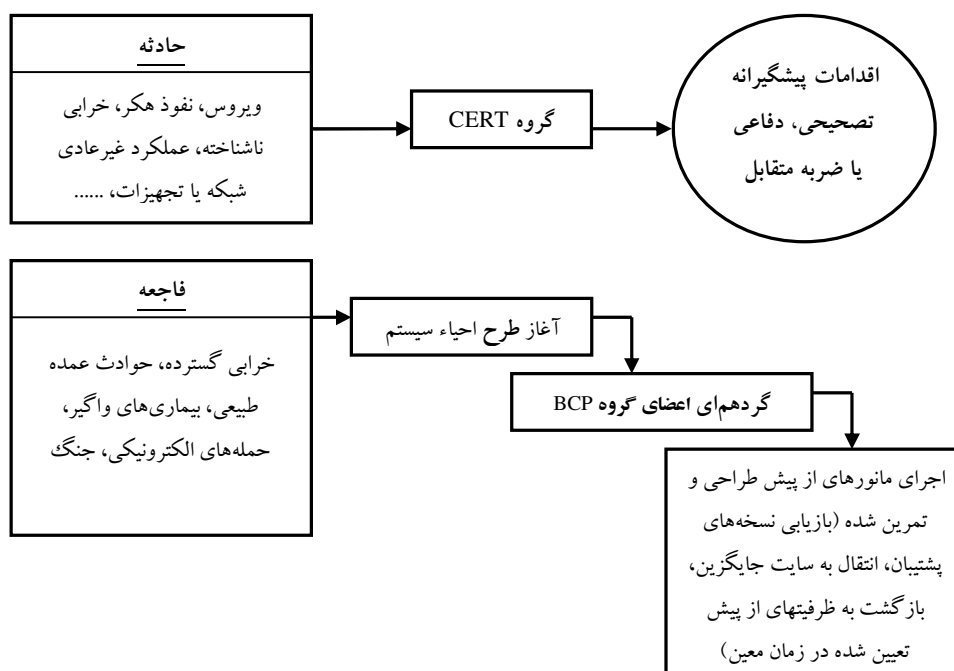
در صورت بروز حوادث عمده یا فجایع طبیعی که قابلیت تهدید موقعیت اطلاعاتی سازمان را دارند، طرح احیاء سیستم به جریان گذاشته خواهد شد. مجری این طرح گروه احیاء سیستم است که دارای مشروعیت اقدام و تصمیم‌گیری در حوزه فعالیت خود و احیاناً سایر حوزه‌های مربوطه می‌باشد. مکانیزم شروع این طرح می‌تواند خودکار و یا براساس اعلام شروع عملیات احیاء از طرف عالی‌ترین مقام سازمان یا جانشین وی باشد.

۲-۱-۱-۳- تهیه لیست دارایی‌های اطلاعاتی

۲-۱-۱-۳-۱- تعریف بنه‌های اطلاعاتی (Information Perimeter)

دسترسی به دارایی‌های اطلاعاتی از طریق مکانیزم‌های دسترسی مربوط به هر دارایی امکان پذیر است. هریک از تجهیزات (سخت‌افزاری و نرم‌افزاری) در یک مکان فیزیکی نگهداری می‌شود. برای مدیریت بهتر این تجهیزات لازم است محدوده‌های جغرافیایی و فیزیکی مشخصی را به عنوان بنه اطلاعاتی تعریف کرده و براساس حساسیت، اهمیت و ارزش هر دسته از تجهیزات مکانیزم‌های حفاظتی لازم را پیش بینی نمود.

بنه اطلاعاتی عبارت است از یک اتاق، طبقه، سازمان، ملک، محدوده، یا هر مکان استقرار دیگری که بتوان آن را با استفاده از دیوارهای فیزیکی (اعم از دیواره ثابت یا موقت) محصور کرد و رفت و آمد افراد یا تبادل اطلاعات آن با سایر شبکه‌ها یا مراجع دیگر را تحت کنترل قرار داد.



ماموریت گروه‌های CERT و احیاء سیستم

۲-۱-ج-۲- شناسایی دارایی‌های نرم‌افزاری و سخت‌افزاری موجود در هر بنة

پس از تعریف محدوده هر بنة اطلاعاتی لازم است کلیه دارایی‌های اطلاعاتی موجود در آن فهرست شوند. این فهرست شامل اطلاعاتی در مورد نام، نوع و ماهیت، محل نگهداری، ارزش، تهدیدات احتمالی، نقاط آسیب پذیر، تحویل گیرنده و سایر اطلاعات مشابه می‌باشد. این اطلاعات می‌توانند کمی (مانند اندازه، وزن)، کیفی (مانند اهمیت سازمانی) و یا اجتماعی (مانند وجهه سازمانی) باشند.

۲-۱-د- تحلیل ریسک و انتخاب ابزار

۲-۱-د-۱- انتخاب روش ارزش گذاری

تصمیم در مورد روش حفاظتی قابل انتخاب برای حفاظت از هر دارایی بستگی به ارزش اطلاعاتی آن دارایی دارد. اهمیت هر نوع دارایی از سازمانی به سازمان دیگر تغییر می‌کند. بنابراین ممکن است یک نوع از تجهیزات ارتباطی (مثلاً "مودم‌ها") در یک سازمان دارای ارزش حیاتی بوده و در سازمان‌های دیگر از ارزش کمتری برخوردار باشد.

تصمیم‌گیری در مورد ارزش دارایی‌های نرم‌افزاری و یا بانک‌های اطلاعاتی دارای اهمیت و پیچیدگی بیشتری است. این پیچیدگی معمولاً "به دلیل ماهیت نوع نرم‌افزار، دسترسی به منابع تولید و توسعه آن و یا ارزش ذاتی اطلاعات نگهداری شده در بانک‌های اطلاعاتی بستگی دارد."

۲-۱-د-۲- شناسایی تهدیدها

وجود نقاط آسیب پذیر باعث ایجاد پتانسیل تهدیدپذیری می‌شود. شناسایی تهدیدات مرتبط با آسیب پذیری دارایی‌های اطلاعاتی، اولین نقطه شروع فعالیت‌های اجرایی امن‌سازی محیط اطلاعاتی می‌باشد.

موفقیت در شناسایی هرچه بیشتر این تهدیدها، موفقیت در به‌کارگیری روش‌های امن‌سازی را به دنبال خواهد داشت.

ساختار سازمانی و تعریف وظائف در واحد امنیت اطلاعات باید به نحوی باشد که انجام عملیات دوره‌ای شناسایی را تضمین کند.

۲-۱-د-۳- شناسایی ابزار دفاعی

پس از شناسایی نقاط آسیب پذیر، گستره فضای عملیاتی و ترسیم برد تهدیدات ممکن، ابزار دفاعی لازم قابل شناسایی هستند.

برخی از این ابزار، ابزاری عام و در دسترس می‌باشند، برخی دیگر ابزار اختصاصی هستند که می‌توان با پرداخت هزینه‌های مربوط به آن دست یافت. مهمترین دسته از ابزارهای دفاعی ابزاری هستند که معمولاً "در دسترس نمی‌باشند و به عبارت دیگر وجود ندارند. به دلیل ماهیت تکنولوژیکی تهدیدات و پیشرفت‌های موجود در این زمینه، در بسیاری از اوقات پس از وقوع حمله و آشکار شدن پیامدهای آن،

نیاز به ابزار جدید احساس می‌شود. بنابراین در سطوح پیشرفته دفاعی، لازم است مکانیزم‌هایی کارا و موثر برای تولید ابزار دفاعی پیش بینی شود.

۲-۱-۴-رتبه‌بندی ریسک

ارزش هر یک از دارایی‌ها چقدر است؟ نقاط آسیب پذیر و تهدیدهای احتمالی کدامند؟ چه ابزاری برای مقابله با تهدیدات لازم است؟ احتمال وقوع حمله به هریک از نقاط آسیب پذیر چقدر است؟ و سوالاتی دیگر از این نوع سوال‌های مهمی هستند که باید پاسخ داده شوند. با پاسخ به هریک از سوالات مطرح شده (کمی یا کیفی) و ترکیب آن‌ها با درجه اهمیت هر یک از انواع دارایی اطلاعاتی، ریسک مربوط به هر دارایی قابل محاسبه و رتبه‌بندی است. برنامه‌ریزی‌های بعدی اجرای کار، براساس مقادیر رتبه‌بندی شده انجام خواهد پذیرفت.

۲-۱-۵- انتخاب محدوده عملیاتی، زمان‌بندی عملیات و مدیریت ریسک

۲-۱-۵-۱- تعیین اولویت عملیات

پس از تعیین رتبه ریسک هریک از دارایی‌های موجود در هر بنه اطلاعاتی، ترتیب اجرای عملیات امن‌سازی در هر بنه تعیین می‌شود. این برنامه با اعمال نظرات مدیریتی قابل اجرا است. به علاوه لازم است بنه‌های مختلف نسبت به یکدیگر نیز رتبه‌بندی و به نوبت تحت عمل قرار گیرد. این کار نیز با استفاده از رویه‌های از پیش تعیین شده و یا تصمیم‌گیری مدیریت سازمان امکان پذیر است.

۲-۱-۵-۲- زمان بندی مراحل امن سازی اطلاعات

عملیات امن‌سازی معمولاً "عملیاتی پرهزینه و دقیق است و به علاوه لازم است در آن تقدم و تاخرهای منطقی رعایت شود. بنابراین زمان بندی این عملیات و دقت در امکان پذیر بودن اجرا این زمان بندی، اهمیت فراوان دارد.

ممکن است لازم باشد قبل از انجام عملیات اصلی امن‌سازی، تعدادی نقطه امن تعریف گردد. این نقاط برای جداسازی تجهیزات و یا شبکه‌های ارتباطی از یکدیگر کاربرد دارند و با تقسیم فضای عملیاتی به محدوده‌های کوچکتر، عملیات پاک سازی را تسهیل می‌کنند.

در صورت تشخیص مدیریت یا وقوع یک حادثه یا تغییرات پیش بینی نشده در ساختار سازمانی یا بدنه اجرایی سازمان، لازم است ممیزی اضطراری انجام پذیرد و پس از ارزیابی اثرات حوادث یا تغییرات، دستورالعمل‌های تصحیحی یا پیشنهادی به مورد اجرا گذاشته شود.

این کار می‌تواند با استفاده از ممیزان داخلی (هنگام ممیزی عادی و در دوره‌های کوتاه مدت) انجام پذیرد و یا در دوره‌های بلند مدت و هنگام اخذ گواهی نامه‌های رسمی از ممیزان رسمی استفاده شود.

۲-۱-ز- عملیات تصحیحی

عملیات تصحیحی عبارت‌اند از صدور پاسخ اضطراری، تدوین طرح‌های دفاعی تازه و احیاء سیستم. برنامه‌ریزی عملیات تصحیحی با استفاده از منابع زیر تسهیل می‌شود:

- مستندات جدید یا به هنگام شده داراییهای اطلاعاتی
- دانش جدید یا اخبار منتشره توسط گروه‌های مرجع
- نتایج حاصل از وقایع یا حوادث
- گزارش‌های داخلی
- بررسی فهرست‌های ثبت وقایع سیستم‌ها (Log File ها)
- نتایج حاصل از تمرین طرح‌های مقابله با شرایط اضطراری یا احیاء سیستم
- ممیزی‌ها
- مشاوره با افراد خبره

۲-۱-ح- به هنگام سازی چرخه فعالیت و بازنگری روش انجام کار

حتی اگر در طول دوره فعالیت چند ساله سازمان، حادثه امنیتی خاصی اتفاق نیفتد نمی‌توان از استحکام دفاعی سازمان اطمینان حاصل کرد. تغییر تکنولوژی، پیشرفت‌های علمی، گسترش دانش موجود در زمینه فعالیت‌های رایان‌های و ورود افراد جدید به فضای حمله و دفاع از عوامل تغییر ماهیت افق عملیاتی می‌باشند. بنابراین لازم است دائماً "و به صورت خودکار، روند عملیات و روش‌های دفاعی مورد بازنگری قرار گرفته و پایگاه دانش سازمان در مورد امنیت اطلاعات به هنگام شود.

۲-۱-ط- آموزش و کسب گواهینامه‌های معتبر داخلی یا بین‌المللی

بهترین مکانیزم‌های امنیت اطلاعات در صورت عدم آگاهی از روش اجرای آن، تبدیل به ابزاری دست و پاگیر و پرهزینه خواهند شد و پس از مدتی به دلیل اثبات ظاهری عدم کارایی کنار گذاشته خواهند شد.

لازم است کلیه اعضاء سازمان از روش، اهداف و استراتژی‌های دفاعی (در حد لازم) آگاه باشند و مسئولیت خود در این زمینه را پذیرفته و در صورت عدم رعایت نکات لازم منتظر عواقب انضباطی آن باشند.

بنابراین لازم است از ابزارهای آموزشی و اطلاع رسانی مناسب استفاده شود و فرهنگ امنیت اطلاعاتی به عنوان یک فرهنگ جاری و پویا در سطح سازمان مطرح شود.

پس از آگاهی افراد، نهادهای همکار و مدیریت سازمان و به‌کارگیری روش‌های امن‌سازی می‌توان کسب گواهینامه‌های محلی یا بین‌المللی را در دستور کار قرارداد.

کسب این گواهینامه‌ها از یک طرف عزم مدیریت سازمان را در کنترل هرچه بهتر محدوده تحت سرپرستی خود یادآوری کرده و از طرف دیگر مشتریان و مراجعه کنندگان سازمان را به اعتماد بیشتر به سازمان ترغیب خواهد کرد و مهر تائیدی بر دستیابی سازمان به اهداف تعریف شده خود در حفظ موجودیت سازمان و افزایش بهره‌وری خواهد بود.

پیاده‌سازی فعالیت‌های نه گانه فوق فرآیندی مهم و کارساز است و نیاز به برنامه‌ریزی، دقت، پایداری و خواست فراوان دارد.

مطالب بعدی که تشکیل دهنده قسمت اصلی این گزارش می‌باشد به تدوین دستورالعمل‌های لازم برای پیاده‌سازی توصیه‌های مطرح شده در این بخش اختصاص داده شده است.

۲-۲- راهنمای استفاده

دستورالعمل‌های حاضر به عنوان دستورالعمل‌های راهنما در زمینه ایجاد سامانه (نظام) مدیریت امنیت اطلاعات (Information Security Management System) منتشر شده است.

کلیه دستورالعمل‌ها بر اساس قواعد تبیین شده در سند دستورالعمل تولید و کنترل اسناد که به همراه همین مجموعه منتشر شده است تدوین و تنظیم شده‌اند.

هدف از نوشتن این دستورالعمل‌ها راهنمایی قدم به قدم استفاده کننده در جهت پیاده‌سازی سامانه (نظام) مدیریت امنیت اطلاعات می‌باشد.

هر دستورالعمل دارای یک شماره اختصاصی به عنوان شماره دستورالعمل می‌باشد. شماره اختصاصی شامل سه جزء به شرح زیر است:

- الف- شناسه اهمیت نهاد و طبقه‌بندی حفاظتی
- ب- شماره مرجع
- ج- اطلاعات تکثیر

شناسه اهمیت نهاد و طبقه‌بندی



شماره مرجع

شماره مرجع به عنوان شناسه اصلی دستورالعمل مورد مراجعه قرار خواهد گرفت.

شناسه اهمیت نهاد و اطلاعات تکثیر برای اعمال مدیریت بهتر توسط نهادهای استفاده کننده پیش بینی شده و توسط ایشان تکمیل خواهد شد.

نحوه ارائه دستورالعمل‌ها و ترتیب انتشار آن‌ها به نحوی است که با مطالعه دستورالعمل ۱-۱ (راهنمای سیاست‌گذاری امنیت اطلاعات) می‌توان شروع به پیاده‌سازی سامانه مدیریت امنیت اطلاعات نمود.

هر جا در متن دستورالعمل به انجام فعلیتی خاص اشاره شده باشد به دستورالعمل اختصاصی بیان کننده چگونگی انجام آن فعالیت اشاره شده است. به عنوان مثال در دستورالعمل ۱-۱ در بخش مسئولیت، مسئولیت تدوین سند به عهده کمیته امنیت اطلاعات گذاشته شده و در همان‌جا به شماره دستورالعملی که مبین چگونگی تشکیل آن کمیته است اشاره شده است (دستورالعمل ۲-۱-۲، هماهنگی امنیت اطلاعات).

هر دستورالعمل متعلق به یک فصل و یک حوزه می‌باشد. فصل‌های مختلف در قالب سه مرحله منتشر خواهد شد. دستورالعمل‌های فعلی متعلق به فصل‌های سیاست‌گذاری امنیتی، سازمان (دهی) امنیت اطلاعات، مدیریت دارایی‌های اطلاعاتی و کنترل دسترسی می‌باشد.

هنگام انتشار هر فصل کلیه حوزه‌ها و دستورالعمل‌های مربوط به آن به صورت یکجا منتشر خواهد شد. در این مرحله حتی الامکان سعی بر آن بوده است که برای جلوگیری از سردرگمی استفاده کنندگان ارجاعات فقط مختص به آن دسته از دستورالعمل‌هایی باشد که تاکنون منتشر شده‌اند. در صورت انتشار دستورالعمل‌های جدید، ارجاعات دستورالعمل‌های قبلی مورد بازبینی قرار گرفته و تغییرات آن مجدداً منتشر خواهد شد.

به کارگیری این دستورالعمل‌ها در دو حالت امکانپذیر است:

- استفاده مستقیم از دستورالعمل به وسیله سازمان و اختصاصی سازی آن برای خود
 - اختصاصی سازی عام دستورالعمل توسط ستاد مرکزی یک وزارتخانه یا سازمان و ارسال آن برای واحدهای پایین دستی جهت اختصاصی سازی مرحله دوم در هر رده تابعه
- در حالت اول لازم است اولاً شناسه اهمیت نهاد و اطلاعات تکثیر از کد دستورالعمل حذف شده و فقط شناسه طبقه‌بندی حفاظتی دستورالعمل تعریف و پس از اختصاصی سازی دستورالعمل به آن تخصیص داده شود و ثانیاً اختصاصی سازی کلیه دستورالعمل‌ها بر اساس شاخص دسته‌بندی تعریف شده از سوی سازمان پدافند غیرعامل (حیاتی، حساس و مهم) برای سازمان بهره‌بردار انجام شود.
- در حالت دوم لازم است به شرح زیر عمل شود:
- الف- هنگام اختصاصی سازی، دسته‌بندی سازمان پدافند غیرعامل برای هر یک از رده‌های تابعه سازمان در نظر گرفته شده و بر اساس آن اختصاصی سازی انجام شود.
 - ب- هنگام اختصاصی سازی، نوع طبقه‌بندی مناسب برای دستورالعمل (با توجه به حوزه اجرای دستورالعمل) تعیین شده و در اختصاصی سازی به آن هم توجه شود.
 - ج- برای کنترل نسخ دستورالعمل‌های دارای طبقه‌بندی تعداد کل نسخه‌های تکثیر شده در قسمت تعداد تکثیر کد دستورالعمل و شماره سریال نسخه‌ای که برای دستگاه خاصی ارسال شده در قسمت شاخص واحد تحویل گیرنده درج گردد تا در صورت افشای دستورالعمل‌های دارای طبقه‌بندی پیگیری نقطه افشاء تسهیل گردد.
 - د- لازم است در کلیه دستورالعمل‌ها شماره مرجع بدون تغییر باقی بماند. در صورت نیاز به نوشتن دستورالعمل جدید برای استفاده در سازمان لازم است با توجه به فصل و حوزه

مرتبط با دستورالعمل شماره سریال جدیدی انتخاب شده و به دستورالعمل جدید تخصیص داده شود.

۲-۳- مثال برای اختصاصی سازی

در نهادهایی که زیر مجموعه‌های مربوط به آن‌ها از دیدگاه سازمان پدافند غیرعامل و در دو سطح مهم و یا حساس طبقه‌بندی می‌شوند و از روش طبقه‌بندی سه سطحی عادی، محرمانه و خیلی محرمانه استفاده می‌کنند دستورالعمل ۱-۱-۱ (سیاست‌گذاری امنیت اطلاعات) دارای نسخه‌های متفاوت زیر خواهد بود:

کد	دسته‌بندی از دیدگاه پدافند غیرعامل
الف	مراکز مهم
ب	مراکز حساس

کد	طبقه‌بندی حفاظتی
۱	عادی
۲	محرمانه
۳	خیلی محرمانه

انواع نسخه‌های قابل تولید: (توضیح اطلاعات تکثیر با توجه به تعداد نسخه انتشار شده و ارسال شده تعیین خواهد گردید).

عنوان دستورالعمل	کد	کاربرد
سیاست‌گذاری امنیت اطلاعات	□-□-۱/۱-۱-۱-الف	قابل استفاده در مراکز مهم با طبقه‌بندی حفاظتی عادی
سیاست‌گذاری امنیت اطلاعات	□-□-۱/۱-۱-۲-الف	قابل استفاده در مراکز مهم با طبقه‌بندی حفاظتی محرمانه
سیاست‌گذاری امنیت اطلاعات	□-□-۱/۱-۱-۳-الف	قابل استفاده در مراکز مهم با طبقه‌بندی حفاظتی خیلی محرمانه
سیاست‌گذاری امنیت اطلاعات	□-□-۱/۱-۱-۱-ب	قابل استفاده در مراکز حساس با طبقه‌بندی حفاظتی عادی
سیاست‌گذاری امنیت اطلاعات	□-□-۱/۱-۱-۲-ب	قابل استفاده در مراکز حساس با طبقه‌بندی حفاظتی محرمانه
سیاست‌گذاری امنیت اطلاعات	□-□-۱/۱-۱-۳-ب	قابل استفاده در مراکز حساس با طبقه‌بندی حفاظتی خیلی محرمانه

لازم است هنگام اختصاصی سازی به نکته زیر توجه شود:

کلیه عبارت‌هایی که بین علامت " (") و " (") درج شده‌اند حذف و به جای آن عبارت متناسب با کاربرد در سازمان متبوع گذاشته شود.

مثال ۱:

اگر محل استفاده از دستورالعمل وزارت ارتباطات و فناوری اطلاعات و حوزه اجرایی آن سطح وزارتخانه باشد عبارت‌ها به صورت زیر تغییر می‌یابند.

((وزارت / سازمان / اداره کل / شرکت / ...))	به	وزارت ارتباطات و فناوری اطلاعات
((بالاترین مقام اجرایی))	به	وزیر

مثال ۲:

اگر محل استفاده از دستورالعمل شرکت ملی نفت ایران می‌باشد و حوزه اجرای آن کلیه تأسیسات و مکان‌های متعلق به شرکت ملی نفت ایران در داخل و خارج کشور باشد:

((وزارت / سازمان / اداره کل / شرکت / ...))	به	شرکت ملی نفت ایران
((بالاترین مقام اجرایی))	به	مدیر عامل

تغییر خواهد یافت.

۲-۴- دستورالعمل تولید و کنترل اسناد

هدف:

این دستورالعمل مبین روش تولید و حداقل الزامات و خصوصیات اسنادی است که در مدیریت و اجرای سیستم مدیریت امنیت اطلاعات ((وزارت / سازمان / اداره کل / شرکت / ...)) براساس نظام مدیریت امنیت اطلاعات به کار گرفته خواهند شد.

مسئولیت‌ها:

متصدیان کلیه فرآیندها (و پردازش‌هایی) که در حوزه اجرا و قلمرو نظام مدیریت امنیت اطلاعات قرار گرفته‌اند مسئولیت تهیه رویه‌های مربوط به انجام هر یک از فرآیندها را عهده دارند.

به علاوه کلیه مستندات مربوط به طراحی و تعیین چارچوب مدیریتی نظام مدیریت امنیت اطلاعات نیز باید با توجه به محتوای سند حاضر ساماندهی شوند.

الزامات:

- لازم است کلیه مستنداتی که برای استفاده در فعالیتهای مدیریت امنیت اطلاعات تولید یا به کار گرفته می‌شوند خصوصیات زیر را داشته باشند:
- دارای شماره اختصاصی باشند.
 - به آسانی قابل شناسایی باشند.
 - در صورتی که برای کاربرد عمومی تهیه نشده باشند با علامت "محرمانه / خیلی محرمانه" و یا هر علامت خاص نهاد بهره‌بردار نشان‌گذاری شده باشند.
 - به آسانی در دسترسی افراد مجاز مستقر در کلیه مکان‌های اجرای عملیات قرار گیرند.
 - به اندازه کافی در مقابل دسترسی‌های ناخواسته یا غیرمجاز حفاظت شوند.
 - به صورت مرتب و دوره‌ای بازنگری شده و تصحیحات لازم براساس سند سیاست‌گذاری امنیت اطلاعات ((وزارت/ سازمان/ اداره کل/ شرکت/ ...)) در آنها انجام پذیرد.
 - دستورالعمل‌های کنترل نسخه (Version Control) در مورد آنها رعایت شود و تاریخ‌های صدور نسخه اولیه و بازنگری‌های بعدی روی آنها درج شده باشد.
 - در صورت باطل شدن سند یا متغی شدن استفاده از آن، این موضوع به اطلاع کلیه افراد مرتبط رسانده شود.
 - در صورتی که پس از باطل شدن یا متغی شدن استفاده از سند، نیاز به نگهداری آن برای استفاده‌های قانونی باشد، تدابیر لازم برای حفظ سند در پیش گرفته شود.

تأییدیه:

لازم است کلیه فرآیندهای مستند شده توسط متصدی فرآیند (فردی که مسئولیت انجام کار با تجهیزات یا نرم‌افزارهای پردازشی به عهده وی می‌باشد) قبل از انتشار، بازبینی و تأیید شود و سپس به تأیید کمیته امنیت اطلاعات برسد. در صورتی که انجام فرآیند مستلزم خروج از مرزهای سازمانی نهاد بهره‌بردار است، باید قبلاً "تأییدیه سایر مراجع مرتبط نیز اخذ شود."

روش تولید سند:

فرآیندها و مستندات مرتبط با هر فرآیند که فعالیت‌های مدیریت و اجرای نظام مدیریت امنیت اطلاعات را پوشش می‌دهند، به طور کلی برای پاسخگویی به دستورالعمل‌ها یا سیاست‌گذاری‌های کمیت‌ه امنیت اطلاعات تهیه و تدوین می‌شوند.

لازم است نکات زیر در طراحی این فرآیندها یا تدوین مستندات مورد توجه قرار گیرند:

- مالکیت، تصدی‌گری و یا مسئولیت افراد در انجام هر بخش از فعالیت‌های ورود اطلاعات، پردازش، تصحیح، گزارش‌گیری، ذخیره و بازیابی و ممیزی داده‌ها تعیین شود.
- ملزومات اجراء یا ارسال نگهداری نرم‌افزار و تجهیزات، کنترل دسترسی، راهبری شبکه، کنترل کانال‌های ارتباطی، پشتیبانی و تامین نیازها در متن سند ذکر شود.
- فعالیت‌هایی کلیدی مانند ایجاد نظام مدیریت امنیت اطلاعات، امن‌سازی محیط و تدوین طرح احیاء سیستم به عنوان فعالیت‌های بنیادی مورد توجه قرار گرفته و در اولویت قرار گیرند.
- معیارهای اندازه‌گیری میزان کارایی فعالیت‌های قید شده در سند (در صورت نیاز) طراحی شده و ابلاغ شوند.
- منابع (شامل نفرات مورد نیاز، مسئولیت‌ها و ابزار و تجهیزات) پیش‌بینی شده و برای تامین آن‌ها برنامه‌ریزی شود.
- به الزامات محیط اجراء (قانون، مقررات، الزامات قراردادی یا سازمانی) توجه شود.
- وقایع مرتبط با موضوع هر سند ثبت و بایگانی شود.

پس از تعیین روش جمع‌آوری یا کسب داده‌های ورودی و ملزومات پردازش، اجراء یا ارسال اطلاعات یا گزارش‌ها لازم است کلیه روش‌های تبادل اطلاعات و ارتباط بین افراد دخیل در اجرای فرآیند در نظر گرفته شده و در مورد آن‌ها تصمیم‌گیری شود. فرآیند باید قابل اجراء بوده و با توجه به منابع و محدودیت‌ها طراحی شود. فرمت دستورالعمل‌های امنیتی مربوط به هر فرآیند در ضمیمه الف درج گردیده است و لازم است کلیه مستندات در قالب این فرمت تهیه گردند.

فهرست اسناد مرجع:

فهرست کلیه فرآیندهای مستند شده موضوع نظام مدیریت امنیت اطلاعات (دستورالعمل‌های امنیت اطلاعات) در "فهرست اسناد مرجع" نگهداری خواهند شد. فهرست اسناد مرجع حاوی اطلاعات زیر در مورد هر یک از اسناد می‌باشد:

- شماره مرجع و نحوه تخصیص آن
- شرح سند (دستورالعمل)
- بازنگری‌ها
- نگهبان، مسئول یا متصدی حفاظت از سند (دستورالعمل) و نظارت بر اجرای آن
- محل نگهداری سند
- طبقه‌بندی حفاظتی
- * نحوه استفاده از "فهرست اسناد مرجع" باید در صدر همان فهرست شرح داده شود.

کنترل تغییرات:

پس از تأیید یک فرآیند و انتشار دستورالعمل (سند) مربوط؛ هر گونه تغییر در روش اجراء یا متن سند منوط به طی مراحل رسمی کنترل تغییرات می‌باشد. در صورتی که به هر دلیل درخواستی برای تغییر در نحوه اجرای فرآیند مطرح شود، اعمال آن فقط با کسب مجوز از متصدی فرآیند یا نماینده قانونی وی امکان‌پذیر خواهد بود.

کلیه درخواست‌های تغییر در روش اجرای فرآیند باید قبلاً از لحاظ تاثیر بر اجرای همان فرآیند و یا سایر فرآیندهای وابسته یا موازی مورد بررسی قرار گیرد.

متصدی فرآیند مسئولیت نگهداری سوابق تغییرات را به عهده دارد. سوابق تغییرات باید به وضوح ثبت و نگهداری شود.

درخواست‌های تغییر باید در فرمت نشان داده شده در ضمیمه "ب" ارائه شوند. در صورت امکان باید دلایل و نحوه تغییرات در سند مربوطه درج شود.

سوابق:

لازم است سوابق کلیه فرآیندها و اسناد نگهداری شود. از این سوابق در تهیه شواهد مربوط به انطباق فرآیند با الزامات قانونی، مقرراتی یا قراردادی استفاده خواهد شد. سوابق کلیه فرآیندها و اسناد باید به صورت واضح و روشن ثبت و نگهداری گردد به طوری که بتوان در زمان مورد نیاز آثار و رد اجرای هر فرآیند را دنبال نمود. فرآیند ثبت سوابق باید نحوه ثبت و محتویات رکورد ثبت شده را معین نماید. مدت زمان نگهداری اطلاعات مربوط به سوابق اجراء و تغییرات، محل نگهداری آن و نوع مجوزهای مورد نیاز برای معدوم‌سازی سوابق باید تعریف و تعیین و برای آن فرآیند خاصی نوشته شده و در "فهرست اسناد مرجع" درج گردد.

مراجع:

فهرست اسناد مرجع

فرمت پیشنهادی دستورالعمل‌های امنیت اطلاعات به شرح مندرج در ضمیمه «الف» همین سند

فرم درخواست تغییرات به شرح مندرج در ضمیمه «ب» همین سند

اخطار مهم:

طبقه‌بندی‌های حفاظتی مندرج در صفحه اول دستورالعمل‌هایی که در طی این طرح تقدیم خواهد شد جنبه مثال داشته و قابل اعمال نمی‌باشد. لازم است طبقه‌بندی‌های حفاظتی با توجه به مقررات اختصاصی هر بهره‌بردار تعیین و اعمال شود.

ضمیمه الف

(فرمت صفحه اول اسناد)

((نام نهاد بهره‌بردار)))

(((فصل)))	(((حوزه)))
((عنوان دستورالعمل)) ((شماره دستورالعمل))	

((طبقه‌بندی حفاظتی)))

((آرم/نام نهاد بهره‌بردار))

تائیدیه نهایی بالاترین مقام اجرایی نهاد بهره‌بردار

نام و نام خانوادگی:

پست سازمانی:

امضاء:

تاریخ:

فهرست گیرندگان :

این سند در ((کمیته / کتابخانه / مرکز اسناد / سرور آدرس [محل نگهداری فایل])) نگهداری می‌شود.

ضمیمه الف

(فرمت صفحه دوم اسناد)
(((نام نهاد بهره‌بردار)))

تأییدیه‌های تکمیلی

(فقط برای اسناد یا فرآیندهایی که در حوزه سیاست‌گذاری و سازماندهی امنیت اطلاعات تدوین می‌شوند و یا بین چند سازمان تبادل می‌گردند.)

سوابق تغییرات :

شرح	تاریخ

(ترتیب درج مطالب در سایر صفحه‌ها)

روند نما:

```
graph RL; In(( )) --> B1[ ]; B1 --> B2[ ]; B2 --> B3[ ]; B3 --> B4[ ]; B3 --> B5[ ]; B4 --> B6[ ]; B4 --> B7[ ]; B6 --> B7;
```


ضمیمه ب

(فرمت فرم درخواست تغییرات)

(((نام نهاد بهره‌بردار)))

فرم درخواست تغییرات

عنوان سند:

شماره سند:

تاریخ درخواست:

دلایل درخواست:

تغییر مورد درخواست:

تائید درخواست؟

تاریخ:

☐ خیر☐ بلی

تائید / رد شده توسط :

عنوان سازمانی:

۳- دستورالعمل‌ها

در ادامه فهرست دستورالعمل‌های اختصاصی امنیت اطلاعات که در این کتاب بررسی شده است، آورده می‌شود:

شماره مرجع	فصل	حوزه	موضوع
۱	سیاست گذاری امنیتی		
۱-۱	سیاست گذاری امنیتی	سیاست گذاری امنیت اطلاعات	
۱-۱-۱	سیاست گذاری امنیتی	سیاست گذاری امنیت اطلاعات	سند سیاست گذاری امنیت اطلاعات
۲-۱-۱	سیاست گذاری امنیتی	سیاست گذاری امنیت اطلاعات	بازنگری سند سیاست گذاری امنیت اطلاعات
۳-۱-۱	سیاست گذاری امنیتی	سیاست گذاری امنیت اطلاعات	سند تعیین قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات
۲	سازمان (دهی) امنیت اطلاعات		
۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	
۱-۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	تعهد و اهتمام مدیریت ارشد سازمان به امنیت اطلاعات
۲-۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	هماهنگی امنیت اطلاعات
۳-۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	تعیین مسئولیت در حوزه امنیت اطلاعات
۴-۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	صدور مجوز استفاده از تجهیزات پردازش اطلاعات

شماره مرجع	فصل	حوزه	موضوع
۵-۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	توافقتنامه‌های حفظ محرمانگی
۶-۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	برقراری ارتباط با مراجع حکومتی
۷-۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	ارتباط با سایر مراجع یا سازمان‌ها یا نهادها (ی دارای اشتراک منافع)
۸-۱-۲	سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی	بازنگری مستقل سامانه امنیت اطلاعات
۲-۲	سازمان (دهی) امنیت اطلاعات	تعامل با اشخاص ثالث (سایر مراجع)	
۱-۲-۲	سازمان (دهی) امنیت اطلاعات	تعامل با اشخاص ثالث (سایر مراجع)	شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری
۲-۲-۲	سازمان (دهی) امنیت اطلاعات	تعامل با اشخاص ثالث (سایر مراجع)	رعایت نکات امنیتی هنگام تعامل با مشتریان یا ارباب رجوع
۳-۲-۲	سازمان (دهی) امنیت اطلاعات	تعامل با اشخاص ثالث (سایر مراجع)	رعایت معیارهای امنیتی در قراردادهای اشخاص ثالث
۳	مدیریت دارایی‌های اطلاعاتی		
۱-۳	مدیریت دارایی‌های اطلاعاتی	مسئولیت حفظ دارایی‌های اطلاعاتی	
۱-۱-۳	مدیریت دارایی‌های اطلاعاتی	مسئولیت حفظ دارایی‌های اطلاعاتی	فهرست موجودی دارایی‌های اطلاعاتی
۲-۱-۳	مدیریت دارایی‌های اطلاعاتی	مسئولیت حفظ دارایی‌های اطلاعاتی	تعیین متصدی و یا مالکیت دارایی‌های اطلاعاتی
۳-۱-۳	مدیریت دارایی‌های اطلاعاتی	مسئولیت حفظ دارایی‌های اطلاعاتی	نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی

شماره مرجع	فصل	حوزه	موضوع
۲-۳	مدیریت دارایی‌های اطلاعاتی	طبقه‌بندی اطلاعات	
۱-۲-۳	مدیریت دارایی‌های اطلاعاتی	طبقه‌بندی اطلاعات	دستورالعمل طبقه‌بندی اطلاعات
۲-۲-۳	مدیریت دارایی‌های اطلاعاتی	طبقه‌بندی اطلاعات	برچسب‌گذاری دارایی‌های اطلاعاتی و نگهداری
۳-۳	مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک	
۱-۳-۳	مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک	گزارش مرحله شناخت سیستم
۲-۳-۳	مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک	ارزیابی ریسک
۳-۳-۳	مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک	مدیریت و مقابله با ریسک
۴-۳-۳	مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک	بیانیه کاربرد پذیری (SOA) اختصاصی
۷	کنترل دسترسی		
۱-۷	کنترل دسترسی	الزامات حوزه فعالیت در کنترل دسترسی	
۱-۱-۷	کنترل دسترسی	الزامات حوزه فعالیت در کنترل دسترسی	سیاست‌گذاری کنترل دسترسی
۲-۷	کنترل دسترسی	مدیریت دسترسی کاربران	
۱-۲-۷	کنترل دسترسی	مدیریت دسترسی کاربران	ثبت کاربر
۲-۲-۷	کنترل دسترسی	مدیریت دسترسی کاربران	مدیریت دسترسی‌های ممتاز
۳-۲-۷	کنترل دسترسی	مدیریت دسترسی کاربران	مدیریت کلمه عبور کاربر
۴-۲-۷	کنترل دسترسی	مدیریت دسترسی کاربران	بازنگری حقوق دسترسی کاربران

شماره مرجع	فصل	حوزه	موضوع
۳-۷	کنترل دسترسی	مسئولیت پذیری کاربران	
۱-۳-۷	کنترل دسترسی	مسئولیت پذیری کاربران	استفاده از کلمه عبور
۲-۳-۷	کنترل دسترسی	مسئولیت پذیری کاربران	تجهیزات کاربری بدون مراقب
۳-۳-۷	کنترل دسترسی	مسئولیت پذیری کاربران	روش مانیتور پاک و میز پاکیزه
۴-۷	کنترل دسترسی	کنترل دسترسی شبکه	
۱-۴-۷	کنترل دسترسی	کنترل دسترسی شبکه	سیاست‌گذاری در استفاده از سرویس‌های شبکه
۲-۴-۷	کنترل دسترسی	کنترل دسترسی شبکه	احراز صلاحیت کاربر برای اتصال به شبکه‌های خارج از سازمان
۳-۴-۷	کنترل دسترسی	کنترل دسترسی شبکه	شناسایی تجهیزات در شبکه
۴-۴-۷	کنترل دسترسی	کنترل دسترسی شبکه	حفاظت از سرویس‌های رفع اشکال از راه دور و پیکربندی درگاه‌ها
۵-۴-۷	کنترل دسترسی	کنترل دسترسی شبکه	جداسازی شبکه‌ها
۶-۴-۷	کنترل دسترسی	کنترل دسترسی شبکه	کنترل اتصال‌های شبکه
۷-۴-۷	کنترل دسترسی	کنترل دسترسی شبکه	کنترل مسیریابی شبکه
۵-۷	کنترل دسترسی	کنترل دسترسی سیستم عامل	
۱-۵-۷	کنترل دسترسی	کنترل دسترسی سیستم عامل	رویه‌های امن آغاز به کار
۲-۵-۷	کنترل دسترسی	کنترل دسترسی سیستم عامل	شناسایی و احراز صلاحیت (تأیید اعتبار) کاربر
۳-۵-۷	کنترل دسترسی	کنترل دسترسی سیستم عامل	سیستم مدیریت کلمه عبور
۴-۵-۷	کنترل دسترسی	کنترل دسترسی سیستم عامل	استفاده از ابزارهای سیستم
۵-۵-۷	کنترل دسترسی	کنترل دسترسی سیستم عامل	محدودیت مدت نشست
۶-۵-۷	کنترل دسترسی	کنترل دسترسی سیستم عامل	محدودیت زمان اتصال
۶-۷	کنترل دسترسی	کنترل دسترسی برنامه‌های کاربردی و داده‌ها	

شماره مرجع	فصل	حوزه	موضوع
۱-۶-۷	کنترل دسترسی	کنترل دسترسی برنامه‌های کاربردی و داده‌ها	محدودسازی دسترسی به اطلاعات
۲-۶-۷	کنترل دسترسی	کنترل دسترسی برنامه‌های کاربردی و داده‌ها	جداسازی سامانه (سیستم)‌های حساس
۷-۷	کنترل دسترسی	پردازش همراه و کار از راه دور	
۱-۷-۷	کنترل دسترسی	پردازش همراه و کار از راه دور	پردازش همراه و مخابرات سیار
۲-۷-۷	کنترل دسترسی	پردازش همراه و کار از راه دور	کار از راه دور

اخطار مهم: لازم است به محض دریافت سایر دستورالعمل‌ها این فهرست به‌هنگام‌سازی شود.

۳-۱- سیاست‌گذاری امنیتی

این بخش شامل دستورالعمل‌های زیر می‌باشد:

۱ - سیاست‌گذاری امنیتی		
سیاست‌گذاری امنیت اطلاعات	۱-۱	
سند سیاست‌گذاری امنیت اطلاعات		۱-۱-۱
بازنگری سند سیاست‌گذاری امنیت اطلاعات		۲-۱-۱
سند تعیین قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات		۳-۱-۱

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سیاست‌گذاری امنیتی	سیاست‌گذاری امنیت اطلاعات
راهنمای سیاست‌گذاری امنیت اطلاعات شماره دستورالعمل : ۱-۱	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: ((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و فقط در اختیار کمیته امنیت اطلاعات خواهد بود. هرگونه درخواستی در زمینه مطالعه این سند قبلاً باید توسط حداقل یک نفر از اعضای کمیته امنیت اطلاعات رسیدگی شده و مجوز کتبی آن صادر شود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب

خواهد شد.

سوابق تغییرات :

تاریخ	شرح

کاربرد و هدف

این سند حاوی مستنداتی است که مبین چارچوب مدیریتی سامانه مدیریت امنیت اطلاعات ((وزارت/ سازمان/ اداره کل/ شرکت/)) می‌باشند و منطبق بر نیازهای مندرج در استاندارد ISO27001:2005 تدوین شده و به اجراء در خواهند آمد.

مسئولیت

مسئولیت تدوین، راهبری و نظارت بر اجرای این سند به عهده کمیته امنیت اطلاعات (موضوع دستورالعمل ۲-۱-۲) به نمایندگی از سوی ((بالاترین مقام اجرایی)) ((وزارت/ سازمان/ اداره کل/ شرکت/)) است. اعضای کمیته امنیت اطلاعات عبارت‌اند از:

- ۱- ((نماینده تام‌الاختیار بالاترین مقام اجرایی سازمان))
- ۲- ((مسئول مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات))
- ۳- ((معاون اداری، مالی و پشتیبانی))
- ۴- ((معاون برنامه‌ریزی))
- ۵- ((معاون فنی))
- ۶- ((مسئول حراست))
- ۷-
- ۸-

توضیح: لازم است تعداد اعضای کمیته امنیت اطلاعات فرد باشد و تصمیمات آن با کسب نصف به علاوه یک آرای اعضا رسمیت می‌یابد.

اسناد مرجع

۱. سند سیاست‌گذاری امنیت اطلاعات به شماره سند ۱-۱-۱
۲. سند تعیین قلمرو به شماره سند ۳-۱-۱
۳. مستندات ارزیابی ریسک شامل :
 - ۱-۳- فهرست دارایی‌های شناسایی شده در مرحله شناخت سیستم به شماره سند ۱-۱-۳
 - ۲-۳- فهرست برچسب‌گذاری دارایی‌ها به شماره سند ۲-۲-۳

۳-۳- گزارش مرحله شناخت سیستم به شماره سند ۳-۳-۱

۴. سند مدیریت ریسک به شماره سند ۳-۳-۳
۵. بیانیه کاربرد پذیری (SOA) اختصاصی سازمان به شماره سند ۳-۳-۴
۶. دستورالعمل‌های کنترلی اختصاصی سازمان به شرح جدول زیر:

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سیاست‌گذاری امنیتی	سیاست‌گذاری امنیت اطلاعات
سند سیاست‌گذاری امنیت اطلاعات شماره دستورالعمل : ۱-۱-۱	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان))

عنوان: ((بالاترین مقام اجرایی سازمان))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و فقط در اختیار کمیته امنیت اطلاعات خواهد بود. هرگونه درخواستی در زمینه مطالعه این سند قبلاً باید توسط حداقل یک نفر از اعضای کمیته امنیت اطلاعات رسیدگی شده و مجوز کتبی آن صادر شود.

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول ((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به عنوان دبیر منصوب خواهد شد.

[illegible]

سیاست‌گذاری امنیت اطلاعات

کاربرد این سند، تبیین سیاست‌گذاری حفاظت از دارایی‌های اطلاعاتی در اختیار (((وزارت/ سازمان/ اداره کل/ شرکت/....))) در مقابل تمام تهدیدهای موجود اعم از داخلی و خارجی و تصادفی و عمدی مربوط به حوزه فعالیت‌های جمع‌آوری، پردازش، تولید، ذخیره‌سازی، توزیع و ارسال اطلاعات می‌باشد.

به کارگیری این سند سیاست‌گذاری در زمینه برقراری و حفظ رابطه مطلوب با ارباب رجوع، مشتریان و کلیه شرکای اداری و تجاری ضروری است و براساس این سند **مقرر می‌گردد** روش‌های برقراری و حفظ ارتباط به گونه‌ای باشد که از موارد زیر اطمینان حاصل شود:

- از اطلاعات در برابر دسترسی‌های غیرمجاز حفاظت به عمل آید.
- محرمانگی اطلاعات رعایت گردد.
- اطلاعات به هیچ وجه نزد افراد غیرمجاز چه به صورت ناخواسته و یا با قصد قبلی و یا در اثر کم توجهی به رعایت اصول مربوط، افشاء نگردد.
- جامعیت اطلاعات از طریق حفاظت از آن در مقابل تغییرات ناخواسته یا غیرمجاز، تضمین گردد.
- اطلاعات در زمان مورد نیاز در اختیار افراد مجاز قرار داده شود.
- کلیه قوانین کشوری و مقررات سازمانی در زمینه تبادل و پردازش اطلاعات و یا استفاده از دارایی‌های اطلاعاتی رعایت گردد.
- طرح پیوستگی عملیات، تهیه شده و به طور دائم به هنگام‌سازی شود و در زمان‌های مناسب تحت آزمایش قرار گیرد.
- آموزش‌های لازم در زمینه حفظ امنیت اطلاعات به کلیه پرسنل شرکت داده شود.
- کلیه موارد نقض امنیت اطلاعات و یا نقاط ضعفی که ممکن است در آینده از آن‌ها برای نقض امنیت اطلاعات سوء استفاده شود شناسایی و گزارش شده و پیگیری بعدی در مورد نحوه مقابله با آن‌ها به مورد اجراء گذاشته شود.

اهداف

- شناسایی ارزش دارایی‌های اطلاعاتی از طریق به کارگیری روش ارزیابی ریسک متناسب با نوع فعالیت (((وزارت/ سازمان/ اداره کل/ شرکت/ ...))) برای درک آسیب‌پذیری‌ها و تهدیدهایی که ممکن است دارایی‌های اطلاعات را در معرض خطر قرار دهد.
- کاهش ریسک به سطح قابل قبولی که از طریق طراحی، به کارگیری و اجرای سیستم کارای مدیریت امنیت اطلاعات، تعیین گشته است.
- رعایت شئون اخلاقی و حفظ کرامت و اطلاعات خصوصی شهروندان کشور جمهوری اسلامی ایران
- رعایت قوانین کشوری و مقررات و سندهای راهبردی کشور شامل:
- سند راهبردی نظام جامع فناوری اطلاعات
- سند راهبردی امنیت فضای تبادل اطلاعات کشور مصوب ۸۴/۴/۸ هیات وزیران و ابلاغیه ۳۳۱۰۱/ت/۲۴۵۳۰ هـ مورخ ۸۴/۴/۲۵
- قانون حفاظت از حقوق پدید آورندگان نرم‌افزار رایان‌های مصوب ۱۳۷۹
- قانون تجارت مصوب ۱۳۱۱/۲/۱۳
- قانون تجارت الکترونیک مصوب ۱۳۸۲
- قانون آزادی اطلاعات مصوب ۸۴/۵/۱۰ به شماره ۲۹۴۱۱/۲۸۴۹۸ و ابلاغیه
- آیین‌نامه گسترش بهره‌برداری از خدمات پول الکترونیکی مصوب ۸۴/۵/۱۰ شماره ۳۳۳۵۹/ت/۲۶۰۱۹ هـ
- آیین‌نامه سازماندهی فعالیت پایگاه‌های اطلاع‌رسانی اینترنتی ایرانی مصوب ۸۵/۹/۵ ۳۵۷۴۱/ت/۱۰۹۰۶۰ هـ
- (((سایر قوانین موضوعه در حوزه فعالیت وزارت/ سازمان/ اداره کل/ شرکت/ ...)))
- رعایت شرط‌های مربوط به امنیت اطلاعات مندرج در قراردادهای منعقد شده با مشتریان
- رعایت دستورالعمل‌های سازمانی (((وزارت/ سازمان/ اداره کل/ شرکت/ ...)))

- انطباق با ISO 27001:2005 یا سایر استانداردهای مرتبط که از طرف موسسه استاندارد و تحقیقات صنعتی ایران منتشر خواهد شد.
- کسب و حفظ گواهینامه استاندارد ISO 27001:2005 یا استانداردهای مرتبط

مسئولیت‌ها

- مسئولیت پشتیبانی از کلیه پرسنل و شرکای تجاری و یا افراد تحت قرارداد و یا طرف قرارداد در زمینه حفاظت از دارایی‌های اطلاعاتی مندرج در حوزه سیستم مدیریت امنیت اطلاعات (که تحت عنوان سند قلمرو پیاده‌سازی سامانه امنیت اطلاعات تعیین گشته است) به عهده (((بالاترین مقام اجرایی))) ((وزارت/ سازمان/ اداره کل/ شرکت/ ...)) می‌باشد.
- این سند به وسیله کارگروه امنیت اطلاعات (موضوع دستورالعمل ۲-۱-۲) پیشنهاد شده و به تصویب کمیته امنیت اطلاعات رسیده است و در زمان‌های مورد نیاز مورد تجدید نظر قرار خواهد گرفت.
- (((مسئول مرکز حراست فناوری اطلاعات یا نهاد متصدی حفظ امنیت اطلاعات))) و یا نهاد جانشین وی محتوای این سند را با استفاده از دستورالعمل‌ها و رویه‌های مناسب پیاده‌سازی خواهد نمود.
- کلیه پرسنل، مستخدمین و افراد طرف قرارداد ((وزارت/ سازمان/ اداره کل/ شرکت/ ...)) موظف‌اند دستورالعمل‌های مربوط به حفظ امنیت اطلاعات را که جزئی از این سند به شمار می‌روند رعایت نمایند.
- کلیه پرسنل موظف‌اند وقایع امنیت اطلاعات و یا ضعف‌های احتمالی که منجر به نقض امنیت اطلاعات خواهد شد را (طبق دستورالعمل‌های مربوط) گزارش نمایند. (هر گونه جست‌وجو به دنبال نقاط ضعف احتمالی بدون کسب مجوز قبلی ممنوع است)
- کلیه اعمال غیر مغرضانه منجر به نقض یا صدمه به امنیت اطلاعات و یا تجهیزات پردازشی ((وزارت/ سازمان/ اداره کل/ شرکت/ ...))، ارباب رجوع و یا مشتریان آن منجر به اقدامات انضباطی و اعمال مغرضانه یا غیرمغرضانه منجر به ایجاد خسارت شامل پیگرد قانونی خواهد شد.

روش‌های عام و خاص

فرآیندهای عام زیر در جهت پشتیبانی این سند و بر اساس دستورالعمل‌های امنیت اطلاعات به کار گرفته خواهد شد:

- امنیت فیزیکی و محیطی
- کنترل دسترسی سیستم‌ها و یا داده‌ها
- آموزش و اطلاع رسانی امنیت اطلاعات
- رفتار سازمانی پرسنل
- استفاده از اینترنت و پست الکترونیک
- استفاده از شبکه داخلی و شبکه گسترده
- تهیه نسخه پشتیبان از اطلاعات
- استفاده از تجهیزات پردازشی قابل حمل
- ذخیره‌سازی و خارج از رده‌سازی اطلاعات محرمانه
- حفاظت در مقابل ویروس
- طرح پیوستگی عملیات (Business Continuity Plan)

لازم است فرآیندهای خاص مختص یا متعلق به سازمان پس از فهرست سازی با لحاظ کردن کنترل‌های مضاعف امن سازی شود. به علاوه لازم است امن سازی و ممیزی امنیت اطلاعات این فرآیندها به نحوی انجام شود که خود باعث نقض کلی امنیت فرآیند نگردد. مبانی و فهرست کلیه سیاست‌هایی که در ((وزارت/ سازمان/ اداره کل/ شرکت/...)) به کار گرفته خواهد شد به شرح ضمیمه این سند خواهد بود.

بازنگری

این سند بر اساس دستورالعمل "بازنگری سند سیاست‌گذاری امنیت اطلاعات (دستورالعمل ۱-۱-۲)" مورد بازنگری قرار خواهد گرفت و در صورت نیاز در جهت بهبود وضعیت عملیات و یا خدمات‌رسانی به مشتریان یا ارباب رجوع ((وزارت/ سازمان/ اداره کل/ شرکت/...)) تغییر خواهد یافت.

ضمیمه یک: مبانی سند سیاست‌گذاری امنیت اطلاعات

هدف

هدف از تدوین این سند مدون سازی و بیان برنامه کلان (((وزارت/ سازمان/ اداره کل/ شرکت))) در زمینه حفظ امنیت اطلاعات در کلیه مراحل جمع‌آوری، پردازش، تولید، ذخیره‌سازی، توزیع، ارسال و بهره‌برداری از داده‌ها و اطلاعات موجود در کلیه تجهیزات و نرم‌افزارهای پردازش اطلاعات می‌باشد.

حفاظت از داده‌ها، اطلاعات، تجهیزات و نرم‌افزارهای پردازشی و همچنین کانال‌های ارتباطی و انتقال اطلاعات که به عنوان دارایی‌های مهم سازمان تلقی می‌شوند باید به نحوی باشد که:

- الف) از محرمانگی اطلاعات حفاظت به عمل آید، یعنی اطلاعات فقط در اختیار افراد یا مراجعی قرار گیرد که مجاز به دریافت آن هستند.
- ب) از صحت و جامعیت اطلاعات جمع‌آوری، پردازش، ذخیره یا توزیع شده اطمینان حاصل شود، یعنی اولاً صحت داده‌ها و اطلاعات تضمین شود و ثانیاً هنگام مطالعه، تصمیم‌سازی یا تصمیم‌گیری در خصوص هر موضوع کلیه اطلاعات مربوط به آن موضوع به طور کامل و جامع در اختیار مرجع مربوط قرار گیرد.
- ج) دسترسی پذیری داده‌ها، اطلاعات یا تجهیزات و نرم‌افزارهای پردازش یا ذخیره اطلاعات و کانال‌های توزیع یا ارسال تضمین گردد، یعنی اطلاعات در زمان مورد نیاز در اختیار مراجع مربوط قرار گیرد.

مسئولیت

مسئولیت اجرای این سند به عهده (((بالاترین مقام اجرایی نهاد بهره‌بردار))) می‌باشد و کمیته امنیت اطلاعات که به موجب این سند و بر اساس دستورالعمل ۱-۲-۲ تشکیل خواهد شد (((بالاترین مقام اجرایی))) را در این خصوص یاری خواهد نمود. (((بالاترین مقام اجرایی))) می‌تواند بخشی یا کلیه مسئولیت و اختیارات لازم جهت اجرای مفاد این سند را به یک یا چند نفر از اعضای کمیته امنیت اطلاعات واگذار نماید. در این صورت لازم است مسئولیت هر یک از افراد در زمینه اجرای هر بخش از این سند به صورت مکتوب و مشخص به وی ابلاغ شود.

الزامات

- ۱- لازم است خط و مشی نظام مدیریت امنیت اطلاعات (بر اساس دستورالعمل ۱-۱-۲) توسط ((بالاترین مقام اجرایی سازمان)) تصویب شده و به اطلاع کلیه آحاد ((وزارت/ سازمان/ اداره کل/ شرکت ...)) و طرف‌های اداری یا تجاری آن برسد.
- لازم است بودجه و منابع مالی لازم برای انجام فعالیت‌های موضوع این سند پیش بینی شده و برنامه زمانبندی تخصیص آن تدوین گردد.
- لازم است جهت اجرای مفاد این سند نهادی اجرایی تشکیل شود. ساختار، جایگاه و وظایف این نهاد در دستورالعمل ۲-۱-۲ تشریح شده است.
- ۲- فرآیند و مراحل اجرایی برپاسازی نظام مدیریت امنیت اطلاعات باید به موجب این سند مستند شده و بر اساس سند راهبردی نظام جامع فناوری اطلاعات و سند راهبردی امنیت فضای تبادل اطلاعات (افتا) به اجرا گذاشته شود.

فرآیند اجرای سند سیاست‌گذاری امنیت اطلاعات

- جهت برپاسازی نظام مدیریت امنیت اطلاعات و استمرار فعالیت‌های آن لازم است مراحل اجرایی زیر به ترتیب به مورد اجرا گذاشته شود:
- الف- تدوین، تصویب و اعلان خط و مشی امنیت اطلاعات سازمان (بر اساس دستورالعمل ۱-۱-۲)
 - ب- تشکیل کمیته امنیت اطلاعات (بر اساس دستورالعمل ۲-۱-۲)
 - ج- تعیین قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات (بر اساس دستورالعمل ۳-۱-۱)
 - د- تشکیل کارگروه امنیت اطلاعات (بر اساس دستورالعمل ۲-۱-۲)
 - ه- تهیه گزارش شناخت وضعیت سازمان از دیدگاه رعایت امنیت اطلاعات (بر اساس دستورالعمل ۱-۳-۳)
 - و- شناسایی، تحلیل و مدیریت ریسک‌های امنیت اطلاعات سازمان (بر اساس دستورالعمل ۳-۳-۳ و ۳-۳-۳)
 - ز- تدوین بیانیه کاربرپذیری اختصاصی سازمان (بر اساس دستورالعمل ۴-۳-۳)

- ح- تصمیم‌گیری در مورد ساختار نهاد اجرایی متصدی امنیت اطلاعات (بر اساس دستورالعمل ۲-۱-۲)
 - ط- تشکیل گروه CERT^۳ (بر اساس دستورالعمل ۲-۱-۲)
 - ی- تدوین طرح احیای سیستم و تشکیل گروه مربوط (بر اساس دستورالعمل‌های ۲-۱-۲ و ۶-۱-۲ و ۷-۱-۲)
 - ک- انجام عملیات تصحیحی و ترمیم رخنه‌ها و آسیب‌پذیری‌های امنیتی (بر اساس ضمیمه سیاست‌گذاری همین سند- ضمیمه یک)
 - ل- به هنگام سازی چرخه فعالیت و بازنگری روش‌های انجام کار
 - م- اقدام جهت کسب گواهینامه‌های معتبر در زمینه مدیریت امنیت اطلاعات یا حفاظت از داده‌ها و سیستم‌های پردازشی (بر اساس دستورالعمل ۸-۱-۲)
- بندهای الف تا ح فوق مربوط به مرحله برپایی و بندهای ط تا م مربوط به استمرار فعالیت‌های نظام مدیریت امنیت اطلاعات می‌باشد.

توضیح: کارگروه امنیت اطلاعات به عنوان بازوی اجرایی کمیته به فعالیت خواهد پرداخت و مأموریت آن پس از تدوین بیانیه کاربردپذیری اختصاصی سازمان (بند ز فوق) پایان می‌پذیرد. در صورت وقوع هر یک از شرایط زیر کمیته می‌تواند کارگروه دیگری را تشکیل داده و انجام فعالیت‌های اجرایی مربوط به خود را به آن واگذار نماید:

- تغییر عمده در روش‌های اجرایی فعالیت سازمان یا مأموریت آن
- تغییر عمده در روش‌های جمع‌آوری، پردازش یا توزیع اطلاعات و یا تغییر تکنولوژی به نحوی که به نظر برسد مطالعات تحلیل ریسک انجام شده قبلی فاقد اعتبار شده‌اند.
- ۱- دریافت ضربه شدید در حوزه امنیت اطلاعات و یا وقوع حمله‌هایی که منجر به فروپاشی سیستم یا قطع کانال‌های ارتباطی سازمان گردد.
- تحت شرایط فوق و یا بنا به تشخیص کمیته امنیت اطلاعات لازم است کارگروه جدیدی تشکیل گردد و با توجه به حوادث وقوع یافته بندهای ه تا ز فرآیند فوق را مجدداً به مورد اجرا گذارد.

³ - CERT: Computer Emergency Response Team

تجهیزات، نرم‌افزارها و ابزار مورد نیاز

تجهیزات، نرم‌افزارها و ابزار مورد نیاز جهت اجرای این سند به دو دسته نیازهای اضطراری و نیازهای برنامه‌ای تقسیم می‌شود.

لازم است تجهیزات، نرم‌افزارها و ابزاری که توسط کمیته امنیت اطلاعات اضطراری تشخیص داده می‌شوند، سریعاً تهیه شده و در اختیار متقاضی گذاشته شود. مسئولیت تهیه این نوع نیازها به عهده کمیته امنیت اطلاعات بوده و لازم است تحت شرایط مندرج در دستورالعمل "صدور مجوز استفاده از تجهیزات پردازش اطلاعات" (دستورالعمل ۱-۲-۴) به کار گرفته شوند.

مرجع

این ضمیمه تحت شماره مرجع □-□/۱-۱-۱/□-□ ثبت شده و بر اساس دستورالعمل ۱-۱ (راهنمای سیاست گذاری امنیت اطلاعات) تدوین گشته است.

سایر مراجع و دستورالعمل‌های مرتبط با این سند عبارت‌اند از:

سند راهبردی نظام جامع فناوری اطلاعات

سند راهبردی امنیت فضای تبادل اطلاعات کشور (افتا)

دستورالعمل ۱-۱-۲

دستورالعمل ۲-۱-۲

دستورالعمل ۳-۱-۱

دستورالعمل ۱-۳-۳

دستورالعمل ۲-۳-۳

دستورالعمل ۳-۳-۳

دستورالعمل ۴-۳-۳

دستورالعمل ۳-۱-۲

دستورالعمل ۶-۱-۲

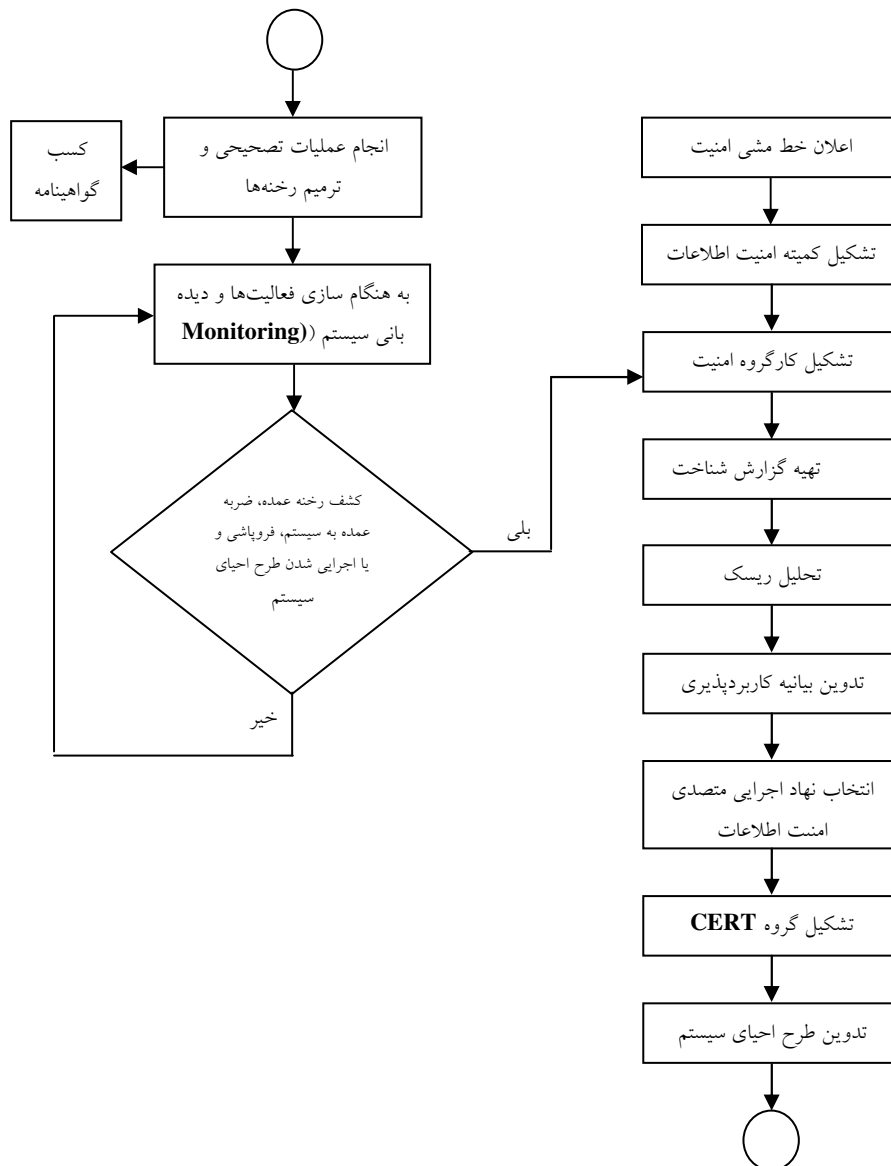
دستورالعمل ۷-۱-۲

دستورالعمل ۸-۱-۲

دستورالعمل ۴-۱-۲

روند نما

روندنمای ایجاد و پیاده‌سازی نظام مدیریت امنیت اطلاعات در نمودار زیر نمایش داده شده است:



ضمیمه دو: فهرست فرآیندهای موضوع سیاست‌گذاری امنیت اطلاعات

این فهرست شامل کلیه فرآیندهایی است که لازم است در اجرای آن‌ها به حفظ امنیت اطلاعات و دارایی‌های اطلاعاتی توجه شود. تصمیم در خصوص نیاز به تدوین سند امنیتی مکتوب در خصوص هر فرآیند به عهده کمیته امنیت اطلاعات می‌باشد.

در صورت نیاز به تدوین سند امنیتی در هر حوزه لازم است مسئولیت نوشتن سند به واحدی که مستقیماً انجام آن فرآیند را به عهده دارد واگذار شود. بازنگری و تأیید سند به عهده مدیر واحد یا مرجع جانشین واحد امنیت اطلاعات خواهد بود. سند مذکور باید طبق قالب معرفی شده در دستورالعمل "تولید و کنترل اسناد" تدوین شود.

در صورت عدم وجود منع حفاظتی پیشنهاد می‌شود که از مشاوره سایر نهادهای تخصصی در حوزه امنیت اطلاعات و در قالب برون سپاری پروژه‌های تدوین سند استفاده شود.

توضیح: از بین فرآیندهای زیر مجموعه سندهای امنیتی مرتبط با فرآیندهای سیاست‌گذاری/امنیت اطلاعات، مدیریت دارایی‌های اطلاعاتی و تحلیل ریسک و کنترل دسترسی به صورت عام تدوین و به همراه این دستورالعمل ارسال شده است. سایر دستورالعمل‌ها نیز متعاقباً ارسال خواهد شد.

در صورتی که ضروری باشد می‌توان متن دستورالعمل‌ها را تغییر داده و با الزامات محیط عملیاتی سازمان منطبق نمود. در این صورت لازم است مفاد "دستورالعمل تولید و کنترل اسناد" به طور کامل رعایت گردد و کلیه تغییرات علاوه بر تأیید توسط کمیته امنیت اطلاعات و ثبت به اطلاع کلیه نهادهای ذیربط رسانده شود. به علاوه در صورت وجود و جاری بودن دستورالعمل‌های امنیتی در سازمان باید کفایت آن‌ها با توجه به الزامات سامانه مدیریت امنیت اطلاعات مورد بررسی قرار گرفته و در صورت تأیید بر اساس "دستورالعمل تولید و کنترل اسناد" بازآرایی و تنظیم شوند. فهرست فرآیندها به شرح زیر است:

الف- حفاظت از سخت‌افزار، دستگاه‌های جانبی و سایر تجهیزات	
الف-۱- خرید و نصب سخت‌افزار	
الف-۱-۱- تعریف نیازهای امنیتی در خرید سخت‌افزار	
الف-۱-۲- تعریف جزئیات توانایی‌های مورد نیاز در خرید سخت‌افزار	
الف-۱-۳- نصب سخت‌افزارهای جدید	
الف-۱-۴- آزمایش سیستم و تجهیزات جدید و صدور مجوز استفاده	

الف-۲- کابل کشی، UPS، چاپگرها و مودم‌ها (بی سیم و کابلی)
الف-۲-۱- تدارک انرژی مورد نیاز برای تجهیزات اصلی
الف-۲-۲- مدیریت و نگهداری ژنراتورهای برق اضطراری
الف-۲-۳- استفاده از دستگاه فاکس / فاکس مودم
الف-۲-۴- استفاده از مودم، DSL / ISDN / بی سیم یا کابلی
الف-۲-۵- استفاده از چاپگر به صورت متمرکز، تحت شبکه و یا مجزا
الف-۲-۶- نصب و نگهداری کابل‌های شبکه
الف-۳- مواد مصرفی
الف-۳-۱- کنترل مواد مصرفی
الف-۳-۲- استفاده از تجهیزات قابل حمل ذخیره اطلاعات شامل دیسک و CD
الف-۴- کار در خارج از شرکت یا ارجاع کار به خارج از سازمان
الف-۴-۱- پیمانکاری یا ارجاع کار به خارج از شرکت
الف-۴-۲- صدور مجوز استفاده از نوت بوک یا کامپیوترهای قابل حمل برای اعضاء شرکت
الف-۴-۳- استفاده از نوت بوک یا کامپیوترهای قابل حمل
الف-۴-۴- کار در خانه یا سایر روش‌های کار خارج از شرکت (کار از راه دور)
الف-۴-۵- انتقال سخت‌افزار از یک مکان به مکان دیگر
الف-۴-۶- استفاده از تلفن همراه
الف-۴-۷- استفاده از کافی نت‌ها یا اتاق‌های کامپیوتر عمومی
الف- - نگهداری به صورت امن
الف-۵-۱- استفاده از قفسه‌های قابل قفل شدن
الف-۵-۲- استفاده از کابینت‌های قفل دار
الف-۵-۳- استفاده از کابینت‌های مقاوم در مقابل آتش
الف-۵-۴- استفاده ایمن
الف-۶- مستندات سخت‌افزار
الف-۶-۱- مدیریت و استفاده از مستندات سخت‌افزار
الف-۶-۲- ثبت و کنترل موجودی سخت‌افزار
الف-۷- سایر موارد مرتبط با سخت‌افزار
الف-۷-۱- خارج از رده کردن تجهیزات
الف-۷-۲- ثبت و گزارش خرابی سخت‌افزار
الف-۷-۳- بیمه سخت‌افزار
الف-۷-۴- بیمه نوت بوک و کامپیوترهای قابل حمل (استفاده در داخل یا خارج کشور)

الف-۷-۵- روش مانیتور پاک
الف-۷-۶- آغاز کار و پایان کار با کامپیوتر
الف-۷-۷- کار با منشی تلفنی الکترونیکی / پست صوتی
الف-۷-۸- انتقال تجهیزات
الف-۷-۹- نگهداری سخت‌افزار (پشتیبانی در محل یا خارج از محل)
الف-۷-۱۰- استفاده از سیستم‌های شماره گیری سریع تلفن
الف-۷-۱۱- نظافت صفحه کلید و صفحه نمایشگر
الف-۷-۱۲- صدمه به تجهیزات
الف-۷-۱۳- استفاده از نوت بوک یا سایر تجهیزات پردازشی قابل حمل در خارج کشور
ب- کنترل دسترسی به اطلاعات و سیستم‌ها
ب-۱- کنترل دسترسی به اطلاعات و سیستم‌ها
ب-۱-۱- مدیریت رویه‌های کنترل دسترسی
ب-۲-۱- مدیریت دسترسی کاربر
ب-۳-۱- امن کردن ایستگاه‌های کاری بدون مراقبت
ب-۴-۱- مدیریت مکانیزم‌های کنترل دسترسی شبکه
ب-۵-۱- کنترل دسترسی به نرم‌افزارهای سیستم عامل
ب-۶-۱- مدیریت کلمه عبور
ب-۷-۱- محافظت در مقابل دسترسی‌های فیزیکی غیر مجاز
ب-۸-۱- محدود ساختن حوزه دسترسی
ب-۹-۱- دیده بانی دسترسی به سیستم و استفاده از آن
ب-۱۰-۱- اعطای حقوق دسترسی به فایل‌ها و اسناد
ب-۱۱-۱- مدیریت دسترسی سیستم‌های حساس (پرخطر)
ب-۱۲-۱- کنترل دسترسی از راه دور
ج- پردازش اطلاعات و مستندات
ج-۱- شبکه‌ها (بی سیم و کابلی)
ج-۱-۱- پیکربندی شبکه‌ها (بی سیم و کابلی)
ج-۲-۱- مدیریت شبکه (بی سیم و کابلی)
ج-۳-۱- دسترسی به شبکه از راه دور (بی سیم و کابلی)
ج-۴-۱- دفاع از شبکه (بی سیم و کابلی)
ج-۲- راهبری و مدیریت سیستم
ج-۱-۲- گزینش مدیران سیستم

ج-۲-۲- مدیریت سیستم‌ها ج-۲-۳- نظارت بر توزیع اطلاعات ج-۲-۴- صدور مجوز دسترسی شخص ثالث ج-۲-۵- مدیریت کلیدهای رمزنگاری ج-۲-۶- مدیریت سیستم‌های عملیاتی و اجرایی ج-۲-۷- مدیریت مستندات سیستم ج-۲-۸- دیده بانی فهرست خطا (Error log) ج-۲-۹- برنامه‌ریزی عملیات سیستم ج-۲-۱۰- تغییرات برنامه‌ریزی شده بر روی عملیات عادی سیستم ج-۲-۱۱- دیده بانی فهرست‌های ممیزی اجرایی (Operational Audit log Monitoring) ج-۲-۱۲- همزمان سازی (Synchronization) ج-۲-۱۳- پاسخ به خطاهای سیستم (System Faults) ج-۲-۱۴- مدیریت و بهره‌برداری از گزارش عملیات پردازشی / اجرایی ج-۲-۱۵- مدیریت تجهیزات
ج-۳- نام‌های الکترونیکی و صفحات وب ج-۳-۱- پیاده‌سازی فایل‌ها و اطلاعات از اینترنت (Downloading) ج-۳-۲- به‌کارگیری و پذیرش امضاهای الکترونیک ج-۳-۳- ارسال نامه‌های الکترونیکی (E-Mail) ج-۳-۴- دریافت نامه الکترونیکی ج-۳-۵- نگهداری و یا حذف نامه‌های الکترونیکی ج-۳-۶- پیکربندی دسترسی اینترنت ج-۳-۷- پیکربندی دسترسی اکس‌ترانت ج-۳-۸- پیکربندی دسترسی اینترنت ج-۳-۹- ایجاد وب سایت / پورتال سازمانی ج-۳-۱۰- دریافت اطلاعات گمراه کننده از طریق نامه الکترونیکی ج-۳-۱۱- ارسال مجدد نامه الکترونیکی ج-۳-۱۲- استفاده از اینترنت در جهت اهداف شرکت ج-۳-۱۳- بیان اطلاعات به هنگام دریافت یا ثبت سفارش کالا از طریق اینترنت ج-۳-۱۴- مرور گرهای وب و موارد خارج از کنترل ج-۳-۱۵- کاربرد موتورهای جست‌وجوگر اینترنت ج-۳-۱۶- نگهداری از وب سایت / پورتال سازمانی

ج-۳-۱۷- فیلتر نمودن مطالب نامناسب اینترنت
ج-۳-۱۸- حصول اطمینان از اصالت سایت / فایل
ج-۴-۱- تلفن و فاکس
ج-۴-۱- برقراری ارتباط به صورت کنفرانس
ج-۴-۲- استفاده از تجهیزات ویدئو کنفرانس
ج-۴-۳- ضبط مکالمات تلفنی یا کنفرانس ها
ج-۴-۴- دریافت اطلاعات با آدرس اشتباه از طریق فاکس یا پست الکترونیک
ج-۴-۵- بیان اطلاعات هنگام سفارش کالا از طریق تلفن
ج-۴-۶- دستورالعمل استفاده از تلفن / Call Center
ج-۴-۷- درخواست اطلاعات از طریق تلفن Call Center
ج-۴-۸- دریافت فاکس‌های ناخواسته
ج-۵-۱- مدیریت داده‌ها
ج-۵-۱- انتقال و تبادل داده‌ها
ج-۵-۲- مدیریت ذخیره اطلاعات / مراکز داده (Data Center)
ج-۵-۳- مدیریت بانک‌های اطلاعاتی
ج-۵-۴- مجوز تغییرات اضطراری اطلاعات
ج-۵-۵- دریافت اطلاعات به وسیله دیسک
ج-۵-۶- ایجاد و پیکربندی Folder / دایرکتوری جدید
ج-۵-۷- اصلاح ساختار دایرکتوری ها
ج-۵-۸- بایگانی اسناد
ج-۵-۹- سیاست‌های نگهداری اطلاعات
ج-۵-۱۰- صفحات گسترده و ابزارهای گزارش گیری سریع
ج-۵-۱۱- پیکربندی بانک‌های اطلاعاتی جدید
ج-۵-۱۲- پیوند اطلاعاتی بین فایل‌ها و اسناد
ج-۵-۱۳- به هنگام سازی گزارش‌های پیش نویس
ج-۵-۱۴- حذف گزارش‌های پیش نویس
ج-۵-۱۵- استفاده از سیستم‌های کنترل نسخ (Version Control)
ج-۵-۱۶- اشتراک داده‌ها در سیستم‌های مدیریت پروژه
ج-۵-۱۷- به هنگام سازی اطلاعات مشتری / ارباب رجوع
ج-۵-۱۸- استفاده از نام‌های بامعنی برای فایل‌ها
ج-۵-۱۹- استفاده از سرصفحه و پاصفحه

ج-۵-۲۰- استفاده و حذف فایل‌های موقت
ج-۵-۲۱- استفاده از فایل‌های اطلاعات مشتری / ارباب رجوع و سایر فایل‌ها
ج-۵-۲۲- ذخیره اطلاعات و داده‌ها به وسیله افراد مختلف
ج-۶- نسخه پشتیبان، بایگانی و بازیابی
ج-۶-۱- راه اندازی مجدد و بازیابی سیستم ((System/Data Recovery
ج-۶-۲- تهیه نسخه پشتیبان از داده‌ها روی کامپیوترهای قابل حمل
ج-۶-۳- مدیریت فرآیندهای پشتیبان‌گیری و بازیابی
ج-۶-۴- ثبت و نگهداری اطلاعات
ج-۶-۵- نگهداری و بایگانی فایل‌های الکترونیکی
ج-۶-۶- بازیابی و بازیافت اطلاعات
ج-۷- نگهداری اسناد مرتبط با فرآیندهای پردازشی
ج-۷-۱- مدیریت نسخه‌های چاپی و کپی اسناد
ج-۷-۲- کپی برداری از اطلاعات محرمانه
ج-۷-۳- بایگانی اسناد و اطلاعات
ج-۷-۴- امضای اسناد و مدارک
ج-۷-۵- بررسی صحت اسناد
ج-۷-۶- تأیید و تصویب اسناد
ج-۷-۷- تأیید امضاء
ج-۷-۸- پذیرش بسته‌های پستی ناخواسته
ج-۷-۹- سبک نگارش و ارائه گزارشات
ج-۷-۱۰- انتقال اسناد مهم و حساس
ج-۷-۱۱- انهدام اسناد غیر قابل استفاده
ج-۷-۱۲- مدیریت اسناد
ج-۸- امن‌سازی اطلاعات
ج-۸-۱- استفاده از تکنیک‌های رمزگذاری
ج-۸-۲- اشتراک گذاری اطلاعات
ج-۸-۳- ارسال اطلاعات برای اشخاص ثالث
ج-۸-۴- نگهداری اطلاعات محرمانه مشتری / ارباب رجوع
ج-۸-۵- نگهداری اطلاعات کارت اعتباری مشتری / ارباب رجوع
ج-۸-۶- خطرهای مرتبط با حوادث مثل آتش سوزی، سیل، زلزله، برای اطلاعات
ج-۸-۷- ارسال گزارش

ج-۸-۸- توزیع اطلاعات حساس از طریق تجهیزات رایانه‌ای یا کانال‌های ارتباطی ج-۸-۹- حذف داده‌های متعلق به دیگران ج-۸-۱۰- حفاظت از اسناد با استفاده از کلمه عبور ج-۸-۱۱- چاپ اسناد طبقه‌بندی شده
ج-۹- سایر روش‌های مرتبط با نگهداری و پردازش اطلاعات ج-۹-۱- استفاده از کنترل دوگانه ورود اطلاعات ج-۹-۲- بارگذاری محافظه‌های صفحه نمایشگر ((Screen Saver ج-۹-۳- استفاده از پیمانکاران در انهدام یا دور ریزی تجهیزات پردازشی ج-۹-۴- استفاده از دستگاه فتوکپی برای استفاده شخصی ج-۹-۵- مصاحبه با رسانه‌های عمومی ج-۹-۶- گفتگو با مشتری/ ارباب رجوع ج-۹-۷- نیاز به کنترل دوگانه و تفکیک وظایف ج-۹-۸- استفاده از سیاست میز پاک ج-۹-۹- بی توجهی در خصوص اطلاعات مرتبط با فرآیندهای پردازشی هنگام تماس با اشخاص ثالث ج-۹-۱۰- بررسی و کنترل صحت و سقم اطلاعات ج-۹-۱۱- سفرهای کاری و تجاری ج-۹-۱۲- کنترل محدودیت‌های اعتباری مشتری هنگام تبادل‌های مالی الکترونیک
د- خرید و استفاده از نرم‌افزارهای کاربردی
د-۱- خرید و نصب نرم‌افزار د-۱-۱- تعیین نیازهای نرم‌افزاری کاربران د-۱-۲- انتخاب بسته‌های نرم‌افزار تجاری (Application Software) د-۱-۳- انتخاب بسته نرم‌افزار دفتری ((Office Software د-۱-۴- استفاده از نرم‌افزارهای دارای مجوز و گواهی ((License د-۱-۵- اجرای نرم‌افزار جدید/ به هنگام شده
د-۲- به هنگام سازی و نگهداری نرم‌افزارها د-۲-۱- استفاده از وصله‌ها ((Patchها برای ترمیم اشکال‌های نرم‌افزار د-۲-۲- به هنگام سازی نرم‌افزارها د-۲-۳- پاسخ به پیشنهادات فروشندگان در ارتباط با به هنگام سازی نرم‌افزارها د-۲-۴- ارتباط بین نرم‌افزارهای کاربردی د-۲-۵- پشتیبانی نرم‌افزارهای کاربردی د-۲-۶- به هنگام سازی سیستم عامل

د-۲-۷- پشتیبانی سیستم‌های عامل
د-۲-۸- ثبت و گزارش خطاهای نرم‌افزاری
د-۳- مطالب دیگری درمورد نرم‌افزارها
د-۳-۱- انهدام (خارج از رده کردن) نرم‌افزارها
ه- توسعه و نگهداری نرم‌افزارهای داخلی (نوشته شده در سازمان)
ه-۱- مکانیزم‌های کنترلی کدهای نرم‌افزاری
ه-۱-۱- مدیریت برنامه‌های عملیاتی کتابخانه‌های ((Library
ه-۱-۲- مدیریت دسترسی به متن برنامه‌های کتابخانه ای
ه-۱-۳- کنترل کد نرم‌افزار در حین توسعه آن
ه-۱-۴- مکانیزم‌های کنترل لیست گیری از برنامه
ه-۱-۵- مکانیزم‌های کنترل متن برنامه‌های کتابخانه‌های
ه-۱-۶- مکانیزم‌های کنترل نسخه‌های قدیمی برنامه‌ها
ه-۲- توسعه نرم‌افزارها
ه-۲-۱- توسعه نرم‌افزارها
ه-۲-۲- انجام اصلاحات اضطراری در نرم‌افزارها
ه-۲-۳- تعیین مالکیت / تصدی سیستم‌های بهبود یافته
ه-۲-۴- حمایت از توسعه سیستم جدید
ه-۲-۵- مدیریت رویه‌های کنترل تغییرات
ه-۲-۶- جداسازی سیستم عملیاتی از سیستم تحت توسعه
ه-۳- آزمایش و آموزش ICT / امنیت ICT
ه-۳-۱- کنترل محیط‌های آزمایشی
ه-۳-۲- استفاده از داده‌های موجود در آزمایش
ه-۳-۳- آزمایش نرم‌افزار قبل از انتقال آن به محیط واقعی
ه-۳-۴- برنامه‌ریزی ظرفیت و آزمایش سیستم‌های جدید
ه-۳-۵- اجرای موازی (Parallel Running)
ه-۳-۶- آموزش سیستم‌های جدید
ه-۴- مستند سازی
ه-۴-۱- مستند سازی‌های سیستم‌های جدید و ارتقاء یافته
ه-۵- سایر توسعه‌های نرم‌افزاری
ه-۵-۱- استفاده از بسته‌های نرم‌افزارهای آماده

و- مبارزه با جرائم کامپیوتری
و-۱- مبارزه با جرائم کامپیوتری
و-۱-۱- دفاع در برابر حمله‌های عمدی و بزهکارانه کامپیوتری
و-۱-۲- به حداقل رسانیدن اثرات شدید حمله‌های کامپیوتری
و-۱-۳- جمع‌آوری مدارک برای پیگرد قانونی بزهکاران کامپیوتری
و-۱-۴- دفاع در برابر حمله‌های عمدی داخلی
و-۱-۵- دفاع در برابر حمله‌های بزهکارانه رایان‌های تصادفی
و-۱-۶- حفاظت در برابر رد سرویس (Denial of Service)
و-۱-۷- حفاظت در برابر هکرها و خراب کاری‌های فنی
و-۱-۸- بررسی اختراهای فریبنده وجود ویروس
و-۱-۹- دفاع در برابر حملات ویروسی
و-۱-۱۰- پاسخگویی به رویداد حوادث ناشی از ویروس
و-۱-۱۱- نصب نرم‌افزارهای پوششگر ویروس‌ها
ز- انطباق با الزامات و سیاست‌گذاری‌های قانونی
ز-۱- انطباق با وظایف قانونی
ز-۱-۱- آگاهی از وظایف قانونی
ز-۱-۲- انطباق با قوانین حفاظت حریم شخصی افراد، حقوق پدیدآورندگان نرم‌افزار، آزادی اطلاعات و مشابه آن
ز-۱-۳- انطباق با قوانین عمومی کپی رایت (حقوق مالکیت معنوی)
ز-۱-۴- انطباق با قوانین کپی رایت پایگاه داده‌ها
ز-۱-۵- انطباق با حقوق کپی رایت و قانون حق استفاده از نرم‌افزار
ز-۱-۶- حفاظت‌های قانونی علیه سوء استفاده از کامپیوترها
ز-۲- انطباق با سیاست‌ها
ز-۲-۱- انطباق با سیاست‌های امنیت اطلاعات بر اساس سند‌های راهبردی در حوزه امنیت اطلاعات
ز-۲-۲- انطباق با راهبردهای آمادگی برای مقابله با شرایط بحرانی بر اساس سند‌های راهبردی در حوزه پدافند غیرعامل
ز-۳- اجتناب از دعوی قضایی
ز-۳-۱- مدیریت ذخیره‌سازی رسانه‌ها و نگهداری سوابق (رکوردهای اطلاعاتی)
ز-۳-۲- حفاظت در برابر توهین و افترا
ز-۳-۳- استفاده از اطلاعات اینترنتی دارای امتیاز انحصاری چاپ و نشر
ز-۳-۴- ارسال الکترونیکی اطلاعات با امتیاز انحصاری چاپ و نشر
ز-۳-۵- استفاده مستقیم از متن گزارشات، کتاب‌ها و اسناد

ز-۴- موارد قانونی دیگر
ز-۴-۱- جمع‌آوری شواهد و مدارک مربوط به رویدادها (امنیت اطلاعات)
ز-۴-۲- تجدید جواز نام قلمرو (Domain Name) / وب سایت
ز-۴-۳- بیمه فعالیت‌های پردازی و پیامدهای ناشی از اختلال در آن
ح- برنامه‌ریزی پیوستگی عملیات
ح-۱- مدیریت پیوستگی عملیات
ح-۱-۱- ایجاد طرح پیوستگی عملیات
ح-۱-۲- ارزیابی ریسک امنیتی طرح پیوستگی عملیات (BCP)
ح-۱-۳- ایجاد BCP
ح-۱-۴- آزمایش (مانور) BCP
ح-۱-۵- آموزش و آگاهی کارمندان در ارتباط با BCP
ح-۱-۶- نگهداری و به‌هنگام سازی BCP
ط- توجه به نیروی انسانی و رابطه آن با امنیت
ط-۱- مستندات قراردادی
ط-۱-۱- تعیین شرایط استخدام
ط-۱-۲- استخدام/ قرارداد با کارمند جدید
ط-۱-۳- عقد قرارداد با منابع خارج از شرکت/ ارائه کنندگان خدمات خارج از شرکت
ط-۱-۴- استفاده از پیمان نامه حفظ اسرار (در مورد کارمندان و اشخاص ثالث)
ط-۱-۵- سوء استفاده از سربرگ‌ها، یادداشت‌ها و فرم‌های چاپی
ط-۱-۶- قرض دادن کلیدهای عبور (فیزیکی/ الکترونیکی) محیط‌های امن به دیگران
ط-۱-۷- روابط مالی بین همکاران
ط-۱-۸- رعایت معیارهای امنیت اطلاعات
ط-۱-۹- رعایت حقوق مالکیت معنوی
ط-۱-۱۰- مسئولیت کارمندان در قبال حفاظت از محرمانگی داده‌ها
ط-۲- اطلاعات شخصی و محرمانه
ط-۲-۱- رعایت حریم خصوصی در محیط کار
ط-۲-۲- نگهداری اطلاعات محرمانه پرسنل
ط-۲-۳- دسترسی به سوابق کارمندان
ط-۲-۴- کنترل مجوزهای امنیتی کارمندان ستادی
ط-۲-۵- تسلیم اطلاعات پرسنلی به سایر کارمندان
ط-۲-۶- افشای اطلاعات حقوق و دستمزد پرسنل

ط-۳- مسئولیت افراد در حفظ امنیت اطلاعات
ط-۳-۱- به کارگیری اینترنت با استفاده از روش‌های پذیرفته شده
ط-۳-۲- محرمانه نگهداشتن کلمات عبور/ شماره‌های شناسایی اختصاصی (PIN)
ط-۳-۳- به اشتراک گذاردن اطلاعات شرکت با دیگر کارمندان
ط-۳-۴- استفاده شخصی از E-mail
ط-۳-۵- استفاده شخصی از سیستم‌های ارتباطی
ط-۳-۶- استفاده شخصی از تلفن‌های همراه شرکت
ط-۳-۷- استفاده از کارت‌های اعتباری شرکت
ط-۳-۸- امضای رسید کالا
ط-۳-۹- امضای صورت وضعیت کارهای انجام شده توسط اشخاص ثالث
ط-۳-۱۰- سفارش کالا و خدمات
ط-۳-۱۱- رسیدگی به مطالبات مالی و فاکتورها
ط-۳-۱۲- تأیید و صدور مجوز برای هزینه‌ها (پرداخت‌ها)
ط-۳-۱۳- پاسخ به پرس و جوهای تلفنی
ط-۳-۱۴- در میان گذاشتن اطلاعات محرمانه با اعضای خانواده
ط-۳-۱۵- شایعات و افشای اطلاعات محرمانه
ط-۳-۱۶- انتشار اطلاعات از طریق مکاتبات غیر ضروری اداری
ط-۳-۱۷- اجرای بازی‌های کامپیوتری بر روی کامپیوترهای اداری
ط-۳-۱۸- استفاده شخصی از کامپیوترهای اداری
ط-۴- مدیریت منابع انسانی
ط-۴-۱- رفتار با مستخدمان ناراضی
ط-۵- ترک استخدام
ط-۵-۱- استعفای کارمندان
ط-۵-۲- تکمیل رویه‌های مربوط به ترک استخدام کارمندان
ط-۵-۳- استخدام کارمندان سابق نزد رقبا
ط-۶- سایر موارد مرتبط با مدیریت منابع انسانی
ط-۶-۱- بهره‌گیری از مشاوران حرفه‌ای
ی- کنترل امنیت اطلاعات در تجارت الکترونیکی
ی-۱- پیامدهای تجارت الکترونیکی
ی-۱-۱- پیکربندی سیستم‌های تجارت الکترونیکی و وب سایت‌ها
ی-۱-۲- امنیت شبکه تجارت الکترونیکی

ی-۱-۳- پیکربندی شبکه تجارت الکترونیکی
ی-۱-۴- استفاده از خدمات سایر سرویس دهندگان برای تجارت الکترونیکی
ک- آموزش و اطلاع رسانی به افراد
ک-۱- اطلاع رسانی
ک-۱-۱- ارائه برنامه‌های اطلاع رسانی به کارمندان دائمی
ک-۱-۲- اطلاع رسانی به طرف‌های قرارداد
ک-۱-۳- ارائه برنامه‌های اطلاع رسانی برای کارمندان موقتی
ک-۱-۴- ارتباط مستقیم مدیریت عالی شرکت با کارمندان در مورد امنیت اطلاعات
ک-۱-۵- ارائه اطلاعات به هنگام و منظم به کارمندان
ک-۲- آموزش
ک-۲-۱- آموزش امنیت اطلاعات سیستم‌های جدید
ک-۲-۲- آموزش مدیران امنیت اطلاعات
ک-۲-۳- آموزش کارمندان بخش امنیت اطلاعات
ک-۲-۴- آموزش کارکنان فنی بخش امنیت اطلاعات
ک-۲-۵- آموزش کارمندان تازه کار بخش امنیت اطلاعات
ل- نکاتی در مورد مکان یابی، استقرار و فضای کار
ل-۱- امنیت محیط و پدافند غیرعامل
ل-۱-۱- تجهیز و آماده سازی سایت کامپیوترها
ل-۱-۲- حفاظت فیزیکی از محل کامپیوترها
ل-۱-۳- تضمین شرایط محیطی و عملیاتی مناسب بر اساس راهبردهای پدافند غیرعامل
ل-۱-۴- کنترل دسترسی فیزیکی نواحی امن
ل-۱-۵- مقابله با افراد ناشناس
ل-۲- ذخیره‌سازی اطلاعات
ل-۲-۱- مدیریت ذخیره‌سازی اطلاعات در محل سایت
ل-۲-۲- مدیریت ذخیره‌سازی اطلاعات در مکانی خارج از سایت اصلی
ل-۳- سایر نکات قابل توجه در امنیت محیطی
ل-۳-۱- استراق سمع الکترونیکی
ل-۳-۲- امنیت کابل کشی
ل-۳-۳- طرح مقابله با حوادث عمده

م- کشف حوادث و واکنش نسبت به آن	
م-۱- گزارش رویدادهای امنیت اطلاعات	
م-۱-۱- گزارش رویدادهای امنیت اطلاعات	
م-۱-۲- گزارش رویدادهای امنیت اطلاعات (IS) به مراجع قانونی	
م-۱-۳- گزارش نقص در امنیت اطلاعات	
م-۱-۴- اعلام نقض امنیت اطلاعات	
م-۱-۵- اخطار به منبع نقض امنیت اطلاعات	
م-۱-۶- هوشیاری در برابر کلاهبرداری و سوء استفاده	
م-۲- رسیدگی به حوادث امنیت اطلاعات	
م-۲-۱- رسیدگی به دلایل و پیامدهای نقض امنیت اطلاعات (IS)	
م-۲-۲- جمع‌آوری مدارک درباره نقض امنیت اطلاعات	
م-۲-۳- ثبت نقض امنیت اطلاعات	
م-۲-۴- پاسخ به رویدادهای امنیت اطلاعات	
م-۳- فعالیت‌های اصلاحی	
م-۳-۱- استفاده از تجربه‌های قبلی در مقابله با رخنه‌های امنیتی	
م-۴- سایر مواد مربوط به رویدادهای امنیت اطلاعات	
م-۴-۱- اطمینان از جامعیت روش رسیدگی به رویدادهای امنیت اطلاعات	
م-۴-۲- بررسی رویدادهای امنیتی ناشی از خرابی سیستم	
م-۴-۳- نقض محرمانگی	
م-۴-۴- ایجاد کنترل دو مرحله‌ای و تفکیک وظایف	
م-۴-۵- استفاده از چک لیست رویدادهای امنیت اطلاعات	
م-۴-۶- حفاظت در برابر استراق سمع الکترونیکی و فعالیت‌های جاسوسی	
م-۴-۷- نظارت بر محرمانگی رویدادهای امنیت اطلاعات	
م-۵- پاسخگویی به حوادث	
م-۵-۱- تشکیل گروه CERT	
ن- طبقه‌بندی داده‌ها و اطلاعات	
ن-۱- تعریف استانداردهای طبقه‌بندی	
ن-۱-۱- تعریف اطلاعات	
ن-۱-۲- الصاق برچسب به اطلاعات و دارایی‌های طبقه‌بندی شده	
ن-۱-۳- ذخیره‌سازی و نگهداری اطلاعات طبقه‌بندی شده	
ن-۱-۴- مجزا کردن (قرنطینه) اطلاعات خیلی محرمانه	

ن-۱-۵- طبقه‌بندی اطلاعات

ن-۱-۶- پذیرفتن مالکیت اطلاعات طبقه‌بندی شده

ن-۱-۷- مدیریت امنیت شبکه

(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
سیاست‌گذاری امنیتی	سیاست‌گذاری امنیت اطلاعات
بازنگری سند سیاست‌گذاری امنیت اطلاعات شماره دستورالعمل : ۲-۱-۱	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود

شماره مرجع: □-□ / □-۱-۲ / □ / □ تاریخ صدور:

صفحه از

تصویب شده در کمیته توسط:		
نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	دبیر*
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

[illegible]

هدف

هدف از تدوین این دستورالعمل اطمینان از بازنگری دوره ای یا اضطراری سند سیاست‌گذاری امنیت اطلاعات (دستورالعمل ۱-۱-۱) می‌باشد.

مسئولیت

مسئولیت اجرای این سند به عهده دبیر کمیته امنیت اطلاعات است.

الزامات

۱- سند سیاست‌گذاری امنیت اطلاعات باید پس از گذشت یکسال از تصویب اولیه آن مورد بازنگری قرار گیرد و مفاد آن با توجه به تجربیات حاصل از اجرای آن مجدداً تأیید یا تصحیح گردد.

بازنگری‌های بعدی در قالب دوره‌های سه ساله به عمل خواهد آمد. انتخاب زمان بازنگری باید به نحوی انجام شود که بتوان نتایج آخرین بازنگری‌های سند راهبردی امنیت فضای تبادل اطلاعات کشور که توسط معاونت فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات منتشر می‌شود را در آن اعمال نمود.

۲- کمیته امنیت اطلاعات می‌تواند در هر زمان و با توجه به وضعیت امنیت دارایی‌های اطلاعاتی سازمان درخواست بازنگری اضطراری سند سیاست‌گذاری امنیت اطلاعات سازمان را بنماید.

فرآیند بازنگری سند سیاست‌گذاری امنیت اطلاعات

با توجه به اینکه سند سیاست‌گذاری امنیت اطلاعات سازمان سند اصلی پشتیبان فعالیت‌های مرتبط با حفظ امنیت اطلاعات می‌باشد لازم است بازنگری آن طبق فرآیند زیر انجام پذیرد:

- الف- لازم است در بازنگری سند امنیت اطلاعات به گزارش‌های جمع‌آوری شده در مورد وقایع، حوادث، نقطه ضعف‌های امنیتی و تهدیدهای ناشی از تغییر تکنولوژی یا محیط عملیاتی سازمان که می‌توانند دارای تأثیرهای عمده در سطح امنیت اطلاعات باشند توجه شود و بر اساس آن‌ها تصحیحات لازم در متن سند سیاست‌گذاری امنیت اطلاعات اعمال شود.

- ب- در صورت تغییر در سند‌های مرجع اصلی مثل سند راهبردی نظام جامع فناوری اطلاعات و سند راهبردی افتا یا صدور سند‌های راهبردی کلان جدید توسط مراجع ذیصلاح، بازنگری در سند امنیت اطلاعات ضروری خواهد بود.
- ج- حتی الامکان قبل از تغییر در متن سند سیاست‌گذاری امنیت اطلاعات باید از طریق اصلاح دستورالعمل‌های امنیت اطلاعات، به نیازهای جدید ایجاد شده پاسخ گفت.
- د- در صورتی که اصلاح در سند سیاست‌گذاری امنیت اطلاعات یا دستورالعمل‌های امنیت اطلاعات مستلزم تغییر فرآیندهای اجرایی یا استفاده از فناوری‌های دیگری به جز آنچه که تاکنون استفاده می‌شده است باشد، ضروری است مجدداً تحلیل ریسک امنیتی انجام شود.
- ه- بازنگری سند سیاست‌گذاری امنیت اطلاعات باید در چهارچوب سند خط و مشی امنیت اطلاعات سازمان (دستورالعمل ۱-۲-۱) و سند تعیین قلمرو (دستورالعمل ۱-۱-۳) انجام پذیرد.

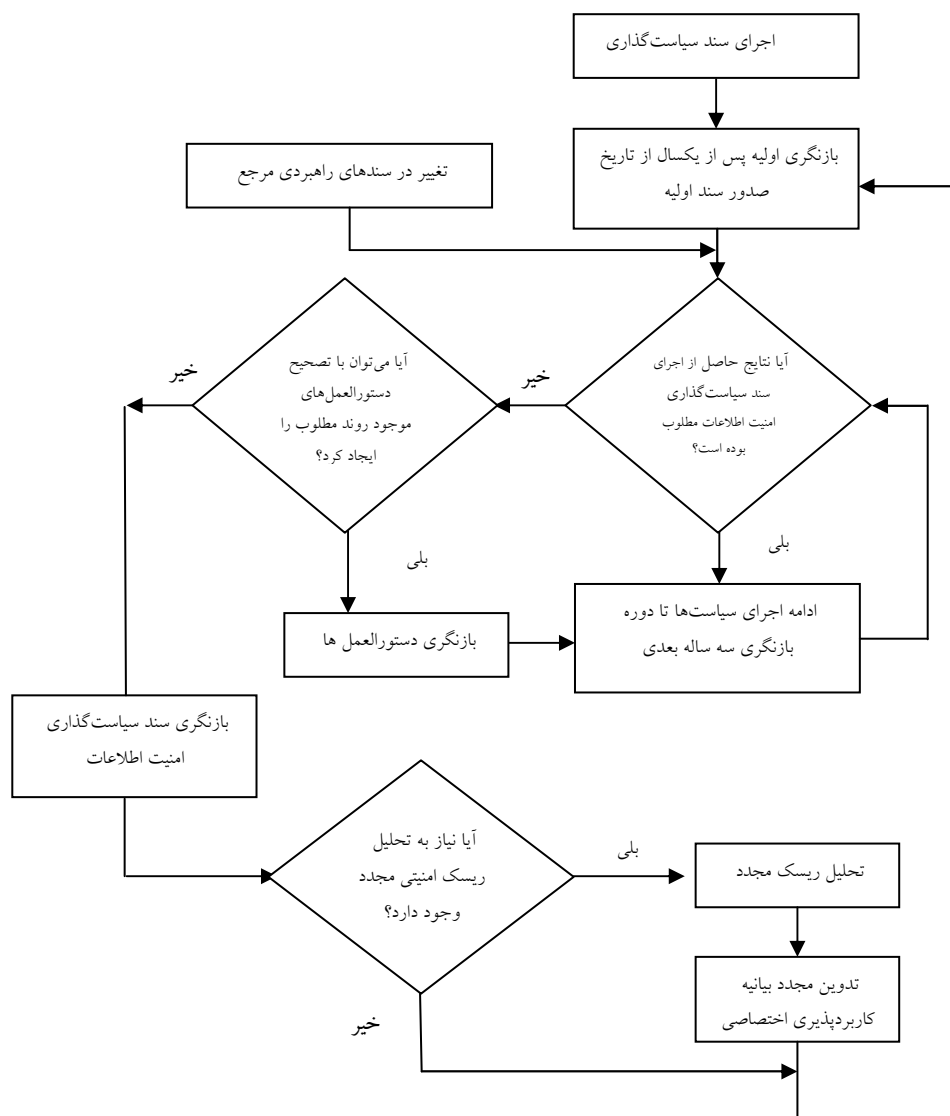
مرجع

این سند تحت شماره مرجع □-□/۱-۲-۱ ثبت شده است. سایر دستورالعمل‌های مرتبط با این دستورالعمل عبارت‌اند از:

- دستورالعمل ۱-۱-۱
- دستورالعمل ۱-۱-۳
- دستورالعمل ۱-۲-۱

روند نما

روند نمای بازنگری سند سیاست‌گذاری امنیت اطلاعات به شرح نمودار زیر است:



(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سیاست‌گذاری امنیتی	سیاست‌گذاری امنیت اطلاعات
سند تعیین قلمرو و پیاده‌سازی سامانه مدیریت امنیت اطلاعات شماره دستورالعمل : ۳-۱-۱	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود

شماره مرجع: □-□/□-۱-۳/□ □ تاریخ صدور:

صفحه از

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات:

تاریخ	شرح

هدف

هدف از اجرای این دستورالعمل تدوین سند تعیین قلمرو (Scope) پیاده‌سازی سامانه مدیریت امنیت اطلاعات می‌باشد.

مسئولیت

مسئولیت اجرای این سند به عهده (((بالاترین مقام اجرایی نهاد بهره‌بردار))) می‌باشد. همچنین سند تعیین قلمرو باید به امضای وی رسیده و به کمیته امنیت اطلاعات ابلاغ شود.

الزامات

کلیه فعالیت‌های مدیریت امنیت اطلاعات باید به نحوی برنامه ریزی و اجراء شود که به‌طور کامل محدوده تعیین شده در سند تعیین قلمرو (همین سند) را پوشش دهد. در سند تعیین قلمرو باید به‌صورت مشخص به مکان‌ها و خدماتی که در حوزه اجرای سیستم مدیریت امنیت اطلاعات قرار می‌گیرند اشاره شود.

فرآیند تدوین سند تعیین قلمرو

الف- فهرست مکان‌ها، خدمات، تجهیزات، نرم‌افزارها، بانک‌های اطلاعاتی و سایر دارایی‌های اطلاعاتی که باید در حوزه اجرای سامانه مدیریت امنیت اطلاعات قرار گیرند در اولین جلسه کمیته امنیت اطلاعات سازمان استخراج شده و برای تصویب به (((بالاترین مقام اجرایی نهاد بهره‌بردار))) پیشنهاد می‌شود.

ب: فعالیت‌های شناخت سیستم و تحلیل ریسک باید کلیه مکان‌ها و اجزای نامبرده شده در سند تعیین قلمرو را تحت پوشش قرار دهد.

ج: در سند تعیین قلمرو باید به ترتیب به اجزای زیر اشاره شود:

مکان‌های جغرافیایی نگهداری دارایی‌های اطلاعاتی

نام سیستم‌های سخت‌افزاری

- نام سیستم‌های عامل

- نام برنامه‌های کاربردی

- نام بانک‌های اطلاعاتی

- نام خدمات ارتباطی

- نوع اطلاعات در اختیار سازمان

- هر نوع دیگر از دارایی‌های اطلاعاتی که ضرورت حفاظت از آن‌ها از طریق سیستم مدیریت امنیت اطلاعات احساس می‌شود.

یک نمونه از سند تعیین قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات در بخش ضمیمه همین سند نشان داده شده است.

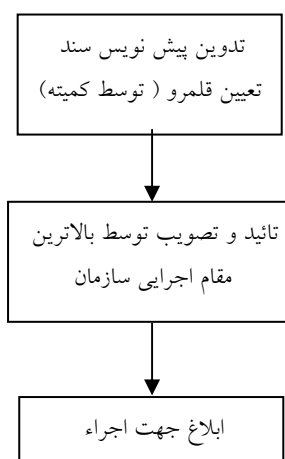
مرجع

این سند بر اساس سند سیاست‌گذاری امنیت اطلاعات تدوین شده و به شماره □-□ / ۱-۱-۱-۱ به ثبت رسیده است. سایر اسناد مرتبط عبارت‌اند از:

دستورالعمل ۱-۱-۱

روند نما

روند نمای تدوین و ابلاغ سند تعیین قلمرو به شرح زیر است:



ضمیمه

نمونه سند تعیین قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات

توجه: متن زیر به عنوان نمونه ارائه شده است و می‌توان آن را بر اساس نیاز تغییر داد.

آرم سازمان

((وزارت/ سازمان/ اداره کل/ شرکت))

سند تعیین قلمرو و حوزه عملکرد

سامانه مدیریت امنیت اطلاعات

به موجب این سند مقرر می‌گردد نظام مدیریت امنیت اطلاعات در حوزه‌های جغرافیایی و عملیاتی زیر و در خصوص کلیه فعالیت‌های مرتبط با جمع‌آوری، پردازش و نگهداری و ارسال داده‌ها و اطلاعات در مکان‌های زیر پیاده‌سازی شود:

۱- پردیس مرکزی ((وزارت/ سازمان/ اداره کل/ شرکت))

۲- ساختمان‌های (یا سایت‌های) واقع در ((آدرس محل))

۳- دارایی‌های اطلاعاتی متعلق به ((وزارت/ سازمان/ اداره کل/ شرکت)) مستقر در ((آدرس محل‌های نگهداری که مالکیت یا اداره آن‌ها به عهده سازمان نمی‌باشد))

۴-

۵-

همچنین کلیه خدمات قابل ارائه از طریق سیستم‌های پردازشی زیر باید با توجه به الزامات نظام مدیریت امنیت اطلاعات ارائه گردند:

.....

.....

.....

.....

((فهرست فوق باید شامل کلیه پردازش‌ها و خدماتی باشد که توسط سازمان از طریق سیستم‌های رایانه‌ای ارائه می‌گردند از قبیل :

نظام اتوماسیون اداری و کنترل‌های داخلی

سیستم دریافت و ثبت تقاضانامه‌ها مثل تقاضای ثبت سفارش، موافقت‌نامه اصولی، پروانه ساختمان،

سیستم‌های صدور مدارک یا مجوز مانند گواهینامه رانندگی، پروانه بهره‌برداری و

سیستم‌های پیگیری مکاتبات یا مراسلات که از طریق کدهای پیگیری عمل میکنند.

سایر سیستم‌های کاربردی اداری، تجاری

بانک‌های اطلاعاتی سرویس دهنده به سیستم‌های فوق

کلیه سیستم‌های مدیریت، راهبری، کنترل، نظارت و پشتیبانی شبکه‌های رایانه‌ای

(((

به علاوه نظام مدیریت امنیت برای حفاظت از دارایی‌های اطلاعاتی زیر به کار گرفته خواهد شد:

اطلاعاتی که حقوق مالکیت معنوی آن متعلق به (((وزارت/ سازمان/ اداره کل/ شرکت)))

می‌باشد.

اطلاعات مربوط به مشتریان یا ارباب رجوع

اطلاعات مربوط به نمایندگان، پیمانکاران یا طرف‌های اداری و تجاری

نیروی انسانی در اختیار

۳-۲- سازمان (دهی) امنیت اطلاعات

این بخش شامل دستورالعمل‌های زیر می‌باشد:

۲- سازمان (دهی) امنیت اطلاعات		
۱-۲	سازمان (دهی) درونی	
۱-۱-۲	تعهد و اهتمام مدیریت ارشد سازمان به امنیت اطلاعات	
۲-۱-۲	هماهنگی امنیت اطلاعات	
۳-۱-۲	تعیین مسئولیت در حوزه امنیت اطلاعات	
۴-۱-۲	صدور مجوز استفاده از تجهیزات پردازش اطلاعات	
۵-۱-۲	توافقنامه‌های حفظ محرمانگی	
۶-۱-۲	برقراری ارتباط با مراجع حکومتی	
۷-۱-۲	ارتباط با سایر مراجع یا سازمان‌ها یا نهادهای دارای اشتراک منافع	
۸-۱-۲	بازنگری مستقل سامانه امنیت اطلاعات	
۲-۲	تعامل با اشخاص ثالث (سایر مراجع)	
۱-۲-۲	شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری	
۲-۲-۲	رعایت نکات امنیتی هنگام تعامل با مشتریان یا ارباب رجوع	
۳-۲-۲	رعایت معیارهای امنیتی در قراردادهای اشخاص ثالث	

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی
ابلاغ تعهد و اهتمام مدیریت ارشد سازمان به حفظ امنیت اطلاعات شماره دستورالعمل : ۱-۱-۲	

عادی

تائیدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به عنوان دبیر منصوب خواهد شد.

شرح	تاریخ

هدف

هدف از تدوین این دستورالعمل بیان ضرورت تعهد و اهتمام مدیریت ارشد (((وزارت/ سازمان/ اداره کل/ شرکت /...))) به حفظ امنیت اطلاعات و تبیین نحوه اعلام آن می‌باشد.

مسئولیت

مسئولیت تهیه خط مشی مدیریت امنیت اطلاعات، اعلام آن و پیگیری اجرای مفاد خط مشی توسط کلیه آحاد (((وزارت/ سازمان/ اداره کل/ شرکت /...))) به عهده (((بالاترین مقام اجرایی))) می‌باشد.

الزامات

لازم است سند خط و مشی مدیریت امنیت اطلاعات (مطابق الگوی معرفی شده در ضمیمه همین سند) تدوین گردد.

- ۱- خط مشی امنیت اطلاعات باید به نحو مناسب به اطلاع کلیه آحاد (((وزارت/ سازمان/ اداره کل/ شرکت /...))), ارباب رجوع، مشتریان، طرف‌های اداری- تجاری و سایر گروه‌های ذینفع رسانده شود.
- متن سند باید گویا، صریح، خلاصه، کافی و تفسیر ناپذیر باشد.

فرآیند

هنگام تدوین سند خط و مشی مدیریت امنیت اطلاعات باید به نکات زیر توجه کرد:

متن سند بدون استفاده از توضیحات غیر ضروری تدوین شده باشد.

اجرای مفاد سند عملی و امکان پذیر باشد.

حجم مطالب مندرج در متن سند به نحوی باشد که بتوان آن را به سادگی در تابلو اعلانات، سایت اطلاع رسانی الکترونیک و یا پوسترهای اطلاع رسانی درج و آگهی نمود.

در متن سند خط مشی باید به رؤس و راهبردهای اصلی در نظر گرفته شده برای پیاده‌سازی مدیریت امنیت اطلاعات اشاره شود.

از آن‌جا که سامانه مدیریت امنیت در جهت استانداردسازی فعالیت‌های مدیریت امنیت اطلاعات پیاده‌سازی می‌شود، لازم است در متن سند خط مشی به نوع استاندارد مرجع (به عنوان مثال استاندارد ISO/IEC-27001 و یا استانداردهای ملی که توسط موسسه استاندارد و تحقیقات صنعتی ایران منتشر می‌شود) اشاره شود.

لازم است مدیر ارشد در متن سند به تعهد خود به پیاده‌سازی نظام مدیریت امنیت اطلاعات و اهتمام به پشتیبانی از اهداف و روش‌های تبیین شده در سند خط مشی از طریق ایجاد ساختارهای مناسب لازم و تأمین و تخصیص بودجه اشاره نماید.

در متن سند باید به انجام ممیزی کفایت نظام مدیریت امنیت اطلاعات اشاره شود.

- لازم است ذیل سند به امضاء ((بالاترین مقام اجرایی)) سازمان برسد.
یادآوری: یک نمونه از سند خط و مشی مدیریت امنیت اطلاعات در ضمیمه همین سند منتشر شده است.

بازنگری

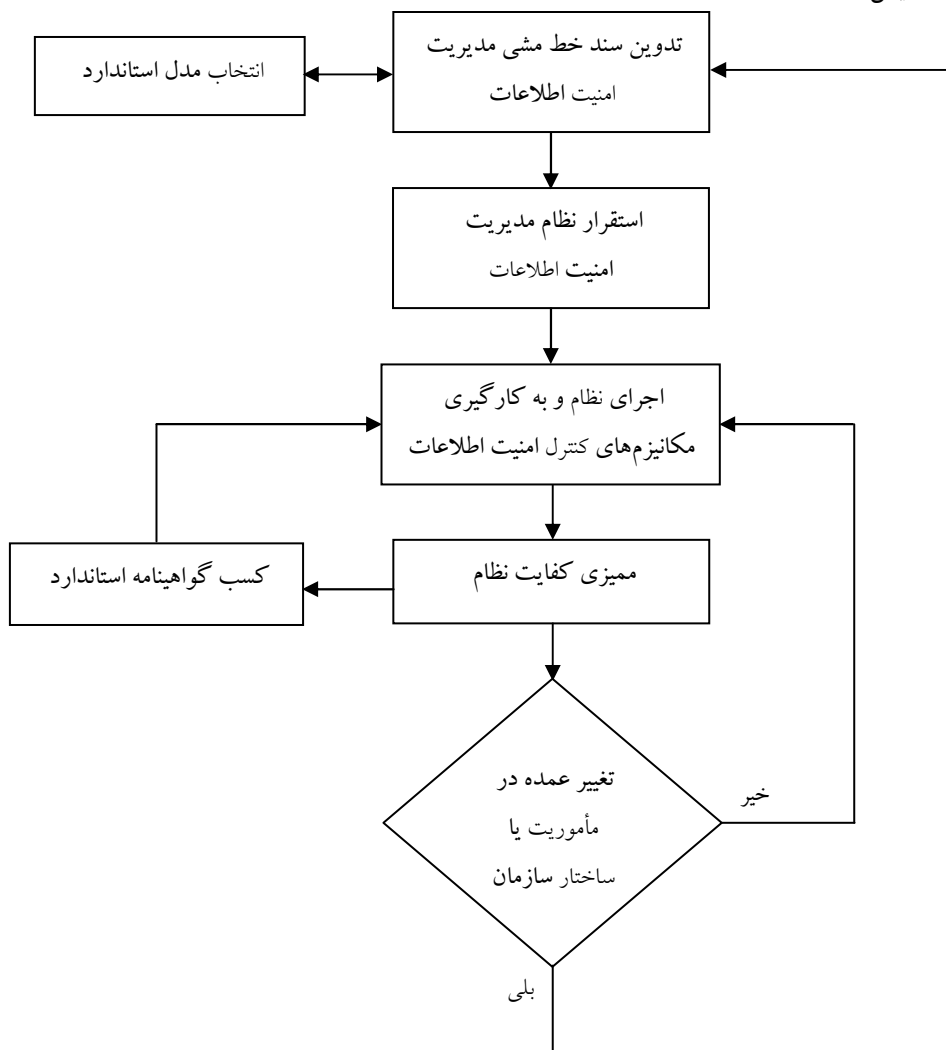
مفاد سند خط و مشی مدیریت امنیت اطلاعات باید با توجه به اهداف مندرج در سند‌های چشم انداز (به عنوان مثال سند چشم انداز بیست ساله کشور- ایران ۱۴۰۴) تدوین شده باشد. بنابراین بازنگری آن فقط در صورت انتشار سند چشم انداز جدید و یا تغییر عمده در ساختار یا مأموریت سازمان ضروری خواهد بود.

مرجع

این سند تحت عنوان دستورالعمل □-□/۱-۲/□-□ به ثبت رسیده است و سند تنظیم شده بر اساس آن (سند خط مشی) به عنوان سند راهبردی اصلی نظام مدیریت امنیت اطلاعات محسوب می‌شود.

روند نما

فرآیند تدوین و پیگیری اجرای خط مشی مدیریت امنیت اطلاعات در فلوچارت زیر نمایش داده شده است.



ضمیمه

توجه: متن زیر به صورت نمونه ارائه گردیده است و می‌توان مفاد آن را بر اساس نیاز تغییر داد.

سند راهبردی (خط مشی) مدیریت امنیت اطلاعات

((وزارت/ سازمان/ اداره کل/ شرکت /...)) که مأموریت ((مأموریت اصلی سازمان)) را به عهده دارد این سند راهبردی را به عنوان خط مشی مدیریت امنیت اطلاعات خود منتشر نموده است.

این ((نهاد)) با توجه به مأموریت خود و بر اساس راهبردها و راهکارهای مندرج در قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران و سند راهبردی نظام جامع فناوری اطلاعات کشور و سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور بهره‌گیری از فناوری‌های برتر روز و امن‌سازی فعالیت‌های مرتبط با آن را در دستور کار خود قرار داده است.

((وزارت/ سازمان/ اداره کل/ شرکت /...)) بر این اعتقاد است که اطلاعات و کانال‌های ارتباطی یکی از با ارزش‌ترین دارایی‌های وی است و باید در چهارچوب قوانین و مقررات کشور جمهوری اسلامی ایران از آن محافظت بعمل آید و به این منظور استاندارد ((نام مدل استاندارد انتخابی)) را به عنوان مرجع اجرایی و مدیریتی خود برگزیده است.

مهمترین راهبردهای این ((نهاد)) در حفظ امنیت اطلاعات عبارت‌اند از:

- حفاظت از محرمانگی اطلاعات برای جلوگیری از افشای غیر مجاز اطلاعات
- حفظ جامعیت و صحت اطلاعات برای جلوگیری از تغییرات غیر مجاز

حفظ دسترسی پذیری اطلاعات جهت دسترسی سریع و آسان مراجع مجاز به اطلاعات در

مواقع نیاز

بنابر راهبردهای فوق ((وزارت/ سازمان/ اداره کل/ شرکت /...)) خود را ملزم به انجام موارد ذیل می‌داند:

- استقرار نظام مدیریت امنیت اطلاعات و ارزیابی مستمر آن
- فرهنگ سازی، اطلاع رسانی و آموزش لازم در خصوص حفاظت از امنیت اطلاعات به کاربران
- تشکیل نهادهای پشتیبان نظام مدیریت امنیت اطلاعات شامل کمیته امنیت اطلاعات، نهاد متصدی حفظ امنیت اطلاعات و گروه مقابله با شرایط اضطراری و تامین نیازهای آن

تدوین طرح مقابله با بحران و تأمین ابزار و ساختار مورد نیاز جهت اجرای آن در مواقع ضروری

((بالاترین مقام اجرایی)) ضمن ارزیابی و بازنگری این نظام مدیریتی به صورت دوره‌ای همواره بر پیشبرد و بهبود آن اهتمام داشته و از تمامی همکاران عزیز انتظار دارد با همدلی صمیمانه در راستای مدیریت امنیت اطلاعات، بهبود امنیت داده‌ها، اطلاعات، سیستم‌ها و شبکه‌های پردازشی همت گمارند.

((عنوان بالاترین مقام اجرایی))

نام :

امضاء :

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی
هماهنگی امنیت اطلاعات شماره دستورالعمل : ۲-۱-۲	

عادی

تائیدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود. طبقه‌بندی اسناد یا ساختارهای تولید یا ایجاد شده بر اساس این سند تابع سطح طبقه‌بندی حفاظتی سازمان متبوع خواهد بود.

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

سوابق تغییرات :

هدف

هدف از تدوین این سند ایجاد هماهنگی بین واحدهای مختلف متصدی راهبری، اجرا، نظارت و پشتیبانی فعالیت‌های مرتبط با مدیریت امنیت اطلاعات در ((وزارت/ سازمان/ اداره کل/ شرکت/)) می‌باشد.

در این سند روش ایجاد ساختارها، وظایف هر یک و نوع ارتباطشان با یکدیگر تبیین شده است. ساختارهایی که لازم است ایجاد شوند عبارت‌اند از:

- کمیته امنیت اطلاعات
- کارگروه امنیت اطلاعات (محدود به یک دوره زمانی خاص)
- نهاد متولی پیاده‌سازی امنیت اطلاعات (در صورت نیاز بر اساس نتایج تحلیل ریسک)
- گروه مقابله با شرایط اضطراری (CERT)
- گروه احیای سیستم

مسئولیت‌ها

مسئولیت ایجاد کمیته امنیت اطلاعات به عهده ((بالاترین مقام اجرایی سازمان)) می‌باشد. کمیته امنیت اطلاعات پس از تشکیل مسئولیت ایجاد، راهبری و نظارت بر فعالیت سایر ساختارهای فوق را به عهده خواهد داشت.

الزامات

تشکیل کمیته امنیت اطلاعات الزامی است.

- ۱- تشکیل کارگروه امنیت اطلاعات در سازمان‌هایی که بر اساس رهنمودهای سازمان پدافند غیرعامل حساس و یا حیاتی شناخته می‌شوند و یا مدیریت و راهبری تأسیسات زیربنایی، ساختمان‌های حساس و شریان‌های اصلی و حیاتی کشور اعم از در دست مطالعه، اجرا و یا در حال بهره‌برداری حساس یا حیاتی را به عهده داشته باشند، الزامی است.
- ۲- تشکیل نهاد اختصاصی جهت پیاده‌سازی نظام مدیریت امنیت اطلاعات در سازمان‌هایی که بر اساس رهنمود سازمان پدافند غیرعامل حساس یا حیاتی شناخته می‌شوند، الزامی است.

در صورتی که ایجاد ساختار جدید یا تغییر در چارت سازمانی بر اساس مقررات یا قوانین دولتی ممنوع یا مشکل باشد لازم است اولاً ساختار جدید به صورت مجازی ایجاد شده و از متوقف ماندن

فعالیت‌های مربوط به آن (حتی از طریق برون سپاری با لحاظ الزامات طبقه‌بندی حفاظتی) جلوگیری شود و ثانیاً بلافاصله پس از تشخیص الزامی بودن ایجاد ساختار یا تغییر چارت بر اساس این دستورالعمل و یا نتایج حاصل از تحلیل ریسک، اقدامات حقوقی لازم جهت کسب مجوز یا تصویب قانون از طریق مراجع ذیربط آغاز شود.

فرآیند

استقرار و پیاده‌سازی نظام مدیریت امنیت اطلاعات فرآیندی است که مستلزم صرف بودجه و / ایجاد ساختار سازمانی مناسب می‌باشد. با توجه به این اصل و نکاتی که در ادامه به آن اشاره خواهد شد، لازم است فعالیت‌های مرتبط با مدیریت و استقرار نظام امنیت اطلاعات بر اساس هماهنگی‌های از پیش به عمل آمده بین واحدهای سازمان و در صورت نیاز برقراری ارتباط با مراجع حکومتی و یا سایر نهادهای فراسازمانی به اجرا گذاشته شود.

توجه به نکات زیر ضروری است:

فعالیت‌های پردازشی اعم از جمع‌آوری، پردازش، تولید، ذخیره‌سازی و انتقال اطلاعات به صورت روزافزون در حال رسوخ به کلیه جنبه‌های زندگی نوع بشر می‌باشد.

فعالیت‌های پردازشی نوین معمولاً بیش از یک نهاد را تحت تأثیر قرار می‌دهند به عنوان مثال هنگام صدور دستور پرداخت الکترونیک مراجع زیر درگیر خواهند شد:

۱- پرداخت کننده

۲- دریافت کننده

۳- بانک عامل پرداخت کننده

۴- بانک عامل دریافت کننده

۵- نهاد ثالث مورد توافق طرفین یا صادر کننده گواهی تبادل

۶- مراجع حکومتی یا قضایی در صورت وقوع اختلاف یا انکار تبادل از سوی طرفین

علاوه بر نکات فوق و با پذیرفتن فرض نیاز به سیستمی جهت پاسخگویی به نیازهای اخلاقی، مقرراتی یا قانونی هنگام اجرای فعالیتهای پردازشی لازم است نهادهای اختصاصی برای مدیریت و راهبری چنین فعالیت‌هایی به وجود آید که اولاً فعالیت‌ها را چنان اجرا نماید که از بروز تعارض و پیامدهای آن جلوگیری نماید و ثانیاً بر رعایت الزامات برقراری ارتباط امن بین طرف‌های مختلف هر تبادل اطلاعاتی (الکترونیکی) نظارت نماید.

بنابراین روابط بین سیستم‌های پردازشی و یا افراد متصدی کار با آن‌ها یا کاربران را می‌توان در قالب دو نوع رابطه تقسیم بندی نمود:

- الف- رابطه بین سازمان‌ها و نهادهایی که دارای استقلال از یکدیگر می‌باشند.
- ب- رابطه بین اجزای درون یک سازمان

جهت هماهنگی بین اجزای دخیل در یک رابطه فراسازمانی لازم است به قوانین و مقررات کشوری (و در صورت نیاز قوانین بین المللی) مراجعه نمود. این بحث خارج از موضوع این دستورالعمل است و بعداً در قالب دستورالعمل‌های مربوطه به فصل انطباق با قوانین به آن پرداخته خواهد شد.

آنچه در این دستورالعمل به آن پرداخته خواهد شد تنظیم و هماهنگی روابط و فعالیت‌های اجزای درونی یک سازمان در جهت استقرار و اجرای نظام مدیریت امنیت اطلاعات می‌باشد.

هماهنگی بین اجزای سازمان در حوزه مدیریت امنیت اطلاعات

جهت انجام امور مدیریت امنیت اطلاعات لازم است فعالیت‌های اجرایی زیر به اجرا گذاشته شود:

- تعیین حوزه فعالیت
- تشکیل نهادهای مربوط
- تعریف وظایف
- تفویض اختیار و تعیین حوزه مسئولیت
- تدوین برنامه
- تخصیص بودجه
- اجرای فعالیت
- نظارت و تصحیح

بر اساس سند سیاست‌گذاری امنیت اطلاعات (موضوع دستورالعمل ۱-۱-۱) کلیه افرادی که بنحوی مرتبط با فعالیت‌های پردازشی اطلاعات هستند در زمینه حفاظت از امنیت اطلاعات در حوزه کاری خود دارای مسئولیت هستند. به عبارت دیگر ممکن است حتی افرادی که مستقیماً با تجهیزات پردازشی سر و کار نداشته باشند دارای مسئولیت در حفظ امنیت اطلاعات و حفاظت از دارایی‌های اطلاعاتی (موضوع دستورالعمل ۱-۱-۳) باشند. بنابراین لازم است جهت هماهنگی بین

افراد و اجزای سازمان در خصوص استقرار و پیاده‌سازی نظام مدیریت امنیت، نهادهای اختصاصی تشکیل شود. شرح وظایف این نهادها و نحوه ارتباط آن‌ها با یکدیگر ذیلاً شرح داده می‌شود.

الف - کمیته امنیت اطلاعات

لازم است کمیته‌ای داخلی متشکل از مدیران ارشد برای مدیریت و نظارت بر امنیت فرآیندهای پردازی یا فرآیندهای مرتبط با آن تشکیل شود.

• الف-۱- اعضای کمیته امنیت اطلاعات عبارت‌اند از:

- نماینده تام‌الاختیار بالاترین مقام اجرایی سازمان به عنوان رئیس کمیته
- مسئول (((مرکز حراست فناوری اطلاعات سازمان یا نهاد متصدی حفظ امنیت اطلاعات))) به عنوان دبیر کمیته
- سایر معاونت‌های سازمان به عنوان عضو
- مسئول حراست به عنوان عضو
- کارشناسان خبره به دعوت کمیته به عنوان مشاور

• الف-۲- وظایف و اختیارات کمیته امنیت اطلاعات

وظیفه کمیته امنیت اطلاعات راهبری و نظارت بر کلیه فعالیت‌های مرتبط با نظام مدیریت امنیت اطلاعات به نمایندگی از طرف (((بالاترین مقام اجرایی سازمان))) می‌باشد. به عبارت دیگر (((بالاترین مقام اجرایی سازمان))) می‌تواند کلیه وظایف خود در زمینه حفاظت از امنیت اطلاعات (به جز تدوین و پشتیبانی خط مشی امنیت اطلاعات) را به کمیته امنیت اطلاعات محول نماید.

حضور سایر معاونت‌های سازمان و مسئول حراست در کمیته امنیت اطلاعات برای ایجاد هماهنگی و اطلاع از تصمیمات مرتبط با امنیت اطلاعات و تسهیل فعالیت‌های بعدی مربوط به پیاده‌سازی مفاد دستورالعمل‌های امنیت اطلاعات ضروری است. از آن‌جا که تصمیم‌های مرتبط با امنیت اطلاعات دارای جنبه‌های مختلف از قبیل تخصیص بودجه جهت تأمین نیازهای امنیت اطلاعات، تغییر در روندهای کاری یا فرآیندهای اجرایی، اعمال محدودیت‌های خاص در دسترسی به تجهیزات یا مکان‌ها و دارایی‌های سازمان و یا حفاظت و حراست نیروی انسانی یا تنظیم روابط

مستخدمین با سازمان می‌باشد، هماهنگی‌های مرتبط با امور فوق به کمیته امنیت اطلاعات که اعضای آن متشکل از مدیران ارشد سازمان می‌باشند محول می‌گردد. همچنین کمیته امنیت اطلاعات مختار است از کارشناسان خبره برای مشاوره استفاده نماید. وظایف و اختیارات اعضای کمیته امنیت اطلاعات به شرح زیر است:

- رئیس کمیته: مدیریت جلسات کمیته امنیت اطلاعات، تصویب دستور کار، دعوت از کارشناسان جهت شرکت در جلسات کمیته به عنوان مشاور و امضای احکام صادره توسط کمیته جهت عضویت افراد در کارگروه امنیت اطلاعات و یا مکاتبات با سایر نهادها و مراجع، حضور در رأی‌گیری‌ها
- دبیر کمیته: پیگیری تشکیل جلسات، تهیه مستندات، آماده سازی مقدمات تشکیل جلسات، تهیه برنامه‌های کاری و ایجاد هماهنگی بین اعضا، تهیه پیش‌نویس مصوبات کمیته امنیت اطلاعات، تهیه صورتجلسه از تصمیمات کمیته امنیت اطلاعات و حضور در رأی‌گیری‌ها
- معاونت‌ها و مسؤول حراست: حضور در تصمیم‌گیری، اعلام نظر و رأی‌گیری‌ها و تسهیل اجرای تصمیمات کمیته امنیت اطلاعات در واحدهای تحت مدیریت خود.
- کارشناسان خبره: حضور در جلسات و ارائه نظرات مشاوره‌ای بدون حق رأی
- رسمیت تصمیمات کمیته / امنیت اطلاعات: تصمیم‌های حائز رأی اکثریت رسمیت یافته و جهت اجرا از طریق رئیس کمیته به مراجع ذیربط ابلاغ می‌شوند. در صورت تساوی آرا در خصوص یک موضوع نظر نهایی رئیس کمیته ملاک رسمیت تصمیم خواهد بود.

به‌علاوه پیشنهاد عضویت افراد در گروه **CERT** و گروه احیای سیستم و نظارت بر عملکرد این دو گروه به عهده کمیته امنیت اطلاعات می‌باشد.

تحلیل ریسک / امنیت اطلاعات که مبنای کلیه فعالیت‌ها و صدور دستورالعمل‌های امنیت اطلاعات قرار خواهد گرفت از مهمترین وظایف اولیه کمیته امنیت اطلاعات می‌باشد و لازم است این کمیته در اولین جلسه پس از تعیین و تصویب قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات (موضوع دستورالعمل ۱-۱-۳) در

خصوص آن تصمیم‌گیری نماید. کمیته امنیت اطلاعات می‌تواند این فعالیت را به کارگروه امنیت اطلاعات (که شرح وظایف آن منعقاباً شرح داده می‌شود) محول نماید.

بررسی و تصویب گزارش تحلیل ریسک و بیانیه کاربرپذیری (سند SOA^۴) پیشنهادی از طرف کارگروه امنیت اطلاعات به عهده کمیته امنیت اطلاعات می‌باشد. در صورت عدم تشکیل کارگروه امنیت اطلاعات وظیفه تدوین گزارش تحلیل ریسک و تدوین بیانیه کاربرپذیری به عهده بخشی از اعضای کمیته امنیت اطلاعات خواهد بود که از سوی رئیس کمیته امنیت انتخاب خواهد شد.

ب- کارگروه امنیت اطلاعات

کارگروه امنیت اطلاعات به عنوان بازوی اجرایی کمیته امنیت اطلاعات و بنا بر تشخیص این کمیته تشکیل می‌شود.

تبصره: تشکیل کارگروه امنیت اطلاعات در سازمان‌هایی که بر اساس رهنمودهای سازمان پدافند غیرعامل حساس یا حیاتی دسته‌بندی می‌شوند و یا دارایی‌های اطلاعاتی حساس یا حیاتی را مدیریت می‌کنند ضروری است. این موضوع در مقدمه این سند شرح داده شده است. کارگروه امنیت اطلاعات در مرحله ابتدایی پیاده‌سازی سامانه مدیریت امنیت اطلاعات و به عنوان یک ساختار موقت تشکیل می‌شود و فعالیت آن پس از انجام امور زیر خاتمه می‌یابد:

- تهیه فهرست موجودی دارایی‌ها (طبق دستورالعمل ۱-۱-۳)
 - برچسب گذاری دارایی‌های اطلاعاتی (طبق دستورالعمل ۲-۲-۳)
 - تدوین گزارش مرحله شناخت سیستم (طبق دستورالعمل ۱-۳-۳)
 - تدوین گزارش شناخت و تحلیل ریسک‌های امنیتی و سند ارزیابی ریسک (طبق دستورالعمل ۲-۳-۳ و ۳-۳-۳)
 - تدوین بیانیه کاربرپذیری (SOA) (اختصاصی (طبق دستورالعمل ۴-۳-۳))
- تبصره: در صورت وقوع هر یک از حوادث زیر تشکیل کارگروه جدید امنیت اطلاعات ضروری است و باید فعالیت‌های فوق تجدید گردد:

⁴ Statement of Applicability

- کشف رخنه عمده در سیستم‌های پردازشی یا ارتباطی
- ضربه عمده به سیستم و یا فروپاشی سیستم
- اجرایی شدن طرح احیای سیستم

• ب-۱- اعضای کارگروه امنیت اطلاعات

در صورت نیاز به تشکیل کارگروه امنیت اطلاعات لازم است افراد زیر به عضویت این کارگروه منصوب شوند.

- رئیس: مسئول مرکز حراست **IT** یا نهاد متصدی امنیت اطلاعات و در غیر اینصورت مسئول واحد فناوری اطلاعات یا نهاد معادل آن
- دبیر کارگروه: یک نفر از معاونت برنامه‌ریزی
- کارشناس ستادی: یک نفر از معاونت مالی، اداری و پشتیبانی
- کارشناس امنیت اطلاعات **IT**: یک یا چند نفر خبره در حوزه فعالیت‌های پردازشی سازمان به دعوت رئیس کمیته امنیت اطلاعات
- کارشناس فنی: یک نفر از معاونت فنی

تبصره: ساختار فوق ساختار پیشنهادی بوده و تعداد و ترکیب افراد می‌تواند با توجه به نوع فعالیت و ماهیت سازمان تغییر نماید. همچنین می‌توان افراد فوق را از بین اعضای کمیته امنیت اطلاعات انتخاب نمود. در سازمان‌هایی که از دیدگاه سازمان پدافند غیرعامل به عنوان سازمان‌های حیاتی طبقه‌بندی می‌شوند لازم است به جز رئیس کارگروه، سایر اعضاء از بین افراد غیر عضو کمیته امنیت اطلاعات انتخاب شوند.

تبصره: پس از تصویب ساختار سازمانی نهاد امنیت اطلاعات (یا مرکز حراست فناوری اطلاعات) کلیه مسئولیت‌ها و وظایف کارگروه به آن نهاد تفویض خواهد شد. همچنین پس از پایان کار کارگروه امنیت اطلاعات می‌توان اعضای آن را به عنوان نهاد جایگزین مرکز حراست فناوری اطلاعات (تا زمان تشکیل مرکز حراست فناوری اطلاعات) به کار گرفت.

ج- مرکز حراست فناوری اطلاعات

مرکز حراست فناوری اطلاعات با هدف تأمین و حفاظت از داده‌ها، توان پردازشی، سخت‌افزار، نرم‌افزار، بانک‌های اطلاعاتی و ارتباطات رایانه‌ای در مقابل نفوذ، دسترسی غیر مجاز و سرقت اطلاعات و نظارت بر عملکرد تأسیسات پشتیبان تجهیزات و توان پردازشی و کانال‌های ارتباطی تشکیل می‌شود.

• ج-۱- جایگاه سازمانی مرکز حراست فناوری اطلاعات یا نهاد متصدی حفاظت

از امنیت اطلاعات

تصمیم‌گیری در مورد تأسیس نهاد و جایگاه سازمانی مرجعی که تصدی حفاظت از امنیت اطلاعات را به عهده دارد به عهده (((بالاترین مقام اجرایی سازمان))) می‌باشد. توجه به نکات زیر ضروری است:

- تأسیس نهاد متصدی حفاظت از اطلاعات در کلیه تأسیسات زیر بنایی و سامانه‌های حساس و شریان‌های اصلی و حیاتی کشور اعم از در دست مطالعه، اجرا و یا در حال بهره‌برداری که از سوی سازمان پدافند غیرعامل کشور به عنوان مراکز حیاتی یا حساس یا مهم دسته‌بندی می‌شوند، الزامی است.
- در مراکزی که مأموریت اصلی آن‌ها انجام فعالیت‌های پردازشی است و یا از دیدگاه سازمان پدافند غیرعامل کشور به عنوان مراکز حیاتی دسته‌بندی می‌شوند این نهاد باید مستقیماً تحت نظر (((بالاترین مقام اجرایی سازمان))) تشکیل شده و به فعالیت بپردازد.
- در مراکزی که بخش عمده خدمات و وظایف آن با استفاده از تجهیزات پردازشی و یا بر اساس پردازش و انتقال اطلاعات انجام می‌شود و یا از دیدگاه سازمان پدافند غیرعامل کشور به عنوان مراکز حساس دسته‌بندی می‌شوند لازم است نهاد متصدی امنیت اطلاعات در حوزه معاونت فنی آن مرکز تشکیل شده و تحت مدیریت معاون فنی به فعالیت بپردازد.
- در سایر سازمان‌ها، نهاد متصدی امنیت اطلاعات در حوزه معاونت مالی، اداری، پشتیبانی تشکیل شده و به فعالیت خواهد پرداخت.

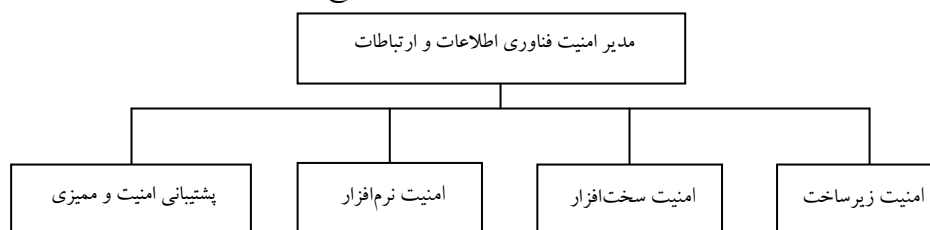
برخی از وظایف نهاد متصدی حفاظت از امنیت اطلاعات ذیلاً شرح داده شده است.
 تخصیص وظایف دیگر و چگونگی تعامل این نهاد با سایر اجزای ((وزارت/ سازمان/ اداره کل/ شرکت/)) از اختیارات ((بالاترین مقام اجرایی سازمان)) می‌باشد.

• ج-۲- وظایف مرکز حراست فناوری اطلاعات

- برقراری ارتباط با سایر مراجع مرتبط با امنیت اطلاعاتی و کسب آخرین اطلاع از روند مقررات و قوانین مرتبط با امنیت اطلاعات (دستورالعمل ۶-۱-۲)
- برقراری ارتباط با سایر مراجع تخصصی مرتبط با امنیت اطلاعات و کسب اطلاع از روند وقایع و حوادث امنیتی (دستورالعمل ۷-۱-۲)
- به هنگام سازی شناسنامه دارایی‌های اطلاعات (دستورالعمل‌های ۱-۱-۳ و ۲-۱-۳)
- تعیین ضوابط کلی حفاظتی جانمایی (موقعیت مکانی) دارایی‌های اطلاعاتی و برقراری امنیت فیزیکی
- تعیین طبقه‌بندی حفاظتی دارایی‌های اطلاعاتی (دستورالعمل‌های ۱-۲-۳ و ۲-۲-۳)
- تدوین و نظارت بر اجرای دستورالعمل‌های کنترل، نگهداری، خارج از رده سازی و امحاء دارایی‌های اطلاعاتی
- تعیین و نظارت بر اجرای رویه‌ها و دستورالعمل‌های کنترل دسترسی دارایی‌های اطلاعاتی
- تدوین و ابلاغ دستورالعمل‌ها و رویه‌های مرتبط با کنترل ورود و خروج دارایی‌های اطلاعاتی و یا رسانه‌های ذخیره اطلاعات مانند دیسک، دیسک نوری، حافظه‌های جانبی و ...
- تدوین و نظارت بر اجرای ضوابط مربوط به رعایت نکات امنیتی در تهیه و به کارگیری دارایی‌های اطلاعاتی (دستورالعمل ۴-۱-۲)
- انجام دوره‌ای تست نفوذپذیری (Penetration Test) و تولید و ارسال گزارش به مراجع مرتبط
- آموزش و اطلاع رسانی در حوزه امنیت و مدیریت امنیت اطلاعات
- مانیتورینگ فعالیت سیستم‌های پردازشی و کانال‌های ارتباطی
- تحلیل و مدیریت ریسک
- تدوین ضوابط قرارداد با اشخاص ثالث و نظارت بر اجرای آن (دستورالعمل ۳-۲-۲)

- پشتیبانی کامل از گروه CERT و گروه احیای سیستم (ضوابط تشکیل و وظایف این گروه‌ها در ادامه همین دستورالعمل تشریح خواهد شد).
- شرکت در جلسات کمیته امنیت اطلاعات به عنوان دبیر
- تدوین و نظارت بر تهیه نسخه پشتیبان از کلیه اطلاعات
- کنترل تغییرات در وضعیت دارایی‌های اطلاعاتی و تحلیل ریسک‌های مربوطه
- بررسی نیازمندیهای فنی جهت پشتیبانی از فعالیت‌های مدیریت امنیت اطلاعات و تدوین برنامه‌های لازم در این زمینه
- جمع‌آوری، ثبت و نگهداری شواهد، وقایع و حوادث امنیتی به شکل اثبات پذیر و غیر قابل انکار جهت اقامه دعوا در مراجع قضایی یا دفاع در مقابل دعوای مطرح شده علیه (((وزارت/ سازمان/ اداره کل/ شرکت /)))

ساختار سازمانی کلی نهاد متصدی امنیت اطلاعات به شرح زیر خواهد بود:



• ج-۳- رده‌های شغلی نهاد متصدی حفاظت از امنیت اطلاعات

وظایف هر یک از اجزای نهاد امنیت اطلاعات عبارت است:

- امنیت زیرساخت: تأمین امنیت زیرساخت‌های ارتباطی LAN، WAN، پروتکل‌های شبکه‌ای و رمزنگاری
- امنیت سخت‌افزار: تأمین امنیت کلیه تجهیزات سخت‌افزاری، امنیت محیطی و فیزیکی و امنیت تأسیسات پشتیبانی از قبیل الکتریسیته، تهویه مطبوع، آب
- امنیت نرم‌افزار: تأمین امنیت کلیه تجهیزات نرم‌افزاری از قبیل سیستم‌های عامل، برنامه‌های کاربردی، ابزارهای سیستم، بانک‌های اطلاعاتی، سایت‌های اطلاع رسانی
- پشتیبانی امنیت و ممیزی: آموزش امنیت اطلاعات، پشتیبانی گروه‌های CERT و احیای سیستم، انطباق با قوانین و مقررات، امنیت نیروی انسانی و سازماندهی

توضیح: تشخیص ضرورت ایجاد نهاد متولی حفاظت از امنیت فناوری‌های اطلاعاتی و ارتباطی و ارائه پیشنهاد در خصوص ضرورت و چگونگی تفکیک وظایف اجزای آن (در نهادهایی که از لحاظ تغییر چارت سازمانی دارای استقلال می‌باشند) به عهده کمیته امنیت اطلاعات تشکیل شده در بالاترین رده ستادی ((وزارت/ سازمان/ اداره کل/ شرکت /)) و تصویب آن به عهده ((بالاترین مقام اجرایی وزارت/ سازمان/ اداره کل/ شرکت /)) می‌باشد.

رده‌های شغلی مورد نیاز جهت فعالیت در نهاد متصدی امنیت اطلاعات به شرح زیر می‌باشد:

#	حوزه کاری	شغل
۱	مدیریت امنیت	مدیر امنیت اطلاعات
۲	امنیت زیرساخت	کارشناس ارشد زیرساخت‌های امنیت
۳	امنیت زیرساخت	کارشناس ارشد پیوستگی عملیات و احیاء سیستم
۴	مدیریت امنیت	کارشناس امنیت ساختار سازمانی و نیروی انسانی
۵	امنیت سخت‌افزار	کارشناس امنیت فیزیکی و کنترل محیطی
۶	امنیت سخت‌افزار	کارشناس امنیت سخت‌افزار
۷	امنیت نرم‌افزار	کارشناس امنیت نرم‌افزار - سیستم عامل
۸	امنیت نرم‌افزار	کارشناس امنیت نرم‌افزار - برنامه‌های کاربردی و سیستم‌های اطلاعاتی
۹	امنیت نرم‌افزار	کارشناس امنیت نرم‌افزار - ابزارهای سیستم
۱۰	امنیت ارتباطات	کارشناس پروتکل‌ها و تجهیزات ارتباطی
۱۱	امنیت ارتباطات	کارشناس نرم‌افزارها و ابزار امنیتی
۱۲	مدیریت امنیت	کارشناس حقوق امنیت اطلاعات و انطباق با قوانین
۱۳	مدیریت امنیت	ممیز امنیت اطلاعات

توضیح: پیشنهاد ضرورت به‌کارگیری هر یک از رده‌های شغلی در نهاد متصدی امنیت اطلاعات (بر اساس نتایج حاصل از تحلیل ریسک و یا دستورالعمل‌های صادره از سمت مراجع مرتبط از قبیل سازمان پدافند غیرعامل) به عهده کمیته امنیت اطلاعات

((وزارت/ سازمان/ اداره کل/ شرکت/)) و تصویب آن به عهده ((بالاترین مقام اجرایی)) می‌باشد.

شرایط احراز و مهارت‌های لازم برای فعالیت در رده‌های شغلی فوق در جدول‌های زیر تشریح شده است:

شرایط احراز رده‌های شغلی امنیت اطلاعات

شغل	شرایط احراز
مدیر امنیت اطلاعات	هفت سال سابقه کار در زمینه امنیت اطلاعات، کارشناس ارشد سیستم/ مخابرات/ سخت‌افزار/ نرم‌افزار/ رمزنگاری
کارشناس ارشد زیرساخت‌های امنیت	پنج سال سابقه کار در زمینه امنیت اطلاعات، کارشناس ارشد مخابرات/ سخت‌افزار/ رمزنگاری
کارشناس ارشد پیوستگی عملیات و احیاء سیستم	پنج سال سابقه کار در زمینه امنیت اطلاعات، کارشناس ارشد سیستم / سخت‌افزار
کارشناس امنیت ساختار سازمانی و نیروی انسانی	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس سیستم
کارشناس امنیت فیزیکی و کنترل محیطی	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس سخت‌افزار
کارشناس امنیت سخت‌افزار	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس سخت‌افزار
کارشناس امنیت نرم‌افزار - سیستم عامل	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس نرم‌افزار
کارشناس امنیت نرم‌افزار - برنامه‌های کاربردی و سیستم‌های اطلاعاتی	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس نرم‌افزار
کارشناس امنیت نرم‌افزار - ابزارهای سیستم	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس نرم‌افزار/ سخت‌افزار
کارشناس پروتکل‌ها و تجهیزات ارتباطی	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس مخابرات/ سخت‌افزار
کارشناس نرم‌افزارها و ابزار امنیتی	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس نرم‌افزار/ سخت‌افزار
کارشناس حقوق امنیت اطلاعات و انطباق با قوانین	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس حقوق
ممیز امنیت اطلاعات	سه سال سابقه کار در زمینه امنیت اطلاعات، کارشناس سیستم / سخت‌افزار/ نرم‌افزار

مهارت‌های لازم برای احراز رده‌های شغلی امنیت اطلاعات

مهارت‌های لازم	شغل
توانایی مدیریتی، سرممیز امنیت اطلاعات و مهارت‌های یکی از رده‌های شغلی امنیت ریزساخت و گذراندن حداقل دو دوره آموزشی دیگر در زمینه امنیت اطلاعات	مدیر امنیت اطلاعات
توانایی برنامه‌ریزی و طراحی سیستم، سرممیز امنیت اطلاعات و مهارت‌های یکی از رده‌های شغلی امنیت نرم‌افزار/ سخت‌افزار/ ارتباطات و گذراندن حداقل دو دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس ارشد زیرساخت‌های امنیت
توانایی برنامه‌ریزی و طراحی سیستم، سرممیز امنیت اطلاعات و مهارت‌های یکی از رده‌های شغلی امنیت نرم‌افزار/ سخت‌افزار/ ارتباطات و گذراندن حداقل دو دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس ارشد پیوستگی عملیات و احیاء سیستم
توانایی شناخت سیستم و طراحی فرایند، ممیز امنیت اطلاعات و گذراندن حداقل سه دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس امنیت ساختار سازمانی و نیروی انسانی
توانایی طراحی فرایند، ممیز امنیت اطلاعات و گذراندن حداقل سه دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس امنیت فیزیکی و کنترل محیطی
توانایی طراحی فرایند، ممیز امنیت اطلاعات و گذراندن حداقل سه دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس امنیت سخت‌افزار
توانایی طراحی فرایند، ممیز امنیت اطلاعات و گذراندن حداقل سه دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس امنیت نرم‌افزار - سیستم عامل
توانایی طراحی فرایند، ممیز امنیت اطلاعات و گذراندن حداقل سه دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس امنیت نرم‌افزار - برنامه‌های کاربردی و سیستم‌های اطلاعاتی
توانایی طراحی فرایند، ممیز امنیت اطلاعات و گذراندن حداقل سه دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس امنیت نرم‌افزار- ابزارهای سیستم
توانایی طراحی فرایند، ممیز امنیت اطلاعات و گذراندن حداقل سه دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس پروتکل‌ها و تجهیزات ارتباطی

مهارت‌های لازم	شغل
توانایی طراحی فرایند، ممیز امنیت اطلاعات و گذراندن حداقل سه دوره آموزشی دیگر در زمینه امنیت اطلاعات	کارشناس نرم‌افزارها و ابزار امنیتی
آشنایی با مباحث مطرح در زمینه حقوق مالکیت معنوی، حقوق امنیت اطلاعات، حفاظت از حریم اطلاعات شخصی افراد، ممیز امنیت اطلاعات و گذراندن حداقل دو دوره آموزشی در زمینه امنیت اطلاعات	کارشناس حقوق امنیت اطلاعات و انطباق با قوانین
توانایی برقراری ارتباط با افراد، استحکام شخصیت، درک ارزش‌های سازمانی، قضاوت منصفانه، استقلال رای، سرممیز امنیت اطلاعات و گذراندن حداقل یک دوره آموزشی دیگر در زمینه امنیت اطلاعات	ممیز امنیت اطلاعات

د- گروه مقابله با شرایط اضطراری رایانه‌ای (CERT)

گروه مقابله با شرایط اضطراری رایانه‌ای (Computer Emergency Response Team) گروهی متشکل از افراد متصدی کار با تجهیزات پردازشی و ارتباطی هستند که از بین افراد سازمان انتخاب شده و وظیفه پاسخ به رویدادهای امنیت اطلاعات را به عهده دارند.

• د-۱- شرایط اضطراری

شرایط اضطراری در امنیت اطلاعات و ارتباطات هنگامی رخ می‌دهد که رویداد یا سلسله رویدادهایی با قابلیت ایجاد اختلال در عملیات سازمانی یا خدمات رسانی به ارباب رجوع واقع شود و در پی آن سازمان از انجام فعالیت‌های اصلی خود باز بماند. چنین رویدادهایی می‌توانند شامل حوادث زیر باشند:

- حوادث رایانه‌ای
- ورود ویروس یا کدهای مخرب
- قطع کانال‌های ارتباطی یا پر شدن ظرفیت آن‌ها
- حمله رایانه‌ای به تجهیزات پردازشی، نرم‌افزارها، بانک‌های اطلاعاتی یا کانال‌های ارتباطی
- سرقت اطلاعات یا تجهیزات پردازشی
- نقص‌های نرم‌افزارهای ناشی از ضعف در برنامه نویسی یا عدم کنترل داده‌های ورودی منجر به اختلال در کار نرم‌افزار
- خرابی سخت‌افزار

- حوادث محیطی
- اختلال در سیستم برق رسانی یا کنترل محیط عملیاتی
- آتش سوزی، طوفان، سیل، زلزله و یا سایر حوادث طبیعی
- جنگ یا اغتشاشات خیابانی و یا سایر حوادث عمدی یا غیرعمدی ناشی از عملکرد افراد
- حوادث فوق قابل تقسیم به دو نوع حوادث جزئی و یا حوادث عمده می‌باشند.
- حوادث جزئی عبارت‌اند از حوادثی که علیرغم ایجاد اشکال در فعالیت سازمان باعث فروپاشی سیستم نمی‌شود و یا فقط در بخش خاصی از خدمات سازمان ایجاد اختلال می‌کند.
- حوادث عمده عبارت‌اند از حوادثی که باعث فروپاشی سیستم شده و یا ادامه ارائه بخش بزرگی از خدمات سازمان را مواجه با اختلال می‌کند.
- مقابله با حوادث اضطراری جزئی به عهده گروه CERT و مقابله با حوادث عمده به طور مشترک به عهده گروه‌های CERT و احیای سیستم با محوریت گروه احیای سیستم می‌باشد.
- در ادامه مطلب نحوه عملکرد و ساماندهی گروه CERT و در بخش بعد چگونگی سازماندهی گروه احیای سیستم شرح داده می‌شود.
- همان‌طور که گفته شد گروه مقابله با شرایط اضطراری رایانه‌ای گروهی متشکل از افراد سازمان می‌باشد که وظیفه مقابله با حوادث و صدور پاسخ‌های اضطراری به آن‌ها را به عهده دارند. انجام این وظیفه از طریق زیر امکانپذیر است:
- آگاهی از روند وقایع و حوادث رایانه‌ای مانند تولید و انتشار ویروس‌های جدید، نقص‌های نرم‌افزاری (سیستم عامل، برنامه‌های کاربردی، بانک‌های اطلاعاتی)، رخنه‌های نرم‌افزاری یا سخت‌افزاری که می‌توان از آن‌ها برای نفوذ به سیستم‌ها یا تحت کنترل قرار دادن آن‌ها سوء استفاده نمود.
- ارتباط با سایر گروه‌های CERT و کسب اطلاع از آن‌ها
- تحت نظر داشتن روند فعالیت سیستم‌های پردازشی و کانال‌های ارتباطی سازمان
- بررسی دوره‌ای گزارش‌های فعالیت سیستم‌های پردازشی (Log Files)
- تحت نظر داشتن وقایع امنیتی (وقایعی که ممکن است زمینه ساز بروز حوادث شوند)
- شناسایی سریع حوزه اثر حوادث

- محدود سازی حوزه اثر حوادث و پیشگیری از گسترش آن
- ترمیم خرابی ناشی از حوادث
- انجام اقدامات پیشگیرانه اضافی برای جلوگیری از حوادث مشابه
- اطلاع به سایر گروه‌های CERT در خصوص حوادث امنیتی و وقایع منجر به آنها

• د-۲- اعضای گروه CERT

اعضای گروه CERT از بین افراد وابسته به نهاد متصدی حفاظت از امنیت فناوری اطلاعات و ارتباطات و سایر واحدهای سازمان انتخاب می‌شوند. تعداد اعضای گروه CERT حداقل سه نفر خواهد بود. تصمیم‌گیری در مورد حداقل تعداد اعضا به عهده کمیته امنیت اطلاعات می‌باشد ولی لازم است حداقل یک نفر از اعضا از بین افراد وابسته به نهاد متصدی حفاظت از امنیت فناوری اطلاعات و ارتباطات انتخاب شود.

تشکیل گروه CERT در کلیه مراجعی که از تجهیزات پردازشی برای ارائه یا تسهیل خدمات خود استفاده می‌کنند الزامی است. این گروه تحت مدیریت کمیته امنیت اطلاعات به فعالیت خواهد پرداخت.

• د-۳- پشتیبانی از گروه CERT

- لازم است گروه CERT از طریق زیر مورد پشتیبانی قرار گیرد:
- عضویت در نظام CERT کشوری یا هر نهاد CERT رسمی دیگری که از سوی دولت جمهوری اسلامی ایران به عنوان مرجع معتمد CERT معرفی خواهد شد.
 - تأمین نیازهای آموزشی
 - برقراری ارتباط با گروه‌های CERT سازمان‌های هم عرض یا سازمان‌هایی که دارای اشتراک منافع یا تشابه فعالیت می‌باشند.
 - پشتیبانی از دستورالعمل‌های اضطراری صادره توسط گروه CERT از طریق الزام واحدهای سازمان به رعایت آنها (به‌صورت موقت و در دوره زمانی که از طرف کمیته امنیت اطلاعات ضروری تشخیص داده می‌شود).

ه- گروه احیای سیستم

گروه احیای سیستم برای رهبری فعالیت‌های مقابله با حوادث عمده‌ای که باعث فروپاشی سیستم شده و یا بخش بزرگی از خدمات سازمان را با اختلال مواجه کند تشکیل می‌شود.

فعالیت گروه احیای سیستم بر اساس طرح از پیش تدوین شده پیوستگی عملیات ((BCP)^۵ انجام می‌پذیرد. (دستورالعمل تدوین طرح پیوستگی عملیات ((BCP متعاقباً ابلاغ خواهد شد). اعضای گروه احیای سیستم باید توانایی کار در شرایط بحرانی و تنش‌های عصبی را داشته و دارای قدرت فرماندهی و مدیریت باشند.

از آن‌جا که ممکن است حوادث عمده باعث صدمه به نیروی انسانی در اختیار سازمان شوند، لازم است افرادی به عنوان افراد جایگزین اعضای گروه احیای سیستم شناسایی شده و در دسترس باشند. به علاوه لازم است حتی الامکان از طریق عقد موافقت‌نامه‌های دو یا چند جانبه با سایر سازمان‌های مشابه مستقر در محل یا سازمان‌های مستقر در استان‌های دیگر گروه‌های مشترک احیای سیستم تشکیل داده شود تا بتوانند در شرایط بسیار دشوار مانند زلزله یا تخریب‌های گسترده در سطح منطقه به یاری یکدیگر بشتابند.

گروه احیای سیستم تحت مدیریت (((بالاترین مقام اجرایی سازمان))) و در هماهنگی با نهاد متصدی امنیت اطلاعات و گروه CERT فعالیت می‌نماید.

مسئولیت تهیه طرح BCP به عهده دبیرخانه امنیت اطلاعات می‌باشد.

لازم است مکانیزم آغاز اجرای طرح BCP از قبل تعریف شده و در هنگام بروز حوادث عمده به صورت خودکار به اجرا گذاشته شود. به عبارت دیگر نباید اعضای گروه احیای سیستم برای اجرای طرح BCP منتظر درخواست سازمان بمانند، بلکه باید در صورت وقوع شرایط خاص (مثل وقوع زلزله بیش از ۴/۵ ریشتر یا هر شدت دیگری که توسط سازمان آتش نشانی یا ستاد مقابله با حوادث پیش بینی نشده و یا سازمان پدافند غیرعامل تعیین می‌شود) اجرای طرح را آغاز نمایند.

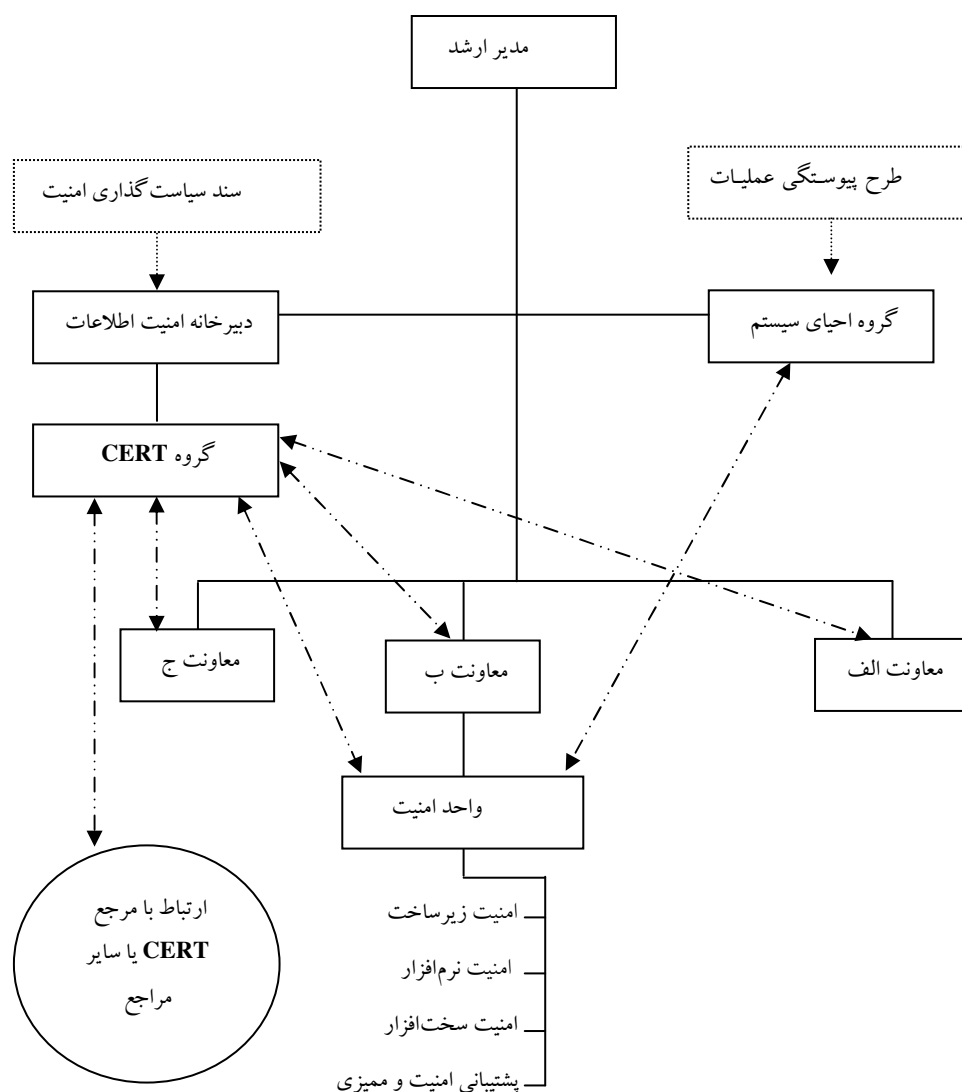
لازم است در طرح BCP به رهنمودهای مراجع ذیصلاح مثل سازمان پدافند غیرعامل و یا آتش نشانی توجه کامل شود.

مأموریت اصلی گروه احیای سیستم در درجه اول حفظ جان افراد اعم از کادر سازمانی و یا سایر شهروندان می‌باشد.

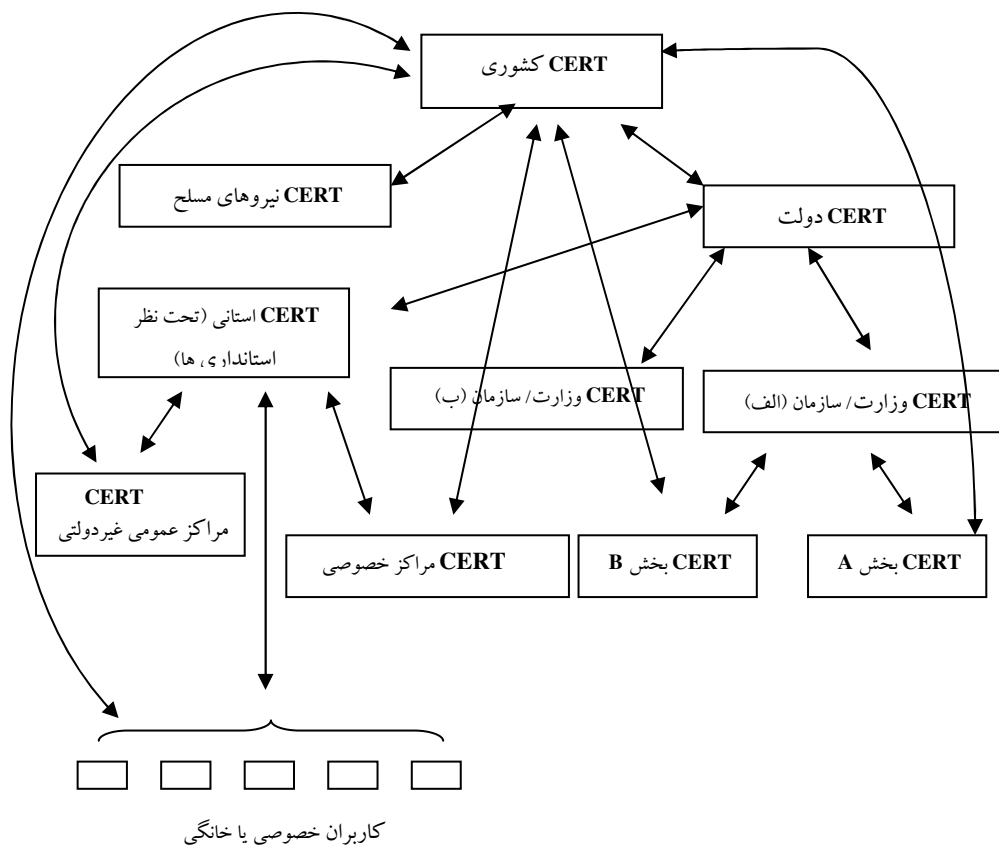
⁵ Business Continuity Plan

و- روابط و ارتباطات درونی مراجع مرتبط با امنیت فناوری اطلاعات و ارتباطات

در نمودارهای زیر نحوه ارتباط و سلسله مراتب مراجع مرتبط با امنیت فناوری اطلاعات و ارتباطات سازمانی و فرا سازمانی نشان داده شده است:



نمودار یک- ارتباطات (درون سازمانی) و ساختار پایه (سلسله مراتبی) برای نهادهای مرتبط با امنیت فناوری اطلاعات و ارتباطات



نمودار دو- نظام ارتباطی و اطلاع رسانی CERT در سطح کشور

مرجع

این دستورالعمل به شماره □-□/۲-۱-۲/□-□ به ثبت رسیده است و سایر مراجع مرتبط با این

دستورالعمل عبارت‌اند از:

دستورالعمل ۱-۱-۱

دستورالعمل ۴-۱-۲

دستورالعمل ۳-۲-۲

دستورالعمل ۱-۱-۳

دستورالعمل ۱-۲-۳

دستورالعمل ۲-۲-۳

دستورالعمل ۱-۳-۳

دستورالعمل ۲-۳-۳

دستورالعمل ۳-۳-۳

دستورالعمل ۴-۳-۳

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی
تعیین مسئولیت در حوزه امنیت اطلاعات شماره دستورالعمل : ۳-۱-۲	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود. سایر اسنادی که بر اساس این سند تولید می‌شوند دارای طبقه‌بندی حفاظتی متناظر با حوزه اجرای خود خواهند بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل بیان ضرورت تفکیک وظایف، تعریف حوزه اختیارات و تعیین مسئولیت هر یک از افراد یا بخش‌های سازمان در حفظ امنیت دارایی‌های اطلاعاتی می‌باشد.

مسئولیت اجرای این سند

نظارت بر پیاده‌سازی مفاد این سند بر عهده کمیته امنیت اطلاعات می‌باشد. اجرای مفاد این سند جز وظایف نهاد متولی حفظ امنیت اطلاعات (به عنوان مثال مرکز حراست فناوری اطلاعات و ارتباطات که در دستگاه‌های دولتی تشکیل خواهد شد می‌باشد). در صورتی که واحد مستقل یا مجزایی برای حفاظت از امنیت اطلاعات در سازمان وجود نداشته باشد مسئولیت اجرای این سند به عهده بالاترین رده اجرایی متولی فعالیت‌های پردازشی سازمان (به عنوان مثال مرکز کامپیوتر، مرکز پردازش داده‌ها، واحد انفورماتیک و...) خواهد بود.

الزامات

لازم است فهرست موجودی دارایی‌های اطلاعاتی (موضوع دستورالعمل ۱-۳-۱) به عنوان مرجع شناسایی دارایی‌های اطلاعاتی سازمان مبنای تعیین مسئولیت قرار گیرد. لازم است هر یک از دارایی‌های تقویم شده در فهرست موجودی دارایی‌های اطلاعاتی به یک نفر تحویل داده شود. به طوری که هر فرد به طور مشخص بداند مسئولیت حفاظت از کدام دارایی را به عهده دارد. تحویل بیش از یک دارایی به یک نفر بلامانع است اما تحویل یک دارایی به بیش از یک نفر ممنوع می‌باشد. حتی الامکان مسئولیت حفاظت از هر دارایی اطلاعاتی به استفاده کننده اصلی همان دارایی سپرده شود.

در شرایطی که ارائه یک سرویس از طریق به کارگیری مجموعه‌ای از دارایی‌های اطلاعاتی امکانپذیر می‌شود لازم است فردی خاص به عنوان متصدی سرویس انتخاب شده و مسئولیت حفاظت از امنیت آن سرویس به وی سپرده شود. در این حالت می‌توان این مسئولیت را به عهده شخصی سپرد که مسئول حفاظت از دارایی اطلاعاتی است که بیشترین نقش در ارائه سرویس را به عهده دارد.

لازم است قبل از سپردن مسئولیت به هر فرد در هر زمینه، وظایف مختلف از یکدیگر تفکیک شده و اختیارات لازم برای ایفای آن وظایف به وی تفویض شود بنحوی که از دخالت بی مورد افراد

در کار یکدیگر به بهانه انجام مسئولیت و همچنین بی توجهی به دارایی‌های اطلاعاتی در اختیار خود به دلیل عدم وجود اختیارات کافی جلوگیری شود.

در صورت لزوم باید شرح وظایف افراد و شرایط احراز شغل مورد بازبینی قرار گرفته و مسئولیت‌های ناشی از تحویل گرفتن دارایی‌های اطلاعاتی و مهارت‌های لازم جهت اجرای وظایف ناشی از آن لحاظ گردد.

لازم است آموزش‌های لازم در خصوص چگونگی استفاده صحیح و حفاظت از دارایی‌های اطلاعاتی در اختیار فرد تحویل گیرنده و سایر افراد دخیل در کار با دارایی‌های اطلاعاتی گذاشته شود.

لازم است مسئولیت جمعی حفاظت از دارایی‌های اطلاعاتی به کلیه افراد و کارکنان سازمان گوشزد گردد. به‌طوری‌که کلیه افراد خود را در قبال امنیت کلی دارایی‌های اطلاعاتی سازمان مسئول بدانند.

فرآیند

به‌طور کلی تفکیک وظایف، تعیین حوزه اختیار، تفویض اختیار و تعیین مسئولیت، اصول مدیریت و رفتار سازمانی را تشکیل می‌دهند. این اصول در حوزه مدیریت امنیت اطلاعات نیز جاری و صادق هستند. باید توجه داشت که ایجاد نهادهای متصدی امنیت اطلاعات (مثل کمیته امنیت اطلاعات و مرکز حراست فناوری اطلاعات) و سپردن فعالیت‌های امنیت اطلاعات به ایشان رافع مسئولیت سایر افراد سازمان در حفظ امنیت اطلاعات و دارایی‌های اطلاعاتی نمی‌باشد.

حفاظت از امنیت دارایی‌های اطلاعاتی هر سازمان به عهده تک تک افراد سازمان می‌باشد. در صورتی‌که سپردن برخی از فعالیت‌های سازمان یا تأمین نیازهای آن و یا حتی ارائه بخشی از خدمات به ارباب رجوع یا مشتریان مستلزم برون سپاری یا استفاده از خدمات پیمانکاری باشد نیز باید به مسئولیت پذیری در زمینه حفظ امنیت اطلاعات توجه کامل نمود و پیمانکاران و افراد تحت مدیریت ایشان را نیز ملزم به رعایت الزامات امنیتی نموده و ضمن تعیین مسئولیت ایشان تضمین‌های لازم را از طریق درج مواد لازم در قراردادهای فی مابین از ایشان اخذ نمود. (دستورالعمل‌های ۱-۲-۲ و ۳-۲-۲). همچنین باید حوزه مسئولیت ارباب رجوع و مشتریان نیز مورد مطالعه قرار گرفته و در صورت نیاز راهنمایی‌های لازم را به ایشان ارائه و حوزه مسئولیت شان را تعریف و ابلاغ نمود (دستورالعمل ۲-۲-۲).

اصولاً باید توجه داشت که موضوع امنیت اطلاعات موضوعی جدا از فعالیت‌های جاری سازمان نیست. هر سیستمی که بدرستی طراحی و به کار گرفته شود سیستمی امن خواهد بود، به عبارت دیگر اگر سیستمی امن نباشد می‌توان نتیجه گرفت که طراحی یا به کارگیری آن صحیح نبوده است.

مرجع

این دستورالعمل به شماره ۳-۱-۲ به ثبت رسیده و سایر مراجع مرتبط با این دستورالعمل عبارت‌اند از:

دستورالعمل ۱-۲-۲

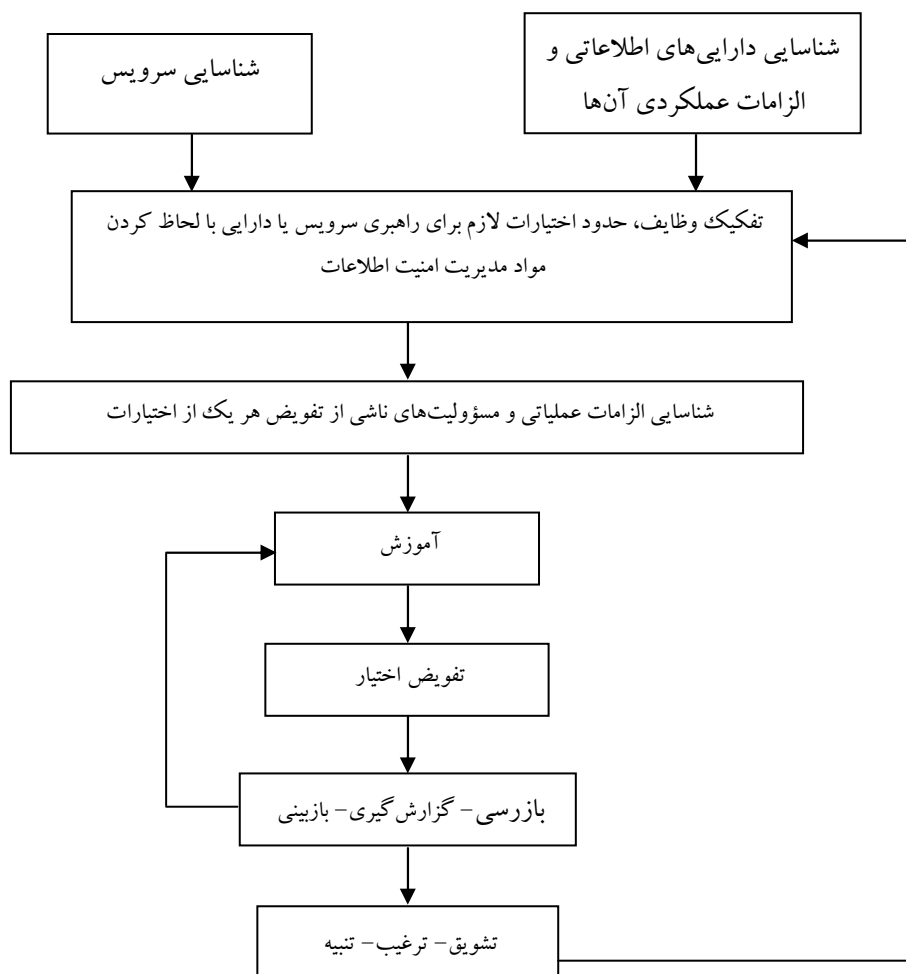
دستورالعمل ۲-۲-۲

دستورالعمل ۳-۲-۲

دستورالعمل ۱-۱-۳

روند نما

روند نمای تفکیک وظایف و تعیین مسئولیت در شکل زیر نشان داده شده است.



(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی
صدور مجوز استفاده از تجهیزات پردازشی اطلاعات شماره دستورالعمل : ۴-۱-۲	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند عادی طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

کلیه مجوزهای صادره بر اساس این دستورالعمل محرمانه تلقی خواهد شد.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	مدیر*
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان مدیر منصوب خواهد شد.

سوابق تغییرات:

تاریخ	شرح

هدف

طراحی فرآیند مدیریتی صدور مجوز استفاده از تجهیزات یا دارایی‌های اطلاعاتی یا تبادل اطلاعات

الزامات

لازم است کلیه دارایی‌های اطلاعاتی قبل از به کارگیری در شبکه‌ها یا سیستم‌های پردازشی و یا استفاده جهت ذخیره‌سازی یا تبادل اطلاعات از دیدگاه مدیریت امنیت اطلاعات مورد بررسی قرار گرفته و پس از تحلیل ریسک مجوز استفاده از آن‌ها صادر شود.

لازم است در کلیه مجوزها به نام فرد تحویل گیرنده (که مسئولیت حفاظت از دارایی به وی سپرده می‌شود) و محل استفاده اشاره شود (دستورالعمل ۳-۱-۲)

- در سازمان‌ها، نهادها یا تأسیساتی که از سوی سازمان پدافند غیرعامل تحت عنوان حساس و حیاتی دسته‌بندی می‌شوند لازم است مدت زمان استفاده از تجهیزات نیز در مجوز مربوطه درج گردد.

- در سازمان‌ها، نهادها یا تأسیساتی که از سوی سازمان پدافند غیرعامل تحت عنوان حیاتی دسته‌بندی می‌شوند لازم است در مجوز استفاده به شرایط محیطی محل نگهداری دارایی اطلاعاتی از قبیل میزان مقاومت محل در مقابل انفجار یا حمله‌های الکترومغناطیسی، زلزله، طوفان، سیل و ... اشاره شود. (دستورالعمل ۷-۶-۲).

- در خصوص دارایی‌های اطلاعاتی که دارای طبقه‌بندی محرمانه یا خیلی محرمانه هستند و یا در مراکز حساس یا حیاتی به کار گرفته می‌شوند لازم است در مجوز استفاده به نظام کنترل دسترسی مورد نیاز نیز اشاره شود. (دستورالعمل‌های ۷-۱-۱ و ۷-۲-۲)

فرآیند

طراحی فرآیند مدیریتی مجوزدهی (صدور مجوز بهره‌برداری) تجهیزات پردازش اطلاعات یا ایجاد کانال‌های ارتباطی، بخشی مهم از ایجاد رویه‌های امن به کارگیری دارایی‌های اطلاعاتی می‌باشد. در طراحی این فرآیند باید کنترل‌های زیر مد نظر قرار گیرد:

الف- تجهیزات جدید باید از نظر مدیریت کاربری، دلیل و روش استفاده و همچنین ریسک‌های مرتبط با استفاده از آن مورد بررسی قرار گیرند.

ب- لازم است مسئولیت بهره‌برداری و حفاظت از دارایی به فرد خاصی واگذار شود.

ج- لازم است عملکرد، سازگاری و انطباق سخت‌افزاری و نرم‌افزاری دارایی جدید با دارایی‌های موجود و یا سایر اجزای سیستم مورد بررسی قرار گیرد.

د- لازم است سیستم‌های تشخیص هویت یا کنترل دسترسی با دقت بیشتری مورد بررسی قرار گیرند و در صورت لزوم تأییدیه‌ها و گواهی‌نامه‌های مربوط از تامین کننده درخواست شود.

ه- در صورتی که دارایی اطلاعاتی در حوزه‌های رمزنگاری یا رمزگشایی مورد استفاده قرار می‌گیرد ترجیحاً باید از محصولات داخلی (دارای تأییدیه از نهادهای مربوط) و یا در درجه بعد از تجهیزات غیر آمریکایی و در صورت ضرورت از تجهیزات آمریکایی که عدم وجود حفره‌ها یا Back Doorهای امنیتی در آنها به اثبات رسیده است استفاده شود.

و- حتی الامکان در نقاط مرزی شبکه‌ها (نقاطی که از طریق آنها ارتباط با اینترنت یا سایر شبکه‌های خارج از سازمان برقرار می‌شود) از تجهیزات غیر هم نام با تجهیزات مسیریابی داخل شبکه استفاده شود.

اسناد مرجع

این سند به شماره □-□/۴-۱-۲/□-□ به ثبت رسیده و سایر اسناد مرتبط با این سند عبارت‌اند از:

دستورالعمل ۲-۱-۳

دستورالعمل ۱-۱-۷

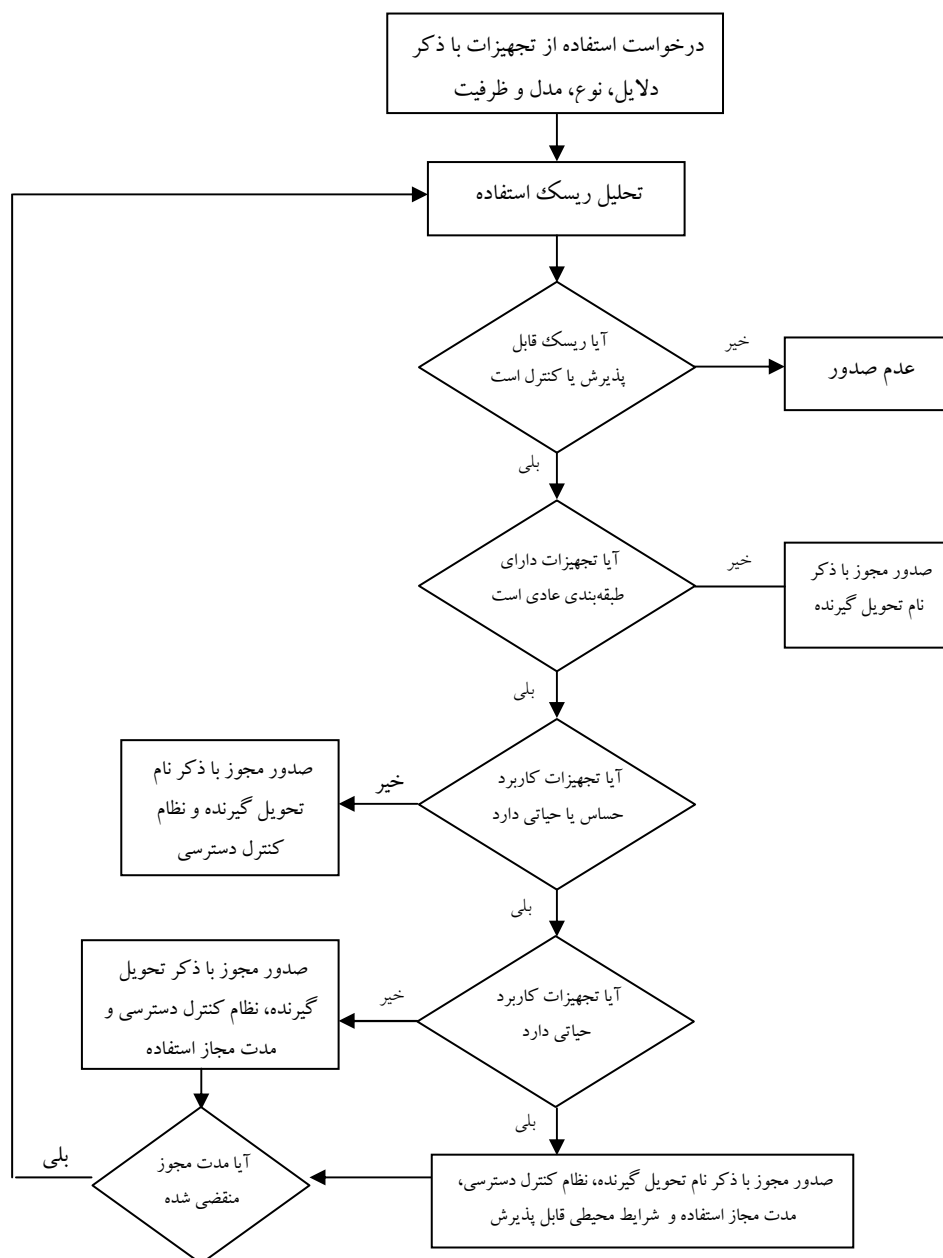
دستورالعمل ۲-۲-۷

دستورالعمل ۲-۶-۷

روند نما

روند نمای صدور مجوز استفاده از تجهیزات (بهره‌برداری) در شکل زیر نمایش داده شده است.

توضیح: منظور از تجهیزات هر گونه دارایی اطلاعاتی اعم از سخت‌افزار، نرم‌افزار، کانال‌های ارتباطی یا تأسیسات پشتیبانی می‌باشد.



(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی
توافق نامه‌های حفظ محرمانگی شماره دستورالعمل : ۵-۱-۲	

عادی

تائیدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند عادی طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود. کلیه توافق نامه‌هایی که بر اساس این سند تنظیم می‌شوند دارای طبقه‌بندی محرمانه می‌باشند مگر آنکه در متن آن ترتیب دیگری اتخاذ شده باشد.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات:

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل تأمین امنیت و حفظ محرمانگی اطلاعات هنگام ارجاع کار (پردازش اطلاعات یا فعالیت‌های مرتبط با آن) به مراجع خارج با از سازمان استفاده از روش عقد موافقت‌نامه‌های دو یا چند جانبه همکاری می‌باشد.

مسئولیت‌ها

مسئولیت پیشنهاد الزامات رعایت امنیت همکاری‌های فراسازمانی با واحد متصدی حفظ امنیت اطلاعات و تصویب آن به عهده کمیته امنیت اطلاعات می‌باشد. مسئولیت درج این الزامات در قراردادهای به عهده واحد حقوقی سازمان و در صورت عدم وجود آن با امضاء کننده نهایی قرارداد یا موافقت‌نامه می‌باشد.

الزامات

لازم است هنگام قرارداد ارجاع کار (اعم از پیمانکاری، تأمین نیروی انسانی، تأمین تجهیزات، تأمین کانال‌های ارتباطی، تأمین فضا در اینترنت، خرید خدمات، تأمین سایت پشتیبان و غیره) به الزامات حفظ محرمانگی و امنیت اطلاعات از سوی پیمانکار یا افراد وابسته به وی، توجه شده و مواد مربوط به آن از طریق درج در قرارداد یا ضمايم و پیوست‌های فنی آن گنجانده شود. هر یک از قراردادهای مرتبط با فعالیت‌های پردازشی باید منظم به پیوست موافقت‌نامه سطح خدمات ((SLA⁶ باشد.

- مواد مرتبط با حفظ امنیت اطلاعات که باید در متن قرارداد به آن‌ها اشاره شود عبارت‌اند از:
- رعایت طبقه‌بندی حفاظتی داده‌ها، اطلاعات، مکان‌ها و تجهیزاتی که در اجرای قرارداد در اختیار پیمانکار قرار می‌گیرند.
- شمول افرادی که به دلیل ارتباط با پیمانکار با داده‌ها، اطلاعات، مکان‌ها و تجهیزات در اختیار پیمانکار سر و کار دارند در رعایت طبقه‌بندی‌های حفاظتی (اعم از افراد در

⁶ Service Level Agreement

استخدام پیمانکار و یا پیمانکاران دست دوم و یا هر نهاد و مرجعی که پیمانکار با وی در ارتباط است).

- روش‌های فیزیکی و منطقی که پیمانکار باید برای حفظ محرمانگی و امنیت اطلاعات به کار گیرد.
- چگونگی تضمین ادامه ارائه خدمات هنگام وقوع شرایط اضطراری یا حمله‌های رایانه‌ای

- نوع تضمین سپرده شده برای جبران خسارت‌های مرتبط با امنیت اطلاعات
 - حقوق ممیزی کارفرما و پیمانکار بر اساس SLA و سایر بندها یا مواد قرارداد
- در صورتی که روابط بین طرفین دارای ماهیت تجاری نباشد لازم است از موافقت‌نامه‌های حفظ محرمانگی که واجد شرایط فوق است استفاده شود. در آن حالت به جای استفاده از لفظ کارفرما و پیمانکار از واژه‌های مناسب استفاده خواهد شد. اما در هر صورت باید مسئولیت حقوقی طرفین در حفظ امنیت اطلاعات و چگونگی جبران زیان‌های ناشی از عدم رعایت الزامات مربوط تعیین گردد. لازم است در توافق نامه حفظ محرمانگی روش و الزامات امحا و انهدام اطلاعات یا اسناد بر اساس درخواست تولید کننده سند یا داده درج و تضمین‌های لازم برای اجرای آن لحاظ گردد.

فرآیند

فرآیند عقد قرارداد و موافقت‌نامه‌های دو یا چند جانبه معمولاً شامل تهیه پیش نویس توسط واحد متقاضی عقد قرارداد، بررسی توسط مرجع حقوقی، بررسی توسط مرجع مالی و امضاء توسط بالاترین مقام اجرایی می‌باشد.

از آنجا که بسیاری از قراردادها یا موافقت‌نامه‌های موجود در زمینه دسترسی به دارایی‌های اطلاعاتی یا تجهیزات پردازشی معمولاً منجر به دسترسی افراد یا مراجع خارج سازمان به اطلاعات طبقه‌بندی شده درون سازمانی می‌گردند، لازم است در کلیه قراردادها یا موافقت‌نامه‌های مربوط شروط و مواد مربوط به حفظ امنیت اطلاعات و عدم افشای اطلاعات گنجانیده شده و تضمین‌های لازم برای رعایت آن کسب شود.

در صورتی که رابطه بین طرفین مستلزم انجام فعالیت‌های تجاری باشد، لازم است قبل از عقد هر گونه قرارداد تجاری موافقت‌نامه عدم افشا (NDA)^۷ به امضای طرفین برسد و عقد قرارداد منوط به وجود موافقت‌نامه عدم افشای امضاء شده باشد. دلیل این موضوع آن است که ممکن است پیمانکار برای ارائه برآورد از رقم انجام کار نیاز به دسترسی به اطلاعات طبقه‌بندی شده و یا مصاحبه با افرادی داشته باشد که اطلاعات حوزه کاری آن‌ها دارای طبقه‌بندی حفاظتی می‌باشد.

اسناد مرجع

این سند به شماره □-□/□-۱-۲/□-□ ثبت شده و اسناد مرتبط با آن عبارت‌اند از:

دستورالعمل ۱-۲-۲

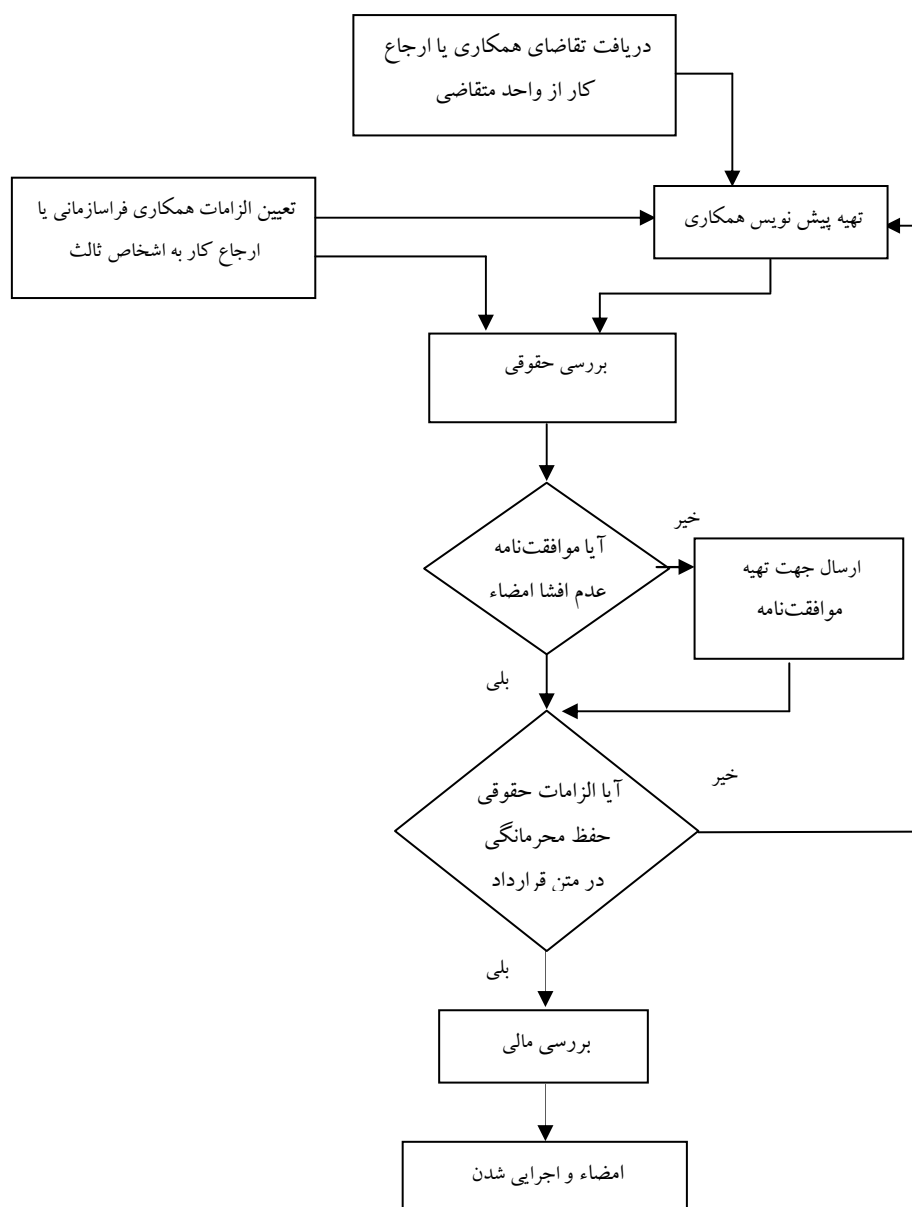
دستورالعمل ۳-۲-۲

دستورالعمل ۱-۱-۷

⁷ Non Disclosure Agreement

روند نما

روند نمای عقد موافقت‌نامه‌های حفظ محرمانگی در شکل زیر نمایش داده شده است.



(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی
برقراری ارتباط با مراجع حکومتی شماره دستورالعمل : ۶-۱-۲	

عادی

تائیدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود. طبقه‌بندی اسناد تولید شده بر اساس این سند تابع سطح طبقه‌بندی حفاظتی سازمان متبوع خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	ریس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	دبیر*
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل تبیین الزام و چگونگی ارتباط با مراجع حکومتی می‌باشد.

مسئولیت

مسئولیت اجرای مفاد این سازمان به عهده نهاد متصدی حفاظت از امنیت دارایی‌های اطلاعاتی (به عنوان مثال مرکز حراست فناوری‌های اطلاعاتی یا ارتباطی) می‌باشد.

الزامات

لازم است کلیه نهادهای حکومتی که بنحوی در خصوص فعالیت‌های پردازش اطلاعات دارای مرجعیت قانونی هستند شناسایی شده و در خصوص چگونگی برقراری ارتباط با ایشان برنامه‌ریزی شود. فهرست عمومی این نهادها و زمینه‌های مرتبط با فعالیت آن‌ها به شرح زیر است:

ردیف	مرجع	حوزه فعالیت
۱	شورای عالی امنیت فضای تبادل اطلاعات	تعیین راهبردها و تدوین اسناد راهبردی در زمینه امنیت فناوری اطلاعات
۲	سازمان پدافند غیرعامل	تدوین اسناد راهبردی دفاع غیرنظامی و تقویت فعالیت‌های مربوط به آن
۳	وزارت اطلاعات	تعریف و شرح وظایف نهاد یا مراکز متصدی حفاظت فناوری‌های اطلاعات و ارتباطات در مراکز دولتی
۴	سازمان آتش نشانی	نظارت بر مکانیزم‌های مقابله با خطر و کمک رسانی در مواقع ضروری
۵	مرکز عملیات امنیتی (SOC) کشوری	تحت نظر قرارداد روند وقایع و حوادث امنیت فناوری‌های اطلاعاتی و ارتباطی و راهبری دفاع رایانه‌ای
۶	CERT کشوری	تولید پاسخ‌های امنیتی در مواقع بروز شرایط اضطراری رایان‌های
۷	نیروی انتظامی و قوه قضائیه	رسیدگی به شکوائیه‌ها، دعاوی و صدور احکام لازم الاجرا
۸	سازمان تنظیم مقررات و ارتباطات رادیویی	تدوین مقررات و نظارت بر تعامل و عملکرد نهادهای مرتبط با پردازش اطلاعات و انتقال داده‌ها

نهادهای موضوع بندهای ۵ و ۶ جدول فوق در حال تشکیل می‌باشند.

فرآیند

با گسترش روز افزون فعالیت‌های پردازشی و متصل شدن شبکه‌های اطلاعاتی به یکدیگر چالش‌های جدیدی در مقابل کلیه سازمان‌های بهره‌بردار از تجهیزات پردازشی و کانال‌های ارتباطی پیش آمده است. پیامدهای این وضعیت را می‌توان به شرح زیر فهرست کرد:

- کاهش تدریجی سوابق کاغذی و عملیات دستی که افراد در انجام آن‌ها دخالت دارند.
- سهولت دسترسی به اطلاعات فردی، تجاری، سازمانی که برخی از آن‌ها محرمانه تلقی می‌شوند.
- تمرکز سوابق انجام فعالیت‌ها یا تبادل اطلاعات در مراکز خاص (تحت عنوان مرکز داده)
- بدیهی است پیامدهای فوق می‌توانند علاوه بر اثرات مثبت فراوان عواقب زیر را به دنبال داشته باشند:
- انجام عملیات به صورت اشتباه و بدون آگاهی افرادی که می‌توانند سریعاً از بروز آن جلوگیری نمایند.
- افشاء اطلاعات فردی، تجاری یا سازمانی نزد افراد یا مراجع غیر مجاز یا سوء استفاده از آن
- انهدام سوابق انجام فعالیت‌ها یا تبادل‌ها (اعم از مالی یا اطلاعاتی) به دلیل نقص در کار مراکز داده یا تجهیزات ذخیره‌سازی

بنابراین لازم است:

- اولاً نسبت به ریسک‌های ناشی از بهره‌برداری از تجهیزات پردازشی و روش‌های مقابله با آن‌ها آگاه بود.
- ثانیاً در صورت وقوع وقایع یا حوادث رایانه‌ای به سرعت نسبت به آن‌ها واکنش نشان داده و از بروز مشکل جلوگیری کرده و یا آن را به حداقل رسانید.
- ثالثاً در صورت لطمه به توان پردازشی سازمان یا افشاء اطلاعات محرمانه نسبت به اقامه دعوا از طریق ارائه مدارک و مستندات محکمه پسند اقدام نمود.

⁸ اسنادی که توسط محاکم قضایی قابل پذیرش باشند. در صورت الکترونیک بودن این اسناد لازم است از طریق نظام صدور گواهی رسمی و زیرساخت کلید عمومی (PKI/CA) پشتیبانی شده باشند.

- رابعاً در صورت اقامه دعوا از طرف افراد یا مراجع دیگر علیه سازمان با استفاده از مدارک، دلایل و مستندات محکمه پسند به دفاع از سازمان پرداخت.

بنابراین می‌توان از طریق برقراری ارتباط مستمر و مؤثر با مراجع حکومتی اولاً به‌طور کامل از روند حوادث و وقایع امنیت اطلاعات آگاهی یافته و از پشتیبانی ایشان در دفاع از دارایی‌های اطلاعاتی بهره برد و ثانیاً با توجه به مشروعیت قانونی این نهادها ضمن عمل به توصیه‌ها، مقررات و قوانین تصویب شده توسط ایشان نسبت به جلوگیری از انحراف فعالیت‌های سازمان از مرزهای قانونی اقدام و از پشتیبانی ایشان در مقابله با فعالیت‌های قانون شکنانه بهره گرفت.

اسناد مرجع

این سند به شماره □-□/۶-۱-۲/□-□ به ثبت رسیده است و سایر اسناد مرتبط با آن عبارت‌اند از:

دستورالعمل ۷-۱-۲

دستورالعمل ۲-۲-۲

دستورالعمل ۳-۲-۲

روند نما

این دستورالعمل فاقد روند نما می‌باشد.

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی
ارتباط با سایر مراجع، سازمان‌ها و نهادهای دارای اشتراک منافع شماره دستورالعمل : ۷-۱-۲	

عادی

تأییدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان))

عنوان: ((بالاترین مقام اجرایی سازمان))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار ((بالاترین مقام اجرایی سازمان))	رییس
	مسئول ((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات))	*دبیر
	معاون ((اداری، مالی و پشتیبانی))	عضو
	معاون ((برنامه ریزی))	عضو
	معاون ((فنی))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات ((معاون پشتیبانی)) سازمان به عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل تبیین ضرورت و روش ایجاد برقراری ارتباط با سایر نهادهایی است که دارای حوزه فعالیت مشترک یا اشتراک منافع با سازمان می‌باشند.

مسئولیت

مسئولیت اجرای این دستورالعمل به عهده نهاد متصدی حفاظت از امنیت اطلاعات (((وزارت/ سازمان/ اداره کل/ شرکت...))) می‌باشد.

موافقت‌نامه‌های تنظیم شده بر اساس این دستورالعمل باید به امضاء (((بالاترین مقام اجرایی))) برسد.

الزامات

- لازم است کلیه نهادهایی که دارای حوزه فعالیت مشترک با سازمان می‌باشند و یا ضمن انجام فعالیت‌های پردازشی و یا انتقال داده نیاز به استفاده از خدمات آن‌ها می‌باشد و یا مراجعه به آن‌ها ضروری است، شناسایی شده و پس از تحلیل ریسک تعامل با آن‌ها (بر اساس دستورالعمل ۲-۲-۱) در خصوص نحوه تعامل با ایشان تصمیم‌گیری شود.
- تصمیم‌گیری در خصوص نیاز به عقد موافقت‌نامه‌های دو یا چند جانبه با هر یک از مجموعه‌ها یا مجموعه‌ای از نهادهای فوق به عهده کمیته امنیت اطلاعات بر اساس تحلیل ریسک انجام شده توسط نهاد متصدی حفاظت از امنیت اطلاعات (((وزارت/ سازمان/ اداره کل/ شرکت...))) می‌باشد.
- در سازمان‌هایی که از طرف سازمان پدافند غیرعامل به عنوان سازمان حساس دسته‌بندی می‌شوند و خدمات مورد نیازشان توسط تأمین کننده‌ای ارائه می‌شود که خود خدمات را از تأمین کننده دیگری دریافت می‌کند، لازم است علاوه بر عقد قرارداد با تأمین کننده بلا واسطه، تضمین‌های لازم از تأمین کننده اصلی از طریق عقد موافقت‌نامه‌های مناسب اخذ شود (به عنوان مثال اگر طرف قرارداد شرکت‌های PAP یا SAP باشند لازم است تضمین‌های لازم از شرکت ارتباطات زیرساخت یا تأمین کننده ارتباطات ماهواره‌ای نیز اخذ گردد). در صورت عدم امکان اخذ این گونه تضمین‌ها عقد قرارداد با این شرکت‌ها ممنوع است.

- در سازمان‌هایی که از طرف سازمان پدافند غیرعامل به عنوان سازمان حیاتی دسته‌بندی می‌شوند، دریافت خدمات فقط از طریق عقد قرارداد با تأمین کننده اصلی مجاز است (به عبارت دیگر دریافت خدمات از طریق عقد قرارداد با واسطه ممنوع می‌باشد).
- الزام سازمان برای ارتباط با سایر مراجع ممکن است به دلیل الزام قانونی، الزام حرفه‌ای، الزام تجاری، الزام اجتماعی و یا الزام اخلاقی باشد. در هر صورت لازم است شرایط و تضمین‌های موافقت‌نامه یا قرارداد مربوط با توجه به نوع الزام و براساس آن تنظیم شود.

فرآیند

سازمان‌هایی که در یک حوزه مشترک فعالیت می‌کنند، معمولاً دارای مسائل مبتلابه مشابهی می‌باشند. دلایل این موضوع عبارت‌اند از:

- فعالیت تحت شرایط قانونی تقریباً مشابه
 - استفاده از نرم‌افزارها و سخت‌افزارها و کانال‌های ارتباطی تقریباً مشابه
 - هدف قرار گرفتن از سوی افراد بدخواه با انگیزه‌های تقریباً مشابه
- علاوه بر موارد فوق در صورت وجود قراردادهای تجاری منصفانه بین بهره‌بردار و تأمین کننده خدمات، بروز اشکالات پیش بینی نشده در فرآیند اجرای خدمات پردازشی موجب قطع ارائه خدمات (مثلاً پهنای باند ارتباطی) و زیان طرفین قرارداد خواهد شد. زیان بهره‌بردار عبارت خواهد بود از عدم رضایت مشتریان یا ارباب رجوع و زیان تأمین کننده عبارت است از عدم النفع به دلیل قطع ارائه خدمات یا پرداخت جریمه به دلیل عدم رعایت الزامات SLA^۹ (موافقت‌نامه سطح خدمات).

به علاوه ممکن است در برخی موارد انتقال و تبادل اطلاعات از طریق به‌جز عقد قرارداد تجاری انجام شود. در این حالت لازم است مواد توافق شده‌ای به عنوان قرارهای لازم الاجرا بین طرفین به اجرا گذاشته شود و در مواقع بروز اشکال یا اختلاف به آن‌ها مراجعه شود.

بنابراین در حالتی که ریسک حاصل از تعامل غیر تجاری (و یا تعامل تجاری که دارای پیامدهای غیر تجاری است) بیش از حد مجاز تعیین شده توسط کمیته امنیت اطلاعات تشخیص داده شود، لازم است جهت مدیریت ارتباط با سایر مراجع، سازمان‌ها یا نهادهای دارای اشتراک منافع از

^۹ Service Level Agreement

طریق عقد موافقت‌نامه‌های همکاری یا تبادل اطلاعات و تجربیات اقدام شود. ضمناً هر گونه تبدلی که منجر تبادل داده‌ها یا اطلاعات دارای طبقه‌بندی حفاظتی باشد فقط بعد از امضای موافقت‌نامه عدم افشاء مجاز خواهد بود.

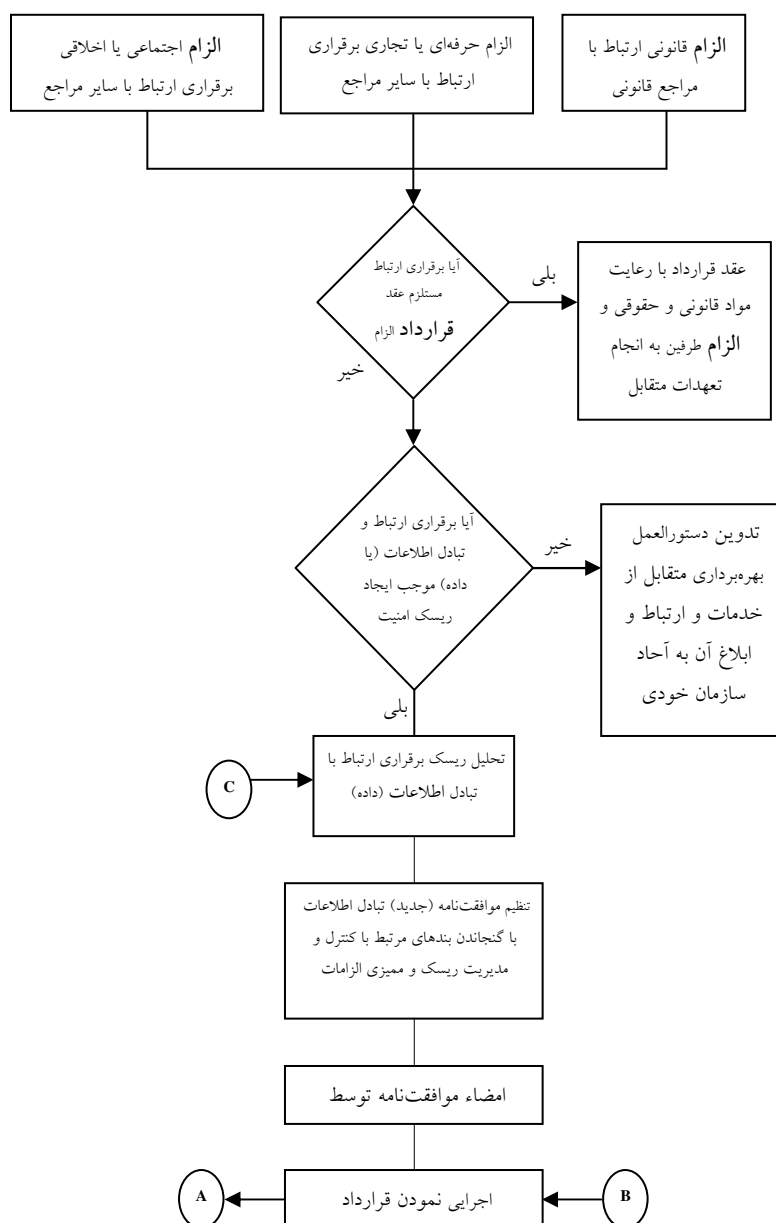
اسناد مرجع

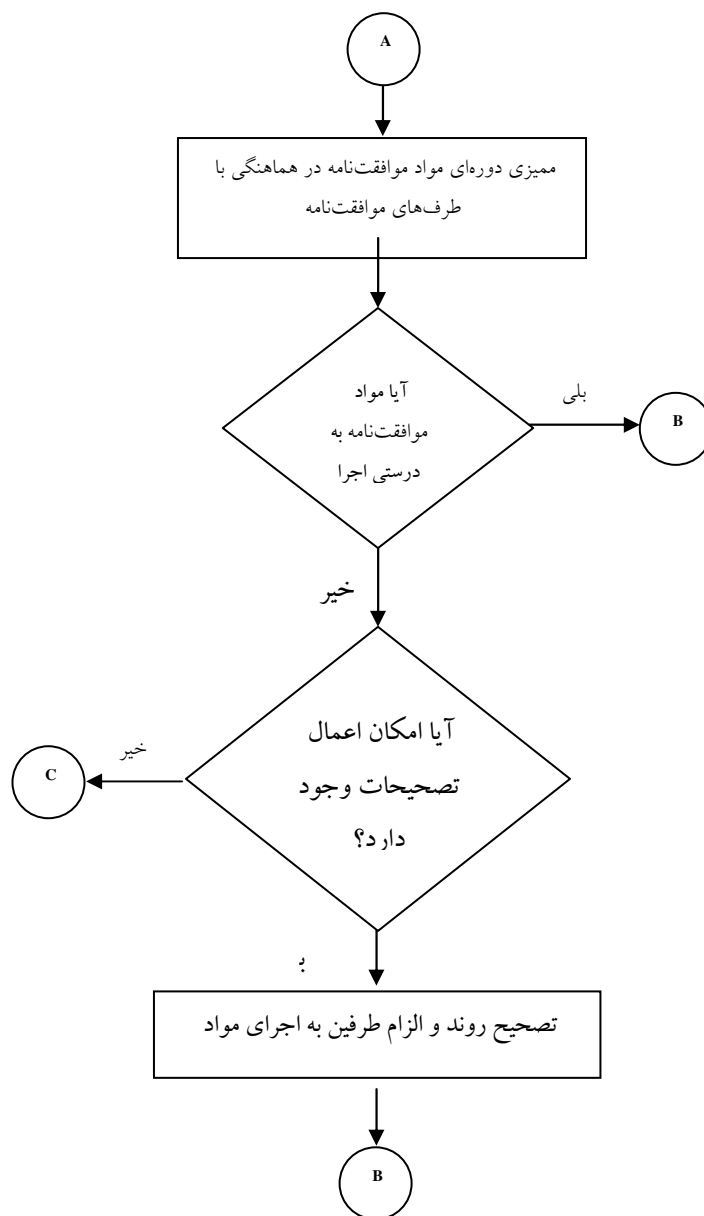
این سند به شماره □-□/۱-۲-۷-□-□ به ثبت رسیده و سایر اسناد مرتبط با این سند عبارت‌اند از:

دستورالعمل ۱-۲-۲

روند نما

روند نمای تعامل با سایر مراجع، سازمان‌ها یا نهادهای دارای اشتراک منافع با سازمان





(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	سازمان (دهی) درونی
بازنگری مستقل امنیت اطلاعات شماره دستورالعمل : ۸-۱-۲	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند عادی طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود. کلیه اسناد و گزارش‌هایی که بر اساس رهنمودهای این دستورالعمل تولید می‌شوند دارای طبقه‌بندی حفاظتی یک رده بالاتر از طبقه‌بندی دارای اطلاعاتی تحت ممیزی خواهند بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد

شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی انجام ممیزی مستقل انطباق اجرای فرآیندها و رویه‌های به کار گرفته شده در سامانه مدیریت امنیت با الزامات، فرآیندها و رویه‌های طراحی و تصویب شده بر اساس نظام استاندارد مرجع می‌باشد.

مسئولیت

- مسئولیت مدیریت فعالیت‌های ممیزی مستقل سامانه مدیریت امنیت اطلاعات به عهده کمیته امنیت می‌باشد.
- مسئولیت اجرای ممیزی‌های داخلی فعالیت‌های سامانه مدیریت امنیت اطلاعات به عهده نهاد متصدی حفاظت امنیت اطلاعات می‌باشد.
- هنگام اجرای ممیزی داخلی هیچ واحد یا بخشی از سازمان مجاز به ممیزی فعالیت‌های حوزه خود نمی‌باشد. در این حالت مسئولیت ممیزی از فعالیت‌های آن واحد از سوی کمیته امنیت اطلاعات به صورت مأموریت به عهده افراد دیگری گذاشته خواهد شد.
- لازم است ممیزی‌های مستقل به صورت دوره‌ای و بر اساس توصیه‌های ممیزی نظام استاندارد مرجع انجام شود. این گونه ممیزی‌ها باید توسط نهادهای مراکزی انجام شود که صلاحیت آن‌ها از سوی مراجع ذیصلاح (مثل نظام تأیید صلاحیت ایران) صحت‌گذاری شده باشد.

الزامات

- حتی‌الامکان لازم است ممیزی سامانه مدیریت امنیت اطلاعات بر اساس متدهای تعریف شده در استانداردهای پذیرفته شده امنیت اطلاعات (مانند استاندارد ISO-27001 یا BS-7799) انجام پذیرد.
- لازم است فعالیت‌های ممیزی به نحوی انجام شود که خود تبدیل به منبع تولید ریسک نگردد.
- حفاظت از گزارش‌های تولید شده در حین ممیزی ضروری است و این گزارش‌ها دارای سطح طبقه‌بندی حفاظتی یک رده بالاتر از سطح طبقه‌بندی دارایی اطلاعاتی ممیزی شده خواهند بود.
- در مراکزی که توسط سازمان پدافند غیرعامل به عنوان سازمان حساس دسته‌بندی شده‌اند، سپردن ممیزی به اتباع خارجی ممنوع است.
 - در مراکزی که توسط سازمان پدافند غیرعامل به عنوان مراکز حیاتی دسته‌بندی می‌شوند سپردن ممیزی به اتباع یا شرکت‌های خارجی ممنوع است.

در کلیه فعالیت‌های ممیزی اولاً لازم است استقلال ممیزی کننده به رسمیت شناخته شده و رعایت گردد و ثانیاً حقوق ممیزی شونده بر اساس مواد مندرج در منشور اخلاقی ممیزی (ضمیمه همین سند) رعایت گردد.

فرآیند

به علت طبیعت خاص ممیزی سیستم‌های اطلاعاتی و مهارت‌های ضروری بر انجام فعالیت‌های ممیزی در سامانه‌های پردازشی، استفاده از استانداردهای اختصاصی در ممیزی این سامانه‌ها ضروری است.

توجه به تعاریف زیر ضروری است:

- **استاندارد:** عبارت است از متنی منسجم و یکپارچه که الزامات و اصول برپایی یک سامانه (در این جا سامانه مدیریت امنیت اطلاعات) را بیان می‌نماید.
- **دستورالعمل:** رهنمودهای لازم در خصوص چگونگی اعمال و اجرای الزامات مندرج در متن استاندارد که حاوی نکات کلی و راهنمایی‌های اصولی در خصوص چگونگی اجرای فعالیت‌ها می‌باشد و می‌توان با توجه به ماهیت سازمان به کارگیرنده، نوع فعالیت و شرایط محیطی اجرا، نسبت به تغییر یا اصلاح متن آن اقدام نمود.
- **رویه:** عبارت است از بیان روش اجرایی انجام یک فرآیند خاص با استفاده از مثال یا تشریح قدم به قدم مراحل صحیح و قابل پذیرش روش انجام کار.

فعالیت ممیزی در سه قالب کلی قابل اجرا می‌باشد:

- ممیزی داخلی توسط افراد سازمان (ممیزی سطح اول)
- ممیزی فعالیت‌ها از طریق عقد قرارداد با پیمانکاران تخصصی امن‌سازی سامانه‌های اطلاعاتی (ممیزی سطح دوم)
- ممیزی فعالیت‌ها از طریق ارجاع به نهادهای ممیزی و صدور گواهی رسمی (ممیزی سطح سوم یا شخص ثالث)

در کلیه روش‌های فوق رعایت اصل استقلال ممیز ضروری است. در ممیزی سطح سوم یا شخص ثالث که توسط نهادهای رسمی ممیزی و صدور گواهی به اجرا گذاشته می‌شود به دلیل حرفه‌ای بودن ممیزان بهترین نتایج قابل کسب است. در این حالت تأثیر سوء ممیزی شونده بر ممیز بسیار ناچیز و قابل چشم پوشی می‌باشد.

در خصوص ممیزی‌های سطح دوم هر چند استقلال ممیز به دلیل وجود رابطه کاری بین پیمانکار و کارفرما قابل خدشه می‌باشد و به دلیل نیاز به استفاده از خدمات تخصصی ایشان و بررسی فنی وضعیت تجهیزات و دارایی‌های اطلاعاتی، استفاده دوره‌ای و تحت کنترل از این نوع فعالیت‌ها مفید به نظر می‌رسد. البته در این نوع فعالیت‌ها لازم است الزامات دستورالعمل ۱-۲-۲ (شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری) مورد توجه قرار گیرد. می‌توان از این نوع ممیزی برای آماده سازی شرایط برای ممیزی شخص سوم بهره برد.

ممیزی سطح اول (انجام ممیزی توسط افراد درون سازمان) به منظور آگاهی از چگونگی وضعیت اجرای فرآیندهای امنیت اطلاعات به عمل آمده و برای بهبود روش‌های انجام کار به اجراء گذاشته می‌شود. لازم است نتایج حاصل از این نوع ممیزی پس از بررسی و پالایش در اختیار ممیزی شونده قرار داده شود.

نکته‌ای که مجدداً بر آن تکیه می‌شود اصل استقلال ممیز است. در شرایطی که فعالیت ممیزی منجر به تهیه گزارش‌های رسمی شود، لازم است اصل استقلال ممیز با توجه به شرایط زیر مورد توجه قرار گیرد.

در صورت انجام فعالیت ممیزی بر اساس قرارداد، نباید پرداخت به ممیز وابسته به محتوی گزارش ممیزی باشد.

ممیز نباید در هیچ یک از مراحل یا بخش‌های فعالیت ممیزی به بررسی تجهیزات، خدمات یا فعالیت‌هایی بپردازد که از طرف خود او تأمین می‌شود.

فعالیت‌های ممیزی نباید در هیچ حالتی منجر به استفاده از تجهیزات، خدمات یا فعالیت‌های آتی شود که فقط توسط ممیز قابل ارائه است.

در صورتی که ممیز یا کارفرما در هر مرحله از فعالیت ممیزی مواجه با وضعیتی شوند که طی آن ممکن است شرایط نقض استقلال ممیز ایجاد شود باید فوراً فعالیت‌های ممیزی متوقف شده و شرایط نقض استقلال برطرف شود. اگر برطرف شدن شرایط نقض استقلال متوقف بر قطع فعالیت ممیز باشد، ادامه فعالیت ممیز ممنوع است. بنابراین لازم است قبلاً در قرارداد فی مابین نسبت به بروز این حالت پیش بینی به عمل آمده و راهکار آن اندیشیده شده باشد.

جدول ممیزی اجرای الزامات استاندارد ISO-27001 در بخش ضمیمه (ضمیمه دو) همین سند درج گردیده است.

مرجع

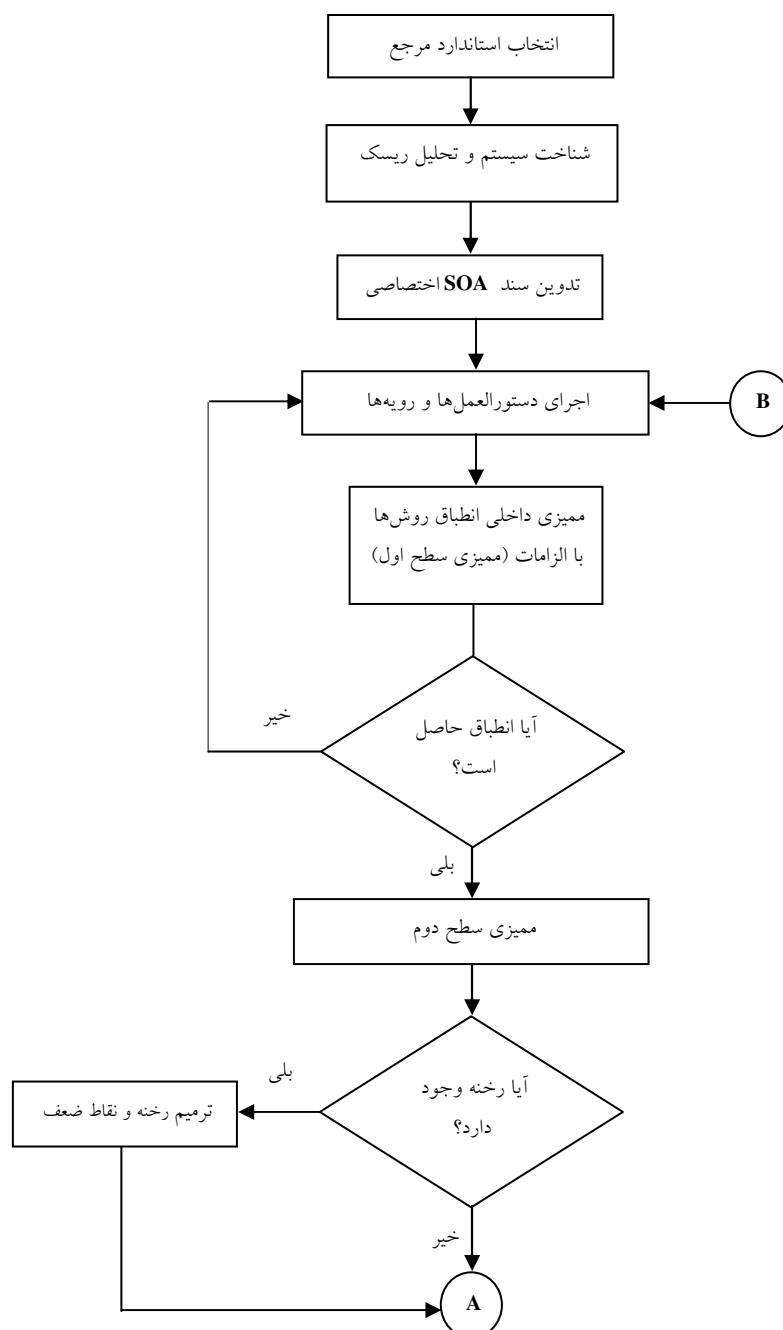
این سند به شماره □-□/۸-۱-۲/□-□ به ثبت رسیده و سایر اسناد مرتبط با این سند عبارت‌اند از:

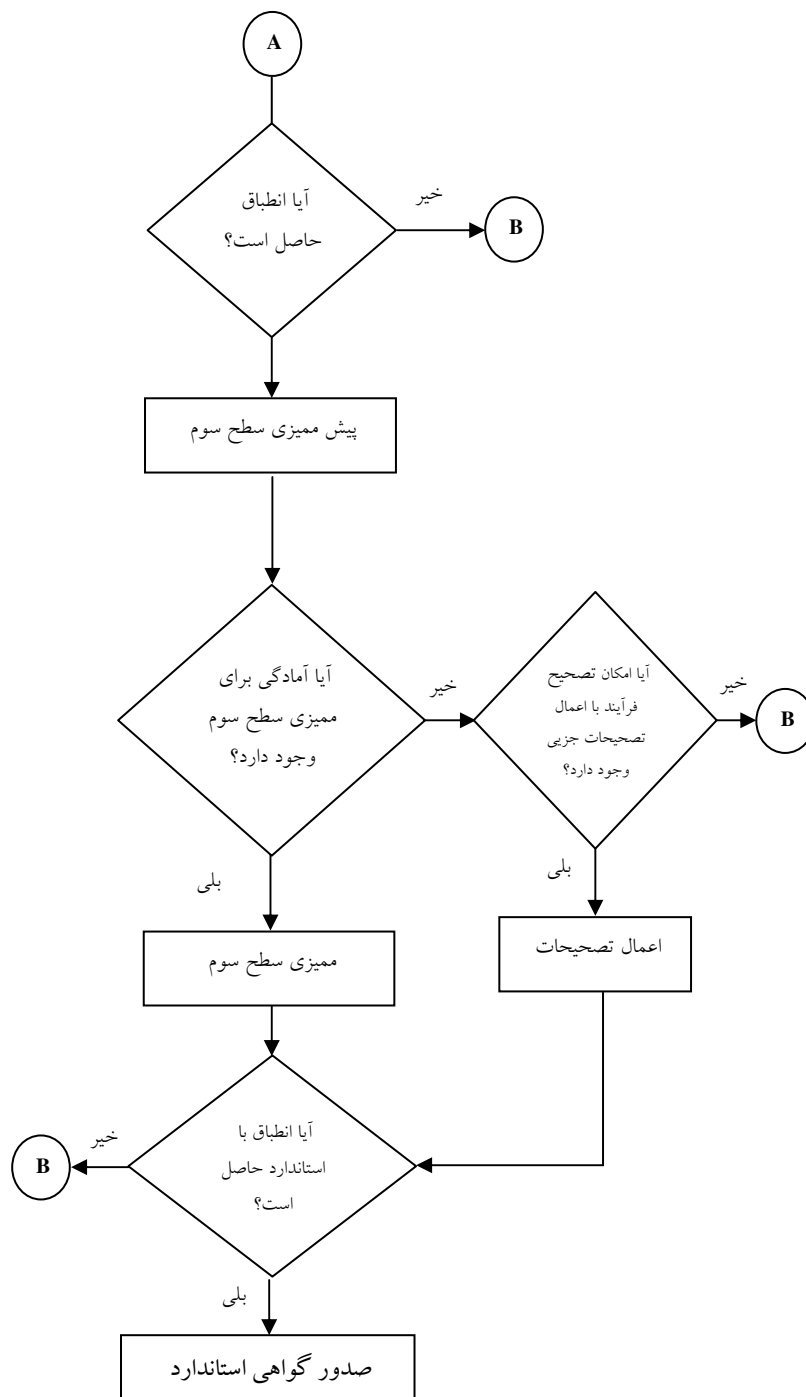
دستورالعمل ۱-۱-۱

دستورالعمل ۱-۲-۲

روند نما

روند نمای انجام فعالیت‌های ممیزی سیستم‌های مدیریت امنیت اطلاعات به شرح زیر می‌باشد.





ضمیمه یک منشور اخلاقی ممیزی

- کلیه افرادی که اقدام به ممیزی سیستم‌های اطلاعاتی می‌نمایند (اعم از ممیزی داخلی، ممیزی بر اساس قرارداد و یا ممیزی شخص ثالث) لازم است نکات اخلاقی زیر را رعایت نمایند:
- بر اساس استانداردها، دستورالعمل‌ها و رویه‌های تدوین و تصویب شده اقدام نموده و به کارگیری آن‌ها را تشویق نماید.
 - کوشا، صادق و امانت دار بوده و عمداً دست به فعالیت‌های غیر قانونی یا غیر اخلاقی نزنند.
 - خصوصی، محرمانه بودن و طبقه‌بندی حفاظتی اطلاعاتی را که به دلیل الزامات کاری در اختیار وی قرار می‌گیرد به‌طور کامل (مگر در هنگام درخواست مراجع قانونی و صلاحیت دار) رعایت نماید و از بهره‌برداری شخصی از آن اطلاعات جداً خودداری نماید.
 - وظایف خود را به‌صورت مستقل و هدفمند به انجام رسانده و از انجام فعالیت‌هایی که استقلال وی را خدشه دار می‌سازد و یا مظنون به خدشه به استقلال وی است خودداری نماید.
 - مهارت و شایستگی خود را در زمینه ممیزی سیستم‌های اطلاعاتی از طریق شرکت در دوره‌های آموزشی افزایش دهد.
 - فعالیت‌های خود را با توجه به اصول حرفه‌ای به انجام رساند.
 - نتایج ممیزی را فقط در اختیار افراد صلاحیت دار قرار دهد. به علاوه کلیه مواردی که عدم اطلاع از آن‌ها می‌تواند باعث ارائه گزارش‌های تحریف شده یا فعالیت‌های غیر قانونی شود را به اطلاع کارفرمای خود برساند.

ضمیمه دو

جدول اهداف و مکانیزم‌های کنترلی استاندارد ISO-27001:2005
(الزامات ممیزی)

ردیف	اهداف کنترلی	مکانیزم کنترلی	الزام اجرایی (دارد/ ندارد)	اجراء (شده/ نشده)
A.5	Security policy			
A.5.1	Information security Policy	A.5.1.1 Information security policy document		
		A.5.1.2 Review of the information Security policy.		
A.6	Organization of information security			
A.6.1	Internal organization	A.6.1.1 Management commitment To information security		
		A.6.1.2 Information security Co-ordination		
		A.6.1.3 Allocation of information security responsibilities		
		A.6.1.4 Authorization process for information processing facilities		
		A.6.1.5 Confidentiality agreements		
		A.6.1.6 Contact with authorities		
		A.6.1.7 Contact with specialist Interest groups		
		A.6.1.8 Independent review of information security		
A.6.2	External parties	A.6.2.1 Identification of risks related to external parties		
		A.6.2.2 Addressing security when Dealing with customers		

ردیف	اهداف کنترلی	مکانیزم کنترلی	الزام اجرایی (دارد/ ندارد)	اجراء (شده/ نشده)
		A.6.2.3 Addressing security in Third party contracts		
A.7	Asset management			
A.7.1	Responsibility of assets	A.7.1.1 Inventory of assets		
		A.7.1.2 Ownership of assets		
		A.7.1.3. Acceptable use of assets		
A.7.2	Information lassification	A.7.2.1 Classification guidelines		
		A.7.2.2 Information labeling and handling		
A.8	Human resource security			
A.8.1	Prior to employment	A.8.1.1 Roles and responsibilities		
		A.8.1.2 Screening		
		A.8.1.3 Terms and conditions of employment		
A.8.2	During employment	A.8.2.1 Management responsibilities		
		A.8.2.2 Information security awareness, education and training		
		A.8.2.3 Disciplinary process		
A.8.3	Termination or change of employment	A.8.3.1 Termination responsibilities		
		A.8.3.2 Return of assets		
		A.8.3.3 Removal of asset rights		
A.9	Physical and environmental security			
A.9.1	Secure areas	A.9.1.1 Physical Security perimeter		

ردیف	اهداف کنترلی	مکانیزم کنترلی	الزام اجرایی (دارد/ ندارد)	اجراء (شده/ نشده)
		A.9.1.2 Physical entry controls		
		A.9.1.3 securing offices, rooms and facilities		
		A.9.1.4 Protecting against external and environmental threats		
		A.9.1.5 Working in secure areas		
		A.9.1.6 Public access, delivery and loading areas		
		A.9.2.1 Equipment sitting and protection		
		A.9.2.2 Supporting utilities		
		A.9.2.3 Cabling security		
		A.9.2.4 Equipment maintenance		
		A.9.2.5 Security of equipment off-premises		
		A.9.2.6 Secure disposal or re-use of equipment		
		A.9.2.7 Removal of property		
A.10	Communications and operations management			
A.10.1	Operational procedures and responsibilities	A.10.1.1 Documented operating procedures		
		A.10.1.2 Change management		
		A.10.1.3 Segregation of duties		
		A.10.1.4 Separation of development, test and operational facilities		
A.10.2	Third party service delivery management	A.10.2.1 service delivery		
		A.10.2.2 Monitoring and review of third party services		

ردیف	اهداف کنترلی	مکانیزم کنترلی	الزام اجرایی (دارد/ ندارد)	اجراء (شده/ نشده)
		A.10.2.3 Managing changes to third party services		
A.10.3	System planning and acceptance	A.10.3.1 Capacity management		
		A.10.3.2 System acceptance		
A.10.4	Protection against malicious and mobile codes	A.10.4.1 Controls against malicious code		
		A.10.4.2 Controls against mobile code		
A.10.5	Back-up	A.10.5.1 Information Back-up		
A.10.6	Network security management	A.10.6.1 Network controls		
		A.10.6.2 security of network services		
A.10.7	Media handling	A.10.7.1 Management of removable media		
		A.10.7.2 Disposal of media		
		A.10.7.3 Information handling procedures		
		A.10.7.4 Security of system documentation		
A.10.8	Exchange of Information	A.10.8.1 Information exchange policies and procedures		
		A.10.8.2 Exchange agreements		
		A.10.8.3 Physical media in transit		
		A.10.8.4 Security of electronic office systems		
		A.10.8.5 Business information systems		
A.10.9	Electronic commerce services	A.10.9.1 Electronic ommerce		
		A.10.9.2 On-line transactions		
		A.10.9.3 Publicly available information		

ردیف	اهداف کنترلی	مکانیزم کنترلی	الزام اجرایی (دارد/ ندارد)	اجراء (شده/ نشده)
A.10.10	Monitoring	A.10.10.1 Audit logging		
		A.10.10.2 Monitoring system use		
		A.10.10.3 Protection of log Information		
		A.10.10.4 Administrator and operator logs		
		A.10.10.5 Fault logging		
		A.10.10.6 Clock synchronization		
A.11	Access control			
A.11.1	Business requirement for access control	A.11.1.1 access control policy		
A.11.2	User access management	A.11.2.1 User registration		
		A.11.2.2 Privilege management		
		A.11.2.3 User password management		
		A.11.2.4 Review of user access rights		
A.11.3	User responsibilities	A.11.3.1 Password use		
		A.11.3.2 Unattended user equipment		
		A.11.3.3 Clear desk and clear screen policy		
A.11.4	Network access control	A.11.4.1 Policy on use of network services		
		A.11.4.2 User authentication for external connections		
		A.11.4.3 Equipment identification in networks		
		A.11.4.4 Remote diagnostic and configuration port protection		
		A.11.4.5 Segregation in networks		

ردیف	اهداف کنترلی	مکانیزم کنترلی	الزام اجرایی (دارد/ ندارد)	اجراء (شده/ نشده)
		A.11.4.6 Network connection control		
		A.11.4.7 Network routing control		
A.11.5	Operating system access control	A.11.5.1 Secure log-on procedures		
		A.11.5.2 User identification and authentication		
		A.11.5.3 Password management system		
		A.11.5.4 Use of system utilities		
		A.11.5.5 Session time-out		
		A.11.5.6 Limitation of connection time		
A.11.6	Application and information access control	A.11.6.1 Information access restriction		
		A.11.6.2 Sensitive system isolation		
A.11.7	Mobile computing and tele working	A.11.7.1 Mobile computing and communications		
		A.11.7.2 Teleworking		
A.12	Information systems acquisitions, development and maintenance			
A.12.1	Security requirements of information systems	A.12.1.1 Security requirements analysis and specification		
A.12.2	Correct processing in applications	A.12.2.1 Input data validation		
		A.12.2.2 Control of internal processing		
		A.12.2.3 Message integrity		
		A.12.2.4 Output data validation		
A.12.3	Cryptographic controls	A.12.3.1 Policy on the use of cryptographic controls		

ردیف	اهداف کنترلی	مکانیزم کنترلی	الزام اجرایی (دارد/ ندارد)	اجراء (شده/ نشده)
		A.12.3.2 Key management		
A.12.4	Security of system files	A.12.4.1 Control of Operational software		
		A.12.4.2 Protection of system test data		
		A.12.4.3 Access control to source code		
A.12.5	Security in development and support processes	A.12.5.1 Chang control procedures		
		A.12.5.2 Technical review of applications after operating system changes		
		A.12.5.3 Restrictions on changes to software packages		
		A.12.5.4 Information leakage		
		A.12.5.5 Outsourced software Development		
A.12.6	Technical vulnerability management	A.12.6.1 Control of technical vulnerabilities		
A.13	Information security incident management			
A.13.1	Reporting information security events and weaknesses	A.13.1.1 Reporting security events		
		A.13.1.2 Reporting security weaknesses		
A.13.2	Management of information security incidents and improvements	A.13.2.1 Responsibilities and procedures		
		A.13.2.2 Learning from information security incidents		
		A.13.2.3 Collection of evidence		
A.14	Business continuity management			
A.14.1	Information security aspects of business	A.14.1.1 Including information security in the		

ردیف	اهداف کنترلی	مکانیزم کنترلی	الزام اجرایی (دارد/ ندارد)	اجراء (شده/ نشده)
	continuity management	business continuity management process		
		A.14.1.2 Business continuity and risk assessment		
		A.14.1.3 Developing and implementing continuity plans		
		A.14.1.4 Business continuity and planning framework		
		A.14.1.5 Testing, maintaining and re-assessing business continuity plans		
A.15	Compliance			
A.15.1	Compliance with legal requirements	A.15.1.1 Identification of applicable legislation		
		A.15.1.2 Intellectual property rights (IPR)		
		A.15.1.3 Protection of organizational records		
		A.15.1.4 Data protection and privacy of personal information		
		A.15.1.5 Prevention of misuse of information processing facilities		
		A.15.1.6 Regulation of cryptographic controls		
A.15.2	Compliance with security policies and standards, and technical compliance	A.15.2.1 Compliance with security policies and standards		
		A.15.2.2 Technical compliance checking		
A.15.3	Information system audit considerations	A.15.3.1 Information system audit controls		
		A.15.3.2 Protection of information system audit tools		

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	تعامل با اشخاص ثالث (سایر مراجع)
شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری شماره دستورالعمل : ۱-۲-۲	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود. کلیه اسنادی که بر اساس رهنمودهای این دستورالعمل تهیه می‌شوند دارای طبقه‌بندی محرمانه خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل الزام سازمان به شناسایی و تحلیل ریسک‌های امنیت اطلاعات حاصل از تعامل با سایر طرف‌های تجاری یا اداری می‌باشد.

مسئولیت

- مسئولیت حفظ امنیت کانال‌های ارتباطی (از قبیل زیرساخت شبکه ای، فیبر نوری، ارتباط بی سیم، خطوط پر ظرفیت یا کم ظرفیت انتقال داده) و سیستم‌های نرم‌افزاری و سخت‌افزاری واسطه به عهده واحد امنیت اطلاعات می‌باشد.
- مسئولیت حفظ امنیت هر نوع دارایی اطلاعاتی که در تعامل یا تبادل اطلاعات با سایر طرف‌های اداری یا تجاری مورد استفاده واقع می‌شود به عهده متصدی یا تحویل گیرنده همان دارایی خواهد بود.
- مسئولیت حفظ امنیت هر نوع سرویس یا خدمات به عهده متصدی یا مدیر تعیین شده برای ارائه آن سرویس می‌باشد.

الزامات

لازم است هنگام تبادل اطلاعات و داده با سایر طرف‌های تجاری یا اداری اعم از تبادل الکترونیک **On Line** یا **Off Line**، تبادل از طریق شبکه بی سیم یا کابلی، تبادل از طریق خطوط عادی یا پر سرعت، تبادل از طریق شبکه‌های نوری، کابل مسی و یا خطوط انتقال نیرو، تبادل از طریق نوارهای مغناطیسی، دیسک‌های نوری یا مغناطیسی، **Flash Memory**، **Flash Disk**، **Hard Disk**، توکن‌های سخت‌افزاری، کارت‌های الکترونیکی هوشمند یا غیر هوشمند و یا هر رسانه دیگری که برای انتقال اطلاعات قابل استفاده است، ریسک‌های مرتبط با انتقال داده مانند انتقال ویروس یا کدهای مخرب، افشای اطلاعات نزد افراد غیر مجاز، شنود یا نسخه برداری از اطلاعات در حال انتقال، تغییر در اطلاعات در حال انتقال یا مفقود شدن آن و یا ارسال اطلاعات به مقصد ناخواسته، بر اساس دستورالعمل ۳-۳-۳ (سند مدیریت ریسک) شناسایی شده و نسبت به کنترل آن‌ها اقدام به عمل آید.

حتی در حالتی که اطلاعات به صورت الکترونیک تبادل یا منتقل نمی‌شود (مثل ارسال شناسه و کلمه عبور به وسیله نامه معمولی) اما محتوی اطلاعات تبادل شده مرتبط با دارایی‌های اطلاعاتی سازمان است، لازم است شناسایی و تحلیل ریسک انجام پذیرد.

در صورتی که تعامل یا تبادل اطلاعات مستلزم انتقال داده یا اطلاعات دارای طبقه‌بندی حفاظتی می‌باشد، لازم است قبل از ارسال اولاً کفایت سطح طبقه‌بندی مرجع دریافت کننده احراز شده و ثانیاً الزامات انتقال در خصوص احراز هویت و صلاحیت، اصالت مبدأ و مقصد و عدم انکار دریافت یا ارسال رعایت گردد.

در صورتی که تعامل یا تبادل اطلاعات مستلزم اعطای حق دسترسی به دارایی‌های اطلاعاتی به طرف مقابل می‌باشد، لازم است الزامات کنترل دسترسی (موضوع دستورالعمل‌های فصل ۷ از ۱-۷-۱ الی ۲-۷-۷) به تناسب کاربرد رعایت گردد.

در صورتی که تعامل یا تبادل اطلاعات مستلزم انتقال اطلاعات یا داده از یک شبکه واسطه (مانند زیرساخت مخابراتی شرکت مخابرات ایران) و یا هر عامل واسطه دیگری باشد، لازم است الزامات مرتبط با دستورالعمل‌های ۲-۱-۷ و ۲-۲-۳ هنگام تحلیل ریسک مورد توجه واقع شود. برقراری ارتباط با سایر شبکه‌ها، تبادل اطلاعات یا داده و تعامل الکترونیکی فقط پس از اثبات الزام قانونی، مقرراتی و یا تجاری مجاز است. در صورتی که تعامل بر اساس موافقت‌نامه یا توافقات مکتوب دو جانبه برقرار می‌شود لازم است الزامات دستورالعمل ۲-۱-۵ (توافقنامه حفظ محرمانگی) رعایت گردد.

- هر گونه تبادل یا تعامل اطلاعاتی بدون کسب مجوز از ((بالاترین مقام اجرایی سازمان))) یا مرجعی که توسط وی تعیین می‌شود ممنوع است.

فرآیند

برای برقراری تعامل و تبادل اطلاعات با سایر طرف‌های تجاری یا اداری که به‌صورت روز افزون در حال افزایش می‌باشد، معمولاً نیاز به انتقال اطلاعات به شکل الکترونیکی، اپتیکی، صوتی و یا امواج الکترومغناطیسی می‌باشد. اطلاعات یا داده‌ها در هر لحظه ممکن است در حال پردازش، در حال انتقال و یا ذخیره شده باشند. بیشترین آسیب پذیری در مرحله انتقال به وجود می‌آید. برقراری تعامل و تبادل اطلاعات به معنی نیاز به انتقال اطلاعات می‌باشد. در این مرحله ممکن است:

- اطلاعات اشتباهاً ارسال شود
- اطلاعات به مقصد اشتباه ارسال شود
- حین انتقال اطلاعات مورد سوء استفاده، افشاء و یا تغییر قرار گیرد

• و یا هنگام انتقال به ویروس یا کدهای ناخواسته آلوده شود.

به علاوه به دلیل نیاز به استفاده از پروتکل‌های ارتباطی برای انتقال داده یا اطلاعات ممکن است از نقاط ضعف و آسیب پذیری این پروتکل‌ها و یا تجهیزات واسطه انتقال (که معمولاً کنترل آن‌ها در اختیار مراجع دیگری است) سوء استفاده شده و برای حمله به سیستم مورد بهره‌برداری (استثمار) قرار گیرند.

بنابراین لازم است در صورت نیاز به انتقال اطلاعات و برقراری ارتباط با سایر مراجع یا طرف‌های اداری- تجاری و یا بهره‌برداری از تجهیزات پردازشی ایشان و یا اعطای حق دسترسی به دارایی‌های اطلاعاتی و یا تجهیزات پردازشی سازمان به طرف‌های اداری و تجاری، قبلاً کلیه ریسک‌های موجود شناسایی و تحلیل شده و یا در صورت ایجاد کوچکترین شک در حین تعامل یا برقراری ارتباط، رابطه موجود متقابل مورد تحلیل موشکافانه قرار گیرد و از ایجاد حالتی که ممکن است منجر به ضربه پذیری شده و یا پتانسیل ضربه پذیری را افزایش دهد جلوگیری به عمل آید.

مرجع

این دستورالعمل به شماره □-□ / ۱-۲-۲ / □-□ به ثبت رسیده و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۳-۳-۳

دستورالعمل ۷-۱-۲

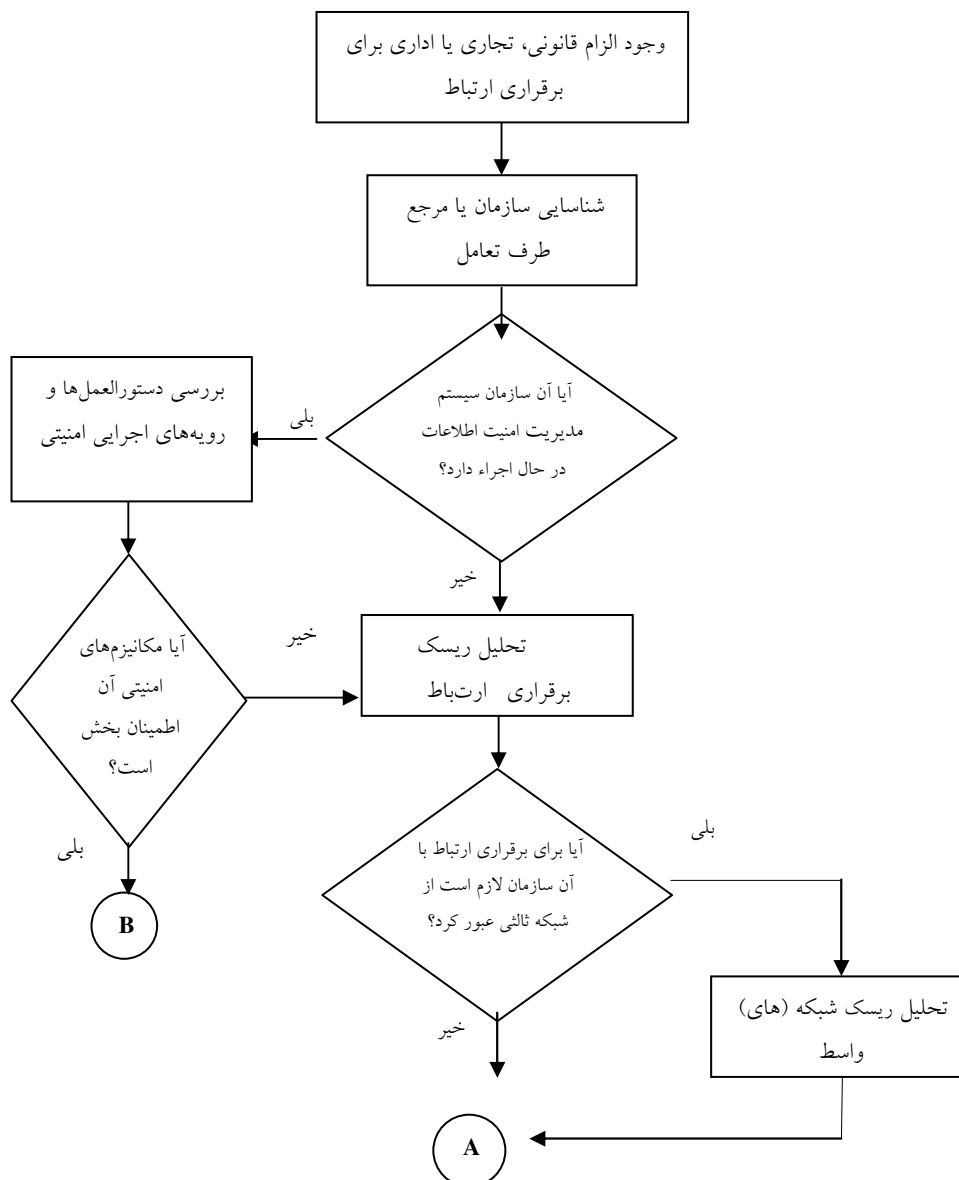
دستورالعمل ۳-۲-۲

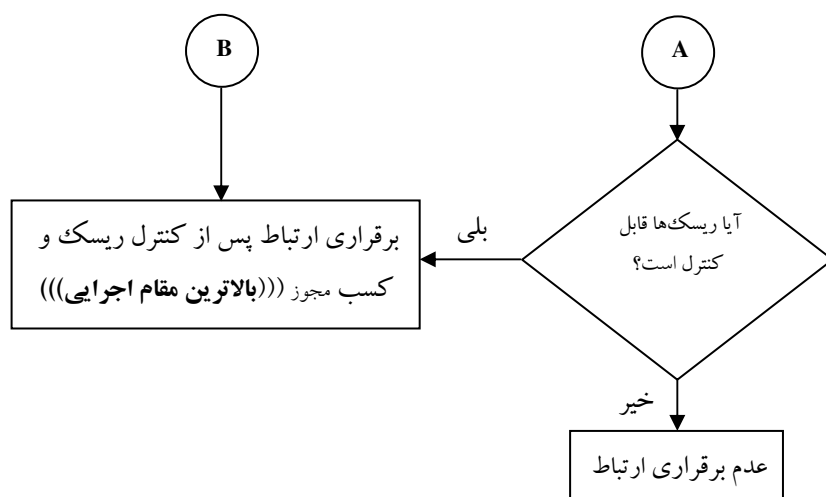
دستورالعمل ۵-۱-۲

روند نما

روند نمای شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری در شکل زیر نشان

داده شده است.





(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	تعامل با اشخاص ثالث (سایر مراجع)
رعایت نکات امنیتی هنگام تعامل با مشتریان یا ارباب رجوع شماره دستورالعمل : ۲-۲-۲	

عادی

تائیدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: ((بالاترین مقام اجرایی سازمان))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند عادی طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات می‌باشد.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل بیان ضرورت انجام و چگونگی رعایت نکات امنیتی هنگام تعامل با مشتریان یا ارباب رجوع می‌باشد.

مسئولیت

- مسئولیت نظارت بر اجرای این سند به عهده نهاد متصدی حفظ امنیت اطلاعات سازمان یا نهاد معادل آن (مرکز حراست فناوری اطلاعات و ارتباطات) می‌باشد.
- مسئولیت پیاده‌سازی اقدامات اجرایی حفاظت از امنیت اطلاعات در هر بخش که مشتریان یا ارباب رجوع به آن مراجعه می‌نمایند اعم از مراجعه حضوری یا مراجعه از طریق شبکه‌های اطلاعاتی به عهده مدیر همان بخش می‌باشد.
- مسئولیت کنترل ورود و خروج ارباب رجوع با واحدهای حراست می‌باشد.

الزامات

نحوه تعامل با مشتری یا ارباب رجوع باید بنحوی باشد که امکان دسترسی اتفاقی یا عمدی غیرمجاز ایشان به دارایی‌های اطلاعاتی سازمانی وجود نداشته باشد.

در صورتی که تعامل با مشتری یا ارباب رجوع مستلزم دسترسی به برخی دارایی‌های اطلاعاتی باشد لازم است آموزش‌های لازم در خصوص کار با آن دارایی به ایشان داده شود. نحوه ارائه آموزش باید متناسب با ماهیت دسترسی بوده و در قالب راهنمای نصب شده در محل بهره‌برداری، جزوه‌های راهنما و یا آموزش تعاملی باشد.

لازم است در مواقعی که احتمال مراجعه افراد کم توان جسمی وجود دارد، نحوه تعامل بنحوی برنامه‌ریزی شود که امکان بهره‌برداری ایشان از خدمات الکترونیکی وجود داشته باشد. به‌خصوص اگر از شناسه کاربری و کلمه عبور استفاده می‌شود نوع مکانیزم دسترسی باید به نحوی طراحی شود که احتمال افشای آن‌ها به دلیل ناتوانی یا کم توانی جسمی وجود نداشته باشد. به‌علاوه لازم است در این خصوص مشاوره‌های لازم از مراجع مربوط مثل وزارت بهداشت، درمان و آموزش پزشکی یا سازمان‌های مردم نهاد فعال در این حوزه گرفته شود.

اگر نوع تعامل مستلزم تحویل تجهیزات کنترل دسترسی (توکن‌های سخت‌افزاری یا کلیدهای نرم‌افزاری) به مشتری یا ارباب رجوع باشد، لازم است آموزش‌های لازم در خصوص نحوه بهره‌برداری و حفاظت از آن یا ریسک‌های مرتبط با بهره‌برداری نادرست از آن به ایشان داده شود.

برقراری رویه‌های امنیتی در تعامل با مشتریان یا ارباب رجوع نباید باعث گریزان شدن مشتریان یا ارباب رجوع از بهره‌برداری از خدمات الکترونیکی شود.

لازم است به طور مداوم و در مراحل مختلف در خصوص خطر افشای پارامترهای دسترسی مثل شناسه کاربری و یا کلمه عبور مشتریان یا ارباب رجوع نزد افراد دیگر (چه توسط کارمندان و چه توسط خود مشتریان یا ارباب رجوع) هشدار داده شود.

لازم است رویه‌های استحکام پارامترهای دسترسی یا کلمه عبور (دستورالعمل‌های ۷-۲، ۱-۷، ۳-۲ و ۷-۳-۱) در خصوص مشتریان یا ارباب رجوع نیز به کار گرفته شود.

در صورتی که دسترسی مشتری به دارایی‌های اطلاعاتی مستلزم پذیرش مسئولیت‌های حقوقی آن از سوی وی باشد لازم است این موضوع قبلاً به اطلاع وی رسیده باشد و مدارکی که مبین حدود مسئولیت‌های وی است به رؤیت و امضای وی برسد.

ایجاد مرکز پاسخگویی^{۱۰} الکترونیک به سؤالات مشتریان یا ارباب رجوع در سازمان‌هایی که ارائه خدمات به مشتریان و ارباب رجوع در آن‌ها به صورت الکترونیک انجام می‌شود ضروری است.

فرآیند

هدف نهایی کلیه سازمان‌ها و بنگاه‌های دولتی یا خصوصی، انتفاعی یا غیر انتفاعی ارائه خدمات یا محصول به مشتریان یا ارباب رجوع می‌باشد. به عبارت دیگر هدف کلیه فعالیت‌های پردازشی تسهیل ارائه خدمات می‌باشد.

تسهیل ارائه خدمات باید بگونه‌ای باشد که علاوه بر افزایش کارایی فعالیت‌ها، امنیت داده‌ها یا اطلاعات و یا به‌طور کلی دارایی‌های اطلاعاتی نیز تأمین گردد.

مشتری یا ارباب رجوع به عنوان نقطه پایانی فعالیت محسوب می‌شوند و هنگامی خدمات تکمیل شده و کار تمام شده ارزیابی خواهد شد که مشتری یا ارباب رجوع دریافت و کفایت آن را اعلام نماید و از انجام آن اظهار رضایت نماید. انجام برخی فعالیت‌ها مستلزم مراجعه مشتری یا ارباب رجوع به دارایی‌های اطلاعاتی و تعامل با آن‌ها می‌باشد.

¹⁰ Help Desk

از آن‌جا که مشتری به عنوان اجزای سازمان محسوب نمی‌گردد نمی‌توان وظایف خاصی را برای وی تعریف نمود و یا از وی انتظار انجام آن را داشت مگر آنکه قبلاً آموزش‌های لازم به وی داده شده و تعهد وی به رعایت الزامات قراردادی اخذ گردد.

علاوه بر آن لازم است تا نحوه تعامل (مشتریان یا ارباب رجوع) با دارایی‌های اطلاعاتی به نحوی تنظیم گردد که منجر به پیچیدگی روش انجام کار و یا کاهش کارایی فرآیندها نگردد. همچنین توجه به کفایت روش‌های تأمین امنیت و سهولت بهره‌برداری از آن‌ها برای جلوگیری از ایجاد ریسک‌های ناشی از تمایل به دور زدن مکانیزم‌های حفاظتی به دلیل پیچیدگی بیش از حد آن‌ها ضروری است.

مرجع

این دستورالعمل به شماره □-□/۲-۲/□-□ به ثبت رسیده و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

دستورالعمل ۱-۲-۷

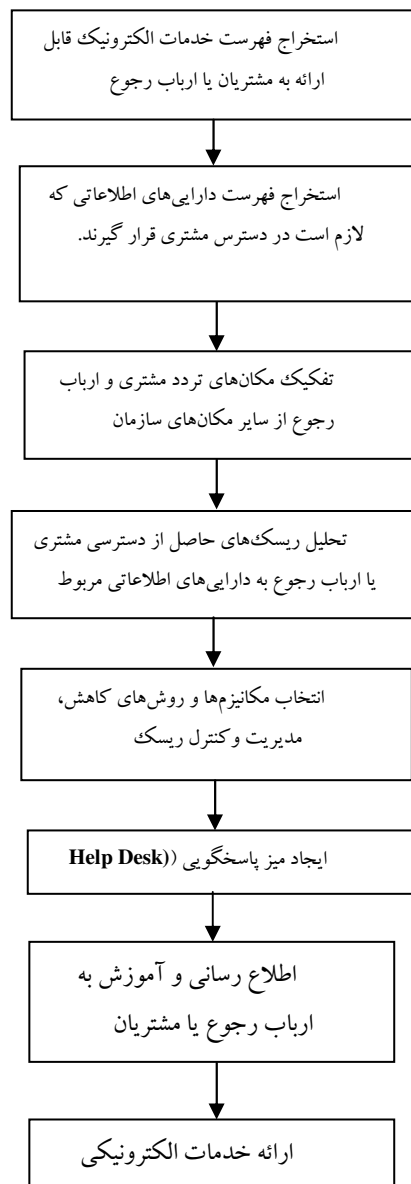
دستورالعمل ۳-۲-۷

دستورالعمل ۱-۳-۷

روند نما

روند نمای رعایت نکات امنیتی هنگام تعامل با مشتریان یا ارباب رجوع در شکل زیر نشان داده

شده است:



(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
سازمان (دهی) امنیت اطلاعات	تعامل با اشخاص ثالث (سایر مراجع)
رعایت معیارهای امنیتی در قراردادهای اشخاص ثالث شماره دستورالعمل : ۳-۲-۲	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات می‌باشد.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل اعلام ضرورت گنجاندن شرایط و مواد مربوط به رعایت الزامات حفظ امنیت اطلاعات در قراردادهای فی مابین می‌باشد.

مسئولیت

مسئولیت اجرای مفاد این دستورالعمل به عهده (((واحدهای امور حقوقی و قراردادهای)))
 (((وزارت/ سازمان/ اداره کل/ شرکت...))) می‌باشد. در صورت عدم وجود این مرجع مسئولیت رعایت مفاد این دستورالعمل به عهده مرجع متقاضی عقد قرارداد خواهد بود.

الزامات

در تنظیم قراردادهای دسترسی شخص ثالث به دارایی‌های اطلاعاتی لازم است لزوم رعایت سیاست‌ها و معیارهای امنیتی دیکته شده توسط کارفرما به عنوان یک ماده مستقل و یا ذیل تعهدات مجری درج شده و جزئی از قرارداد باشد.

لازم است نحوه جبران ضرر و زیان ناشی از عدم اجرای تعهدات فوق به روشنی بیان گردد.
 روش‌های حفاظت از دارایی‌های اطلاعاتی که به دلیل الزامات قراردادی در اختیار مجری قرار می‌گیرد باید در متن قرارداد یا پیوست‌های فنی آن ذکر گردد.

لازم است روش عودت دارایی‌های اطلاعاتی یا نحوه انهدام داده‌ها یا اطلاعاتی که به دلیل الزامات قراردادی در اختیار مجری قرار گرفته است و یا در حین اجرای قرارداد تولید شده‌اند (به‌خصوص داده‌ها و اطلاعاتی که از دیدگاه کارفرما واجد طبقه‌بندی حفاظتی می‌باشند) به روشنی در متن قرارداد و یا پیوست‌های فنی آن درج شود.

لازم است در متن قرارداد یا پیوست‌های فنی آن به حقوق مالکیت معنوی طرفین و یا نسخه برداری از داده‌ها و اطلاعات تولید شده اشاره شده و شرایط آن به روشنی شرح داده شود.
 لازم است در متن قرارداد یا پیوست‌های فنی آن سطح کیفیت خدمات قابل ارائه از طرف مجری و سطوح غیر قابل پذیرش خدمات تعیین گردد.

در صورتی که قرارداد در خصوص تأمین کانال‌های مخابراتی باشد لازم است سطح کیفیت خدمات در قالب SLA^{۱۱} تبیین شده و به امضاء طرفین برسد.

در صورتی که طرف قرارداد تابع دولت دیگری به‌جز دولت جمهوری اسلامی ایران باشد لازم است به تابعیت قانونی قرارداد و پیامدهای احتمالی ناشی از تابعیت حقوقی و ارجاع داور یا حکمیت به مراجع خارجی توجه شود. به علاوه لازم است الزامات مربوط به حفظ حریم حقوق افراد و حقوق مالکیت معنوی (IPR)^{۱۲} و تفاوت در تعریف آن‌ها در سیستم‌های قضایی مختلف توجه نمود.

در صورتی که اجرای قرارداد مستلزم عبور داده یا اطلاعات از مرزهای بین‌المللی است لازم است به الزامات قانونی کشورهای که در مسیر عبور داده یا اطلاعات قرار می‌گیرند توجه شود. به‌خصوص لازم است در تبادل اطلاعات مالی به تبعات ناشی از قوانین محلی یا قطع‌نامه‌های لازم الاجرای بین‌المللی مانند قطع‌نامه‌های شورای امنیت سازمان ملل متحد یا آرای قضات محلی در خصوص دعاوی افراد یا دولت‌ها علیه دولت جمهوری اسلامی ایران یا اتباع آن توجه شود.

- لازم است در متن قراردادهایی که از طرف ((بالاترین مقام اجرایی سازمان)) به عنوان قراردادهای مهم تلقی می‌شوند به حق ممیزی کارفرما در خصوص مواد یا بندهای مرتبط با حفظ امنیت اطلاعات اشاره شده و مکانیزم آن پیش‌بینی شود.

لازم است در متن قرارداد به مسؤولیت‌های مدنی پیمانکار در خصوص رعایت معیارهای لازم امنیتی علاوه بر آن دسته از معیارها یا شروطی که توسط کارفرما به آن‌ها اشاره شده است، اشاره شده و قرارداد به نحوی تنظیم شود که عدم اشاره کارفرما به برخی از موارد لازم موجب سلب مسؤولیت مجری نگردد.

با توجه به لزوم صرف هزینه بیشتر برای رعایت الزامات قراردادی از سوی مجری، لازم است هنگام افزودن شروط امنیتی به قرارداد به منطقی بودن و تناسب شروط و ارزش قرارداد توجه شود. در صورتی که انجام کار مستلزم ارجاع کار از سوی مجری به مرجع ثالثی باشد لازم است اولاً مجری کلیه مسؤولیت‌های ناشی از فعالیت‌های مرجع ثالث را بپذیرد و ثانیاً قبل از ارجاع کار به مرجع ثالث موافقت کتبی کارفرما را اخذ نماید.

¹¹ Service Level Agreement

¹² Intellectual Property Rights

فرآیند

حفظ امنیت اطلاعات هنگام ارجاع فعالیت‌های پردازشی یا فعالیت‌های مرتبط به تعامل با دارایی‌های اطلاعاتی به سازمان‌های دیگر یا افراد ضروری است. لازم است نکات مربوط به ریسک‌های مرتبط با فرآیندهای پردازشی اطلاعات، محیط‌های کاری یا شبکه‌هایی که داده یا اطلاعات در آن به جریان گذاشته می‌شود مورد توجه واقع شود.

ارجاع کار ممکن است مربوط به مدیریت، کنترل و یا اجرای برخی یا کلیه فرآیندهای پردازشی یا تجهیزات پردازش اطلاعات باشد. هنگام ارجاع کار لازم است به مواد زیر توجه شود:

چگونگی رعایت نیازهای قانونی مثل مقررات حفظ اسرار

چگونگی شمول کلیه افراد یا مراجعی که بنحوی در جریان پردازش اطلاعات دخالت خواهند

داشت، اعم از افراد تحت مدیریت مجری، پیمانکاران دست دوم یا اشخاص ثالث.

چگونگی تضمین ادامه ارائه خدمات هنگام وقوع حادثه امنیتی اعم از حوادث طبیعی مانند

زلزله، طوفان، سیل و یا غیر طبیعی مانند جنگ، آشوب، حمله‌های رایانه ای، سرقت اطلاعات و غیره.

حقوق ممیزی و چگونگی اعمال آن

تابعیت قانونی طرفین و الزامات مربوط به آن

قراردادهای ارجاع کار باید به نحوی تنظیم شود که اجازه افزایش سطوح امنیتی به طرفین را

بدهد.

لازم است توجه شود که قراردادهای ارجاع کار می‌تواند باعث بروز برخی از سؤالات پیچیده

شود که یافتن پاسخ آن‌ها آسان نخواهد بود. بنابراین در قراردادهای مهم لازم است اولاً از مشاوره

حقوقی مناسب بهره برد و ثانیاً در انتخاب مجری به صلاحیت‌های اخلاقی و حسن شهرت وی

توجه نمود و برای این پارامترها وزن بیشتری از شاخص قیمت در نظر گرفت.

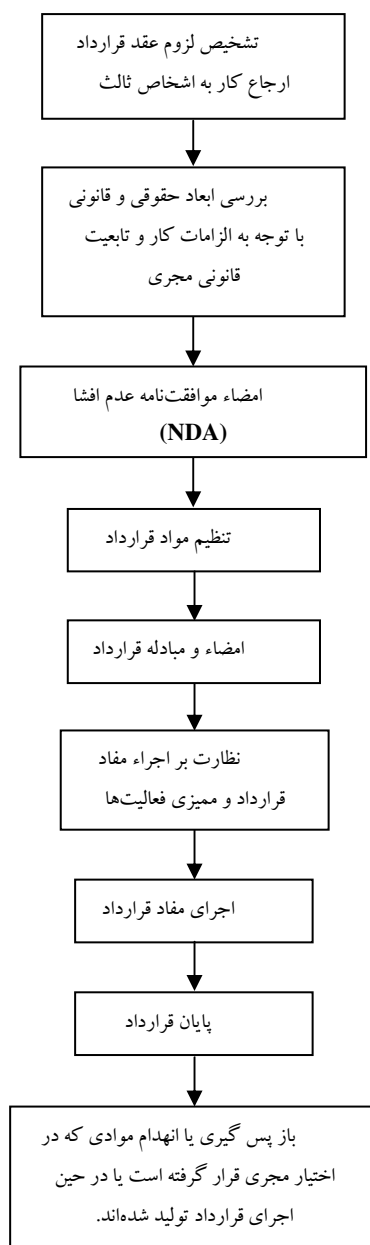
مرجع

این دستورالعمل به شماره □-□/۳-۲-۲/□-□ به ثبت رسیده است.

روند نما

روند نمای رعایت معیارهای امنیتی در قراردادهای اشخاص ثالث در شکل زیر نمایش داده

شده است:



۳-۳- مدیریت دارایی‌های اطلاعاتی

این بخش شامل دستورالعمل‌های زیر می‌باشد:

۳ - مدیریت دارایی‌های اطلاعاتی		
مسئولیت حفظ دارایی‌های اطلاعاتی		۱-۳
فهرست موجودی دارایی‌های اطلاعاتی		۱-۱-۳
تعیین متصدی و یا مالکیت دارایی‌های اطلاعاتی		۲-۱-۳
نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی		۳-۱-۳
طبقه‌بندی اطلاعات		۲-۳
دستورالعمل طبقه‌بندی اطلاعات		۱-۲-۳
برچسب‌گذاری دارایی‌های اطلاعاتی و نگهداری		۲-۲-۳
شناخت سیستم و تحلیل ریسک		۳-۳
گزارش مرحله شناخت سیستم		۱-۳-۳
ارزیابی ریسک		۲-۳-۳
مدیریت و مقابله با ریسک		۳-۳-۳
بیانیه کاربرد پذیری (SOA) اختصاصی		۴-۳-۳

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	مسئولیت حفظ دارایی‌های اطلاعاتی
فهرست موجودی دارایی‌های اطلاعاتی شماره دستورالعمل : ۱-۱-۳	

محرمانه

تائیدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود. کلیه اسناد و گزارش‌هایی که بر اساس رهنمودهای این دستورالعمل تولید می‌شوند حداقل دارای طبقه‌بندی حفاظتی خیلی محرمانه خواهند بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تهیه فهرست موجودی دارایی‌های اطلاعاتی تقویم کلیه دارایی‌های اطلاعاتی موجود در حوزه قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات (موضوع دستورالعمل ۱-۱-۳) می‌باشد به نحوی که هیچیک از دارایی‌های اطلاعاتی که باید مورد محافظت قرارگیرند از قلم نیافتد. مالکیت این دارایی‌ها طبق دستورالعمل ۱-۲-۳ تعیین خواهد شد. نحوه استفاده از دارایی‌ها نیز در دستورالعمل ۱-۳-۳ بیان می‌گردد.

مسئولیت

مسئولیت تهیه فهرست موجودی دارایی‌های اطلاعاتی به عهده مدیر امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و یا واحد جایگزین آن می‌باشد. فهرست دارایی‌های اطلاعاتی بر اساس فرم دارایی‌های اطلاعاتی (ضمیمه همین دستورالعمل) تشکیل خواهد شد. مسئولیت تکمیل فرم دارایی‌های اطلاعاتی برای هر دارایی به عهده استفاده‌کننده از همان دارایی می‌باشد. (در صورتی که بیش از یک نفر از یک دارایی اطلاعاتی استفاده می‌کنند لازم است هر یک از آن‌ها یک فرم مجزا را برای همان دارایی تکمیل نمایند). مسئولیت بررسی صحت مندرجات فرم‌ها و تخلیص آن‌ها و ارسال به واحد امنیت اطلاعات نیز به عهده مدیر یا مسئول واحدهای مختلف سازمان می‌باشد.

الزامات

فهرست دارایی اطلاعاتی حداقل باید دارای مشخصات ذیل باشد. این موارد باید برای تمام دارایی‌ها به‌طور دقیق و مشخص بیان شده باشد.

شماره اختصاصی

عنوان دارایی

گروه دارایی

نام متصدی یا مالک یا تحویل‌گیرنده آموزش دیده دارایی اطلاعاتی (طبق دستورالعمل ۱-۳-۲)

طبقه‌بندی حفاظتی دارایی اطلاعاتی (طبق دستورالعمل ۱-۲-۳)

مجوزهای دسترسی پیش فرض (حیطه مجاز به بهره‌برداری از اطلاعات و حداقل شرایط

بهره‌برداری از اطلاعات)

به علاوه لازم است مدارک زیر برای هر دارایی اطلاعاتی به فرم مربوط به آن پیوست گردد:

راهنمای استفاده

شرایط اولیه استفاده/ بهره‌برداری از دارایی

شرایط خاص بهره‌برداری از دارایی اطلاعاتی مورد نظر مالک/متصدی دارایی اطلاعاتی)

در خصوص دارایی‌های اطلاعاتی دارای طبقه‌بندی حفاظتی لازم است تا موارد ذیل نیز به‌طور کامل برای دارایی‌های اطلاعاتی مشخص و قید گردد:

ارزش، اهمیت و تأثیر دارایی در پیشرفت امور سازمان

سطح آسیب پذیری و یا احتمال ریسک

مجوز دسترسی در صورت تفویض اختیارات

عوامل تهدید دارایی

سایر اطلاعات مفید در مورد دارایی اطلاعاتی:

ارتباط با سیستم‌های اطلاعاتی

نام مسئول تعیین مجوز دسترسی به دارایی اطلاعاتی به کاربران

نام مسئول آموزش دیده نگهداری و تهیه پشتیبان از دارایی‌های الکترونیکی

فهرست فرآیندهای مجاز پردازش اطلاعات

شاخص صحت اطلاعات و اعتبار

فرآیند

دارایی‌های حوزه فناوری اطلاعات عبارت است از تمام دارایی‌های اطلاعاتی اعم از فیزیکی و یا منطقی و یا سایر دارایی‌هایی که در تداوم عملیات فناوری اطلاعات و یا تولید، پشتیبانی، انتقال، بهره‌برداری، حفاظت و یا نگهداری دارایی اطلاعاتی نقش دارند و در قلمرو پیاده‌سازی سامانه امنیت اطلاعات قرار می‌گیرند. فهرست موجودی دارایی‌های اطلاعاتی فهرستی است که از تمام دارایی‌های اطلاعاتی موجود در حوزه فناوری اطلاعات و جهت سهولت نظارت بر اساس سیستم مدیریت امنیت اطلاعات، تهیه می‌شود.

تقسیم بندی پیشنهادی دارایی‌های اطلاعاتی در ضمیمه ۱ این دستورالعمل ذکر شده است. نحوه تهیه و بروزرسانی این فهرست عبارت است از:

ارائه پیش فهرست دارایی‌های اطلاعاتی (ضمیمه ۱ این دستورالعمل) از طرف کمیته امنیت اطلاعات.

تکمیل فرم شناسنامه دارایی (ضمیمه ۲) توسط استفاده کننده از هر دارایی اطلاعاتی. (لازم است تا برای کلیه دارایی‌های اطلاعاتی موجود در قلمرو سیستم مدیریت امنیت اطلاعات، فرم شناسنامه دارایی تکمیل و در اختیار واحد امنیت اطلاعات، مرکز حراست فناوری اطلاعات یا نهاد متصدی حفظ امنیت اطلاعات قرار گیرد).

بازنگری و تهیه فهرست دارایی‌های اطلاعاتی. (واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات موظف است تا پس از دریافت شناسنامه دارایی‌ها نسبت به تهیه فهرست مطابق نیازمندیهای مورد اشاره در این سند اقدام نماید).

تعیین متصدی یا مالک دارایی‌های اطلاعاتی که در خصوص بهره‌برداری از آن دارایی آموزش کافی دیده باشد. (نام متصدی یا تحویل گیرنده یا مالک دارایی‌ها طبق دستورالعمل ۳-۱-۲ تعیین و در این فهرست لحاظ می‌گردد).

تکمیل ملاحظات امنیتی در فهرست دارایی‌ها طبق دستورالعمل ۳-۲-۱. (لازم است طبقه‌بندی حفاظتی تک تک دارایی‌های اطلاعاتی تعیین شده و در فهرست دارایی‌ها لحاظ گردد).

شناسایی ارزش و آسیب پذیری دارایی. (معیارهای ریسک دارایی‌های اطلاعاتی جزئی از فهرست دارایی‌ها می‌باشد که طبق دستورالعمل ۳-۳-۲ (ارزیابی ریسک) شناسایی و تعیین می‌گردند. همچنین باید عوامل تهدید دارایی‌ها طی فرآیند تحلیل ریسک مشخص شوند و لازم است تا پس از انجام هر مرحله تحلیل ریسک، مندرجات فهرست دارایی‌های اطلاعاتی به هنگام شود).

اسناد مرجع

این سند به شماره □-□/۱-۳/□-□ به ثبت رسیده و سایر اسناد مرتبط با این سند عبارت‌اند از:

- تقسیم بندی و گروه بندی دارایی‌های اطلاعاتی (ضمیمه ۱ این دستورالعمل)

- فرم شناسنامه دارایی‌های اطلاعاتی (ضمیمه ۲ این دستورالعمل)

- دستورالعمل ۳-۱-۱

- دستورالعمل ۳-۱-۲

- دستورالعمل ۳-۱-۳

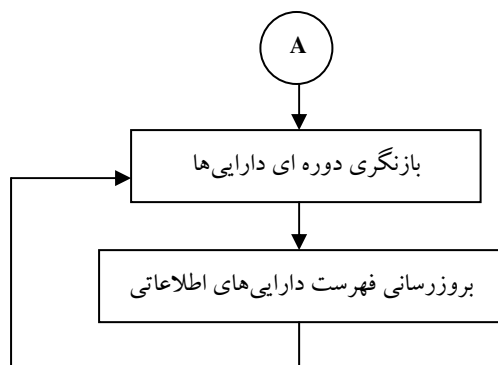
- دستورالعمل ۳-۲-۱

- دستورالعمل ۳-۳-۲

روند نما

روندنمای تهیه و نگهداری فهرست دارایی‌های اطلاعاتی به شرح زیر است:





توضیح

لازم است به تفاوت بین بهره‌برداران، متصدی یا تحویل گیرنده و استفاده کنندگان دارایی‌های اطلاعاتی به شرح زیر توجه شود:

- بهره‌برداران عبارت‌اند از سازمان‌ها یا مراجعی که از دارایی‌های اطلاعاتی برای پیشبرد اهداف سازمانی خود استفاده می‌نمایند. دارایی اطلاعاتی در حال بهره‌برداری ممکن است تحت مالکیت قانونی بهره‌بردار بوده (مانند سرورها یا مسیربای‌های خریداری شده) و یا به عنوان امانت در اختیار وی قرار داده شده باشد (مانند دستگاه‌های POS که از طرف بانک‌ها به بهره‌بردار امانت داده می‌شود و یا تجهیزات ارتباطی یا مسیربایی امانت داده شده از طرف تامین کننده خدمات ارتباطی به بهره‌بردار یا امانت داده شده توسط مشتری به شرکت مخابرات).
- متصدی یا تحویل گیرنده یا مالک دارایی اطلاعاتی طبق تعریف پذیرفته شده در مدیریت امنیت اطلاعات عبارت است از فرد و فقط فردی که مسئولیت مدیریت (و حفاظت) از دارایی اطلاعاتی رسماً به وی سپرده شده است.
- استفاده کنندگان عبارت‌اند از کلیه افرادی که جهت دریافت خدمات از دارایی اطلاعاتی استفاده می‌نمایند و لزوماً جزء دو گروه فوق نمی‌باشند.

ضمیمه ۱

تقسیم بندی و گروه بندی دارایی‌های اطلاعاتی

فهرست اولیه دارایی‌های اطلاعاتی (فقط به عنوان مثال)

۱- داده‌های دیجیتالی یا الکترونیکی

۱-۱- بانک‌های اطلاعاتی (SQL, My SQL, ORACLE, MDB, ACCESS, Ingress, FOX,...)

۲-۱- فایل‌های داده (xls, .jpg, .doc, .txt, .pdf, ...)

۳-۱- مستندات سیستم‌ها

۴-۱- راهنمای استفاده

۵-۱- مستندات آموزشی (متن، تصویر، صدا، فیلم، چندرسانه ایی)

۶-۱- فرآیندهای عملیاتی یا پشتیبان

۷-۱- فرآیندهای اعتباری، امنیتی

۱-۷-۱- گواهی‌ها یا Licenseها

۲-۷-۱- کلمه‌های عبور یا گذر واژه‌ها (۱-۲-۷-۱- متقارن ۲-۲-۷-۱- زوج کلید)

۳-۷-۱- مجوزهای الکترونیکی

۴-۷-۱- تنظیمات و پیکربندی

۵-۷-۱- نسخه پشتیبان اطلاعات حساس

۸-۱- پشتیبان

۱-۸-۱- پشتیبان اطلاعات پیکربندی شبکه، سرورها و تجهیزات مخابراتی

۲-۸-۱- پشتیبان اطلاعات

۹-۱- اطلاعات پیکربندی شبکه، سیستم‌ها، تجهیزات مخابراتی، سرورها

۲- اسناد و داده‌های فیزیکی

۱-۲- اسناد اداری

۱-۱-۲- اسناد مکاتباتی

۲-۱-۲- اسناد دستورالعمل‌ها

۳-۱-۲- قراردادها

۴-۱-۲- نامه‌ها

-
- ۲-۱-۵- اسناد تجاری
 - ۲-۱-۶- درخواستهای نیروی انسانی
 - ۲-۱-۷- مدارک و سوابق نیروی انسانی
 - ۲-۱-۸- محتویات پرونده‌ها
 - ۲-۱-۹- محتویات زونکن‌ها
 - ۲-۱-۱۰- محتویات برجسب‌ها
 - ۲-۱-۱۱- فرم‌های خام
 - ۲-۲- اسناد مالی
 - ۲-۲-۱- اسناد نقدی یا ارزشمند
 - ۲-۲-۱-۱- پول
 - ۲-۲-۱-۲- سفته
 - ۲-۲-۱-۳- چک
 - ۲-۲-۱-۴- اوراق بهادار
 - ۲-۳-۲- اسناد مالی اعم از برگه‌های تکمیل شده بدهکار، بستانکار و سندهای ممیزی و دفترداری
 - ۲-۳-۳- اسناد باطله
 - ۲-۴- اسناد حفاظتی، امنیتی
 - ۲-۴-۱- اسناد احراز هویت (کارت‌ها و ...)
 - ۲-۴-۲- اسناد دارایی‌های اطلاعاتی، امنیتی
 - ۲-۴-۳- گزارش‌های بازرسی، حفاظت، نظارتی
 - ۲-۴-۴- فرم‌های دسترسی
 - ۲-۵- مستندات سیستم و نرم‌افزارها
 - ۲-۵-۱- مستندات سخت‌افزارها (راهنمای استفاده کننده (User Manual)، مرجع فنی (Technical Reference)، نقشه‌های شماتیک و تفصیلی، ابزار SDK)
 - ۲-۵-۲- مستندات نرم‌افزاری (راهنمای استفاده کننده (User Manual)، مرجع فنی (Technical Reference)، ابزار SDK)
 - ۲-۵-۳- مستندات شبکه شامل نقشه‌های شماتیک و تفصیلی توپولوژی و آدرس‌دهی و مسیریابی

۳- دارایی‌های نرم‌افزاری

۱-۳- سیستم‌های اطلاعاتی

۱-۱-۳- سیستم‌های تولید داخل سازمان (Applicationهای اختصاصی)

۲-۱-۳- سیستم‌های تولید خارج سازمان (Applicationهای اختصاصی سازی شده)

۳-۱-۳- سیستم‌های عمومی یا آماده (Tools، Packageها، نرم‌افزارهای متن‌باز، Freewareها)

۲-۲-۳- سیستم‌های عامل شامل کلیه سیستم‌های عامل سرورها و ایستگاه‌های کاری اعم از:

۱-۲-۳- سیستم عامل سرورهای Windows

۲-۲-۳- سیستم عامل سرورهای Linux

۳-۲-۳- سیستم عامل سرورهای Novell

۴-۲-۳- سیستم عامل‌های Thin Client

۵-۲-۳- سیستم عامل‌های Mainframe

۶-۲-۳- سیستم عامل‌های خانواده Windows

۷-۲-۳- سیستم عامل‌های خانواده Linux

۸-۲-۳- سیستم عامل‌های خانواده Apple

۹-۲-۳- سیستم عامل‌های Smart Phoneها و PDAها

۱۰-۲-۳- سیستم عامل‌های تجهیزات ارتباطی یا کنترل و مدیریت ترافیک مانند Cisco IOS،

۱۱-۲-۳- سیستم عامل‌های خانواده MS-DOS

۱۲-۲-۳- سیستم عامل‌های سایر تجهیزات مثل POS، ATM و....

۳-۳- ابزارهای امنیتی، نفوذ، ضد نفوذ

۱-۳-۳- فایروال‌ها و پراکسی‌ها

۲-۳-۳- ضد ویروس‌ها

۳-۳-۳- IDS و HIDS و تجهیزات مشابه

۴-۳-۳- UTM و تجهیزات مشابه

۵-۳-۳- تجهیزات رمزنگاری

۶-۳-۳- سیستم‌های مبتنی بر Tokenهای هوشمند یا عادی (اعم از سخت‌افزاری،

نرم‌افزاری، بیومتریک، تماسی، مجاورتی، ...)

- ۳-۴- ابزار مدیریت - پیکربندی شبکه
- ۳-۵- ابزار گرافیکی، نمایشی
- ۳-۶- ابزارهای تولید نرم‌افزار (CASE Tools)
- ۳-۷- راه اندازه‌های سخت‌افزارها ((Device Drivers
- ۳-۷-۱- راه اندازه چاپگر
- ۳-۷-۲- راه اندازه کارت شبکه
- ۳-۷-۳- راه اندازه اسکنر
- ۳-۷-۴- راه اندازه‌های کارت گرافیکی
- ۳-۷-۵- راه اندازه‌های مادربرد
- ۳-۷-۶- راه اندازه‌های خاص یا سایر راه اندازه‌های دیگر
- ۳-۸- Samples و نمونه‌ها
- ۴- دارایی‌های سخت‌افزاری (فیزیکی، منقول)
- ۴-۱- کامپیوترهای شخصی
- ۴-۱-۱- مانیتور
- ۴-۱-۲- کیس و قطعات داخلی آن مانند مادربرد، کارت گرافیک، CPU،
- ۴-۱-۳- کیبورد
- ۴-۱-۴- موس
- ۴-۱-۵- Speaker
- ۴-۱-۶- چاپگر
- ۴-۱-۷- اسکنر
- ۴-۱-۸- قلم نوری
- ۴-۲- کامپیوتر قابل حمل
- ۴-۳- تجهیزات ذخیره اطلاعات قابل حمل (Portable) و دستگاه‌های تکثیر اطلاعات
- ۴-۳-۱- CD
- ۴-۳-۲- DVD، HDVD، Blue Ray، ...
- ۴-۳-۳- فلاپی یا دیسک مغناطیسی و انواع آن

- ۴-۳-۴ Hard Disk
- ۴-۳-۵ Flash Memory
- ۴-۳-۶ Tape و انواع آن
- ۴-۳-۷ دستگاه تکثیر (کپی کاغذ)
- ۴-۴ تجهیزات ذخیره اطلاعات ثابت
 - ۴-۴-۱ Hard Disk
 - ۴-۴-۲ حافظه‌های داخلی و جانبی رایانه
 - ۴-۴-۳ سایر تجهیزات ذخیره اطلاعات ثابت
 - ۴-۵ کامپیوترهای سرور
 - ۴-۶ تجهیزات ارتباطی، مخابراتی
 - ۴-۶-۱ مسیریاب‌ها (هسته و توزیع)، مودم‌ها، مودم روترها،
 - ۴-۶-۲ تکرارکننده، هاب، سویچ و مراکز IP، MPLS، ATM، SDH، F/R، GSM، CDM، PBX
 - ۴-۶-۳ فایروال
 - ۴-۶-۴ تلفن و فکس
 - ۴-۶-۵ کابلها (نوری، مسی، فولادی، ...)
 - ۴-۶-۶ شبکه بی سیم
 - ۴-۶-۷ مجموعه ایستگاه‌های دریافت و ارسال ماهواره ایی
 - ۴-۶-۸ معماری زیرساخت ارتباطی
 - ۴-۷ تغذیه پشتیبان UPS
 - ۴-۸ تجهیزات امنیتی
 - ۴-۸-۱ توکن
 - ۴-۸-۲ پلمب
 - ۴-۸-۳ کلید
 - ۴-۸-۴ تجهیزات نظارت تصویری (نوری، X-RAY، تشخیص حرکت، ...)
 - ۴-۸-۵ تجهیزات کنترل نفوذ فیزیکی (نوری، حرارتی، صوتی یا الکترومغناطیسی، ...)
 - ۴-۸-۶ تجهیزات کنترل شنود (مختل کننده‌های صوتی یا الکترومغناطیسی)

۴-۸-۷- تجهیزات محافظت الکترومغناطیسی

۴-۸-۸- تجهیزات آتش نشانی

۴-۸-۹- تجهیزات محافظت در مقابل سیل یا آب گرفتگی

۴-۸-۱۰- تجهیزات محافظت در مقابل زلزله

۴-۸-۱۱- تهویه، تصفیه آب و پشتیبانی حیات

۵- نیروی انسانی

۵-۱- پرسنل سازمان اعم از رسمی، قراردادی، روزمزد، پیمانی

۵-۱-۱- کارکنان اجرایی

۵-۱-۲- مدیران اجرایی

۵-۱-۳- مدیران ارشد و میانی

۵-۱-۴- کارکنان بازرسی

۵-۱-۵- کارکنان حفاظت و حراست

۵-۱-۶- کارکنان خدماتی

۵-۲- مشتریان

۵-۳- ارباب رجوع

۵-۴- پیمانکاران

۵-۵- قابلیت‌های نیروی انسانی

۵-۵-۱- دانش و مهارت نیروی انسانی

۵-۵-۲- اعتقادات نیروی انسانی

۵-۵-۳- تجربیات

۵-۵-۴- آموزش‌ها و دوره‌ها

۶- خدمات

۶-۱- خدمات پردازشی

۶-۲- خدمات مخابراتی، ارتباطی و مکاتبات

۶-۳- حمل و نقل

۶-۴- نظافت

-
- ۶-۵- تعمیر و نگهداری
 - ۶-۶- گرمایش
 - ۶-۷- سرمایش
 - ۶-۸- آب، برق، گاز
 - ۶-۹- تهویه
 - ۶-۱۰- اورژانس
 - ۶-۱۱- آتش نشانی
 - ۶-۱۲- ژنراتور برق اضطراری
 - ۶-۱۳- تغذیه کارکنان
 - ۶-۱۴- سرویس بهداشتی
 - ۷-۷- ارزش‌های سازمانی
 - ۷-۱- فرهنگ سازمانی
 - ۷-۲- سیستم‌های سازمانی (روال‌ها و فرآیندها)
 - ۷-۳- طرح تداوم عملیات
 - ۷-۴- طرح بازگشت به حالت پایدار قبلی
 - ۷-۵- اعتبار نزد افکار عمومی
 - ۷-۶- پاسخگویی، شفافیت
 - ۷-۷- مسئولیت پذیری سازمان
 - ۷-۸- جلب رضایت مشتریان و ارباب رجوع
 - ۷-۹- فرهنگ مدیریت سازمان
 - ۸- اماکن (فیزیکی، غیرمنقول)
 - ۸-۱- روابط عمومی
 - ۸-۲- مکان‌های درمانگاهی
 - ۸-۳- مکان‌های بازرسی
 - ۸-۴- استراحتگاه
 - ۸-۵- اماکن تبادل اطلاعات برون سازمانی

-
- ۶-۸- مکان‌های اجرایی
 - ۷-۸- مرکز امنیت
 - ۸-۸- اتاق سرور
 - ۹-۸- اتاق طراحی و تولید سیستم‌های اطلاعاتی
 - ۱۰-۸- محل نگهداری اسناد و مدارک، بایگانی
 - ۱۱-۸- مکان نصب تجهیزات مخابراتی
 - ۱۲-۸- مکان نصب تجهیزات ارتباطی شبکه
 - ۱۳-۸- مکان نگهداری تجهیزات، اسناد و مدارک مانند کمد های دیواری یا ثابت
 - ۱۴-۸- مکان‌های تعمیر و سرویس تجهیزات
 - ۱۵-۸- مکان ارائه سرویس اینترنت
 - ۱۶-۸- مکان ارائه سرویس راه دور
 - ۱۷-۸- مکان سرویس فکس و مخابره
 - ۱۸-۸- مکان جلسات و همایشها
 - ۱۹-۸- مکان کنترل تجهیزات قسمت‌ها مانند اتاق کنترل سالن همایشها
 - ۲۰-۸- انبار
 - ۲۱-۸- کتو
 - ۲۲-۸- کمد
 - ۲۳-۸- قفسه
 - ۲۴-۸- صندوق
 - ۲۵-۸- گاوصندوق

ضمیمه ۲

فرم شناسنامه دارایی اطلاعاتی

فرم پیشنهادی زیر جهت تشکیل شناسنامه دارایی اطلاعاتی ارائه گردیده است (در صورت نیاز میتوان اجزای آن را تغییر داده و با نیازهای سازمانی منطبق نمود):

((وزارت/ سازمان/ اداره کل/ شرکت/ ...)))	
فرم مشخصات دارایی اطلاعاتی	شماره سریال فرم:

شماره اختصاصی:	شماره اموال:	عنوان دارایی:
متصدی، تحویل گیرنده یا مالک دارایی:		گروه دارایی:
طبقه‌بندی دارایی:		محل نگهداری:
مجوز دسترسی پیش فرض:		محل استفاده:
ارزش دارایی (ریالی):		
نوع آسیب پذیری دارایی (توضیح داده شود):		
میزان آسیب پذیری دارایی:		
عوامل تهدید دارایی اطلاعاتی (توضیح داده شود):		

نام تکمیل کننده شناسنامه دارایی:	تاریخ تهیه/بروزرسانی:
	امضاء:

توضیحات مربوط به تکمیل فرم در ادامه شرح داده شده است.

راهنمای تکمیل فرم شناسنامه دارایی اطلاعاتی:

- شماره اموال یا شماره اختصاصی: شماره ای است که برای شناسایی یک دارایی به کار می‌رود. در مواردی که سیستم شماره گذاری اموال در سازمان وجود دارد می‌توان از شماره اموال سازمانی استفاده کرد. در غیر اینصورت نیاز است تا یک روش مشخص برای شماره گذاری اموال توسط واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات ارائه شود. شماره اموال می‌تواند ترکیبی از شماره قسمت مالک دارایی و یک شماره افزایشی در نظر گرفته شود.
- گروه دارایی: از جدول ضمیمه ۱ این دستورالعمل استخراج شود. در صورتی که این فهرست کامل نباشد باید عناوین گروه‌ها به مرکز حراست فناوری اطلاعات ارائه تا به فهرست اضافه شود. ارزش یک دارایی: تخمینی است از:
 - ۱- قیمت تمام شده
 - ۲- هزینه ای که نیاز است تا دارایی فوق تهیه و جایگزین گردد.
 - ۳- هزینه ای که در اثر فقدان دارایی به عنوان ضرر و زیان به سازمان تحمیل می‌گردد.
 - مجوز دسترسی پیش فرض: عبارت است از نحوه دسترسی به دارایی طی روال عادی بهره‌برداری از دارایی در صورتی که هیچ گونه روال تعیین دسترسی به این دارایی تعریف نشده باشد. نوع آسیب پذیری: جهت استخراج نوع آسیب پذیری از فهرست مندرج در ضمیمه ۳ همین دستورالعمل استفاده شود. میزان آسیب پذیری: جهت تعیین میزان آسیب پذیری به دستورالعمل ۳-۳-۲ (ارزیابی ریسک) مراجعه شود. عوامل تهدید دارایی اطلاعاتی: عبارت‌اند از شرایط یا عواملی که امکان سوء استفاده از آسیب پذیری را فراهم می‌نمایند. به عنوان مثال یکی از آسیب پذیری‌های مانیتور (نمایشگر) مشاهده اطلاعات مجرمانه در حال نمایش روی آن به وسیله افراد غیر مجاز است. بنا براین قرار دادن مانیتور در مکانی که در معرض دید افراد غیرمجاز است به عنوان عامل تهدید محسوب می‌شود. ضربه ناشی از این عامل تهدید عبارت است از نقض محرمانگی. (محرمانگی، جامعیت (صحت) و دسترسی پذیری سه رکن اصلی امنیت اطلاعات را تشکیل می‌دهند. برای درک بهتر عوامل تهدید به دستورالعمل ۳-۳-۲ (ارزیابی ریسک) مراجعه شود.

ضمیمه ۳

دارایی‌های اطلاعاتی و آسیب پذیری ها

فهرست زیر حاوی آسیب پذیری‌های عمده دارایی‌های اطلاعاتی می‌باشد. با توجه به پیشرفت فناوری، ورود محصولات جدید به بازار و افزایش دانش و آگاهی افراد از یک سو و نیازهای سازمانی از سوی دیگر، لازم است این فهرست همیشه به هنگام سازی شود. مسئولیت به هنگام سازی این فهرست به عهده مسئول واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و یا واحد جانشین وی می‌باشد.

۱- داده‌های منطقی و یا الکترونیکی

۱-۱- بانک‌های اطلاعاتی

۱-۱-۱- SQL، Oracle،

- دسترسی به ساختار و اطلاعات از طریق دسترسی به سرور

- تغییر اطلاعات به صورت غیر مجاز

- استخراج اطلاعات به صورت غیر مجاز

- آسیب پذیری در مقابل حمله‌های تزریق

- ضعیف بودن مکانیزم‌های کنترل دسترسی

۱-۱-۲- Fox

- عدم امکان کنترل دسترسی به اطلاعات

- نیاز به اشتراک گذاری فایل جهت دسترسی به اطلاعات و امکان حذف و یا آسیب به فایل‌ها

- عدم امکان مدیریت صحیح اطلاعات مانند محدودیت‌ها در مقادیر اطلاعات

- حساسیت بسیار زیاد نسبت به قطع برق

۱-۱-۳- Access

- آسیب پذیری ها:

- امکان شکستن رمز بانک و دستیابی به ساختار و اطلاعات

- امکان از بین رفتن کل اطلاعات با حذف فایل MDB

۲-۱- فایل‌های داده:

- عدم امکان کنترل دسترسی به اطلاعات
- حذف فایل و از بین رفتن اطلاعات
- ویروس پذیری و انتقال ویروس از طریق انتقال فایل

۳-۱- مستندات سیستم‌ها (و)

۴-۱- راهنمای استفاده

- مفقود شدن و یا عدم نگهداری صحیح
- عدم دسترسی بموقع به مستندات و یا محدودیت در دسترسی
- نگهداری نامناسب روی CD، دیسکت

۵-۱- مستندات آموزشی

- حجم بالای مستندات
- مشکلات ناشی از پیچیدگی تهیه مستندات بروز و جامع
- محتوای غلط و یا قدیمی و عدم تطابق با فرآیندهای جاری

۶-۱- فرآیندهای عملیات پشتیبان

- غیر فعال شدن مکانیزم پشتیبان
- عدم وجود فضای کافی جهت پشتیبان
- عدم پیکربندی مناسب
- عدم تعیین مسئول مستقیم تهیه نسخه پشتیبان
- عدم اطمینان از صحت روش پشتیبان‌گیری
- عدم تعریف رویه و ترتیب بارگذاری مجدد فایل‌های پشتیبان

۷-۱- فرایندهای اعتباری، امنیتی

۱-۷-۱- گواهی‌ها

- پایان اعتبار گواهی و محدودیت زمانی آن

- تکثیر گواهی و استفاده غیر مجاز از گواهی‌ها

- ابطال گواهی به علت نقص تعهدات

۲-۷-۱- گذر واژه (Password)

۱-۲-۷-۱- گذر واژه متقارن

- سرقت کلید

- ضعیف بودن کلید و قابل حدس یا کشف نمودن

۲-۲-۷-۱- گذر واژه نامتقارن

- سرقت کلید خصوصی و دستیابی به سایر پارامترهای حساس

- کافی نبودن طول کلید و ضعیف بودن الگوریتم آن

- اتمام اعتبار گواهی کلید

۳-۷-۱- مجوزهای الکترونیکی

- جعل مجوز

- سرقت مجوز

- اتمام اعتبار مجوز و لغو دسترسی

- احتمال عدم دسترسی به سرور مجوزدهی و اختلال در دسترسی

۴-۷-۱- تنظیمات و پیکربندی نرم‌افزار یا سخت‌افزار

- پیکربندی نامناسب

- عدم ثبت و نگهداری پیکربندی مناسب جهت تکرار پیکربندی

- تغییر پیکربندی و به تبع آن نقض سیاست‌ها

۱-۷-۵- نسخه پشتیبان اطلاعات حساس

- آسیب دیدن نسخه پشتیبان

- قدیمی بودن نسخه پشتیبان

- عدم امکان تهیه نسخه پشتیبان از اطلاعات حساس

۱-۶- پشتیبان

- آسیب دیدن نسخه پشتیبان

- قدیمی بودن نسخه پشتیبان

- سازگار نبودن فایل‌های مختلف یک نسخه پشتیبان

۱-۷- اطلاعات پیکربندی

- پیکربندی غلط و افزایش آسیب پذیری شبکه

- عدم پیکربندی یکسان در صورت پیکربندی مجدد

- زمان بر بودن پیکربندی

- نیاز به دسترسی فیزیکی جهت پیکربندی

۲- اسناد و داده‌های فیزیکی

۲-۱- اسناد

- فسادپذیری کاغذ و یا آسیب پذیری فیزیکی سند

- مشخص نبودن طبقه‌بندی حفاظتی سند

- قابل حمل بودن سند و عدم امکان کنترل انتقال اسناد

- جعل سند

- قابل تکثیر بودن سند

- عدم امکان حفاظت از محتوای سند

- عدم امکان ثبت وقایع مانند زمان مشاهده سند یا افرادی که سند را رؤیت کرده‌اند.

- هزینه تهیه سند اصل در صورت آسیب سند

- آسیب پذیری هنگام انتقال اسناد

- حجم اسناد بایگانی

۲-۲- اسناد باطله:

- وجود اطلاعات طبقه‌بندی شده در اسناد باطله

- عدم دقت لازم در نگهداری اسناد باطله

- استفاده مجدد اسناد باطله

۳-۲- اسناد حفاظتی، امنیتی

۱-۳-۲- اسناد احراز هویت

- تکثیر و یا جعل سند

- خاتمه اعتبار سند

۲-۳-۲- اسناد متعلق به دارایی‌های اطلاعاتی

- حساس بودن و حیاتی بودن اسناد

- بروز نبودن اسناد

۳-۳-۲- گزارش‌های بازرسی

- شفافیت و صحت گزارش

- زمان ارائه گزارش

۴-۳-۲- فرم‌های دسترسی

- مخدوش بودن یا شدن فرم

- تائید و امضای فرم اشتباه توسط مالک یا متصدی دارایی

- کم و یا زیاد شدن عوامل دسترسی بر روی فرم پس از تأیید (دست بردن در متن)

۳- دارایی‌های نرم‌افزاری

توجه: استفاده از نرم‌افزارهای بدون پشتیبانی، **Crack** شده و کپی غیر قانونی به‌خصوص نرم‌افزارهای ایرانی تحت پوشش قانون حفاظت از حقوق پدیدآورندگان نرم‌افزار به طور کلی از عوامل تهدیدزای مهم به شمار می‌رود.

۱-۳- سیستم‌های اطلاعاتی

- دسترسی به اطلاعات جهت مشاهده، تغییر، حذف

- نیاز به پشتیبانی مداوم جهت عملکرد مطلوب

- عمر محدود سیستم‌ها و نیاز به بازنگری

- کامل نبودن مستندات سیستم‌های اطلاعاتی

- ضعف‌های بنیادی منجر به فروپاشی سیستم یا رخنه به مکانیزم‌های کنترلی یا حفاظتی

۱-۳-۱- سیستم‌های تولید داخل سازمان

- دشواری نگهداری متن معتبر برنامه

- پیچیدگی مدیریت پروژه و رعایت استانداردهای تولید نرم‌افزار

- عدم بررسی آسیب پذیری‌ها به علت اطمینان به افراد سازمان

۱-۳-۲- سیستم‌های تولید خارج سازمان

- هزینه تولید سیستم

- کوتاهی در پشتیبانی سیستم و اجرای تعهدات شرکت تولید کننده

- عدم دسترسی کامل به کد منبع

- آسیب پذیری‌های سیستم و اطلاع افراد خارج سازمان از مکانیزم‌های عملیاتی و امنیتی

۱-۳-۳- سیستم‌های عمومی و آماده

- عدم پشتیبانی تولید کننده

- عدم امکان بررسی متن نرم‌افزار و شناسایی آسیب پذیری‌های آن

۲-۳- سیستم عامل

۱-۲-۳- سرورهای Windows

- جذابیت برای حمله از طرف کاربران آماتور
- عدم به‌روز رسانی و نصب Patchها
- تحریم یا قطع پشتیبانی سیستم عامل
- عدم امکان بررسی حفره‌ها و Back doorها و ضعف‌های بنیادی

۲-۲-۳- سرورهای Linux

- عدم وجود متولی و پشتیبان سیستم عامل
- دسترسی به کل سیستم عامل در صورت دسترسی به کاربر Root
- جذابیت برای حمله از طرف کاربران حرفه‌ای

۳-۲-۳- سرورهای Novell

- حساسیت به قطع منبع تغذیه و آسیب سیستم عامل
- عدم پشتیبانی محصول

۲-۳-۴- سایر سیستم‌های عامل

- تفاوت نگارش‌های مختلف و Patchهای نصب شده
- آسیب‌پذیری‌های خاص هر سیستم عامل

۳-۳- ابزارهای امنیتی / نفوذ

- دسترس پذیر بودن ابزارها برای همه
- بهره‌برداری از ابزار نامناسب، مخرب، ناقص در مدیریت شبکه
- ضعف‌ها و کاستی‌های ابزارها و عدم وجود یک ابزار جامع
- عدم وجود متولی پشتیبانی و تولید ابزارها

۴-۳- ابزار مدیریت و پیکربندی شبکه

- سوءاستفاده از ابزارها

- عدم وجود رویه و ابزار یکپارچه مناسب و سازگار

۳-۵- ابزار گرافیکی و نمایشی

- تولید محصولات ناسازگار با برخی سیستم‌ها و محدودیت بهره‌برداری از مستندات تولید شده

۳-۶- ابزار تولید نرم‌افزار

- تنوع ابزار تولید و عدم دستورالعمل جامع در بهره‌برداری از آن‌ها

- آسیب‌پذیری‌های اختصاصی هر ابزار

- ضعف روش تولید متن برنامه یا امکان تعبیه درهای پشتی (Back Door) هنگام برنامه‌نویسی

۳-۷- راه اندازه‌های سخت‌افزارها

- نحوه نگهداری راه اندازه‌ها و دسترس پذیر بودن آن‌ها

- مهم تلقی نشدن نسخه راه اندازه و سیستم عامل‌های پشتیبانی کننده

۳-۸- Samples و نمونه‌ها

- محتوای اسناد نمونه و دارا بودن اطلاعات طبقه‌بندی شده

- نامناسب و یا غلط بودن نمونه و تولید اسناد غلط بر اساس نمونه

- عدم حفاظت کافی به دلیل درج نشدن در فهرست موجودی دارایی‌های اطلاعاتی

۴- دارایی‌های سخت‌افزاری

۴-۱- کامپیوترهای شخصی

۴-۱-۱- مانیتور

- امکان شنود تشعشعات و امواج مانیتور

- دیده شدن صفحه مانیتور

۴-۱-۲- کیس

- دسترسی به محتوای کیس و پلمب نشدن آن‌ها
- نامناسب بودن مکان استقرار، نحوه اتصالات و شرایط محیطی مانند گرد و غبار
- آلودگی‌های صوتی فن کیس

۴-۱-۳- کیبورد و موس

- نظافت و بهداشت صفحه کلید و موس
- کیفیت صفحه کلید و موس
- قابلیت مشاهده کلمه عبور هنگام تایپ آن

۴-۱-۴- Speaker

- پخش صوت
- تشعشعات بلندگو و امکان استفاده از بلندگو به عنوان میکروفن
- ۴-۱-۵- چاپگر
- آسیب پذیری فیزیکی چاپگرها در قبال استفاده ناصحیح از آن‌ها
- افشاء اطلاعات از طریق درام چاپگر
- افشاء اطلاعات از طریق ریون، کاربن، دور ریختنی‌ها یا چاپ مواد ناخواسته

۴-۱-۶- اسکنر

- حساسیت تجهیزات اسکن در قبال استفاده ناصحیح
- امکان تبدیل اسناد فیزیکی به دیجیتال و تکثیر یا ارسال سریع آن‌ها

۴-۱-۷- قلم نوری

- نظافت و بهداشت
- نحوه استفاده از قلم نوری

۴-۲- کامپیوترهای قابل حمل

- حمل و نقل آسان کامپیوتر به مکان‌های خارج از کنترل سازمان

-انتقال راحت و بی‌خطر یا کدهای مخرب یا بدافزار به سازمان

-آسیب پذیری‌های فیزیکی

-محتوای اطلاعاتی

-نحوه نگهداری اطلاعات بر روی این رایانه‌ها

-سهولت سرقت یا دسترسی در مکان‌های استراحت مثل هتل‌ها

۴-۳- تجهیزات ذخیره اطلاعات و قابل حمل

-سهولت تکثیر و انتقال یا سرقت اطلاعات

-آسیب پذیری‌های فیزیکی این نوع رسانه‌ها

-نحوه نگهداری و استفاده از این رسانه‌ها

-امکان زیاد انتقال و بی‌خطر

۴-۴- تجهیزات ذخیره اطلاعات

-طول عمر رسانه‌ها و امکان آسیب به اطلاعات

-امکان بازیابی اطلاعات از رسانه‌های بلااستفاده و یا آسیب دیده

-سرقت رسانه‌های حاوی اطلاعات

۴-۵- سرورها

-دسترسی مستقیم به سرور

-شناسایی، دستیابی به سرورها و اطلاعات آن‌ها

-نوع خدمات ارائه شده از سوی سرورها

۴-۶- تجهیزات ارتباطی و مخابراتی

-شنود اطلاعات

-از کار انداختن تجهیزات

- جایگزینی، سرقت تجهیزات

- قطع ارتباطات

- حمله‌های DoS

۴-۷- تغذیه پشتیبان UPS

- عدم عملکرد صحیح، فاسد شدن باتری UPS

- تحمیل بار بیش از حد

۴-۸- تجهیزات امنیتی

- سرقت تجهیزات امنیتی

- جعل تجهیزات امنیتی

- آسیب دیدن، خرابی و قطع سرویس

- استفاده از نقاط ضعف تجهیزات امنیتی

۵- نیروی انسانی

۵-۱- پرسنل سازمان

- نارضایتی و عدم انجام وظایف

- بدخواهی و انجام اقدامات مخرب

- رهایی و یا انفصال از خدمت به صورت طبیعی یا غیر طبیعی

- خطای نیروی انسانی

- دانش و آگاهی‌های حفاظتی، کاری، تخصصی و...

- مدیریت و رهبری

۵-۲- مشتریان

- افشای اطلاعات فی مابین

- عدم رعایت تعهدات و پیمان‌ها

۵-۳- ارباب رجوع

- نارضایتی

- عدم رعایت حریم همکاری و دسترسی غیر مجاز

- پنداشت همکار بودن از ارباب رجوع

۵-۴- پیمانکاران

- حضور در اماکن مختلف سازمانی

- دسترسی به دارایی‌های اطلاعاتی

- عدم رعایت تعهدات و پیمان‌ها

۵-۵- ابعاد نیروی انسانی

۵-۵-۱- دانش و مهارت نیروی انسانی

- عدم آگاهی دقیق و لازم از دانستنیهای مورد نیاز

- عدم بروزرسانی معلومات

- بهره‌برداری از دانش نیروی انسانی توسط سازمان‌های رقیب

۵-۵-۲- اعتقادات نیروی انسانی

- تهاجم فرهنگی، رسوخ در عقاید و اصول

- عدم التزام به قوانین و مقررات و اخلاق

- تخریب اعتقادات سازمان و تضعیف قوا

۵-۵-۳- تجربیات و

۵-۵-۴- آموزش‌ها و دوره‌ها

- کسب تجربه و بهره‌گیری از آن در خارج از سازمان و هدر رفتن سرمایه‌های سازمانی

- آشنایی با ساختار، اطلاعات سازمان و شناخت نقاط ضعف و قوت سازمان

- سوءاستفاده و فشار به سازمان در قبال انجام کار
- از بین رفتن سرمایه گذاری‌های سازمان بر روی نیروی انسانی
- عدم برنامه ریزی جهت نگهداشت و حفظ دانش سازمان

۶- خدمات

۱-۶- خدمات پردازشی

۲-۶- خدمات مخابراتی و ارتباطی

- وقفه در ارائه خدمات
- شنود و جاسوسی
- تزریق اطلاعات غلط و شایعه پراکنی

۳-۶- حمل و نقل

- قطع سرویس یا خدمات
- سرقت
- تصادف و حادثه

۴-۶- نظافت

- پراکنده شدن عوامل بیماری زا در اثر قطع خدمات
- ایجاد مشکلات زیستی جهت کارکنان

۵-۶- تعمیر و نگهداری

- اختلال در فرآیندها به علت اختلال در سرویس تعمیر و نگهداری
- سرقت تجهیزات و اطلاعات در حین تعمیر و نگهداری
- عدم تبحر کافی و آسیب رسانیدن به سایر بخشها

۶-۶- گرمایش (و)

۶-۷- سرمایه‌ش (و)

۶-۸- آب و برق، گاز

- ایجاد مشکلات زیستی جهت کارکنان

- اختلال در فرآیندهای سازمان به علت عدم تأمین برق، تأمین شرایط محیطی مناسب

- آسیب به تجهیزات در اثر نشت آب، انفجار گاز

۶-۹- تهویه

- ایجاد مشکلات زیستی برای کارکنان

- انتشار گازهای سمی یا زیان آور در محیط

۶-۱۰- اورژانس

- عدم حضور و خدمات اورژانس به نیروی انسانی در مواقع بحرانی

۶-۱۱- آتش‌نشانی

- تأخیر در اطفای حریق و از بین رفتن تجهیزات

۶-۱۲- ژنراتور برق اضطراری

- قطع سرویس در شرایط قطع برق

- عدم سرویس و نگهداری تجهیزات و عدم راه اندازی بموقع

۶-۱۳- تغذیه کارکنان

۶-۱۴- سرویس بهداشتی

- ایجاد مشکلات زیستی برای کارکنان

۷- ارزش‌های سازمانی

۷-۱- فرهنگ سازمانی

- تخریب فرهنگ سازمانی و اخلاق در فرآیندها

۲-۷- سیستم‌های سازمانی

-استقرار دشوار، پرهزینه، زمان بر یک سیستم در یک سازمان

-انحراف در فعالیت‌های سازمان

۳-۷- طرح تداوم عملیات

-وقفه در امور به علت عدم وجود طرح مناسب

۴-۷- طرح بازگشت به حالت پایدار قبلی

-فراهم نبودن شرایط مورد نیاز پیش بینی شده در طرح

۵-۷- اعتبار نزد افکار عمومی

-خداشه به اعتبار سازمان و اختلال در مأموریت‌های سازمان

-عدم اطمینان و بروز مشکلات نیروی انسانی

۶-۷- پاسخگویی، شفافیت

۷-۷- مسئولیت پذیری سازمان

۸-۷- جلب رضایت مشتریان و ارباب رجوع

۹-۷- فرهنگ مدیریت سازمانی

- تقابل نیروی انسانی و مدیران به علت سوءمدیریت

۸- اماکن

۱-۸- روابط عمومی

-نقص در ارائه خدمات به مراجعین و ایجاد نارضایتی

-عدم اطلاع رسانی مطلوب به مراجعین

۲-۸- مکان‌های درمانگاهی

-انتشار عوامل بیماری زا

- ازدحام و تأخیر در ارائه خدمات

۳-۸- مکان‌های بازرسی

- عبور غیر مجاز و عدم توجه بازرسی

- محل نگهداری امانات و امکان سرقت

۴-۸- استراحتگاه‌ها

- عدم شرایط مناسب جهت ارائه خدمات

- تکمیل ظرفیت

۵-۸- اماکن تبادل اطلاعات بیرون سازمانی

- ازدحام و تأخیر در تبادل اطلاعات

- تحویل اشتباهی اطلاعات، خدمات

۶-۸- مکان‌های اجرایی

- سرقت یا شنود اسناد در جریان کار

- اخلال در روند امور

۷-۸- مرکز امنیت

- رخنه، نفوذ جهت کسب اطلاعات حساس و امنیتی

- دسترسی به مرکز کنترل سیستم‌ها و غیر فعال نمودن دیده بانی

۸-۸- اتاق سرور

- دسترسی به تجهیزات حساس مانند سرورها

- دسترسی به اطلاعات و اتصالات شبکه

۹-۸- اتاق طراحی و تولید سیستم‌های اطلاعاتی

- دستیابی به مستندات طراحی و اطلاعات حساس

- ایجاد وقفه در فرآیند تولید سیستم‌های اطلاعاتی

۸-۱۰- محل نگهداری اسناد و مدارک و بایگانی

- حریق، سیل و رخداد‌های طبیعی و غیر طبیعی که باعث از بین رفتن اسناد می‌گردد.

- دسترسی به اسناد و مدارک و سرقت آن‌ها، شنود، تکثیر و...

۸-۱۱- مکان نصب تجهیزات مخابراتی

- عدم دسترسی بموقع به تجهیزات نصب شده جهت سرویس، نگهداری

- امکان نصب تجهیزات شنود مخابراتی

۸-۱۲- مکان نصب تجهیزات ارتباطی شبکه

- قطع و ممانعت از سرویس

- نصب تجهیزات شنود

۸-۱۳- مکان‌های نگهداری تجهیزات، اسناد، مدارک مانند کمدها

- عدم استحکام لازم در مقابل آسیب‌های عمدی و غیرعمدی

- عدم رعایت نکات حفاظتی جهت بسته بودن درب‌ها

۸-۱۴- مکان‌های تعمیر و سرویس تجهیزات

- عدم رعایت نکات امنیتی در نگهداری قطعات حاوی اطلاعات و یا تجهیزات حساس

- آلودگی و گرد و غبار و مواد شیمیایی

۸-۱۵- مکان ارائه سرویس اینترنت

- امکان ارسال اطلاعات از طریق شبکه اینترنت

- اتصال تجهیزات داخلی به شبکه اینترنت

۸-۱۶- مکان ارائه سرویس راه دور

- امکان قطع سرویس و نصب تجهیزات شنود

- امکان ارسال اطلاعات غیر مجاز

۸-۱۷- مکان سرویس فکس و مخابره

- امکان جا ماندن اسناد گرفته شده یا فرستاده شده

- امکان دریافت اطلاعات قسمت‌ها و افراد دیگر به صورت غیر مجاز

۸-۱۸- مکان جلسات و همایش‌ها

- ورود افراد غیر مجاز به مکان جلسات

- امکان جا ماندن و یا اسناد و مدارک شرکت کنندگان

۸-۱۹- مکان کنترل تجهیزات قسمت‌ها مانند اتاق کنترل سالن‌ها

- امکان شنود اطلاعات جلسات محرمانه

- امکان پخش غیر مجاز

۸-۲۰- انبار

- سرقت اقلام و دارایی‌ها

- آسیب به اموال و دارایی‌ها در اثر حوادث طبیعی یا غیر طبیعی

۸-۲۱- محل‌های نگهداری موقت

- ضعیف بودن قفل‌ها و تجهیزات حفاظتی و امکان سرقت

- آسیب پذیر بودن قفسه و کمد در اثر حوادث طبیعی و غیر طبیعی

۸-۲۲- گاوصندوق

- باز بودن درب گاوصندوق و احتمال سرقت

- گم شدن کلید و عدم دسترسی بموقع به دارایی‌های حساس

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی های اطلاعاتی	مسؤولیت حفظ دارایی های اطلاعاتی
تعیین متصدی و یا مالک دارایی اطلاعاتی شماره دستورالعمل : ۲-۱-۳	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

این دستورالعمل نحوه تعیین متصدی و یا مالک دارایی‌های اطلاعاتی مندرج در فهرست دارایی‌های اطلاعاتی (دستورالعمل ۱-۳-۱) را بیان می‌دارد. هدف از این اقدام تعیین شخصی است که مسئولیت رعایت ضوابط و شرایط امنیت اطلاعات را در خصوص حفاظت از امنیت دارایی‌های اطلاعاتی بر عهده دارد.

مسئولیت‌ها:

مسئولیت تعیین مالک یا متصدی هر دارایی اطلاعاتی (موضوع دستورالعمل تدوین فهرست موجودی دارایی‌های اطلاعاتی - دستورالعمل ۱-۳-۱) به عهده مدیران بخش‌های بهره‌بردار از دارایی‌های اطلاعاتی می‌باشد.

الزامات:

- هر دارایی الزاماً باید دارای یک مالک یا متصدی مشخص باشد که مسئولیت حفظ دارایی اطلاعاتی و رعایت نکات امنیتی مربوط به آن بر عهده وی می‌باشد.
- هر دارایی اطلاعاتی می‌تواند دارای زنجیره سلسله مراتبی از مالکان یا متصدیان باشد که در سلسله مراتب مسئولیت سازمانی تعیین می‌گردد. بالاترین شخص مسئول دارایی‌های اطلاعاتی، بالاترین شخص سازمان می‌باشد.
- مسئول دارایی اطلاعاتی موظف است تا بر نحوه رعایت دستورالعمل‌های امنیت اطلاعات در هنگام بهره‌برداری از دارایی‌ها توسط سایر اشخاص نظارت داشته باشد.
- مسئول دارایی موظف است تا بر اساس معیارها و ضوابط دستورالعمل طبقه‌بندی اطلاعات موضوع دستورالعمل ۱-۳-۲، طبقه‌بندی دارایی‌های اطلاعاتی را تعیین و اعلام نماید.
- در صورت تغییر مالک دارایی اطلاعاتی مسئول مافوق موظف است تا نسبت به تعیین و اعلام متصدی یا مالک جدید اقدام نموده و مراتب را به واحد امنیت اطلاعات، مرکز حراست فناوری اطلاعات و یا نهاد جایگزین آن اعلام نماید.

- در صورت لزوم خصوصیات و شرایط متصدیان و مالکان دارایی‌های اطلاعاتی باید توسط واحد امنیت اطلاعات، مرکز حراست فناوری اطلاعات و یا نهاد جایگزین تعیین و به قسمت‌ها اعلام شود.
- لازم است تا در خصوص دارایی‌های اطلاعاتی سرمایه‌ای، فرم تحویل دارایی تکمیل و تعهدات لازم از متصدی یا تحویل گیرنده دارایی اطلاعاتی اخذ گردد.
- مالکیت و یا متصدی بر دارایی‌های اطلاعاتی شامل مالکیت معنوی نیز بوده و لازم است تا علاوه بر تعیین مالکان معنوی آثار، ضوابط و مقررات مربوط به حقوق مالکیت معنوی نیز رعایت گردد.
- در صورت لزوم سایر افراد مرتبط با دارایی نیز باید تعریف و مشخص شوند. از جمله این ارتباطات می‌توان به متصدیان حمل و نقل، پشتیبانی، نگهداری و حراست اشاره نمود.

فرآیند:

برای اطمینان از بهره‌برداری در شرایط قابل پذیرش دارایی‌های اطلاعاتی طبق دستورالعمل ۳-۱ (نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی) لازم است هر دارایی اطلاعاتی موجود در قلمرو پیاده‌سازی نظام مدیریت امنیت اطلاعات (موضوع دستورالعمل ۱-۱-۳) به طور صریح و واضح به یک فرد از آحاد سازمان سپرده شود. این فرد باید در مورد نحوه بهره‌برداری امن از دارایی اطلاعاتی تحت مسئولیت خود آموزش دیده باشد. به علاوه لازم است ابزار و اختیارات لازم برای حفاظت از دارایی اطلاعاتی در اختیار وی گذارده شود.

همچنین لازم است برای جلوگیری از ناهماهنگی در تعامل با دارایی‌های اطلاعاتی و پیشگیری از تبعات و آسیب پذیری‌های ناشی از آن، متصدی یا تحویل گیرنده دارایی اطلاعاتی در موارد زیر به عنوان مرجع اصلی محسوب شده و نظرات وی در اولویت قرار گیرد:

- تعیین طبقه‌بندی حفاظتی دارایی اطلاعاتی
- تعریف سیاست‌ها و مکانیزم‌های کنترل دسترسی
- تایید فرم‌های درخواست دسترسی

تجهیزات و ابزار:

فرم تحویل دارایی اطلاعاتی (طبق پیوست ۱)

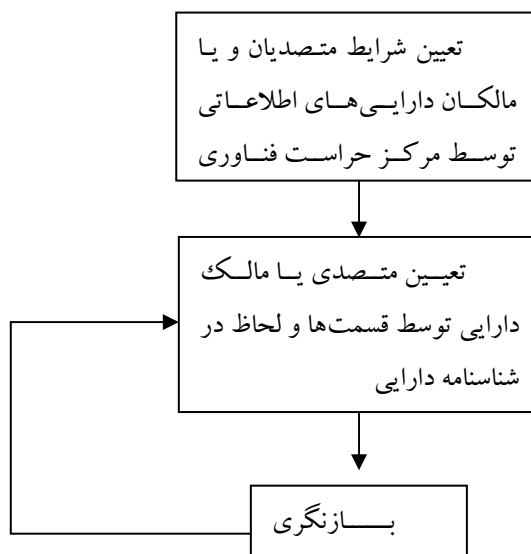
مرجع:

این دستورالعمل به شماره □ - □ / □ - □ / ۲-۱-۳ - □ - □ ثبت گردیده وسایر اسناد مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۳
- دستورالعمل ۱-۲-۳
- دستورالعمل ۳-۱-۳

روندنما:

روندنمای تعیین متصدی یا مالک دارایی اطلاعاتی به شرح ذیل است:



ضمیمه ۱

(((وزارت/ سازمان/ اداره کل/ شرکت/ ...)))

فرم تحویل دارایی اطلاعاتی به متصدی یا مالک دارایی*

شماره فرم :	طبقه‌بندی:
دارایی اطلاعاتی:	طبقه‌بندی دارایی اطلاعاتی:
عنوان دارایی اطلاعاتی:	
نام متصدی/ تحویل گیرنده/ مالک:	سمت یا مسئولیت:
قسمت:	تاریخ تحویل:
شرایط دارایی حین تحویل:	
شرایط بهره‌برداری: (به شرح پیوست فرم تحویل که به رویت و امضای تحویل گیرنده رسیده است)	
موارد مجاز استفاده:	
تحویل گیرنده	نام : امضاء:
تحویل دهنده	نام : امضاء:
مسئول واحد امنیت اطلاعات یا نهاد جایگزین آن:	
نام :	امضاء:
شرایط دارایی حین تحویل:	

- این فرم بر اساس نیاز سازمان بهره‌بردار قابل تغییر است.
- توضیح:** لازم است شرایط بهره‌برداری به این فرم پیوست شده و به رویت و امضای تحویل گیرنده برسد

(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	مسئولیت حفظ دارایی‌های اطلاعاتی
نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی شماره دستورالعمل : ۳-۱-۳	

عادی

تائیدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

این دستورالعمل مبین چگونگی نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی به منظور کاهش زیان‌های قابل پیشگیری و یا تبعات امنیتی ناشی از بهره‌برداری نادرست از دارایی‌های اطلاعاتی است.

مسئولیت‌ها:

- مسئولیت رعایت مفاد این دستورالعمل به عهده کلیه بهره‌برداران از دارایی‌های اطلاعاتی می‌باشد.
- مسئولیت تدوین شرایط و نحوه استفاده قابل پذیرش از هر دارایی‌های اطلاعاتی به عهده متصدی یا تحویل گیرنده یا مالک همان دارایی اطلاعاتی می‌باشد.

الزامات:

استفاده صحیح از یک دارایی اطلاعاتی بدین معنی است که بهره‌برداری از یک دارایی اطلاعاتی در جهت اهداف تعیین شده سازمان صورت پذیرد و شیوه استفاده به نحوی باشد که کمترین مخاطرات را برای دارایی‌های اطلاعاتی و فرآیندهای سازمانی ایجاد نماید.

نحوه استفاده قابل پذیرش از دارایی‌ها علاوه بر ملاحظات امنیتی باید مواردی همچون شرایط تعیین شده توسط سازنده یا تامین کننده، شرایط محیطی محل استفاده، نحوه استفاده صحیح و شرایط پس از بهره‌برداری از دارایی‌ها را نیز بیان کند.

لازم است تا جهت استفاده از کلیه تجهیزات پردازش یا دارایی‌های اطلاعاتی مندرج در فهرست دارایی‌های اطلاعاتی، مجوزهای مورد اشاره در دستورالعمل ۲-۱-۴ (صدور مجوز استفاده از دارایی‌های اطلاعاتی) اخذ گردد.

لازم است تا کلیه افراد قبل از استفاده از دارایی‌های اطلاعاتی دارای طبقه‌بندی حفاظتی، توافق نامه حفظ محرمانگی (موضوع دستورالعمل ۲-۱-۵) را پذیرفته و امضاء نموده باشند.

- لازم است تا واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن با تعامل با مالکان و متصدیان دارایی‌های اطلاعاتی، شرایط و ضوابط دسترسی افراد به دارایی‌ها و شرایط اختصاصی مدنظر قسمت مربوطه را اخذ و در دستورالعمل اختصاصی بهره‌برداری از هر

دارایی اطلاعاتی لحاظ نمایند. (نحوه استفاده و شرایط خاص مالکان/ متصدیان دارایی‌های اطلاعاتی).

نحوه استفاده و دسترسی به دارایی‌های اطلاعاتی پیرو سیاست‌های کنترل دسترسی مورد اشاره در دستورالعمل ۷-۱-۱ بوده و در صورت بیان شرایط دیگر مبنی بر اخذ مجوز خاص، این مجوزها باید اخذ و رعایت گردد.

لازم است رویدادها و یا موارد استفاده ناصحیح از دارایی‌ها توسط متصدیان/مالکان دارایی‌ها، ممیزان امنیت و یا مراجع و افرادی که نظارت بر بهره‌برداری امن از دارایی‌های اطلاعاتی به عهده آن‌ها گذاشته شده است، طبق فرم مندرج در ضمیمه ۱ این دستورالعمل مکتوب و به واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن اعلام گردد.

فرآیند:

- مراحل تعیین نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی به شرح زیر است:
- اعلام شرایط استفاده عام از دارایی‌های موضوع این دستورالعمل توسط واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن به قسمت‌ها.
 - تعیین شرایط اختصاصی استفاده از دارایی‌های اطلاعاتی توسط مالکان، متصدیان دارایی‌ها و اعلام آن طبق دستورالعمل ۳-۱-۱ از طریق شناسنامه دارایی‌های اطلاعاتی به واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن.
 - اخذ مجوز استفاده از تجهیزات پردازش اطلاعات مطابق دستورالعمل ۲-۱-۴ برای فرد، یا واحدی که قصد بهره‌برداری از دارایی‌های اطلاعاتی دارد.
 - اخذ توافق نامه حفظ محرمانگی از افرادی که قصد بهره‌برداری از دارایی‌ها را دارند.
 - اخذ مجوز دسترسی به دارایی‌های اطلاعاتی پیرو سیاست‌های مندرج در ۷-۱-۱.
 - بررسی مجوزهای دسترسی و انجام عملیات ایجاد دسترسی.
 - تحویل مستندات بهره‌برداری صحیح از دارایی مانند راهنماها، دستورالعمل‌های اختصاصی بهره‌برداری و فرم‌های ضمیمه این دستورالعمل و تحویل مجوز دسترسی ایجاد شده (نام و کلمه عبور) و سایر تجهیزات دسترسی به کاربر منجمه دستورالعمل‌های ۷-۳-۱، ۷-۳-۲، ۷-۵-۱، ۷-۵-۴

فرآیند نظارت بر استفاده صحیح از دارایی‌ها به شرح زیر است:

- تهیه فهرست بررسی (Check List) ارزیابی استفاده از دارایی‌های اطلاعاتی
- تدوین برنامه نظارت و ممیزی (خودارزیابی و ممیزی سطح دوم) توسط واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن و جمع بندی نتایج حاصل بر اساس برنامه زمانبندی شده توسط کمیته امنیت اطلاعات (براساس سطح طبقه‌بندی حفاظتی دارایی‌ها)

توصیه‌های عام بهره‌برداری از برخی دارایی‌های اطلاعاتی در ضمیمه ۲ همین متن آورده شده است.

روندها: این دستورالعمل فاقد روند‌ها می‌باشد

ضمیمه ۲

((وزارت / سازمان / اداره کل / شرکت / ...)))
فرم ثبت استفاده ناصحیح از دارایی اطلاعاتی

شماره دارایی اطلاعاتی:		طبقه‌بندی حفاظتی:
نام دارایی اطلاعاتی:		
نام بهره‌بردار:		
تاریخ:	ساعت:	محل بهره‌برداری:
شرح گزارش:		
نام گزارش دهنده/ممیز:		سمت:
امضاء:		
نام متصدی/تحويل گیرنده / مالک:		سمت:
امضاء:		

* : حتی الامکان این گزارش به رویت و امضای متصدی/تحويل گیرنده / مالک برسد.

ضمیمه ۳

نحوه استفاده قابل پذیرش-عناوین اختصاصی

استفاده از دستگاه فاکس / فاکس مودم

باید از ارسال اطلاعات برای افراد نامحرم جلوگیری شود و نیز از دریافت اطلاعات مشکوک باید امتناع کرد.

ممکن است دستگاه فاکس مقصد به صورت عمدی یا تصادفی برای ارسال پیام دریافت شده به مکان دیگری برنامه‌ریزی شده باشد، برای جلوگیری از این مشکل باید دستگاه به‌طور مرتب چک شود.

ممکن است پیام به دلیل شماره گیری اشتباه و یا غلط بودن شماره ذخیره شده در حافظه به مکان دیگری ارسال شود. بنابراین نیاز به دقت ارسال کننده فاکس دارد.

بهتر است یکی از افراد معتمد سازمان مسئول استفاده از این دستگاه‌ها باشد و دریافت و ارسال اطلاعات با هماهنگی وی صورت گیرد.

تجهیزات پشتیبانی مانند دستگاه فتوکپی و یا فاکس باید به نحوی در منطقه امن پیش بینی شود که نیازی به خارج کردن اطلاعات نباشد. در صورت چاپ اسناد دارای طبقه‌بندی حفاظتی لازم است همیشه یک نفر مراقب در کنار دستگاه حضور داشته باشد

لازم است تجهیزات ارتباطی فاکس مودم و فاکس بر اساس دستورالعمل ارائه شده از طرف سازنده و در دوره‌های زمانی مناسب و از پیش تعیین شده مورد بازرسی قرار گیرند.

مواد چاپی مورد استفاده در دستگاه‌های فاکس یا چاپگر باید تحت شرایط ایمنی تعیین شده از طرف سازنده، نگهداری شوند و امنیت مکان نگهداری نیز تأمین شود.

نقاط ارسال و دریافت نامه و دستگاه‌های فاکس یا تلکس بدون استفاده، باید حفاظت شده و نباید بدون مراقبت رها شوند.

استفاده از مودم ISDN/DSL

هنگام استفاده از خطوط تلفنی برای ارسال اطلاعات باید از عدم شنود غیر مجاز اطلاعات با چک کردن مداوم خطوط تلفنی اطمینان حاصل نمود.

- لازم است خدمات شرکت‌های ارائه دهنده خدمات DSL از طریق اخذ SLA و کنترل پارامترهای آن تحت مراقبت قرار گیرد.

استفاده از چاپگر به صورت متمرکز، تحت شبکه و یا مجزا

- ممکن است اطلاعاتی که به عنوان پیش‌نویس چاپ شده‌اند و یا اطلاعات باقی مانده روی کاغذ کاربن یا ریبون‌های چاپ، افشاء شده و در فعالیت‌های غیر قانونی مورد استفاده قرار گیرند.

در برخی از سازمان‌ها که خروجی‌های زیاد دارند، عملیات چاپ به صورت پیوسته انجام می‌پذیرد. در این حالت احتمال اختلاط اطلاعات محرمانه با اطلاعات عادی افزایش بسیار خواهد یافت.

کلید رسانه‌ها باید تحت شرایط ایمنی تعیین شده از طرف سازنده، نگهداری شوند و امنیت مکان نگهداری نیز تأمین شود. همچنین لازم است کلید رویه‌ها و سطوح مجوزدهی به دقت مستندسازی شود.

اطلاعات حساس یا طبقه‌بندی شده را پس از چاپ باید فوراً از دستگاه پرینتر دور کرد. دستگاه‌های چاپگر در خارج از ساعات کاری، باید قفل شده و یا در مقابل استفاده‌های غیر مجاز به هر روش ممکن حفاظت شوند.

لازم است کاغذها و سایر رسانه‌های ذخیره اطلاعات، به خصوص در ساعات غیر کاری، در کابینت‌های قفل دار و یا مکان‌های مناسب در نظر گرفته شده برای آن نگهداری شوند.

استفاده از تجهیزات قابل حمل ذخیره اطلاعات شامل دیسک و CD

برای جلوگیری از خراب شدن رسانه‌های ذخیره‌سازی قابل حمل بهتر است آن‌ها را در محفظه‌های مخصوص نگهداری کرد.

بهتر است رسانه‌های قابل حمل در اختیار افراد مشخصی قرار گیرد و آن‌ها مسئولیت جلوگیری از خروج اطلاعات حساس توسط رسانه‌های قابل حمل را به عهده داشته باشند.

- اگر در یک سیستم (PC, Notebook, Thin Client, Blade System, PLC, CNC,....)

اطلاعات بسیار محرمانه‌ای موجود باشد که تحت هیچ عنوان نباید به بیرون سازمان درج کند، بهتر است امکان اتصال رسانه‌های قابل حمل به این سیستم را از طریق نرم‌افزارها و یا سخت‌افزارهای مخصوص این کار محدود کرد.

در صورتی که دیگر نیازی به اطلاعات موجود در رسانه نمی‌باشد، باید این اطلاعات به روش امن پاک شود.

در بخش‌هایی از سازمان که دارای اطلاعات محرمان‌های هستند بهتر است از ورود و خروج رسانه قابل حمل به آن قسمت جلوگیری کرد و در صورت نیاز برای جابجایی اطلاعات داخل آن بخش از رسانه‌های قابل حمل داخلی آن بخش استفاده کرد.

- لازم است تأییدیه لازم برای همراه بردن این رسانه‌ها (انتقال به خارج از محیط معمولی کار) کسب شود و اطلاعات مربوط به این کار برای رسیدگی‌های ممیزی بعدی ثبت و نگهداری شود.

کلیه رسانه‌ها باید تحت شرایط ایمنی تعیین شده از طرف سازنده، نگهداری شوند و امنیت مکان نگهداری نیز تأمین شود. همچنین لازم است کلیه رویه‌ها و سطوح مجوزدهی به دقت مستندسازی شود.

بهتر است از پرچسب‌هایی روی دستگاه‌های قابل حمل استفاده گردد تا در صورت خروج غیر مجاز بتوان خروج آن‌ها را شناسایی نمود.

انهدام اسناد و امحاء

هنگامی که یک سند مورد نیاز نباشد و یا پیش نویس، باطله، زائد و یا مواد مصرفی مانند کاربن‌ها و ریبون‌ها و از قبیل آن باشد بهترین روش حفاظت از آن انهدام و امحاء آن است. تا زمانی که عمل امحاء صورت نگرفته باشد، دارایی‌ها طبقه‌بندی خود را حفظ نموده و باید حفاظت‌های لازم در خصوص آن‌ها رعایت شود.

برای انهدام اسناد یا اطلاعات طبقه‌بندی شده، صادر کنندگان اسناد موظف‌اند به طور مداوم (حداقل سالی یکبار) اسناد یا اطلاعات تولید شده را بازدید و بررسی کنند و در صورتی که نگهداری آن لزومی نداشته باشد نسبت به انهدام آن‌ها اقدام کنند.

جهت انهدام اسناد یا اطلاعات طبقه‌بندی شده، سازمان تولید کننده سند یا اطلاعات ملزم به رعایت ضوابط "آیین نامه و روش اجرایی ترتیب و نگهداری و ضبط اسناد ملی و امحای اوراق زائد" به منظور تشخیص و نگهداری اسناد ملی می‌باشد.

هر گاه در بررسی اسناد یا اطلاعات مشخص شد که سند یا اطلاعات طبقه‌بندی شده‌ای از نظر حفاظتی باید منهدم شود و در صورتی که آن سند یا اطلاعات از نظر نگهداری اسناد ملی نیز جزو اسناد با ارزش نباشد، باید بلافاصله منهدم گردد.

در صورتی که نیاز باشد لازم است تا کمیته‌ای جهت بررسی و امحاء اسناد یا اطلاعات تشکیل و نسبت به امحاء آن اقدام نمایند. وظایف اعضای کمیته امحاء عبارت است از

الف) وظایف نماینده تولید کننده سند یا اطلاعات:

ارایه اسناد یا اطلاعات امحایی برابر (فرم امحا) به کمیته امحا.
انجام اقدامات لازم جهت نقل و انتقال مطمئن اسناد یا اطلاعات به محل امحا.
انهدام اسناد یا اطلاعات با استفاده از روش‌های مناسب
تنظیم صورت جلسه اسناد یا اطلاعات امحا شده و ارسال آن جهت اعضاء کمیته.

ب) وظایف نماینده واحد امنیت اطلاعات

نظارت بر حسن اجرای اصول و مقررات حفاظتی توسط تولیدکننده سند یا اطلاعات.
اعمال تمهیدات حفاظتی لازم.

طرق انهدام اسناد و مدارک طبقه‌بندی شده

الف) اسناد یا رسانه‌های حاوی اطلاعات سری و بکلی سری ابتدا توسط دستگاه خردکن منهدم و سپس سوزانده شوند.

ب) اسناد خیلی محرمانه و محرمانه بنا به تشخیص کمیته امحا باید به طریق زیر منهدم شود:
خردکن به وسیله دستگاه

پودر کردن به وسیله ماشین‌های الکتریکی
سوزاندن (پس از سوزاندن باید آن را کاملاً به هم زد)
خمیر کردن با مواد شیمیایی

انهدام اسناد یا اطلاعات توسط دارندگان سند

الف) صادر کننده سند یا تولیدکننده اطلاعات موظف است پس از تعیین تکلیف اسناد در کمیته تشخیص و تفکیک، مراتب را به کلیه دارندگان سند یا اطلاعات اعلام کند.

ب) لازم است دارندگان اسناد یا اطلاعات جهت انهدام اسناد یا اطلاعاتی که مجوز امحای آن به شرح بند (الف) صادر شده است اقدام نمایند. روش این کار باید در توافقنامه‌های حفظ محرمانگی (موضوع دستورالعمل ۲-۱-۵) قید شود.

ج) گیرندگان اسناد یا اطلاعات طبقه‌بندی شده موظف‌اند در مورد انهدام اسناد یا اطلاعاتی که از سایر سازمان‌ها دریافت کرده‌اند بررسی‌های مداوم معمول و در صورتی که نیازی به

نگهداری آن اسناد نداشته باشند مراتب عدم نیاز خود را به تولید کننده سند یا اطلاعات اعلام کرده و تولید کننده سند یا اطلاعات موظف است در صورت تأیید عدم نیاز دستور را به گیرندگان سند یا اطلاعات اعلام کند.

بدیهی است این دستور انهدام شامل گیرندگان بوده و تولید کننده جهت انهدام اسناد خود باید از طریق کمیته تشخیص و تفکیک اقدام کند.

تهیه طرح‌های حفاظتی اسناد در وضعیت‌های فوق العاده

متصدیان یا تحویل گیرندگان دارایی‌های اطلاعاتی موظف‌اند از نگهداری اسناد یا اطلاعات در مناطق آسیب پذیر خودداری کرده و در مواقع عادی به منظور مقابله با تهدیدهای ناشی از وضعیت فوق العاده مانند: بلایای طبیعی، حملات دشمن، اغتشاشات در داخل و خارج از کشور نسبت به تهیه طرح و پیش بینی‌های لازم با هماهنگی واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و رعایت موارد ذیل اقدام نماید:

تقدّم و تأخّر اسناد یا اطلاعات موجود جهت تخلیه و انهدام تعیین شود.

محل امن جهت انتقال اسناد یا اطلاعات، شناسایی و به وضوح قید شود.

تأمین اسناد یا اطلاعات هنگام تغییر مکان مدنظر قرار گیرد.

تکلیف اسناد یا اطلاعات باقی مانده و اسناد یا اطلاعاتی که امکان انتقال آن نبوده تعیین گردد.

با توجه به موقعیت مکانی و امکانات موجود روش انهدام مشخص گردد.

مجریان تعیین و وظایف آن‌ها مشخص گردد.

فرم امحای اسناد طبقه‌بندی شده
(نمونه)

شماره نام/پرونده نام فایل/ بانک اطلاعاتی	نوع طبقه‌بندی	تعداد برگه‌ها/ حجم	شرح مختصری از پرونده/ نامه/ فایل/ بانک اطلاعاتی	شماره صورتجلسه امحا/ مورخ

اسناد بالا توسط کمیته امحاء (امضاءکنندگان زیر) مورد رسیدگی و ممیزی قرار گرفته
و به روش..... امحاء شد.

اعضای کمیته:

.....امضاء.....تاریخ..... نماینده صادر کننده سند

.....امضاء.....تاریخ..... نماینده واحد امنیت اطلاعات

.....امضاء.....تاریخ..... (۱)

(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
مدیریت دارایی های اطلاعاتی	طبقه بندی اطلاعات
طبقه بندی دارایی های اطلاعاتی شماره دستورالعمل : ۱-۲-۳	

عادی

تأییدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: ((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان

به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

این دستورالعمل نحوه طبقه‌بندی اطلاعات را جهت حفاظت مؤثر از دارایی‌های اطلاعاتی فهرست شده در فهرست موجودی دارایی‌های اطلاعاتی (مشروح در دستورالعمل ۱-۱-۳) بیان می‌دارد. همچنین طبقه‌بندی دارایی‌ها مشخص می‌نماید که در صورت به خطر افتادن امنیت یک دارایی، چه تأثیری در تحقق اهداف سازمان داشته و درجه حساسیت آن به چه میزان است.

مسئولیت‌ها:

- مسئولیت تعریف شاخص‌های طبقه‌بندی اطلاعات بر عهده مدیر واحد امنیت اطلاعات است و طبقه‌بندی‌های انجام شده توسط مدیران قسمت‌ها به وسیله وی به تأیید نهایی می‌رسد.
- مسئولیت تعیین طبقه‌بندی حفاظتی هر دارایی‌های اطلاعاتی بر عهده متصدی، تحویل گیرنده و یا مالک همان دارایی اطلاعاتی می‌باشد.
- مسئولیت بررسی و تأیید طبقه‌بندی دارایی‌های اطلاعاتی تعیین شده به وسیله متصدیان دارایی‌های اطلاعاتی بر عهده مدیران قسمت‌ها می‌باشد.

الزامات:

دستورالعمل طبقه‌بندی، نحوه تعیین اهمیت، اولویت و درجه بندی حفاظتی هر دسته از دارایی‌های سازمان را بیان می‌دارد. این دستورالعمل ممکن است جهت حفاظت از دارایی‌های سازمان مورد بازبینی مجدد قرار گرفته و یا سطوح دیگری به آن اضافه گردد. در این صورت این کار باید توسط واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات ((وزارت/ سازمان/ اداره کل/ شرکت/)) صورت پذیرد و دستورالعمل تهیه شده به تمامی قسمت‌ها اعلام گردد.

باید نکات مربوط به تعداد طبقه‌های تعریف شده و مزایای حاصل از آن به دقت تحت نظر قرار گیرد و در صورت تعریف عناوین مشابه با سایر سازمان‌ها، تفاوت‌ها و جزئیات تمایز این عناوین به اطلاع تمامی قسمت‌ها برسد.

هر قسمت موظف است تا تمامی دارایی‌های اطلاعاتی حوزه خود را طبقه‌بندی نموده و در فرم شناسنامه دارایی‌های اطلاعاتی (موضوع دستورالعمل ۱-۱-۳) ذکر نماید. این طبقه‌بندی باید مورد

بررسی و تأیید واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن قرار گیرد.

لازم است تا پس از تعیین طبقه‌بندی اطلاعات هر دارایی، میزان طبقه‌بندی آن در برچسب‌های دارایی‌های اطلاعاتی (موضوع دستورالعمل ۳-۲-۲) ذکر گردد.

طبقه‌بندی دارایی‌ها ممکن است پس از گذشت زمان تغییر نمایند. لذا لازم است تا طی زمانبندی مناسبی که توسط واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات صورت می‌پذیرد، (حداکثر در بازه‌های زمانی یکساله) مورد بازبینی قرار گیرند.

مسئولیت حفاظت از دارایی‌های طبقه‌بندی شده بر عهده متصدی یا مالک دارایی اطلاعاتی بوده و قابل تفویض به غیر نمی‌باشد. همچنین این فرد موظف است تا آموزش‌ها و آگاهی‌های لازم در خصوص حفاظت از دارایی‌های اطلاعاتی طبقه‌بندی شده را به مجموعه تحت مدیریت خود منتقل نماید.

بهره‌برداری و نگهداری دارایی‌های طبقه‌بندی شده باید بگونه‌ای باشد که امنیت دارایی‌ها را مد نظر قرار دهد لذا لازم است تا موارد مندرج در دستورالعمل ۳-۱-۳ (در خصوص نحوه استفاده قابل پذیرش از دارایی‌های اطلاعاتی) رعایت شود.

تمامی دارایی‌های اطلاعاتی که دارای طبقه‌بندی بالاتری نسبت به شاخص‌های این دستورالعمل می‌باشند باید مجزا گردند. همچنین این نوع دارایی‌ها باید تحت مراقبت شدید قرار گرفته و در مکان‌هایی امن و دور از دسترس افراد غیر مجاز قرار گیرند. لذا در صورت وجود چنین دارایی‌هایی واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات موظف است تا دستورالعمل‌های خاص بهره‌برداری و حفاظت از این نوع دارایی‌ها را تدوین و ابلاغ نماید.

در تعریف طبقه‌بندی و شیوه‌های حفاظتی باید نکات مربوط به نحوه کنترل دسترسی، اشتراک گذاری، نگهداری و انهدام یا امحاء دارایی‌های اطلاعاتی مشخص شده باشد.

فرآیند:**۱- الگوهای پیش فرض طبقه‌بندی حفاظتی دارایی‌های اطلاعاتی عبارت است از:**

طبقه حفاظتی	نوع دارایی اطلاعاتی
خیلی محرمانه	به دارایی‌هایی اطلاق می‌شود که به خطر افتادن امنیت آن‌ها باعث لطمه و آسیب به بخشی از منافع کشور می‌شود. نمونه‌هایی از اطلاعات خیلی محرمانه عبارت‌اند از تحقیق، تولید و نگهداری تجهیزات نظامی، طرح‌های مربوط به حفظ امنیت داخلی شهرها، سوابق امنیتی دارایی‌های اطلاعاتی سازمان از جمله نیروی انسانی شاغل سازمان.
محرمانه	این طبقه‌بندی به دارایی‌های اطلاق می‌شود که انتشار آن بین عموم آزاد نبوده و افشای آن باعث بروز اختلال در بخشی از سیستم‌ها و فرآیندهای داخلی سازمان می‌گردد. به علاوه اطلاعات مربوط به حریم خصوصی افراد حداقل دارای طبقه‌بندی محرمانه می‌باشد.
عادی	دارایی‌هایی که جزو هیچ یک از طبقه‌بندی‌های ذکر شده قرار نگیرد دارای طبقه‌بندی عادی محسوب می‌شود.
محدود	ممکن است یک دارایی دارای طبقه‌بندی عادی بوده ولی شرایط خاصی و محدودیت‌هایی در خصوص نحوه استفاده، مکان و زمان بهره‌برداری از آن دارایی متصور باشد. در این صورت از لفظ محدود به منظور رعایت شرایط و ضوابط خاص مندرج در شناسنامه دارایی اطلاعاتی (مشروح دستورالعمل ۱-۳-۱) استفاده گردد.
حساس	ممکن است یک دارایی اطلاعاتی دارای طبقه‌بندی عادی تا خیلی محرمانه باشد ولی شرایط خاص حفاظتی برای آن نیاز باشد در این صورت لازم است تا از عنوان حساس به منظور رعایت شرایط خاص حفاظتی استفاده گردد. به عنوان مثال ممکن است یک کلمه عبور دارای طبقه‌بندی خیلی محرمانه باشد ولی جهت حفاظت از امنیت آن ممکن است استفاده از سخت‌افزارهای مناسب جهت حفاظت همه جانبه از آن، ضروری باشد. در صورت لزوم باید نکات امنیتی خاص مانند مکان نگهداری اسناد یا اطلاعات طبقه‌بندی شده، حق کپی اسناد خیلی محرمانه، دسترسی توسط اشخاص خاص مکتوب و رعایت گردد.

۲- انجام عمل طبقه‌بندی

پس از تعریف معیارها، لازم است تا کلیه متصدیان و یا مالکان دارایی‌های اطلاعاتی موضوع دستورالعمل ۱-۳-۱ (فهرست موجودی دارایی‌های اطلاعاتی) نسبت به انجام طبقه‌بندی دارایی‌های اطلاعاتی در اختیار خود اقدام نمایند. این اطلاعات به همراه شرایط خاص بهره‌برداری از دارایی و

سایر شرایط حفاظت از دارایی باید در شناسنامه دارایی اطلاعاتی ثبت و تحویل واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات گردد.

۳- تأیید مراکز حراست

پس از مشخص شدن طبقه‌بندی لازم است تا مسئولین واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات نسبت به ارزیابی طبقه‌بندی انجام شده اقدام نمایند. در صورت لزوم اصلاحات صورت گرفته و به مالکان دارایی‌های اطلاعاتی داده شود.

۴- درج طبقه‌بندی در برچسب‌های دارایی‌های اطلاعاتی

لازم است تا پس از تأیید طبقه‌بندی دارایی‌ها، نسبت به درج طبقه‌بندی در برچسب دارایی اطلاعاتی اقدام شود.

۵- بازنگری

با توجه به حساسیت دارایی‌های اطلاعاتی یک سازمان ممکن است لازم باشد تا معیارهای طبقه‌بندی پیچیده تری تدوین و مورد استفاده قرار گیرد. در این صورت طبقه‌بندی یک دارایی متشکل از مجموعه‌ای از معیارها بوده و هر معیار می‌تواند در چند سطح تعریف گردد. در صورت لزوم به تدوین چنین طبقه‌بندی، واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات موظف است تا نسبت به تدوین دستورالعمل طبقه‌بندی اطلاعات متناسب با نیازمندی‌های سازمانی اقدام نماید.

۶- بررسی دوره‌ای

با توجه به اینکه طبقه‌بندی اطلاعات ممکن است با گذشت زمان تغییر نماید لازم است تا طبقه‌بندی‌های انجام شده حداقل هر یک سال یکبار مورد بازبینی و بررسی قرار گیرد.

مرجع:

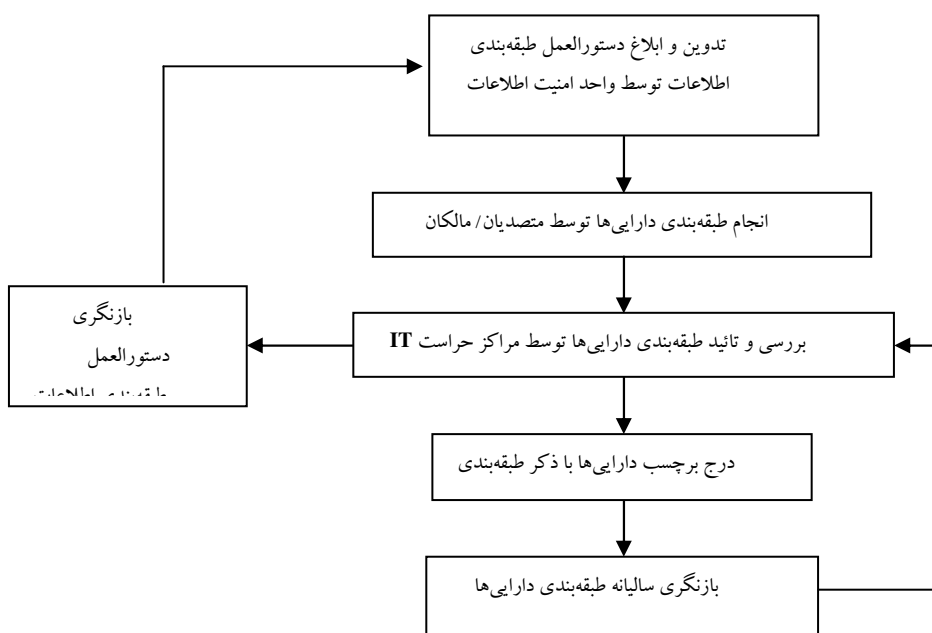
این دستورالعمل به شماره □ - □ / □ - □ / □ - □ ثبت گردیده و سایر اسناد مرتبط با

آن عبارت‌اند از:

- دستورالعمل ۲-۲-۳

- دستورالعمل ۳-۱-۳

روند نما:



(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	طبقه‌بندی اطلاعات
برچسب گذاری دارایی‌های اطلاعاتی شماره دستورالعمل : ۲-۲-۳	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام‌الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل عبارت است از اطمینان از اعلام قابل رؤیت ماهیت یک دارایی اطلاعاتی برای جلوگیری از آسیب پذیری‌های امنیتی یا تبعات ناشی از آن که ممکن است به دلیل نا آگاهی افراد از مشخصه‌های دارایی اطلاعاتی یا الزامات کار با آن به وجود آید.

مسئولیت‌ها:

مسئولیت تهیه برچسب اختصاصی هر دارایی اطلاعاتی به عهده متصدی، تحویل گیرنده و یا مالک همان دارایی می‌باشد.

مسئولیت تعیین روش‌های الصاق برچسب‌ها و محتوی آن‌ها به عهده واحد امنیت اطلاعات می‌باشد.

مسئولیت نظارت بر الصاق برچسب به دارایی‌های اطلاعاتی به عهده مدیران قسمت‌ها می‌باشد.

الزامات:

برچسب دارایی‌های اطلاعاتی فیزیکی از نوع برچسب فیزیکی قابل رؤیت بوده که مشخصاتی نظیر تاریخ برچسب، نام دارایی، طبقه‌بندی شماره اموال، متصدی یا مالک دارایی و مکان استفاده از دارایی را نشان می‌دهد.

برچسب دارایی‌های منطقی از نوع منطقی بوده و علاوه بر موارد فوق، از یک امضای دیجیتال برای بررسی صحت برچسب برخوردار خواهد بود.

شکل و محتوای برچسب توسط واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات تعیین و در اختیار قسمت‌ها قرار می‌گیرد.

برچسب‌های تهیه شده باید حداقل شرایط و کیفیت را متناسب با محل و نوع دارایی، داشته باشند.

فرآیند:

تعریف مجموعه‌ای از فرآیندهای مناسب برای برچسب گذاری و کنترل اطلاعات براساس چهارچوب طبقه‌بندی تعریف شده از سوی سازمان دارای اهمیت بسیار است. این روش‌ها باید کلیه دارایی‌های اطلاعاتی که در قالب فیزیکی و یا الکترونیکی نگهداری می‌شوند را در بر گرفته و پوشش دهد. روش‌های تعریف شده برای برچسب گذاری هر طبقه باید در کلیه مراحل زیر مورد توجه قرار گیرد و برچسب‌های الصاق شده در کلیه مراحل زیر قابل مشاهده و انتقال باشد:

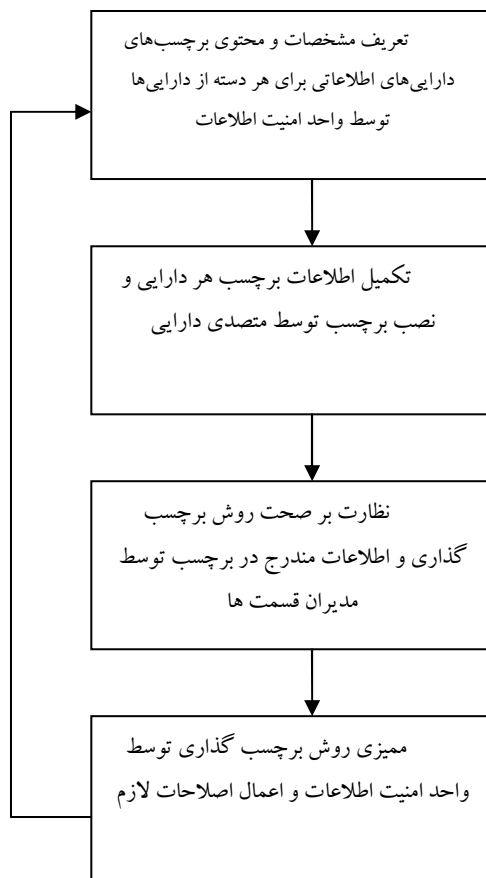
- الف) کپی یا نسخه برداری
- ب) ذخیره، اعم از ذخیره موقت و یا پشتیبان‌گیری
- پ) ارسال به وسیله پست، فاکس و یا پست الکترونیک
- ت) ارسال به وسیله پیام‌های صوتی شامل تلفن‌های همراه، پست صوتی،

منشی‌های الکترونیک

- ث) هنگام انهدام یا امحاء داده‌ها یا دارایی‌های اطلاعاتی
- خروجی سیستم‌های اطلاعاتی که دارای طبقه‌بندی اطلاعاتی هستند نیز شامل برچسب گذاری امنیتی می‌شود. برچسب تخصیص داده شده باید قواعد طبقه‌بندی مطرح شده در دستورالعمل ۱-۲-۳ (طبقه‌بندی دارایی‌های اطلاعاتی) را پوشش دهد.
- این خروجی‌ها عبارت‌اند از مواد چاپی، اطلاعات نمایش داده شده روی صفحه نمایشگر، رسانه‌های ذخیره اطلاعات (نوارهای دیسک، سی دی‌ها، نوار ضبط صوت، حافظه Flash، ...)، پیام‌های الکترونیکی و انتقال فایل. برچسب گذاری فیزیکی همراه با استفاده از فناوری **RFID** معمولاً مناسب‌ترین روش برچسب گذاری است.
- برخی از دارایی‌های اطلاعاتی مانند اسناد ذخیره شده در قالب الکترونیکی قابل برچسب گذاری فیزیکی نمی‌باشند. در این حالت باید از روش‌های الکترونیکی برچسب گذاری استفاده نمود.
- نرم‌افزارها و برنامه‌های کاربردی بخش عمده‌ای از دارایی‌های اطلاعاتی را تشکیل می‌دهند. هدف اصلی در پیاده‌سازی نظام مدیریت امنیت اطلاعات نهایتاً حفاظت از دارایی‌های اطلاعاتی نرم‌افزاری در قالب فایل‌های داده، بانک‌های اطلاعاتی، نرم‌افزارهای پردازشی یا سایت‌های ارتباطی یا اطلاع رسانی می‌باشد. برچسب گذاری این دسته از دارایی‌های اطلاعاتی از اهمیت و همچنین پیچیدگی زیاد برخوردار است. لازم است هنگام مراجعه افراد به این دسته از دارایی‌های اطلاعاتی برچسب مشخصات مربوط حاوی شرایط بهره‌برداری یا تعامل با آن دارایی اطلاعاتی به‌طور واضح به اطلاع کاربر برسد.

روندنما:

روند نمای فعالیت تهیه و الصاق برچسب به شرح زیر است:



(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک
گزارش شناخت سازمان / سیستم شماره دستورالعمل: ۱-۳-۳	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع:

این سند به عنوان سند محرمانه طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات می‌باشد. کلیه اسنادی که بر اساس این سند تولید یا گردآوری می‌شوند حداقل دارای طبقه‌بندی خیلی محرمانه خواهند بود. تصمیم‌گیری در خصوص سطح حداکثری طبقه‌بندی حفاظتی این اسناد به عهده تهیه کننده یا گردآورنده سند می‌باشد.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل تبیین ضرورت مستندسازی وضعیت ساختار، تجهیزات و روش‌های استفاده از تجهیزات و دارایی‌های اطلاعاتی می‌باشد. این مستندات با رویکرد بهره‌برداری از آن‌ها برای شناسایی نقاط آسیب‌پذیر و رفع آن‌ها، بهبود عملکرد و تصحیح روش‌های ارائه خدمات رایانه‌ای و امن‌سازی دارایی‌های اطلاعاتی متعلق به ((وزارت/ سازمان/ اداره کل/ شرکت/...)) تهیه خواهند شد.

مسئولیت:

مسئولیت تهیه گزارش شناخت سازمان به عهده کارگروه امنیت اطلاعات می‌باشد. این گزارش باید به کمیته امنیت اطلاعات ارسال شود و یک نسخه از آن نیز به رؤیت ((بالاترین مقام اجرایی سازمان)) برسد.

الزامات:

- لازم است گزارش شناخت سازمان حداقل دارای بخش‌های زیر باشد:
- ۱- خلاصه تاریخچه فعالیت سازمان و تاریخچه بهره‌برداری از سامانه‌های رایانه‌ای
 - ۲- ساختار و چارت سازمانی
 - ۳- وضعیت فعلی سازمان، نحوه بهره‌برداری از سامانه‌های رایانه‌ای و خدمات قابل ارائه توسط آن‌ها
 - ۴- آخرین تحول مهم در وضعیت سامانه‌های پردازشی و ارائه خدمات رایانه‌ای
 - ۵- هدف‌گذاری و برنامه‌های آینده تحول در نحوه ارائه خدمات (تبدیل خدمات معمولی به خدمات رایانه‌ای و یا بهبود روش‌های فعلی ارائه خدمات رایانه‌ای) در قالب افق‌های زمانی زیر:
- افق کوتاه مدت (برنامه یکساله)
 - افق میان مدت (برنامه‌های منطبق بر هدف‌گذاری‌های برنامه چهارم و پنجم توسعه اقتصادی، اجتماعی دولت جمهوری اسلامی ایران مصوب مجلس شورای اسلامی، سند امنیت فضای تبادل اطلاعات کشور- افتا و سند راهبردی نظام جامع فناوری اطلاعات کشور)
 - افق بلند مدت (چشم انداز بیست ساله - ایران ۱۴۰۴)

۶- پلان مکان‌های استقرار املاک سازمان (که بر اساس سند تعیین قلمرو پیاده‌سازی نظام مدیریت امنیت اطلاعات در حوزه مدیریت مستقیم کمیته امنیت اطلاعات سازمان قرار دارند)

۷- پلان مکان‌های استقرار تجهیزات و دارایی‌های اطلاعاتی و جانمایی آن‌ها

۸- مکان‌های ارائه خدمات رایانه‌ای از قبیل سایت سازمانی، کیوسک‌های اطلاعاتی، تجهیزات دریافت و پرداخت، محیط Web، محیط‌های BBS و غیره

۹- نقشه معماری و توپولوژی شبکه‌های ارتباطی سازمان (WAN, MAN, CAN, LAN)

۱۰- فهرست کانال‌های ارتباطی با سایر شبکه‌های خارج از کنترل سازمان شامل نوع، ظرفیت، نام مرجع کنترل کننده شبکه اعم از شبکه‌های باسیم، بی سیم، ماهواره‌ای، فیبر نوری که برای انتقال داده، صوت و یا تصویر به کار گرفته می‌شوند.

۱۱- فهرست موجودی دارایی‌های اطلاعاتی (موضوع دستورالعمل ۳-۱-۱) همراه ذکر نام

مالک، متصدی و یا تحویل گیرنده (موضوع دستورالعمل ۳-۱-۲) هر یک از اجزای آن

۱۲- مکانیزم‌های کنترلی و امنیتی فعلی برای حفاظت از دارایی‌های اطلاعاتی

فرآیند شناخت سازمان / سیستم:

هدف از پیاده‌سازی سامانه مدیریت امنیت اطلاعات نظام مند نمودن فعالیت‌های مرتبط با ایجاد و حفظ امنیت اطلاعات می‌باشد. برای دستیابی به این هدف لازم است از روشی سازمان یافته سود برده شود. به‌طور کلی فرض بر آن است که در بخش بزرگی از نهادها یا سازمان‌های دولتی و خصوصی نظام‌های یکپارچه مدیریت امنیت اطلاعات وجود ندارد و فعالیت‌های مرتبط با حفظ امنیت هنوز به‌طور کامل در برنامه‌های توسعه‌ای وارد نشده‌اند.

مرحله شناخت سیستم یکی از مراحل اساسی در ایجاد نظام مدیریت امنیت اطلاعات است. بر

اساس نتایج حاصل از این مرحله می‌توان به اطلاعات زیر دست یافت:

- تاریخچه فعالیت سازمان
- تاریخچه بهره‌برداری از سامانه‌های پردازشی و خدمات رایانه‌ای
- برنامه‌های سازمان در خصوص ارائه سرویس‌ها و خدمات جدید مبتنی بر فناوری‌های اطلاعاتی
- توان پردازشی سازمان

- نوع تجهیزات و دارایی‌های اطلاعاتی و ظرفیت‌های هر یک
 - کفایت توان پردازش موجود برای پاسخگویی به نیازهای فعلی
 - تناسب برنامه‌های توسعه ظرفیت پردازش یا انتقال داده‌ها و اطلاعات با برنامه‌های توسعه‌ای آتی سازمان
 - توزیع جغرافیایی املاک و مکان‌های استقرار تجهیزات و دارایی‌های اطلاعاتی
 - توزیع جغرافیایی مکان‌های ارائه خدمات رایانه‌ای
 - تنوع تجهیزات و دارایی‌های اطلاعاتی
 - نوع کانال‌های ارتباطی و نحوه انتقال داده‌ها
 - تنوع و خصوصیات سازمان‌های دیگری که ارتباط اطلاعاتی با آن‌ها وجود دارد.
- اطلاعات و مدارک جمع‌آوری شده در این مرحله به عنوان اطلاعات پایه برای مرحله ارزیابی و مدیریت ریسک به کار گرفته خواهد شد.
- نوع و نحوه جمع‌آوری اطلاعات لازم برای تکمیل گزارش مرحله شناخت سیستم در ادامه شرح داده شده است.

الف- خلاصه تاریخچه فعالیت سازمان و تاریخچه بهره‌برداری از سامانه‌های رایانه‌ای

این بخش از گزارش باید حداقل حاوی مطالب زیر باشد:

- الف-۱- تاریخ تأسیس
- الف-۲- مأموریت اصلی سازمان
- الف-۳- حوزه جغرافیایی ارائه خدمات (محلی، منطقه‌ای، کشوری)
- الف-۴- دسته‌بندی (طبقه‌بندی) در نظر گرفته شده برای سازمان از دیدگاه سازمان پدافند غیرعامل
- الف-۵- آمار نیروی انسانی، بودجه پیش‌بینی شده و بودجه صرف شده در پنج سال گذشته
- الف-۶- تاریخ استفاده کاربردی از تجهیزات پردازشی در ارائه خدمات سازمان به تفکیک خدمات داخلی (امور داخلی مثل سیستم‌های حضور و غیاب، حقوق و دستمزد، حسابداری، کنترل پروژه، ...) و خدمات ارائه شده به ارباب رجوع یا سایر مراجع

خارج از سازمان (مثل اطلاع رسانی از طریق BBS، اینترنت، Call Center،

خدمات فروش یا دریافت و پرداخت الکترونیکی، ...)

الف-۷- فهرست خدمات پردازشی فعلی سازمان به تفکیک خدمات داخلی یا خدمات

ارائه شده به ارباب رجوع

الف-۸- نیروی انسانی، بودجه پیش بینی شده و بودجه صرف شده در بخش پردازش

اطلاعات یا خدمات رایانه‌ای در پنج سال گذشته

ب- ساختار و چارت سازمانی

این بخش از گزارش باید حداقل حاوی مطالب زیر باشد:

ب-۱- مستندات قانونی و حقوقی فعالیت، قوانین و مقررات اجرایی مربوط به حوزه

فعالیت و اسناد مکتوب مرتبط با فعالیت‌های پردازشی موجود در حوزه فعالیت

ب-۲- چارت سازمانی

ب-۳- فهرست فرآیندهای سازمانی و خدمات قابل ارائه توسط سازمان

ب-۴- شرح وظائف مختصر هر یک از مشاغل موجود در چارت سازمانی

ج- وضعیت فعلی سازمان و نحوه بهره‌برداری از سامانه‌های رایانه‌ای و خدمات قابل ارائه

توسط آن‌ها

این بخش از گزارش باید حداقل حاوی مطالب زیر باشد:

ج-۱- فهرست و شرح فرآیندهای پردازشی یا فرآیندهایی که منجر به ارائه خدمات

رایانه‌ای به ارباب رجوع یا سایر بهره‌برداران می‌گردد.

ج-۲- شرح کامل وظائف هر یک از مشاغل موجود در چارت سازمانی که مرتبط با

فرآیندهای فوق هستند و دارای نقش مستقیم در پیش برد فرآیند مربوط می‌باشند.

د- آخرین تحول مهم در وضعیت سامانه‌های پردازشی و ارائه خدمات رایانه‌ای

این بخش از گزارش باید حداقل حاوی مطالب زیر باشد:

د-۱- عنوان تحول (به عنوان مثال افتتاح مرکز داده، ارائه خدمات از طریق اینترنت، بهبود

شبکه LAN، ایجاد شبکه WAN، آموزش نیروی انسانی، استفاده از یک استاندارد

جدید، ارائه یک خدمت جدید از طریق شبکه،)

د-۲- شرح فعالیت انجام شده

د-۳- بودجه صرف شده

د-۴- میزان بهبود یا افزایش کارایی فعالیت انجام شده (به عنوان مثال صرفه جویی در هزینه، رضایت ارباب رجوع، رضایت کارمندان، پاسخ گویی به مقررات و قوانین، پیاده‌سازی برنامه‌های توسعه‌ای، تعالی سازمانی،)

و- هدفگذاری‌ها و برنامه‌های آینده تحول در نحوه ارائه خدمات

این بخش باید حداقل حاوی مطالب زیر باشد:

و-۱- شرح فعالیت‌هایی که طی یکسال آینده انجام خواهد شد و بودجه در نظر گرفته شده برای انجام آن

و-۲- فهرست فعالیت‌های برنامه‌ریزی شده جهت انجام در پنج سال آینده (بر اساس اسناد بالادستی مثل برنامه‌های توسعه، سندهای راهبردی افتا و نظام جامع فناوری اطلاعات کشور) و بودجه برآورد شده برای انجام آن‌ها

و-۳- چشم انداز طراحی شده برای افق بلند مدت با هدفگذاری‌های پنج ساله بر اساس برنامه چشم انداز ایران ۱۴۰۴

ز- پلان مکان‌های استقرار املاک سازمان

این بخش از گزارش باید حداقل حاوی مطالب زیر باشد:

ز-۱- مکان استقرار

توجه:

در صورتی که حوزه جغرافیایی مکان استقرار یا ارائه خدمات محدود به یک شهر یا یک استان باشد، حوزه ارائه خدمات محلی محسوب می‌شود و لازم است مکان‌های استقرار روی نقشه‌های ۱:۱۰۰۰۰ و یا ۱:۲۵۰۰۰ مشخص گردد.

در صورتی که حوزه جغرافیایی مکان استقرار یا ارائه خدمات محدوده فراتر از یک استان و کمتر از نصف تعداد استان‌های کشور باشد حوزه ارائه خدمات منطقه‌ای محسوب شده و علاوه بر تهیه نقشه‌های فوق لازم است مکان‌های استقرار بر روی نقشه‌های کشوری با مقیاس مناسب مشخص گردد.

در صورتی که حوزه جغرافیایی مکان استقرار یا ارائه خدمات کل سطح کشور یا خارج از آن باشد حوزه ارائه خدمات کشوری محسوب شده و لازم است مکان‌های استقرار علاوه بر نقشه‌های فوق بر روی نقشه‌های مناسب مشخص گردد.

ز-۲- در صورتی که ارائه خدمات به واحدهای سازمان یا ارباب رجوع از طریق شبکه‌های اطلاع رسانی (به عنوان مثال اینترنت یا اینترنت) اعم از بی سیم، باسیم، فیبر نوری و یا هر نوع کانال انتقال دیگر انجام می‌شود لازم است نقطه ارائه خدمات (POP)^{۱۳} یا حوزه ارائه خدمات (Service Coverage) بر روی نقشه‌های جغرافیایی مناسب ترسیم گشته و ظرفیت‌های مربوط مثل پهنای باند، تعداد کانال‌های ارتباطی، توان قابل دریافت، نوع و مشخصات تجهیزات دریافت یا برقراری ارتباط و غیره همراه آن درج گردد.

ز-۳- لازم است تأسیسات و ساختمان‌ها و کاربری‌های اطراف مکان استقرار املاک یا دارایی‌های عمده اطلاعاتی سازمان شناسایی شده و در صورت شناسایی به عنوان منبع تهدید با علائم مناسب علامت گذاری شوند (به عنوان مثال وجود پمپ بنزین، انبار سوخت، پست‌های توزیع نیرو، رودخانه (به‌خصوص رودخانه‌های فصلی)، محلات جرم خیز و...) در اطراف مکان‌ها به عنوان منبع تهدید تلقی می‌شوند.

ح- پلان‌های محل استقرار تجهیزات و دارایی‌های اطلاعاتی و جانمایی آن‌ها

این بخش از گزارش باید حداقل حاوی مطالب زیر باشد.

ح-۱- جانمایی هر یک از تجهیزات یا دارایی‌های اطلاعاتی فیزیکی در پلان ساختمان محل استقرار

ح-۲- نقشه کامل تأسیسات مثل آب، برق، گاز، هوای فشرده، سیستم اطفاء حریق، تهویه و ...

ح-۳- نقشه شبکه‌های ارتباطی مثل کابل تلفن، کابل‌های شبکه، فیبر نوری و...

ط- مکان‌های ارائه خدمات رایانه‌ای

این بخش از گزارش باید حاوی اطلاعات زیر باشد.

¹³ Point of Presence

ط-۱- فهرست خدمات رایانه‌ای که سازمان به ارائه آن‌ها می‌پردازد به تفکیک خدمات داخلی یا خدمات قابل ارائه به ارباب رجوع (مانند سیستم اتوماسیون، سیستم حقوق و دستمزد، اطلاع رسانی، دریافت فرم‌های تقاضا و...)

ط-۲- نوع ارائه خدمات (مانند ارائه از طریق کیوسک‌های اطلاع رسانی، کیوسک‌های دریافت و پرداخت، شبکه داخلی سازمان، اینترنت سازمانی، اینترنت و...)

ط-۳- مکان‌های ارائه خدمات (مانند اتاق دبیرخانه، بخش خدمات پس از فروش، سالن انتظار، محیط Web، تمام محوطه سازمان از طریق شبکه بی سیم،) به‌طور کلی لازم است ماهیت کلیه مکان‌هایی که خدمات در آن‌ها قابل ارائه به درخواست کنندگان خدمات (اعم از کارمندان داخلی و ارباب رجوع) می‌باشد، ذکر گردد.

ک- نقشه معماری و توپولوژی شبکه‌های ارتباطی سازمان

این بخش از گزارش باید حاوی اطلاعات زیر باشد:

ک-۱- توپولوژی شبکه ارتباطی سازمان با ذکر انواع تکنولوژی‌های به کار گرفته شده و ظرفیت‌های انتقال

ک-۲- نقشه‌های معماری شبکه با ذکر نوع تجهیزات، آدرس شبکه و نقش هر یک از تجهیزات اعم از مخابراتی، پردازشی و امنیتی

توجه ۱: لازم است این اطلاعات دارای طبقه‌بندی محرمانه یا بالاتر باشد. (سطح حداکثری طبقه‌بندی با توجه به نظر مالک یا تحویل گیرنده و یا متصدی تجهیزات تعیین خواهد شد).

توجه ۲: سطح طبقه‌بندی سند نباید کمتر از سطح طبقه‌بندی هیچیک از تجهیزات یا دارایی‌های اطلاعاتی مندرج در آن باشد.

توجه ۳: لازم است حین جمع‌آوری اطلاعات شناخت سازمان یا بعد از آن تدابیر لازم برای حفاظت از این اسناد که جزو اسناد مهم سازمانی تلقی می‌شوند در نظر گرفته شده و این اسناد در محل‌های امن نگهداری شوند.

ل- فهرست کانال‌های ارتباطی با سایر شبکه‌ها

این بخش از گزارش باید حداقل حاوی مطالب زیر باشد.

ل-۱- نام کانال و کاربرد آن

ل-۲- نوع تکنولوژی مورد استفاده

ل-۳- ظرفیت کانال

ل-۴- نام مرجع، سازمان و یا شرکت تامین و یا کنترل‌کننده کانال (مثل شرکت مخابرات ایران و...)

ل-۵- اطلاعات نقطه تماس مرجع تامین و یا کنترل‌کننده کانال

مرجع

این دستورالعمل به شماره □-□-۱-۳-۳/□-□ ثبت شده است و سایر دستورالعمل‌های

مرتبط با آن عبارت‌اند از:

- دستورالعمل ۳-۱-۱

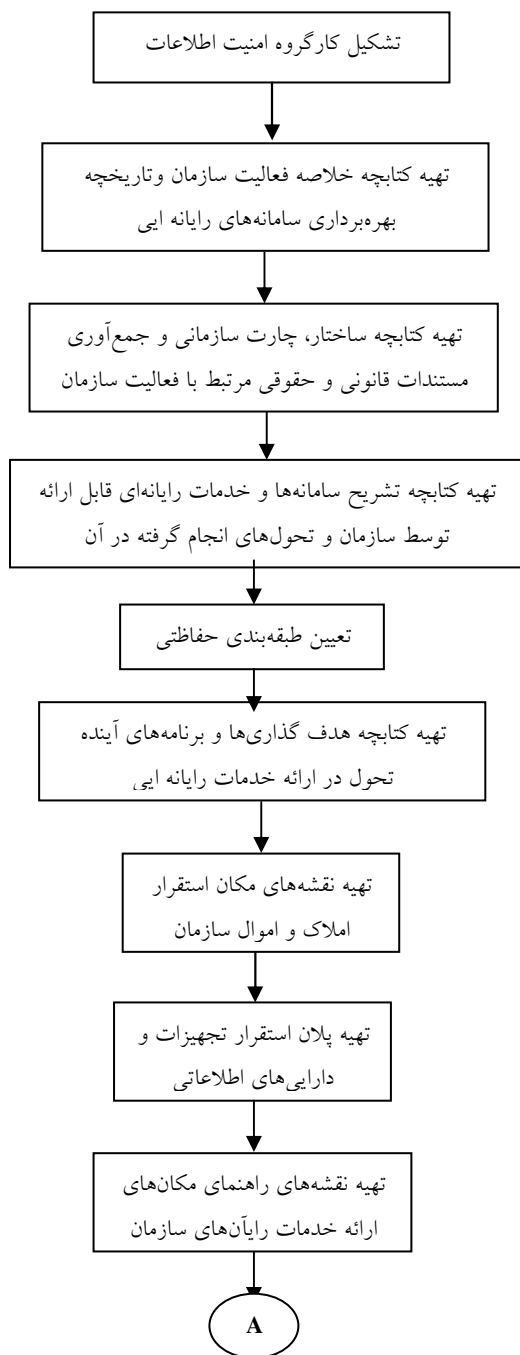
- دستورالعمل ۱-۱-۳

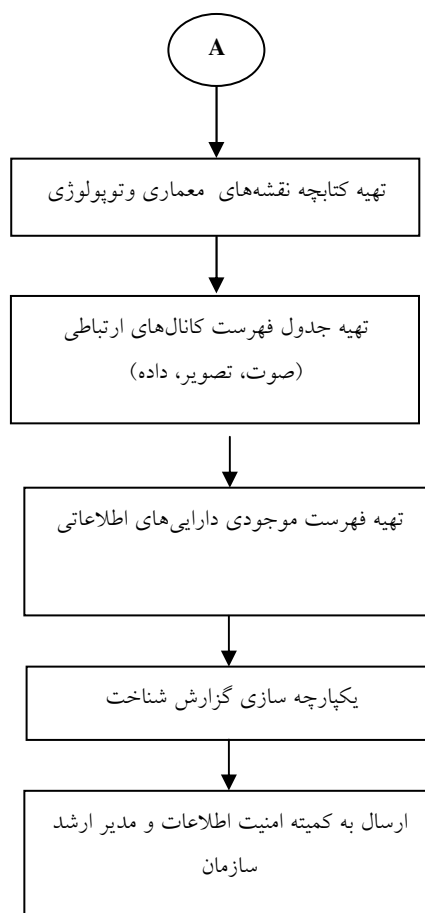
- دستورالعمل ۲-۱-۳

- دستورالعمل ۲-۳-۳

روند نما

روند نمای شناخت سازمان / سیستم در شکل زیر نشان داده شده است.





(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک
ارزیابی ریسک	
شماره دستورالعمل : ۲-۳-۳	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به عنوان دبیر منصوب خواهد شد.

[illegible]

هدف

این دستورالعمل مبین مسئولیت‌ها، متدولوژی و روش‌های ارزیابی ریسک قابل اجراء در ((وزارت/ سازمان/ اداره کل/ شرکت /...)) برای ارزیابی ریسک‌های مرتبط با دارایی‌های اطلاعاتی تحت مالکیت یا مدیریت و موجود در قلمرو پیاده‌سازی نظام مدیریت امنیت اطلاعات (موضوع دستورالعمل ۱-۳) می‌باشد. هدف از تدوین این دستورالعمل ارائه روشی ساده و قابل اجراء برای ارزیابی ریسک امنیت اطلاعات در حوزه‌های محرمانگی، جامعیت (صحت) و دسترسی پذیرای اطلاعات می‌باشد.

مسئولیت

- مسئولیت ارزیابی ریسک مرتبط با هر فرآیند یا هر جزء از دارایی‌های اطلاعاتی با مالک، متصدی و یا تحویل گیرنده فرآیند یا دارایی اطلاعاتی (موضوع قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات (دستورالعمل ۱-۳)) می‌باشد. به عنوان مثال مسؤول اتاق سرور مسؤول ارزیابی و مستندسازی ریسک کلیه فرآیندهای مرتبط با فعالیت تجهیزات مستقر در اتاق سرور (موجود در قلمرو پیاده‌سازی) و استخراج شاخص ریسک مربوط می‌باشد.
- مسئولیت ارزیابی ریسک کلی و مقایسه ریسک واحدهای مختلف با یکدیگر و تعیین اولویت‌های امن‌سازی بخش‌ها، فرآیندها و یا دارایی‌های اطلاعاتی با نهاد متصدی امنیت اطلاعات (به عنوان مثال مرکز حراست فناوری اطلاعات یا ارتباطات و یا نهادهای معادل آن) می‌باشد. در صورت عدم وجود این نهاد، این مسئولیت به عهده کمیته امنیت اطلاعات خواهد بود.

الزامات

- لازم است ارزیابی ریسک برای کلیه بخش‌ها، فرآیندها و دارایی‌های اطلاعاتی موجود در سند قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات به انجام رسد. این ارزیابی باید برای کلیه دارایی‌های اطلاعاتی لازم برای اجرای هر فرآیند و کلیه فرآیندهای قابل اجرا در هر بخش از سازمان به عمل آید، به نحوی که بتوان:
- اولاً دارایی‌های اطلاعاتی را از لحاظ مقدار ریسک مرتبط با استفاده از آن‌ها نسبت به یکدیگر رده بندی کرد. مثال: ریسک سرقت اطلاعات از کامپیوترهای متصل به شبکه بیشتر

از ریسک سرقت اطلاعات از کامپیوترهای مجزا می‌باشد. همچنین استفاده از شبکه‌های بی سیم ریسک را افزایش می‌دهد.

ثانیاً فرآیندهای اجرایی مختلف را از لحاظ مقدار ریسک مرتبط با اجرای آن‌ها نسبت به یکدیگر رده بندی کرد. مثال: ریسک امنیتی فروش تلفنی بیشتر از فروش معمولی و ریسک امنیتی فروش الکترونیکی بیشتر از فروش معمولی یا تلفنی می‌باشد.

ثالثاً بخش‌های مختلف سازمان را از لحاظ پتانسیل آسیب پذیری در مقابل تهدیدهای مختلف موجود در زمینه امنیت اطلاعات دسته‌بندی نمود. مثال: ریسک امنیتی مکان‌هایی که به ارایه خدمات حضوری به ارباب رجوع می‌پردازند بیشتر از مکان‌های دیگر سازمان است و به همین ترتیب ریسک امنیتی ساختمانی که در مجاورت یک پمپ بنزین قرار گرفته بیشتر از ساختمان‌های دیگر است.

- لازم است فعالیت‌های امن‌سازی بر اساس تحلیل نتایج حاصل از ارزیابی ریسک اولویت بندی شوند به نحوی که:

دارایی‌های اطلاعاتی دارای بیشترین آسیب پذیری (با ریسک بالا) در اولویت قرار گرفته و رویه‌های مدیریت و کنترل ریسک (دستورالعمل ۳-۳-۳) در مورد آن‌ها به اجرا گذاشته شود. پس از امن‌سازی دارایی‌های اطلاعاتی فوق فرآیندهای دارای بیشترین آسیب پذیری (با ریسک بالا) در اولویت قرار گرفته و رویه‌های مدیریت و کنترل ریسک (دستورالعمل ۳-۳-۳) در مورد آن‌ها به اجرا گذاشته شود.

○ پس از طی دو مرحله فوق به عنوان مراحل اضطراری، اولویت بندی سایر دارایی‌ها و فرآیندهای اجرایی تعیین و رویه‌های مدیریت و کنترل ریسک در مورد آن‌ها به اجرا گذاشته شود.

○ در آخرین مرحله وضعیت ریسک باقیمانده^{۱۴} بخش‌های مختلف سازمان نسبت به یکدیگر مجدداً ارزیابی شده و برنامه مدیریت و کنترل آن‌ها تدوین شود.

- لازم است ارزیابی ریسک برای کلیه دارایی‌های اطلاعاتی مندرج در فهرست موجودی دارایی‌های اطلاعاتی (دستورالعمل ۳-۱-۲) به انجام رسد.

^{۱۴} - ریسک باقیمانده عبارت است از آن مقدار از ریسک که پس از اجرای امن‌سازی به‌طور طبیعی باقی خواهد ماند و یا با نظر مدیریت قابل پذیرش محسوب می‌شود.

لازم است کلیه دارایی‌های اطلاعاتی قبلاً ارزش گذاری شوند. ارزش هر دارایی اطلاعاتی به وسیله مالک، متصدی و یا تحویل گیرنده آن دارایی تعیین خواهد شد. هنگام ارزش گذاری باید کلیه آثار ناشی از فقدان یا عدم عملکرد صحیح هر یک از دارایی‌های اطلاعاتی و زیان حاصل از آن برای سازمان و یا مشتریان و ارباب رجوع در نظر گرفته شود. ارزش گذاری می‌تواند به صورت کیفی یا کمی باشد. در صورت ارزش گذاری کیفی می‌توان از شاخص‌های بسیار پر ارزش، پر ارزش، ارزش متوسط و یا کم ارزش استفاده کرد. در صورت ارزش گذاری کمی می‌توان از ارزش ریالی دارایی اطلاعاتی و یا هزینه‌های پرداخت شده جهت دستیابی به آن دارایی استفاده کرد.

- لازم است آسیب پذیری‌های احتمالی هر دارایی فهرست شوند. نقاط آسیب پذیر نشاندهنده نقاط ضعف هر دارایی و عوامل تولید ریسک می‌باشد.

لازم است تهدیدهای موجود برای هر دارایی فهرست شوند. تهدیدها عبارت‌اند از شرایطی که ممکن است باعث سوء استفاده از نقاط آسیب پذیر هر دارایی اطلاعاتی یا فرآیند شده و یا موجب ضربه پذیری از آن نقطه شوند.

- لازم است برای هر یک از تهدیدهای فهرست شده فوق مکانیزم‌های کنترلی مناسب بر اساس مدل استاندارد مرجع شناسایی شده و طبق دستورالعمل مدیریت و مقابله با ریسک (دستورالعمل ۳-۳-۳) به اجراء گذاشته شود.

از آن‌جا که ممکن است مکانیزم‌های کنترلی به دفعات و برای امن‌سازی فرآیندهای مختلف مورد اشاره واقع شوند، لازم است فهرست خلاصه‌ای از آن‌ها تحت عنوان فهرست مکانیزم‌های کنترلی شناسایی شده بر اساس ارزیابی ریسک تهیه شود تا بتوان بیانیه کاربردپذیری (SOA) اختصاصی سازمان (دستورالعمل ۳-۳-۴) را بر اساس آن تدوین نمود.

- لازم است گزارش جمع بندی ارزیابی ریسک امنیتی به کمیته امنیت اطلاعات ارسال شود. در این گزارش باید به نام دارایی‌هایی که حفاظت از آن‌ها دارای اهمیت زیاد می‌باشد اشاره شود.

- لازم است کمیته امنیت اطلاعات امن‌سازی دارایی‌های اطلاعاتی دارای اهمیت زیاد را مستقیماً تحت نظر بگیرد.

- لازم است سایر دارایی‌ها بر اساس رهنمودهای مندرج در سند راهنمای سیاست گذاری امنیت اطلاعات (دستورالعمل ۱-۱) تحت محافظت قرار گیرند.

- ممکن است برخی دارایی‌های اطلاعاتی در مرحله اول ارزیابی از نظر پوشیده باقی بمانند. بنابراین لازم است شناسایی دارایی‌های اطلاعاتی به صورت مستمر (و در دوره‌های زمانی قابل توجیه) و یا به خصوص هنگام تغییر در فرآیندهای اجرایی، تغییر در روش انجام کار، تغییر مکان دارایی‌های اطلاعاتی و یا بهره‌برداری از فرآیندها یا دارایی‌های اطلاعاتی جدید انجام پذیرد.

فرآیند ارزیابی ریسک امنیت اطلاعات

فرآیند ارزیابی ریسک امنیت اطلاعات شامل کلیه مسئولیت‌ها، متدولوژی و رویه‌های قابل اجراء توسط برنامه ریزان، بهره‌برداران و کاربران ((وزارت/ سازمان/ اداره کل/ شرکت /...)) در حوزه ارزیابی ریسک‌های موجود در زمینه محرمانگی، جامعیت، دسترسی پذیری داده‌ها و اطلاعات و دارایی‌های اطلاعاتی متعلق به ((وزارت/ سازمان/ اداره کل/ شرکت /...)) می‌باشد. منظور از داده‌ها، اطلاعات و دارایی‌های اطلاعاتی آن دسته از دارایی‌های اطلاعاتی می‌باشد که در حوزه قلمرو تعریف شده برای پیاده‌سازی سامانه مدیریت امنیت اطلاعات (موضوع دستورالعمل ۱-۳-۱) مبتنی بر ((استاندارد مرجع)) قرار گرفته‌اند.

الف- مسئولیت ارزیابی ریسک

مسئولیت ارزیابی ریسک هر فرآیند یا دارایی اطلاعاتی به عهده متصدی فرآیند یا مالک یا تحویل گیرنده دارایی اطلاعاتی می‌باشد. این مسئولیت به صورت سلسله مراتبی به مسئولین رده بالاتر منتقل می‌شود. بنابراین به عنوان مثال، متصدی اتاق سرور مسئولیت شناسایی ریسک و استخراج شاخص ریسک کلیه فرآیندهای مرتبط با فعالیت تجهیزات اتاق سرور (در قلمرو ISMS) را به عهده دارد. علاوه بر آن در صورتی که متصدی اتاق سرور تحت نظر مدیر واحد کامپیوتر فعالیت نماید مدیر واحد کامپیوتر نیز مسئولیت بررسی و تأیید نهایی شاخص ریسک استخراج شده را به عهده دارد.

نظارت بر فعالیت‌های ارزیابی ریسک بر عهده کمیته امنیت اطلاعات می‌باشد. در صورتی که ارزیابی ریسک برای اولین بار به اجرا گذاشته شود آن ارزیابی، ارزیابی ریسک اولیه محسوب شده و مسئولیت پیشبرد آن با کارگروه امنیت اطلاعات و یا هر مرجع دیگری است که توسط کمیته امنیت اطلاعات تعیین شود.

ب- شناسایی فرآیندهای اجرایی در حوزه خدمات رایانه‌ای

فرآیندهای اجرایی موجود در حوزه ارائه خدمات رایانه‌ای بر اساس سند تعیین قلمرو (دستورالعمل ۱-۳-۱) شناسایی خواهند شد. لازم است فرآیندهای اصلی منجر به ارائه خدمات به مشتریان و به دنبال آن فرآیندهای پشتیبانی که فرآیندهای اصلی را امکان‌پذیر می‌سازند شناسایی گردند. به عنوان مثال کلیه فرآیندهای قابل اجرا در اتاق سرور بر روی سروهای مختلف فرآیند اصلی محسوب می‌شود. به علاوه فرآیند تأمین انرژی در مواقع قطع برق (مثل استفاده از UPS یا ژنراتور اضطراری) فرآیند پشتیبان محسوب می‌شود.

همچنین در یک سازمان متعارف ارائه خدمات الکترونیک در محیط Web فرآیند اصلی و تأمین خطوط مخابراتی برای دسترسی به محیط Web فرآیند پشتیبانی محسوب می‌گردد. اما در یک شرکت مخابراتی مثل شرکت مخابرات استان تهران یا شرکت‌های PAP^{۱۵} فرآیند تأمین خطوط مخابراتی به عنوان یک فرآیند اصلی محسوب می‌شود. لازم است ارزیابی ریسک برای هر دو دسته فرآیندهای اصلی و فرآیندهای پشتیبان به انجام برسد.

ج- شناسایی دارایی‌های اطلاعاتی

متصدی هر فرآیند باید مطالعه کاملی از فرآیند تحت مدیریت خود به عمل آورد و کلیه دارایی‌های اطلاعاتی مرتبط با پردازش آن فرآیند را شناسایی نماید. همچنین لازم است کلیه دارایی‌های اطلاعاتی که ممکن است به نحوی در حوزه اجرای مدیریت امنیت اطلاعات قرار گیرند نیز شناسایی شوند. از دسته‌بندی زیر می‌توان به عنوان دسته‌بندی مرجع استفاده کرد:

دسته‌بندی دارایی اطلاعاتی	شکل دارایی اطلاعاتی
داده‌های الکترونیکی و مواد مرتبط با آن	بانک‌های اطلاعاتی، فایل‌های داده، مستندات سیستم، راهنمای استفاده، مواد آموزشی، فرآیندهای عملیاتی یا پشتیبان، حقوق مالکیت معنوی داده‌های الکترونیکی، طرح تداوم عملیات (Business Continuity Plan)، طرح بازگشت به حالت پایدار قبلی (Fall Back Arrangements)
اسناد کاغذی	قراردادها، دستورالعمل‌ها، اسناد تجاری، سوابق نیروی انسانی، اسناد خرید، صورتحساب‌ها

¹⁵ Port Access Provider در ایران شرکت‌های ندا)

دسته‌بندی دارایی اطلاعاتی	شکل دارایی اطلاعاتی
دارایی‌های نرم‌افزاری	برنامه‌های کاربردی، سیستم عامل، ابزارهای تولید نرم‌افزار، ابزارهای سیستم
دارایی‌های فیزیکی (سخت‌افزاری)	کامپیوتر، مسیریاب، هاب، فایروال، تجهیزات مخابراتی، تجهیزات ذخیره اطلاعات، رسانه‌های مغناطیسی یا نوری، کابینت‌ها، گاو صندوق‌ها، اتاق‌ها و سایر تجهیزات
نیروی انسانی و افراد	پرسنل سازمانی، مشتریان و ارباب رجوع، نمایندگان، پیمانکاران، نیروهای حراستی، نیروهای خدماتی و سایر افراد
خدمات	خدمات پردازشی، خدمات مخابراتی و ارتباطی، گرمایش، گاز، آب، تهویه، سیستم دزدگیر، آتش نشانی، ژنراتورهای برق و UPS
ارزش‌های سازمانی	اعتبار نزد افکار عمومی، پاسخگویی و شفافیت، مسئولیت‌پذیری سازمان، جلب رضایت مشتریان یا ارباب رجوع

پس از شناسایی دارایی اطلاعاتی لازم است وجود آن در فهرست موجودی دارایی‌های اطلاعاتی (موضوع دستورالعمل ۳-۱-۱) مورد بررسی قرار گیرد و در صورت عدم وجود دارایی در آن، فهرست مذکور تصحیح و به هنگام سازی شود.

د- ارزش گذاری دارایی‌های اطلاعاتی

ارزش هر یک از دارایی‌های شناسایی شده به وسیله متصدی فرآیند تعیین خواهد شد. لازم است متصدی فرآیند علاوه بر ارزش ظاهری دارایی‌های اطلاعاتی اثرات ناشی از فقدان یا عدم عملکرد صحیح همان دارایی‌های اطلاعاتی و زیان حاصل از آن برای سازمان و یا مشتریان و ارباب رجوع را در نظر بگیرد.

زیان‌های فوق باید از دیدگاه فقدان دارایی اطلاعاتی، سرقت آن، در دسترس نبودن و یا سایر نقض‌های امنیتی مورد توجه قرار گیرد.

ارزش گذاری دارایی اطلاعاتی می‌تواند به سه روش کیفی، کمی و یا ترکیبی انجام پذیرد. در روش ارزش گذاری کیفی هر دارایی با دارایی‌های دیگر مقایسه شده و در یکی از دسته‌های زیر جای داده می‌شود:

- دسته ۱: بسیار پر ارزش (به عنوان مثال نیروی انسانی یا بانک‌های اطلاعاتی یا اتاق‌های سرور)
- دسته ۲: پر ارزش (به عنوان مثال سرورهای اصلی یا رسانه‌های ذخیره اطلاعات یا تجهیزات ارتباطی)

دسته ۳: ارزش متوسط (به عنوان مثال کامپیوترها، پرینترها یا سایر تجهیزات جانبی)

دسته ۴: کم ارزش (دیسک‌های خالی، کاغذهای چاپ نشده، میز و قفسه‌های عادی)

(دسته‌های فوق را می‌توان با صلاح‌دید کمیته امنیت اطلاعات کم یا زیاد نمود)

در روش ارزش‌گذاری کمی می‌توان از هزینه پرداخت شده برای خرید دارایی اطلاعاتی و یا

هزینه صرف شده برای دستیابی به آن استفاده نمود.

به عنوان مثال اگر برای خرید یک مسیر یاب مبلغ پانزده میلیون ریال هزینه شده باشد ارزش آن

مسیر یاب در ارزیابی ریسک پانزده میلیون ریال در نظر گرفته خواهد شد و یا اگر برای خرید یک

نرم‌افزار بانک اطلاعاتی مثل **SQL** مبلغ چهل هزار ریال پرداخت شده باشد، ارزش آن نرم‌افزار

چهل هزار ریال محسوب خواهد شد.

نکته قابل توجه در این روش ارزش‌گذاری دارایی‌های اطلاعاتی است که در طول زمان کسب

شده یا به وجود آمده‌اند.

به عنوان مثال ارزش داده‌های موجود در یک بانک اطلاعاتی عبارت است از هزینه‌ای که صرف

جمع‌آوری آن اطلاعات شده است و می‌تواند شامل هزینه‌های زیر باشد:

- هزینه نیروی انسانی مستقیم به کار گرفته شده برای جمع‌آوری اطلاعات (A)
- هزینه داده‌های خریداری شده برای تکمیل بانک اطلاعاتی (B)
- سایر هزینه‌های غیر مستقیم پرداخت شده برای جمع‌آوری و حفظ بانک اطلاعاتی (C)

$$A + B + C = \text{ارزش داده‌های موجود در بانک اطلاعاتی}$$

به عنوان مثالی دیگر ارزش فایل‌های متنی تولید شده به وسیله یک منشی یا تایپیست (در

صورتی که فایل‌های عادی بدون طبقه‌بندی حفاظتی باشند) را می‌توان با استفاده از حقوق پرداخت

شده به منشی برای تایپ آن فایل‌ها تخمین زد.

در خصوص تعیین ارزش فایل‌های خاص یا دارای طبقه‌بندی حفاظتی می‌توان از مشاوره افراد

خبره سازمان بهره برد.

در روش ارزش‌گذاری ترکیبی می‌توان از ترکیب روش‌های کیفی و کمی بهره برد.

به عنوان مثال در این حالت ارزش مسیر یاب موجود در سیستم ارتباطی بر اساس ترکیبی از

قیمت آن و اهمیت آن در برقراری ارتباط تعیین می‌شود. در این حالت ممکن است قیمت پانزده

میلیون ریال آن (که قبلاً به آن اشاره شد) در مقایسه با قیمت سایر تجهیزات مثل سرورها، بانک‌های

اطلاعاتی و یا نیروی انسانی ارزش قابل توجهی نداشته باشد اما به دلیل قرار گرفتن آن در یک نقطه حیاتی دارای نقش مهمی بوده و لازم است به آن توجه شود.

لازم است ارزش گذاری‌ها به نحوی انجام شود که بتوان نهایتاً آن‌ها را در قالب یک شاخص (ترجیحاً کمی) خلاصه نمود. بنابراین لازم است روش‌هایی برای تبدیل ارزش‌های کمی و کیفی دارایی‌ها به یکدیگر (به‌خصوص تبدیل ارزش‌های کیفی به کمی) ایجاد شود.

هـ- شناسایی نقاط آسیب پذیر

فرآیند شناسایی نقاط آسیب پذیری هر دارایی اطلاعاتی عبارت است از فهرست نمودن آسیب پذیری‌های احتمالی هر دارایی اطلاعاتی.

به عنوان مثال می‌توان نقاط آسیب پذیر زیر را برای دارایی‌های اطلاعاتی مختلف فهرست نمود:

ر	دارایی اطلاعاتی	آسیب پذیری (نمونه)
۱	کامپیوتر شخصی	سرقت اطلاعات موجود روی هارد دیسک
۲	کامپیوتر شخصی	خرابی سخت‌افزار
۳	دیسکت	سرقت
۴	دیسک	خراب شدن فایل‌های ذخیره شده
۵	کانال ارتباطی	محدودیت ظرفیت
۶	اتاق سرور	آب گرفتگی
۷	سوییچ شبکه	تبدیل شدن به هاب در صورت پر شدن حافظه و جدول‌های مسیریابی
۸	کابل‌های شبکه یا پورت باز شبکه	شنود اطلاعات

و- شناسایی تهدیدها

تهدیدها عبارت‌اند از شرایطی که ممکن است باعث فعال شدن یا سوءاستفاده از آسیب پذیری‌ها شده و یا ضربه پذیری از آن نقطه افزایش یابد.

در مرحله شناسایی تهدیدها لازم است کلیه تهدیدهای مرتبط با آسیب پذیری هر دارایی اطلاعاتی فهرست شوند. به عنوان مثال می‌توان به جدول زیر توجه کرد.

#	دارایی اطلاعاتی	آسیب پذیری	تهدید مرتبط با آن آسیب پذیری
۱	کامپیوتر شخصی	سرقت اطلاعات موجود روی هارد دیسک	امکان دسترسی افراد غیر مجاز به کامپیوتر، وجود پورت USB، وجود دیسک درایو.....
۲	کامپیوتر شخصی	خرابی سخت‌افزار	نگهداری نادرست، کیفیت پایین قطعات
۳	دیسکت	سرقت	امکان دسترسی افراد غیر مجاز، نگهداری در محل غیر امن

#	دارایی اطلاعاتی	آسیب پذیری	تهدید مرتبط با آن آسیب پذیری
۴	دیسک	خراب شدن فایل‌های ذخیره شده	نگهداری نادرست، استفاده از دیسک درایو خراب، ویروسی شدن فایل‌ها
۵	کانال ارتباطی	محدودیت ظرفیت	امکان اجرای حمله DoS و قطع کانال به دلیل پر شدن ظرفیت کانال
۶	اتاق سرور	آب گرفتگی	عبور لوله‌های آب از نزدیکی اتاق سرور، قرار گرفتن در زیر زمین، امکان وقوع بارندگی شدید، نداشتن تجهیزات تخلیه آب
۷	اتاق سرور	دسترسی غیرمجاز به اطلاعات از پشت سرور	ورود افراد غیرمجاز به اتاق سرور
۸	سوییچ شبکه	تبدیل شدن به هاب در صورت پر شدن حافظه و جدول‌های مسیریابی	امکان دسترسی از خارج شبکه سازمان به شبکه داخلی، افشاء آدرس IP، نقص در سیستم کنترل دسترسی
۹	کابل‌های شبکه یا پورت باز شبکه	شنود اطلاعات	امکان انتقال توت بوک به داخل سازمان و متصل کردن آن به پورت شبکه، امکان دریافت تشعشع الکترومغناطیسی از طریق جریان‌های القایی اطراف کابل‌های مسی

همان‌طور که دیده می‌شود فهرست نقاط آسیب پذیر و تهدیدهای مرتبط با هر یک می‌تواند فهرستی طولانی باشد. بهتر است این فهرست‌ها قبلاً به صورت عام تهیه شده و در اختیار مالک، متصدی و یا تحویل گیرنده دارایی اطلاعاتی قرار گیرد به نحوی که وی بتواند نقاط آسیب پذیر و تهدیدهای مرتبط با دارایی اطلاعاتی یا فرآیند تحت مدیریت خود را از بین آن‌ها استخراج نماید. فهرست خلاصه آسیب پذیری‌ها و حمله‌های شبکه‌ای در ضمیمه همین دستورالعمل ارائه شده است.

ز- شناسایی اهداف، مکانیزم‌های کنترلی و روش‌های حفاظتی

پس از شناسایی تهدیدهای مرتبط با هر یک از نقاط آسیب پذیر دارایی‌های اطلاعاتی می‌توان برای مقابله با هر نوع یا دسته‌ای از تهدیدها از مکانیزم‌های کنترلی خاص استفاده کرد. انتخاب مکانیزم‌های کنترلی باید بر اساس اهداف کنترلی انجام شود. به عنوان مثال استفاده از کلمه عبور (موضوع دستورالعمل ۷-۳-۱) یکی از اهداف کنترلی بر اساس استاندارد مدیریت امنیت اطلاعات ISO-27001 می‌باشد. یکی از مکانیزم‌های مرتبط با این هدف فعال کردن مکانیزم تعریف نام کاربر و

کلمه عبور در هنگام آغاز به کار با دارایی‌های اطلاعاتی مختلف مثل کامپیوتر شخصی، سیستم عامل Windows و یا برنامه‌های کاربردی می‌باشد.

همچنین روش‌های حفاظتی متناسب با کاربرد، اهمیت و خصوصیات دارایی اطلاعاتی شناسایی و انتخاب خواهد شد. به عنوان مثال روش شناسایی دوره‌ای پورت‌های بدون استفاده شبکه داخلی (LAN) سازمان و پلمپ کردن یا غیر فعال کردن آن‌ها می‌تواند یکی از روش‌های پیاده‌سازی مکانیزم جلوگیری از اتصال غیر مجاز و کنترل اتصال‌های شبکه باشد.

از آن‌جا که ممکن است اهداف و مکانیزم‌های کنترلی به دفعات مورد اشاره واقع شوند لازم است فهرست خلاصه‌ای تحت عنوان مکانیزم‌های شناسایی شده بر اساس ارزیابی ریسک تهیه شود و بر اساس آن بیانیه کاربرد پذیری (SOA) اختصاصی سازمان (موضوع دستورالعمل ۳-۳-۴) تدوین شود.

بیانیه کاربرد پذیری اختصاصی سازمان مبین فهرست جامع اهداف و مکانیزم‌های کنترلی است که توسط سازمان برای مدیریت امنیت اطلاعات به کار گرفته خواهند شد.

ح- ارسال گزارش به کمیته امنیت اطلاعات

لازم است در پایان فرآیند ارزیابی ریسک گزارش ارزیابی ریسک امنیت اطلاعات سازمان به کمیته امنیت اطلاعات ارسال شود. این گزارش حاوی جمع بندی وضعیت‌هایی است که متصدیان فرآیند برای هر یک از دارایی‌های اطلاعاتی استخراج کرده و بر اساس ارزش هر یک از دارایی‌های اطلاعاتی طبقه‌بندی کرده‌اند. کمیته امنیت اطلاعات با توجه به این گزارش‌ها آن دسته از دارایی‌های اطلاعاتی که حفاظت از آن‌ها دارای اهمیت زیاد برای فعالیت‌های ((وزارت/ سازمان/ اداره کل/ شرکت/...)) و خدمت رسانی به مشتریان و ارباب رجوع خود است را شناسایی کرده و نسبت به به کارگیری مکانیزم‌های کنترلی برای حفاظت از دارایی‌های اطلاعاتی پرارزش تصمیم‌گیری می‌نماید. سایر دارایی‌ها بر اساس سیاست‌گذاری‌های قابل تدوین طبق سند راهنمای سیاست‌گذاری امنیت اطلاعات (دستورالعمل ۱-۱) قابل حفاظت خواهند بود.

ابزار و تجهیزات مورد استفاده در ارزیابی ریسک امنیتی

برای ارزیابی ریسک، نیاز به ابزار خاصی به جز جداول و فرم‌های دسته‌بندی اطلاعات جمع‌آوری شده در مورد دارایی‌های اطلاعاتی وجود ندارد. البته ابزارهای نرم‌افزاری نیز برای سهولت

انجام ارزیابی ریسک تولید شده و در دسترس می‌باشند که برخی از آن‌ها عبارت‌اند از COBRA, XRM, Security by Analysis, MELISA, CORA, AnalyZ, BIS Risk Assessor و غیره.

ممکن است دسترسی به ابزار فوق مشکل و یا به لحاظ ملاحظات حفاظتی استفاده از نرم‌افزارهای خارجی یا خارج از کنترل حفاظتی غیر ممکن باشد.

بنابراین روش ارزیابی ریسک مبتنی بر استفاده از جداول و پرسشنامه‌ها به‌طور کامل در ضمیمه این سند شرح داده شده است. بهره‌برداران احتمالی می‌توانند با انتقال این جداول به محیط‌های کاری مناسب مانند Excel یا با برنامه نویسی، سیستم‌های ارزیابی ریسک اختصاصی خود را تولید نمایند.

توجه: ارزیابی ریسک مستلزم تولید اطلاعات در مورد اطلاعات یا تولید اطلاعات در مورد دارایی‌های اطلاعاتی می‌باشد. لازم است از این اطلاعات حفاظت کافی به عمل آید. نتایج ارزیابی ریسک نشان‌دهنده نقاط ضعف سازمان و روش‌های دفاعی سازمان در برابر حمله‌های رایانه‌ای یا سوءاستفاده از تجهیزات رایانه‌ای می‌باشد. دستیابی افراد غیر مجاز به این اطلاعات می‌تواند خود عامل تهدید بسیار شدیدی باشد. بنابراین هنگام ارزیابی ریسک لازم است کلیه اطلاعات تولید شده به نحو مناسب تحت حفاظت قرار گیرند.

اگر در مرحله ارزیابی ریسک نیاز به استفاده از آزمون‌های نفوذ (Penetration Test) باشد، لازم است در خصوص انتخاب افراد جهت اجرای تست نفوذ و قراردادهای فی مابین در خصوص رعایت الزامات امنیتی بر اساس دستورالعمل‌های توافق‌نامه‌های حفظ محرمانگی (دستورالعمل ۲-۱-۵)، شناسایی ریسک‌های تعامل با سایر طرف‌های تجاری یا اداری (دستورالعمل ۲-۲-۱) و رعایت معیارهای امنیتی در قراردادهای اشخاص ثالث (دستورالعمل ۲-۲-۲) دقت کافی به عمل آید.

مرجع

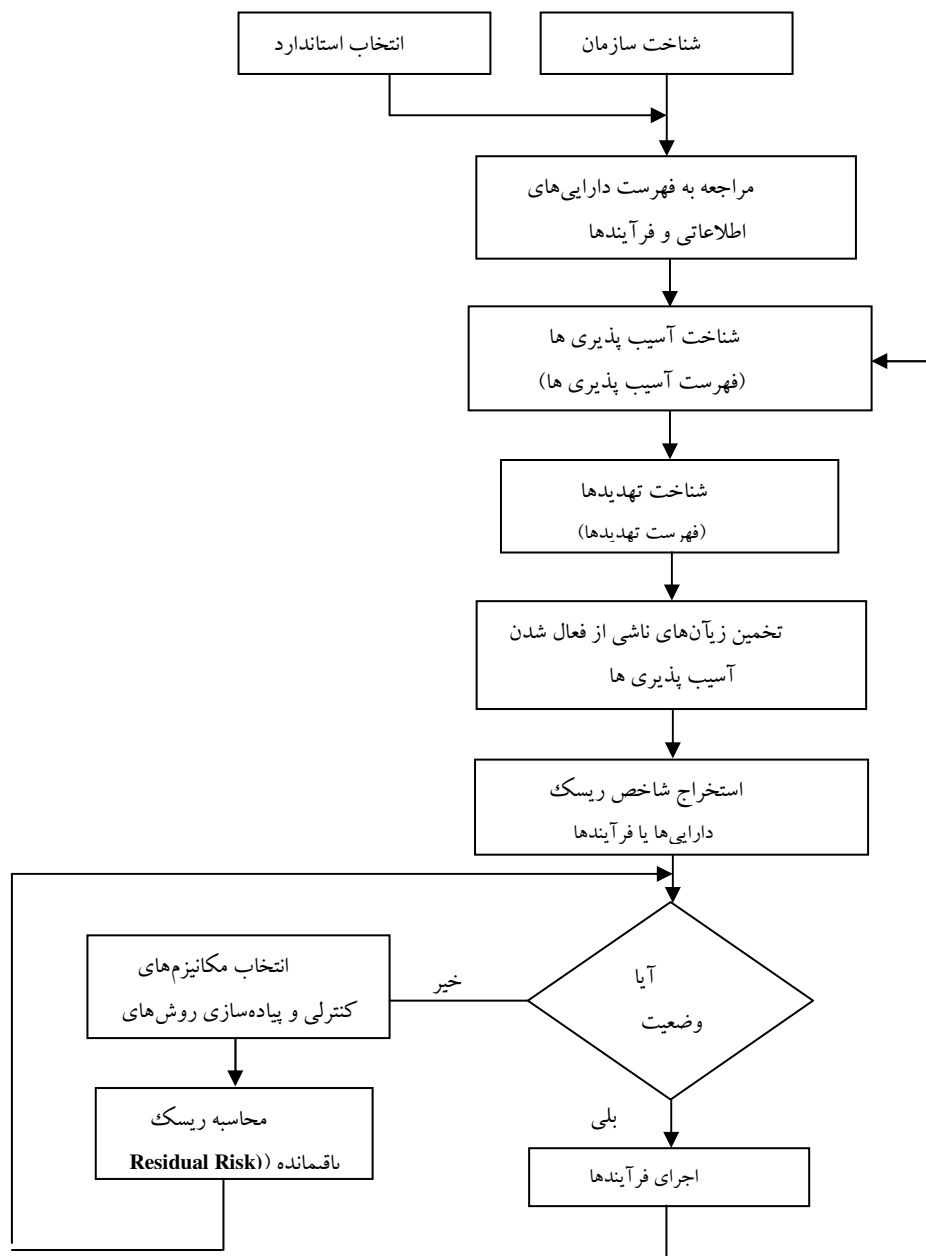
این سند به شماره □-□/۲-۳-۳/□-□ ثبت گردیده و سایر اسناد مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱
- دستورالعمل ۳-۱-۱
- دستورالعمل ۳-۳-۳
- دستورالعمل ۲-۱-۳
- دستورالعمل ۴-۳-۳

-
- دستورالعمل ۱-۳-۷
 - دستورالعمل ۵-۱-۲
 - دستورالعمل ۱-۲-۲
 - دستورالعمل ۲-۲-۲

روند نمای ارزیابی و کنترل ریسک

روند نمای چگونگی اجرای مراحل ارزیابی و کنترل ریسک در شکل زیر نشان داده شده است:



ضمیمه یک مدل ارزیابی و تحلیل ریسک

مقدمه

این مدل به عنوان روشی کارآ و سهل برای ارزیابی و تحلیل ریسک امنیت اطلاعات ارائه می‌گردد. هدف از ارائه این روش آموزش مراحل ارزیابی ریسک امنیت اطلاعات می‌باشد، بنابراین سعی شده است تا با ارائه مثال‌های ساده مراحل مختلف کار تشریح شوند.

بدیهی است برای رعایت سادگی و درک بهتر مطلب سعی شده است از مثال‌های واضح و وضعیت‌های عام استفاده شود. بنابراین ملاک‌های دسته‌بندی و جداول ارائه شده را می‌توان بنا به نوع و ماهیت فرآیند و دارایی‌های اطلاعاتی تحت بررسی تغییر داده یا تکامل بخشید. استفاده از خلاقیت و تصور منطقی به درک بهتر شرایط، شناسایی نقاط آسیب پذیر و تبیین تهدیدات احتمالی کمک می‌کند.

یکی دیگر از کاربردهای نتایج حاصل از ارزیابی و تحلیل ریسک تهیه طرح احیای سیستم (DRP)^{۱۶} می‌باشد. کاربرد طرح احیای سیستم یا احیای سیستم پس از وقوع فاجعه، تضمین بازگشت به سطحی قابل قبول از ظرفیت‌های عملیاتی پس از مدت معینی از وقوع حوادث عمده یا فجایع طبیعی یا غیرطبیعی مانند جنگ، سیل، زلزله و آتش سوزی‌های عمده و یا حمله‌های رایانه‌ای منجر به فروپاشی سیستم می‌باشد. تصور اینکه چه حوادثی ممکن است سیستم را در آینده تهدید کند و یا تنش‌های ناشی از وقوع حوادث تا چه حد سیستم را تحت تأثیر قرار می‌دهد، به طراحی کارآتر فرآیندهای کنترلی یا احیای سیستم کمک خواهد نمود. در این جا اشاره به مثالی واقعی مفید به نظر می‌رسد.

شرکت کانتور فیتزجرالد (Cantor Fitzgerald) یکی از بنگاه‌های صدمه دیده در حادثه ۱۱ سپتامبر ۲۰۰۱ بوده است. مکان این شرکت بین طبقات ۱۰۱ تا ۱۰۵ برج شماره یک مرکز تجارت جهانی (WTC) قرار داشته است. این مکان بالاتر از محل اصابت هواپیما به برج قرار داشته و به همین دلیل کلیه کارمندان و تجهیزات مستقر در محل متعلق به این شرکت از بین رفت. ۶۵۸ نفر از کارمندان مستقر در محل کشته شدند. این شرکت هنگام حمله یک چهارم از کل تبادلهای مالی

Disasters Recovery Plan¹⁶ -

اوراق بهادار بازار وقت آمریکا را به عهده داشت. پیش از وقوع حمله یک سایت جایگزین تجهیز شده ولی به‌طور کامل عملیاتی نشده بود، اما یک هفته پس از وقوع حادثه این شرکت شروع به ارائه خدمات نمود. هیچکس هنگام طراحی سیستم تصور برخورد عمدی یک هواپیما با برج و از دست رفتن بیش از دو سوم کارمندان شرکت را نمی‌کرده است، اما توان تصور و خلاقیت طراحان طرح پیوستگی عملیات و احیا پس از وقوع حادثه، آنچنان قوی بوده است که پس از وقوع این حادثه در کمترین زمان ممکن شرکت را به وضعیت عملیاتی بازگردانده است.

شرایط فعلی کشور جمهوری اسلامی ایران، تعارض‌های منطقه‌ای و بین‌المللی، رقابت‌های اقتصادی، سیاسی، نظامی و حتی مذهبی نیاز به تصور حالت‌های غیر ممکن را گوشزد می‌کند. توجه کامل به آسیب‌پذیری‌های دارایی‌های اطلاعاتی و تهدیدهای ذاتی یا محیطی ناشی از به کارگیری آن‌ها موجب افزایش توان پیش‌بینی و صحت فعالیت‌های ارزیابی ریسک خواهد گردید.

مرحله اول و زیر بنای اساسی امن‌سازی سیستم، ارزیابی ریسک می‌باشد. هر چه این مرحله بهتر به اجرا گذاشته شود زیربنا و پی بندی مستحکم تری را در اختیار خواهد گذاشت و می‌توان بر روی این پی بندی بنای مستحکم تری را برپا نمود.

الف- تعاریف

در این مدل تعاریف زیر به کار گرفته شده است:

دارایی اطلاعاتی: هر گونه نرم‌افزار، سخت‌افزار، اطلاعات چاپی، نیروی انسانی، تأسیسات، کانال‌های مخابراتی و ارتباطی و یا تجهیزات دیگری که برای تداوم عملیات سامانه IT مورد نیاز باشد.

توجه ۱: در سازمان‌های عادی می‌توان تعریف دارایی‌های اطلاعاتی را به کمیته امنیت اطلاعات سپرد. به عنوان مثال کمیته امنیت اطلاعات می‌تواند تجهیزات فرعی که برای تداوم سامانه IT مورد نیاز باشند یا تأسیسات را از شمول دارایی‌های اطلاعاتی خارج نماید.

توجه ۲: در سازمان‌هایی که از سوی سازمان پدافند غیرعامل به عنوان سازمان‌های مهم یا حساس دسته‌بندی می‌شوند، لازم است نیروی انسانی در زمره دارایی‌های اطلاعاتی محسوب شده و ارزیابی ریسک با توجه به آن عمل آید.

توجه ۳: در سازمان‌هایی که از سوی سازمان پدافند غیرعامل به عنوان سازمان‌های حیاتی دسته‌بندی می‌شوند لازم است ارزیابی ریسک برای کلیه دارایی‌ها، اعم از اطلاعاتی و غیر اطلاعاتی

(بدون حذف هیچ یک از عوامل مشهود یا غیر مشهود مرتبط با سامانه‌های پردازشی یا ارتباطی) به عمل آید.

تهدید: عبارت است از هر فرد، واقعه یا موقعیت که پتانسیل تخریب یک دارایی خاص یا برخی از دارایی‌ها را داشته باشد. مکانیزم اثر تهدید عبارت است از بهره‌برداری از آسیب پذیری‌های سامانه‌ها، سیستم‌ها، فرآیندها و یا دارایی‌های اطلاعاتی به محض فعلیت پیدا کردن عامل تهدید. آسیب پذیری: عبارت است از ضعف در یک بخش از سامانه، سیستم، فرآیند یا دارایی اطلاعاتی که می‌توان از طریق آن به سوء استفاده از سیستم (استثمار سیستم) پرداخت و یا به معیارها و یا قواعد امنیتی آن تجاوز نمود.

تنش: تغییر در شرایط عادی عملکرد سامانه، فرآیند یا دارایی عملیاتی. قاعده: هرگونه تهدید ممکن است منجر به تنش ناخواسته در سیستم شود. قاعده: هرگونه تنش ناخواسته ممکن است منتهی به نقص در مأموریت اصلی سیستم گشته و یا باعث بروز وقایع یا حوادث ناخواسته خواهد شد. قاعده: تهدیدها ممکن است ناشی از عملکرد عامل انسانی و یا تغییر در شرایط محیطی باشند. قاعده: تهدیدهای ناشی از عملکرد عامل انسانی ممکن است ناشی از افراد خودی یا افراد بیگانه باشند. قاعده: عملکرد عوامل انسانی ممکن است خصمانه یا غیر خصمانه و یا به عبارت دیگر عمدی یا سهوی باشد.

قاعده: عملکرد عمدی یا سهوی نیز ممکن است سازمان یافته یا بدون هدف باشد.

ب- مراحل ارزیابی و تحلیل ریسک

مراحل ارزیابی ریسک به ترتیب عبارت‌اند از:

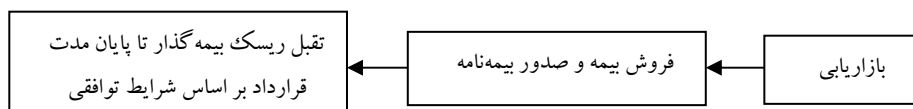
- شناسایی فرآیندهای اجرایی
- تعیین معیارهای عملیاتی که لازم است برای دستیابی به امنیت به کار گرفته شوند.
- شناسایی یا تعریف دارایی‌ها
- جمع‌آوری اطلاعات در مورد دارایی‌های اطلاعاتی در جهت شناسایی ریسک‌های حاصله
- تخصیص شاخص ارزش دارایی (کیفی یا کمی)
- تعیین درجه اهمیت (شاخص اهمیت)
- شناسایی آسیب پذیری‌های هر دارایی

- تعیین آسیب پذیری‌های پر اهمیت
- شناسایی حوزه‌های تهدید
- شناسایی مکانیزم‌های حفاظتی موجود
- تعیین آسیب پذیری‌های تحت کنترل
- تعیین شاخص ضربه پذیری
- پیشنهاد مکانیزم‌های حفاظتی
- تعیین ضربه پذیری باقیمانده (ریسک باقیمانده)
- محاسبه ریسک

در ادامه مطلب هر یک از مراحل فوق به طور کامل شرح داده خواهد شد.

ب-۱- شناسایی فرآیندهای اجرایی

فرآیندهای اجرایی عبارت‌اند از آن دسته از فعالیت‌هایی که باید به دنبال یکدیگر یا موازات هم به اجراء درآیند تا منجر به ارائه یک خدمت یا بخشی از آن شوند. انتخاب نقطه شروع یا پایان هر فرآیند به عهده متصدیان برنامه‌ریزی، طرح عملیات و یا مدیر مربوطه می‌باشد. به عنوان مثال فروش بیمه شخص ثالث یکی از خدمات‌های ارائه شده توسط شرکت‌های بیمه می‌باشد. این خدمت را می‌توان به عنوان مثال به سه بخش زیر تقسیم کرد:



شاید در نگاه اول نتوان تهدید امنیتی خاصی در بخش‌های فوق مشاهده کرد. اما لازم است به

مطالب زیر توجه شود:

بردارهای اصلی امنیت اطلاعات عبارت‌اند از:

محرمانگی

جامعیت (صحت)

دسترس پذیری

به بردارهای اصلی فوق می‌توان دو بردار مکمل زیر را نیز افزود:

- انکارناپذیری

- اعتبار سازمانی و خوشنامی

برخی از آسیب‌پذیری‌های سازمانی در فروش بیمه شرکت X را می‌توان به شرح زیر فهرست کرد:

- لطمه به اعتبار سازمانی به دلیل تبلیغ مزایای غیر واقعی یا کذب خرید بیمه از شرکت X (در مرحله بازاریابی توسط عامل تبلیغ یا دستبرد در مواد تبلیغاتی توسط افراد دیگر اعم از مواد تبلیغاتی چاپی یا الکترونیکی)
- فروش جعلی بیمه توسط نماینده یا افراد دیگر (با استفاده از اوراق آرم‌دار یا جعل سایت فروش الکترونیکی)
- فروش بیمه و تقبل ریسک افرادی که وجود ندارند (جعل مدارک خریدار یا شناسه‌های الکترونیکی اثبات کننده وجود خریدار)
- نقص در اطلاعات یا مشخصه‌های بیمه‌گذار (اعم از اطلاعات الکترونیکی یا غیر آن)
- نقص در اطلاعات یا مشخصه‌های بیمه‌شده (اعم از اطلاعات الکترونیکی یا غیر آن)
- درج تاریخ و زمان غیر واقعی در مدارک (اعم از کتبی یا الکترونیکی)
- ایراد در اطلاعات پایه موردنیاز جهت محاسبه ریسک خریدار (مثل سوابق رانندگی)
- انکار خرید یا فروش از سوی طرفین معامله اعم از خریدار، عامل یا نماینده و فروشنده
- تغییر غیر مجاز در شرایط بیمه یا مشخصات خریدار
- درج اطلاعات غیرواقعی حادثه یا شرایطی که منجر به پرداخت خسارت به خریدار بیمه می‌باشد.
- انتشار اسرار سازمانی یا اطلاعات خصوصی مشتریان یا فروش یا تحویل آن به مراجع غیر مجاز

البته فهرست فوق را می‌توان طولانی‌تر کرد.

شرایطی که منجر به سوءاستفاده از آسیب‌پذیری‌های فوق شده و منجر به وارد شدن زیان به

شرکت X می‌شود را شرایط تهدید می‌نامیم.

به عنوان مثال عدم استفاده از سرور زمان (Time) جهت سنکرون کردن شبکه (Synchronization)

در شبکه اطلاعاتی یا شبکه فروش الکترونیکی عامل تهدید مهمی است و می‌تواند موجب فعال شدن

آسیب‌پذیری درج تاریخ و یا زمان غیرواقعی گردد.

بنابراین لازم است کلیه فرآیندهای اجرایی که از دارایی‌های اطلاعاتی برای انجام آن‌ها استفاده می‌شود مورد بررسی دقیق قرار گرفته و آسیب‌پذیری مربوط به انجام هر بخش از فرآیند شناسایی شده و تهدیدهای مربوط به هر آسیب‌پذیری فهرست شوند.

برای این کار می‌توان از جدول زیر استفاده کرد:

جدول شناسایی آسیب‌پذیری‌ها و تهدیدهای فرآیندهای اجرایی

شماره فرآیند	عنوان فرآیند	شماره فعالیت	عنوان فعالیت	آسیب‌پذیری	تهدید
۱	فرآیند ۱	۱-۱	فعالیت ۱-۱	آسیب‌پذیری ۱-۱-۱	تهدید ۱-۱-۱-۱
					تهدید ۲-۱-۱-۱
				آسیب‌پذیری ۲-۱-۱	تهدید ۱-۲-۱-۱
					تهدید ۲-۲-۱-۱
					تهدید ۳-۲-۱-۱
					
		۲-۱	فعالیت ۲-۱	آسیب‌پذیری ۱-۲-۱	تهدید ۱-۱-۲-۱
					تهدید ۲-۱-۲-۱
					
				آسیب‌پذیری ۲-۲-۱	تهدید ۱-۲-۲-۱
					تهدید ۲-۲-۲-۱
۲	فرآیند ۲	۱-۲	فعالیت ۱-۲	آسیب‌پذیری ۳-۲-۱	
					
					
				آسیب‌پذیری ۱-۱-۲	تهدید ۱-۱-۱-۲
					تهدید ۲-۱-۱-۲
					

مسئولیت تکمیل این جدول به عهده متصدی هر فرآیند می‌باشد.

بدیهی است متصدی فرآیند از همکاری سایر افراد سازمان در تکمیل این جدول استفاده خواهد

نمود.

ب-۲- شناسایی یا تعریف دارایی‌های اطلاعاتی

مرحله دوم در ارزیابی ریسک مراجعه به فهرست موجودی دارایی‌های اطلاعاتی (موضوع دستورالعمل ۱-۳-۱) می‌باشد. لازم است این فهرست در مرحله ارزیابی ریسک مورد بازنگری مجدد قرار گرفته و به هنگام‌سازی شود. در صورت عدم وجود این فهرست ضروری است نسبت به تهیه آن اقدام شود.

لازم است کلیه دارایی‌های اطلاعاتی موجود در فهرست دارایی‌های اطلاعاتی از دیدگاه شناسایی ریسک‌های مرتبط با آن‌ها مورد بررسی دقیق قرار گرفته و کلیه خصوصیات آن‌ها اعم از شرایط محیطی، شرایط کار، برنامه‌های نگهداری و تعمیرات، ظرفیت و مکان نگهداری مورد مطالعه قرار گیرد.

همچنین در این مرحله با توجه به خصوصیات دارایی‌های اطلاعاتی لازم است آسیب‌پذیری‌های مربوط به آن دارایی و همچنین شرایطی که منجر به ضربه‌پذیری سازمان از آن آسیب‌پذیری می‌شوند (تهدیدها) مطالعه و جمع‌آوری شود. برای سهولت انجام این مرحله استفاده از جدول زیر مفید است:

جدول شناسایی آسیب‌پذیری‌ها و تهدیدهای فرآیندهای اجرایی

شماره دارایی	نام دارایی اطلاعاتی	آسیب‌پذیری	تهدید
۱	دارایی اطلاعاتی ۱	آسیب‌پذیری ۱-۱	تهدید ۱-۱-۱
			تهدید ۲-۱-۱
			
		آسیب‌پذیری ۲-۱	تهدید ۱-۲-۱
			تهدید ۲-۲-۱
			تهدید ۳-۲-۱
			
۲	دارایی اطلاعاتی ۲	آسیب‌پذیری ۱-۲	تهدید ۱-۱-۲
			تهدید ۲-۱-۲
			
		آسیب‌پذیری ۲-۲	
			
.....			

توضیح: مسؤولیت تکمیل این جدول برای هر دارایی اطلاعاتی به عهده تحویل گیرنده، متصدی و یا مالک همان دارایی است.

ب-۳- تعیین فعالیت‌های مهم در هر فرآیند و درجه‌بندی آن‌ها

فرآیندهای مختلف دارای اهمیت متفاوت می‌باشند. همچنین فعالیت‌های مختلف هر فرآیند نیز نسبت به یکدیگر دارای اهمیت‌های متفاوت می‌باشند.

به عنوان مثال برخی از فعالیت‌ها یا فرآیندها را می‌توان هم به صورت عادی و هم به صورت الکترونیکی انجام داد و یا ممکن است برخی از خدمات، فرآیندها یا فعالیت‌های جنبه پیش‌نیاز یا مکمل برای سایر خدمات، فرآیندها و یا فعالیت‌ها باشند.

از آن‌جا که منابع سازمان و بالطبع منابع امن‌سازی اعم از نیروی انسانی و بودجه نامحدود نیست، لازم است معیاری برای تخصیص بهینه آن‌ها وجود داشته باشد.

کارآمدترین معیار می‌تواند نظر افراد خبره در خصوص میزان اهمیت و نقش هر فرآیند یا فعالیت در تکمیل خدمات سازمان باشد.

بنابراین لازم است جدول شناسایی آسیب‌پذیری و تهدیدهای فرآیندهای اجرایی مورد بررسی قرار گرفته و فرآیندها و فعالیت‌های مهم شناسایی و استخراج شوند و در جدولی به شرح زیر با ذکر درجه اهمیت فهرست شوند:

جدول درجه‌بندی شده و فعالیت‌های مهم سازمانی

شماره فعالیت	عنوان فعالیت	عنوان فرآیند مربوط	درجه اهمیت
۲-۱	فعالیت ۲-۱	فرآیند ۱	حساس
۳-۲	فعالیت ۳-۲	فرآیند ۲	حیاتی
۶-۴	فعالیت ۶-۴	فرآیند ۶	مهم
....			

توضیح: مندرجات جدول فوق به صورت نمونه ذکر شده‌اند.

مسؤولیت تهیه جدول فوق برای هر فرآیند به عهده متصدی همان فرآیند می‌باشد.

درجه‌های اهمیت قابل تخصیص به هر فعالیت عبارت‌اند از:

- حیاتی
- حساس
- مهم

- فعالیت‌های حیاتی آن دسته از فعالیت‌ها هستند که در صورت توقف منجر به توقف ارائه خدمات سازمان خواهند شد.
مثال: توقف فعالیت صدور بیمه‌نامه موجب توقف فرآیند فروش خواهد شد. فروش بیمه‌نامه هدف اصلی شرکت بیمه می‌باشد. بنابراین فعالیت صدور بیمه‌نامه یک فعالیت حیاتی در شرکت بیمه می‌باشد.
 - فعالیت‌های حساس آن دسته از فعالیت‌هایی هستند که در صورت توقف منجر به نارضایتی شدید ارباب رجوع از نحوه ارائه خدمات سازمان خواهند شد.
مثال: توقف فعالیت ارزیابی خسارت در یک شرکت بیمه موجب نارضایتی شدید مشتریان خواهد شد. ارزیابی سریع خسارت یکی از وظائف اصلی شرکت بیمه می‌باشد. بنابراین فعالیت ارزیابی خسارت یک فعالیت حساس در شرکت بیمه می‌باشد.
 - فعالیت‌های مهم آن دسته از فعالیت‌هایی هستند که دارای اهمیت زیاد در پشتیبانی حرکت به سمت اهداف یا انجام وظائف اصلی سازمان می‌باشند.
مثال: تأخیر در فعالیت پرداخت خسارت نهایی به خسارت دیدگان مشتری شرکت بیمه موجب نارضایتی مشتری خواهد گردید. پرداخت به موقع خسارت می‌تواند به عنوان نقطه تمایز شرکت بیمه از شرکت‌های رقیب محسوب گردد. بنابراین فعالیت پرداخت خسارت به عنوان یک فعالیت مهم در شرکت بیمه تلقی می‌گردد.
- تذکر: انتخاب درجه اهمیت فعالیت‌های شناسایی شده به عهده مدیران ارشد یا کارشناسان خبره سازمان می‌باشد.

ب-۴- تعیین آسیب‌پذیری‌های پر اهمیت

همان‌طور که در خصوص فعالیت‌ها گفته شد دارایی‌های اطلاعاتی مختلف نیز در معرض آسیب‌پذیری‌هایی هستند که نسبت به یکدیگر پرخطر یا کم‌خطر می‌باشند. بنابراین لازم است فهرست آسیب‌پذیری‌های شناسایی شده تشکیل و نسبت به یکدیگر درجه‌بندی شوند. درجه آسیب‌پذیری‌ها باید با توجه به نوع آسیب‌پذیری و خطر ناشی از آن آسیب‌پذیری و مستقل از کاربرد یا نوع دارایی اطلاعاتی مربوطه تخصیص داده شود. بدیهی است نوع دارایی اطلاعاتی یا کاربرد آن نیز دارای اهمیت می‌باشد. این موضوع بعداً مورد رسیدگی قرار خواهد گرفت.

بهتر است برای درجه‌بندی آسیب‌پذیری‌ها از مقیاس‌های کمی استفاده شود. همچنین باید درجه تخصیص داده شده به هر آسیب‌پذیری متناسب با شدت زیان ناشی از آن آسیب‌پذیری باشد. به علاوه بهتر است برای تمایز بهتر شدت اثرات ناشی از آسیب‌پذیری از مقیاس‌های نمایی طبق جدول زیر استفاده شود.

جدول ارزیابی زیان احتمالی ناشی از آسیب‌پذیری

شدت زیان ناشی از آسیب‌پذیری	کم	قابل توجه	زیاد	بسیار زیاد	شدید
شاخص آسیب‌پذیری	۱	۲	۴	۸	۱۶

مسئولیت تهیه جدول ارزیابی زیان‌های احتمالی به عهده مسئول امنیت یا جانشین وی می‌باشد.

جهت تسهیل در تعیین آسیب‌پذیری‌های پر اهمیت لازم است جدولی به شرح زیر تشکیل شود.

جدول آسیب‌پذیری‌های پر اهمیت شناسایی شده

نوع آسیب‌پذیری	شدت زیان ناشی از آسیب‌پذیری	شاخص آسیب‌پذیری
آسیب‌پذیری A	کم	۱
آسیب‌پذیری B	زیاد	۴
آسیب‌پذیری C	شدید	۱۶
آسیب‌پذیری D	کم	۱
آسیب‌پذیری F	قابل توجه	۲

توضیح: مقادیر مندرج در جدول فوق به صورت نمونه درج شده‌اند.

مسئولیت تهیه جدول فوق به عهده مسئول امنیت یا جانشین وی می‌باشد.

ب-۵- شناسایی حوزه‌های تهدید

تهدید طبق تعریف عبارت است از شرایطی که امکان سوءاستفاده از آسیب‌پذیری‌های بالقوه را فراهم ساخته و پتانسیل ضربه‌پذیری را افزایش می‌دهد.

برای هر آسیب‌پذیری می‌توان تهدیدهای مختلفی را برشمرد به عنوان مثال آسیب‌پذیری اصلی صفحه نمایشگر (مانیتور) دسترسی افراد غیر مجاز به اطلاعات کشف (رمز نشده) می‌باشد.

بدیهی است اطلاعاتی که روی صفحه نمایش دیده می‌شود حتی اگر در حالت ذخیره، معیارهای رمزنگاری در خصوص آن رعایت شود، در حالت نمایش به صورت عادی نمایش داده می‌شود. بنابراین وضعیت امنیتی مانیتور را می‌توان به شرح زیر فهرست کرد:

دسته‌بندی آسیب پذیری‌ها و تهدیدهای شناسایی شده برای مانیتور

نوع دارایی اطلاعاتی	آسیب پذیری	تهدید
۱- مانیتور	۱-۱- خرابی و نقص فنی	۱-۱-۱- ضربه
		۱-۱-۲- ریختن مایعات
		۱-۱-۳- نوسان برق
	۲-۱- سرقت	۱-۲-۱- عدم رعایت امنیت محیطی
	۳-۱- مشاهده اطلاعات از طرف افراد غیر مجاز	۱-۳-۱- قراردادن در محل غیر مناسب
		۲-۳-۱- عدم استفاده از Screen Saver
		۳-۳-۱- شنود اطلاعات در حال گذر از کابل اتصال مانیتور به کامپیوتر

از بین تهدیدهای فوق تهدیدهای ضربه، ریختن مایعات، نوسان برق، قرار داشتن در محل غیر مناسب و عدم رعایت امنیت محیطی تهدیدی مشترک برای تقریباً همه دستگاه‌ها و قطعات الکترونیکی یا تجهیزات پردازشی می‌باشد. تهدیدهای فوق کلاً مربوط به حوزه امنیت محیطی و فیزیکی می‌باشد.

حوزه امنیت محیطی و فیزیکی یکی از حوزه‌های مستقل و مهم امنیت اطلاعات می‌باشد که در کلیه استانداردهای مرجع امنیت اطلاعات از جمله **ISO/IEC 27001** تحت یک فصل مجزا به آن‌ها پرداخته شده است. بنابراین یکی از مراحل ارزیابی ریسک، ارزیابی حوزه‌های تهدید و شناسایی آن‌ها می‌باشد.

جهت تسهیل در انجام این مرحله استفاده از جدول زیر مفید است:

دسته‌بندی حوزه‌های تهدید موجود برای مانیتور

تهدید	حوزه تهدید
تهدید ۱-۱-۲	امنیت محیطی و فیزیکی
تهدید ۲-۱-۳	امنیت نیروی انسانی
تهدید ۳-۱-۴	امنیت ارتباطات و عملیات
تهدید ۴-۷-۲	امنیت محیطی و فیزیکی
تهدید ۵-۳-۷	امنیت توسعه و نگهداری سیستم
تهدید ۷-۷-۱	امنیت کنترل دسترسی

توضیح ۱: تهدیدهای موجود در جدول فوق فقط تهدیدهایی هستند که مربوط به آسیب پذیری‌های موجود در جدول آسیب پذیری‌های پر اهمیت می‌باشند. درج تهدیدهای مربوط به آسیب پذیری‌های بدون اهمیت در جدول فوق ضروری نیست.

توضیح ۲: تهدیدهای فهرست شده در جدول فوق به صورت نمونه درج شده‌اند. مسئولیت تهیه جدول فوق به عهده مسؤول امنیت یا جانشین وی می‌باشد.

ب-۶- شناسایی مکانیزم‌های حفاظتی موجود و آسیب پذیری‌های تحت کنترل

می‌توان گفت هر نوع سازمان، نهاد یا مرکزی که از سیستم‌های اطلاعاتی یا تجهیزات شبکه‌ای استفاده می‌کند تاکنون به نوعی در معرض تهدیدها و آسیب پذیری‌های ناشی از کاربرد دارایی‌های اطلاعاتی، اعم از ورود و ویروس، از دست رفتن اطلاعات، سرقت اطلاعات، اشتباه در محاسبات یا گزارش‌ها، دسترسی افراد غیر مجاز به شبکه یا سوءاستفاده از آن و یا موارد مشابه قرار داشته است. معمولاً بعد از وقوع هر حادثه تمهیداتی برای جلوگیری از تکرار آن مثل نصب ضد ویروس، تخصیص کلمه‌های عبور، نصب تجهیزات امنیتی مثل فایروال، تهیه نسخه پشتیبان و امثال آن‌ها در نظر گرفته شده و به اجرا گذاشته می‌شود. به عبارت دیگر سازمان سعی در حفظ و افزایش امنیت دارایی‌های اطلاعاتی خود می‌نماید. اینگونه فعالیت‌ها مکانیزم‌های حفاظتی سازمان را تشکیل

می‌دهند. این نوع تمهیدات در برخی از سازمان‌ها کارا، مؤثر و جاری هستند و در برخی سازمان‌های دیگر برنامه‌ریزی نشده و یا متروک می‌باشند.

شناسایی مکانیزم‌های حفاظتی موجود و آسیب‌پذیری‌هایی که توسط آن‌ها تحت کنترل قرار گرفته یا حذف شده‌اند یکی دیگر از مراحل ارزیابی ریسک می‌باشد. این کار با دو هدف انجام می‌شود:

اولاً: جلوگیری از صرف هزینه‌های مضاعف برای فعالیت‌هایی که قبلاً با کارایی قابل قبول به انجام می‌رسیده‌اند.

ثانیاً: بازنگری مجدد مکانیزم‌های حفاظتی موجود و اطمینان از کارایی، اثربخشی و اجرای مستمر آن‌ها

مکانیزم‌های حفاظتی برای جلوگیری از ایجاد شرایط تهدید به کار گرفته می‌شوند. جهت تسهیل در شناسایی مکانیزم‌های حفاظتی تشکیل جدول زیر مفید می‌باشد.

جدول شناسایی مکانیزم‌های حفاظتی

شماره مکانیزم	نام مسئول اجرا	حوزه تهدید	وضعیت اجرا	آخرین تاریخ بازنگری در مکانیزم

مسئولیت تهیه جدول فوق به عهده مسئول امنیت اطلاعات یا جانشین وی می‌باشد.

پس از تهیه جدول فوق لازم است فهرست آسیب‌پذیری‌های تحت کنترل نیز تهیه و در جدول زیر درج گردد:

جدول آسیب‌پذیری‌های تحت کنترل تا تاریخ:

شماره آسیب‌پذیری	عنوان آسیب‌پذیری	مکانیزم حفاظتی		کفایت (بلی / خیر)
		شماره	عنوان	

مسئولیت تهیه جدول فوق به عهده مسئول امنیت یا جانشین وی می‌باشد.

ب-۲- تعیین شاخص احتمال وقوع حادثه

دریافت ضربه ناشی از سوءاستفاده از آسیب پذیری موجود دارایی اطلاعاتی به دلیل عدم توانایی در حذف عامل تهدید منجر به وقوع حادثه خواهد شد.

بنابراین سلسله مراتب وقایع زیر منجر به وقوع حادثه به شرح زیر است:

عدم توانایی در شناسایی پتانسیل تهدید

عدم توانایی در جلوگیری از تبدیل پتانسیل تهدید به واقعه تهدیدآمیز

وجود نقطه آسیب پذیر در دارایی اطلاعاتی

حمله عامل تهدید به نقطه آسیب پذیر

اختلال در کار دارایی اطلاعاتی و یا سوءاستفاده از نقطه آسیب پذیری برای اختلال در کار سایر دارایی‌های اطلاعاتی یا فعالیت‌های سازمان

نقص در عملکرد دارایی اطلاعاتی یا فعالیت اجرایی مربوط به آن

توقف یا انحراف در فرآیند اجرایی

توقف یا انحراف در فرآیند اجرایی موجب زیان (مادی یا معنوی) سازمان خواهد گردید. در سلسله مراتب فوق دو پدیده مهم را می‌توان شناسایی کرد که دارای ماهیت مستقل بوده و در صورت حذف هر یک می‌توان سلسله وقایع وقوع حادثه را متوقف نمود. این دو پدیده عبارت‌اند از:

- تبدیل پتانسیل تهدید به واقعه تهدید آمیز
- اختلال در کار دارایی اطلاعاتی

تبدیل پتانسیل تهدید به واقعه تهدید آمیز را می‌توان به عبارت ساده‌تر به عنوان احتمال وقوع حمله فرض کرد.

احتمال وقوع هر اتفاق را می‌توان به صورت کمی به صورت زیر نمایش داد:

$$0 \leq A \leq 1$$

یا به عبارت ریاضی

$$0 \leq P(A) \leq 1$$

$P(A)=0$ یعنی احتمال وقوع واقعه A وجود ندارد و به همین ترتیب $P(A)=1$ یعنی این واقعه حتماً اتفاق خواهد افتاد. به عنوان مثال احتمال ورود ویروس به شبکه سازمان در صورت اتصال شبکه سازمان به اینترنت و یا امکان انتقال اطلاعات به سازمان از طریق دیسک، دیسک نوری،

Cool disk، Flash Memory و سایر رسانه‌های الکترونیکی حتی با وجود استفاده از نرم‌افزارهای ضد ویروس همیشه وجود دارد. به عبارت دیگر

$$1 = (\text{ورود ویروس به شرط ارتباط با خارج از سازمان}) P$$

آنچه در ارزیابی ریسک مهم است احتمال وقوع حادثه نمی‌باشد (زیرا فرض بر آن است که احتمال وقوع هر نوع حادثه‌ای باید مفروض دانسته شود) بلکه برآورد دفعات وقوع آن حادثه در یک دوره زمانی می‌باشد. بنابراین شاخص احتمال وقوع حادثه امنیتی به شرح زیر تعریف می‌شود:

شاخص احتمال وقوع حادثه عبارت است از تعداد پیش بینی شده برای وقوع یک حادثه در طول یکسال.

مثال: برخی از شاخص‌های حدسی پیش وقوع حوادث رایانه‌ای مختلف در جدول زیر نمایش داده شده است:

جدول نمونه شاخص احتمال وقوع حوادث رایانه‌ای

ردیف	حادثه	شاخص احتمال وقوع (تعداد احتمالی وقوع در یک سال)
۱	زلزله	۱
۲	آتش سوزی	۱
۳	سیل / آب گرفتگی	۱
۴	خرابی سخت‌افزاری	۱
۵	حمله‌های اینترنتی	۲
۶	سوءاستفاده‌های اینترنتی	۲
۷	سرقت	۳
۸	دسترسی غیر مجاز	۶
۹	اشتباه کاربر	۱۲
۱۰	ورود ویروس	۱۲
۱۱		

توضیح: شاخص احتمال وقوع حداقل ۱ می‌باشد. یعنی باید احتمال وقوع هر حادثه را حداقل یکبار در سال در نظر گرفت.

ب- ۸- تعیین ضریب اهمیت دارایی‌های اطلاعاتی

دارایی‌های اطلاعاتی از جنبه‌های مختلف دارای اهمیت می‌باشند. برخی از شاخص‌های اهمیت دارایی‌های اطلاعاتی را می‌توان به شرح زیر فهرست کرد:

ارزش ظاهری یا ارزش ریالی دارایی اطلاعاتی

ارزش داده‌ها یا اطلاعات ذخیره شده در آن دارایی

نقش آن دارایی در انجام بخشی از فعالیت‌ها یا فرآیندهای سازمانی

مکان استقرار

مواد فوق را می‌توان در دو قالب ارزش ریالی و اهمیت جایگاه خلاصه کرد.

- ارزش ریالی قابل استخراج از طریق بررسی مدارک و مستندات خرید یا نگهداری دارایی اطلاعاتی می‌باشد که از آن به عنوان "ارزش ریالی دارایی" یاد می‌شود.
- اهمیت جایگاه یا ارزش ذاتی دارایی عبارت است میزان اهمیت دارایی در مقایسه با سایر دارایی اطلاعاتی در جهت تداوم ارائه خدمات اطلاعاتی سازمان. برای تعیین ارزش ذاتی دارایی اطلاعاتی لازم است دارایی‌های اطلاعاتی مختلف نسبت به یکدیگر مقایسه شده و در طبقات مربوط قرار داده شوند. برای سهولت عملیات بعدی به هر طبقه از دارایی‌ها یک شاخص کمی تخصیص داده می‌شود، طبقه‌ها و شاخص‌های قابل انتخاب برای دارایی‌های اطلاعاتی به شرح زیر است:

ارزش ذاتی	شاخص ارزش ذاتی
کم ارزش	۱
پر ارزش	۳
بسیار پر ارزش	۹

ضریب اهمیت هر دارایی اطلاعاتی از حاصلضرب ارزش ریالی دارایی اطلاعاتی و شاخص ارزش ذاتی همان دارایی به دست می‌آید.

برای سهولت محاسبه ضریب اهمیت هر دارایی اطلاعاتی می‌توان از جدول نمونه زیر استفاده کرد:

جدول محاسبه ضریب اهمیت دارایی‌های اطلاعاتی

شماره دارایی a	عنوان دارایی اطلاعاتی b	ارزش ریالی c	ارزش ذاتی d	شاخص ارزش ذاتی e	ضریب اهمیت دارایی f = e x c
مثال :					
xxxx	سرور ارتباطات	۶۰/۰۰۰/۰۰۰	پر ارزش	۳	۱۸۰/۰۰۰/۰۰۰
xxxxy	سرور بانک داده‌ها	۶۰/۰۰۰/۰۰۰	بسیار پر ارزش	۹	۵۴۰/۰۰۰/۰۰۰

ب-۹- محاسبه شاخص ریسک

آخرین مرحله در ارزیابی ریسک، محاسبه شاخص ریسک هر دارایی اطلاعاتی می‌باشد. شاخص ریسک هر دارایی اطلاعاتی به صورت زیر محاسبه می‌شود:

$$R_i = \text{شاخص ریسک دارایی اطلاعاتی } i$$

$$F_i = \text{ضریب اهمیت دارایی اطلاعاتی } i$$

$$P_{ij} = \text{شاخص احتمال وقوع حادثه } j \text{ برای دارایی اطلاعاتی } i$$

$$V_{\max i} = \text{بزرگترین شاخص آسیب پذیری دارایی اطلاعاتی } i$$

(مثال: اگر یک دارایی اطلاعاتی دارای دو نوع آسیب پذیری ۲ و ۱۶ باشد $V_{\max i}=16$ خواهد بود)

$$R_i = F_i * (P_{ij}) * V_{\max i}$$

ب-۱۰- محاسبه ریسک جغرافیایی و انتخاب سرپل امن‌سازی

تعریف مرز جغرافیایی اولین قدم در ایجاد یک نظام دفاعی می‌باشد. این موضوع در تأمین امنیت اطلاعات نیز صادق است. لازم است مرزهای جغرافیایی مکان‌های استقرار تجهیزات و دارایی‌های اطلاعاتی به دقت تعریف شود و کلیه اقدامات دفاعی با توجه به حدود جغرافیایی مکان استقرار دارایی‌های اطلاعاتی برنامه‌ریزی و اجرا شود.

دلیل این موضوع نیاز به شروع اقدامات امنیتی از یک نقطه و گسترش آن به نقاط و مکان‌های دیگر سازمان می‌باشد. به عنوان مثال در صورت اقدام به نصب آنتی ویروس لازم است به ترتیب کلیه فایل‌های موجود بر روی یک رسانه، یک رایانه، یک شبکه مجازی، یک شبکه محلی و یک شبکه گسترده پاکسازی شوند. نصب آنتی ویروس به صورت تصادفی و بر روی رایانه‌های مختلف کاری بیهوده و بدون نتیجه می‌باشد، چرا که امکان انتقال کدهای مخرب از یک کامپیوتر پاکسازی نشده یا فاقد آنتی ویروس به یک شبکه همیشه وجود دارد.

همچنین وقتی قرار است یک شبکه تحت حفاظت، به وسیله فایروال از شبکه‌های دیگر جدا شده و تحت کنترل قرار گیرد باید کلیه کانال‌های ورود و خروج اطلاعات به آن شبکه مسدود شده و ارتباطات فقط از طریق فایروال برقرار شود. وجود یک کامپیوتر متصل به مودم در آن شبکه موجب نقش بر آب شدن کلیه سیاست‌گذاری‌های امنیتی و مکانیزم‌های حفاظتی خواهد شد.

حال باید دید کدام بخش از سازمان باید به عنوان نقطه شروع عملیات امن‌سازی یا به عبارت دیگر سرپل امن‌سازی انتخاب شود.

با توجه به محدودیت منابع و بودجه بهتر است همیشه آن بخشی از سازمان به عنوان سرپل امن‌سازی انتخاب شود که بیشترین ضربه پذیری از آن نقطه وجود دارد.

بیشترین ضربه پذیری مربوط به آن بخش یا محدوده جغرافیایی است که شاخص ریسک محاسبه شده مربوط به آن بیشترین مقدار را داشته باشد. برای محاسبه شاخص ریسک جغرافیایی هر محدوده می‌توان از فرمول زیر استفاده کرد:

$R_r =$ شاخص ریسک جغرافیایی بخش r سازمان

$Rir =$ شاخص ریسک دارایی اطلاعاتی i موجود در محدوده جغرافیایی r

$R_r = \sum R_{ri}$ {برای کلیه دارایی‌های اطلاعاتی مهم بخش مربوط}

پس از محاسبه شاخص ریسک برای هر ناحیه جغرافیایی (که برای سهولت از آن به نام بنه اطلاعاتی نام برده می‌شود)، با توجه به مقدار شاخص ریسک فهرست مرتب شده بنه‌های اطلاعاتی بر اساس شاخص ریسک تهیه و امن‌سازی بنه‌ها به ترتیب از بنه‌ای که بزرگترین شاخص ریسک را داراست آغاز می‌شود.

در این جا لازم است توضیح کوتاهی در خصوص بنه اطلاعاتی ارائه شود:

بنه اطلاعاتی عبارت است از یک اتاق، طبقه، سازمان، ملک، محدوده، یا هر مکان استقرار دیگری که بتوان آن را با استفاده از دیوارهای فیزیکی (اعم از دیواره ثابت یا موقت) محصور کرد و رفت و آمد افراد یا تبادل اطلاعات آن با سایر شبکه‌ها یا مراجع دیگر را تحت کنترل قرار داد.

ب-۱۱- پیشنهاد مکانیزم‌های حفاظتی

پس از انتخاب نقطه شروع امن‌سازی یا سرپل امن‌سازی لازم است با توجه به نوع تهدیدها و حوزه‌های وقوع تهدید به انتخاب مکانیزم‌های امن‌سازی پرداخت. همان‌طور که قبلاً گفته شد حوزه‌های امنیت اطلاعات (بر اساس استاندارد ISO-27001) عبارت‌اند از:

- امنیت نیروی انسانی: اطمینان از کفایت نیروی انسانی و رعایت امنیت در به‌کارگیری نیروی انسانی و آموزش ایشان
- امنیت فیزیکی و محیطی: برای حفاظت از دارایی‌های اطلاعاتی در مقابل تهدیدات محیطی طبیعی یا عمدی مثل زلزله، سیل، آتش سوزی، طوفان، سرقت، تخریب عمدی یا غیرعمدی، حمله الکترونیکی، دسترسی غیر مجاز فیزیکی و غیره
- مدیریت ارتباطات و عملیات: برای امن‌سازی کانال‌های ارتباطی و عملیات اجرایی سیستم‌های اطلاعاتی
- کنترل دسترسی: برای جلوگیری از دسترسی منطقی غیر مجاز به دارایی‌های اطلاعاتی از قبیل سیستم عامل، نرم‌افزارها، برنامه‌های کاربردی، بانک‌های اطلاعاتی، تجهیزات ذخیره و بازیابی، تجهیزات مسیریابی، سویچینگ و غیره
- بهره‌برداری، توسعه و نگهداری سیستم‌های اطلاعاتی: برای لحاظ کردن الزامات امنیتی هنگام تهیه نرم‌افزارهای اطلاعاتی و به‌کارگیری آنها
- مدیریت وقایع سیستم‌های اطلاعاتی: برای اطمینان از رسیدگی به کلیه وقایع و حوادث امنیتی و برنامه‌ریزی برای پیشگیری از وقوع مجدد آنها و همچنین جلوگیری از شرایطی که ممکن است بعداً منجر به وقوع حادثه شوند.
- مدیریت پیوستگی و تداوم عملیات: برای اطمینان از مقاومت سیستم‌ها و دارایی‌های اطلاعاتی سازمان هنگام دریافت ضربه و حملات شدید رایانه و احیای سیستم در صورت خارج از رده شدن برخی یا تمام دارایی‌های اطلاعاتی یا نیروی انسانی

- انطباق: برای اطمینان از انطباق روش‌ها و فعالیت‌های سازمان با قوانین و مقررات و رعایت اصول حرفه‌ای در ممیزی امنیت فعالیت‌های پردازشی

مکانیزم‌های امن‌سازی با توجه به نوع آسیب پذیری‌ها و تهدیدها انتخاب می‌شوند. استانداردهای مدیریت امنیت اطلاعات معمولاً فهرستی از مکانیزم‌های کنترلی را در اختیار قرار می‌دهند. این فهرست، فهرستی عام است و لازم است هر سازمان از بین آن‌ها مکانیزم‌های مورد نظر خود را انتخاب کند.

به مجموعه‌ای از مکانیزم‌هایی که از بین مکانیزم‌های فوق انتخاب می‌شود فهرست دستورالعمل‌های کاربردی اختصاصی یا به عبارت رسمی‌تر "بیانیه کاربرد پذیری اختصاصی" ¹⁷ (SOA) گفته می‌شود. لازم است برای اجرای هر بند از SOA یک دستورالعمل اختصاصی و مجزا تدوین شود.

دستورالعمل‌های حاضر که شما در حال مطالعه آن می‌باشید (از دستورالعمل ۱-۱ تا ۷-۷-۲) بر اساس این الزام تدوین شده‌اند.

یادآور می‌شود که هر سازمان با توجه به نوع نیاز خود می‌تواند دستورالعمل‌های حاضر را به عنوان دستورالعمل سازمان خود پذیرفته و به اجرا گذارد و یا خود اقدام به تصحیح این دستورالعمل یا نوشتن دستورالعمل‌های جدید نماید.

هر دستورالعمل مبین الزامات مختلفی می‌باشد. ممکن است لازم باشد به ازاء هر دستورالعمل و بر اساس فرآیند مندرج در آن، رویه‌های عملیاتی مبین چگونگی روش قدم به قدم پیاده‌سازی مکانیزم امنیتی تدوین شود. رویه عملیاتی امن‌سازی مبین چگونگی روش امن‌سازی هر دارایی اطلاعاتی می‌باشد. ممکن است لازم باشد به ازای هر دارایی اطلاعاتی بیش از یک رویه تدوین شود. به عنوان مثال جهت امن‌سازی سرورهای اصلی بانک اطلاعاتی سازمان ممکن است نیاز به تدوین رویه‌های زیر باشد:

رویه تأمین انرژی

رویه تأمین تهویه

¹⁷ - Statement of Applicability

رویه امن‌سازی در مقابل زلزله/ آتش سوزی/ آب گرفتگی/ حمله الکترومغناطیسی
 رویه امن‌سازی در مقابل دسترسی غیر مجاز فیزیکی یا منطقی
 رویه امن‌سازی در مقابل خرابی سخت‌افزار
 رویه تهیه نسخه پشتیبان از اطلاعات

ب-۱۲- تعیین ریسک باقیمانده

پیاده‌سازی مکانیزم‌های امنیتی به معنای دستیابی به امنیت ۱۰۰٪ نمی‌باشد. اصولاً دستیابی به امنیت کامل غیر ممکن است. همیشه برخی از آسیب پذیری‌ها وجود دارند که راهی برای غلبه بر آن‌ها وجود ندارد. پس از انتخاب مکانیزم‌های امنیتی لازم است مجدداً ارزیابی ریسک به عمل آید و ریسک باقیمانده^{۱۸} (مجموع ریسک‌هایی که قابل مدیریت بر اساس دستورالعمل ۳-۳-۳) نیستند شناسایی و محاسبه گردند.

ریسک باقیمانده نشان‌دهنده میزان ضربه پذیری باقیمانده سازمان و حوزه‌های پر خطر فعالیت سازمان می‌باشد.

فرض می‌شود صفر کردن ریسک باقیمانده غیر ممکن است. اما لازم است به‌طور مداوم فعالیت‌های سازمان، روش‌های انجام آن‌ها و دارایی‌های اطلاعاتی مورد بررسی قرار گرفته و سعی در حذف نقاط آسیب‌پذیر آن‌ها یا کاهش شرایط تهدید گردد.

¹⁸ -Residual Risk

ضمیمه دو

آسیب پذیری‌ها و روش‌های حمله

الف- آسیب پذیری‌ها

آسیب پذیری‌های منجر به حمله‌های رایانه‌ای را می‌توان به دو دسته کلی تقسیم کرد:

آسیب پذیری‌های فنی شامل:

ضعف‌های نرم‌افزاری (Software Bugs)

خطا در پیکربندی (Configuration Error)

آسیب پذیری نیروی انسانی (استفاده از مهندسی اجتماعی یا Social Engineering)

الف-۱- آسیب پذیری‌های فنی

آسیب پذیری‌های فنی به دو دسته ضعف‌های نرم‌افزاری و خطا در پیکربندی تقسیم می‌شود.

الف-۱-۱- ضعف‌های نرم‌افزاری

ضعف‌های نرم‌افزاری تشکیل دهنده بخش عمده آسیب پذیری‌های رایانه‌ای می‌باشند. افراد هکر (Hackers) یا حمله کننده احتمالی (Attackers) با آگاهی از این نوع ضعف‌های نرم‌افزاری می‌توانند به نقاط ضعف سیستم حمله کرده و باعث از کار افتادن آن و یا سوءاستفاده از سیستم‌های رایانه‌ای شوند.

ضعف‌های نرم‌افزاری را می‌توان به دو دسته عمده تقسیم کرد:

ضعف‌های بنیادی

ضعف در برنامه نویسی

ضعف‌های بنیادی آن دسته از ضعف‌هایی هستند که مربوط به ذات نرم‌افزار می‌باشد. به عنوان مثال برخی از بانک‌های داده قدیمی مثل SQL یا Oracle یا نسخه‌های جدید تصحیح نشده آن‌ها در مقابل حمله تزریق SQL (SQL Injection) آسیب پذیر می‌باشند. در این نوع حمله که معمولاً جهت عبور از مکانیزم‌های کنترل دسترسی و دسترسی غیر مجاز به اطلاعات به اجرا در می‌آید، حمله کننده با ورود رشته‌های معینی از کاراکترها به همراه کاراکتر Quotation (" یا ") و قابلیت عملگر منطقی "OR" سعی در تولید رشته‌هایی از نام کاربر و کلمه عبور دلخواه می‌کند که در تمام اوقات نتیجه جست‌وجو در بانک نام کاربری و کلمه عبور را به صورت True به تابع کنترل دسترسی باز می‌گرداند. در این حالت معمولاً حمله کننده علاوه بر ورود به سیستم به سایر

کلمه‌های عبور معتبر سیستم نیز دست پیدا می‌کند و می‌تواند از آن‌ها برای دستیابی به مقاصد بعدی خود استفاده نماید.

برخی دیگر از ضعف‌های نرم‌افزاری ناظر بر ماهیت نرم‌افزار و روش‌های بهره‌برداری از آن می‌باشد. به عنوان مثال پروتکل TCP/IP که به عنوان پروتکل اصلی در مسیریابی و انتقال داده در اینترنت و بسیاری از شبکه‌ها مورد استفاده قرار می‌گیرد دارای روش خاصی (روش سه مرحله‌ای Hand Shaking) برای برقراری ارتباط بین طرف‌های دو سوی ارتباط می‌باشد. بسیاری از مدل‌های حمله بر اساس این روش سه مرحله‌ای طراحی شده و به اجرا گذاشته می‌شوند.

دسته‌ای دیگر از ضعف‌های نرم‌افزاری مربوط به نوع تعامل نرم‌افزار با فضای عملیاتی و مدیریت حافظه می‌باشد. به عنوان مثال در زبان برنامه نویسی C و برخی دیگر از زبان‌های برنامه نویسی سطح پایین، کنترل اشاره گر (Pointer) در مرحله برپایی زبان مورد توجه قرار نگرفته و در صورت عدم توجه برنامه نویس به این ضعف می‌تواند موجب فروپاشی سیستم و یا به عبارت دیگر هنگ کردن کامپیوتر گردد. حمله‌های منجر به سر ریز پشته (Buffer Overflow) از این دسته حملات می‌باشند.

ضعف در برنامه نویسی یکی دیگر از عوامل ایجاد آسیب پذیری‌های رایان‌های می‌باشند. برخی از عوامل ایجاد ضعف در برنامه نویسی را می‌توان به شرح زیر فهرست کرد:

مستند نبودن مراحل برنامه نویسی

عدم توجه به ضعف‌های ذاتی محیط‌های برنامه نویسی و پیش بینی نکردن روش‌های مقابله با آن‌ها

عدم وجود روش مناسب جهت کنترل نسخه (Version Control) و تداخل ماژول‌های نسخه‌های مختلف با یکدیگر

عدم پیش بینی روش‌های مدیریت خطا

عدم رعایت سلسله مراتب کنترل دسترسی (سیاست‌گذاری کنترل دسترسی، کنترل دسترسی عام، کنترل دسترسی خاص)

عدم رعایت اصول مدیریت و بهینه سازی حافظه

عدم پیش بینی حجم داده‌های تولیدی یا ظرفیت پردازش

عدم رعایت اصول تکمیل تراکنش در پردازش‌های متوالی و وابسته

عدم کنترل ورودی و خروجیهای اطلاعاتی
 عدم پیش بینی تهیه نسخه پشتیبان از داده‌ها
 عدم رعایت جداسازی داده‌های آزمایشی از داده‌های واقعی
 عدم رمزنگاری داده‌های ذخیره شده
 فهرست فوق را می‌توان تکمیل تر نمود و موارد دیگری را به عنوان ضعف در برنامه نویسی بر شمرد.

به‌طور کلی تمام فعالیت‌های رایانه‌ای بر مبنای چگونگی عملکرد نرم‌افزارها برنامه‌ریزی می‌شوند (حتی سخت‌افزارهای مختلف نیز از طریق نرم‌افزارهای مخصوص به خود اعم از نرم‌افزارهای کنترلی [Driver] و یا سیستم‌های نهفته [Embedded System] کنترل می‌شوند). به همین دلیل می‌توان بخش عمده‌ای از آسیب پذیری‌های رایانه‌ای (آسیب پذیری‌های منطقی) را پیامد وجود ضعف‌های نرم‌افزاری دانست.

الف ۱-۲- خطا در پیکربندی

بخش دیگری از عوامل آسیب پذیری رایانه‌ای را خطا در پیکربندی تشکیل می‌دهد. خطا در پیکربندی ناظر بر عدم پیکربندی صحیح نرم‌افزارها یا سخت‌افزارهای مختلف می‌باشد. در این حالت پارامترهای سیستم به درستی انتخاب یا تنظیم نمی‌شوند و این موضوع باعث ایجاد ضعف در عملکرد سیستم یا مدیریت آن می‌شود. به عنوان مثال افزودن اشتباهی یک عضو به یک VPN تعریف شده در پروتکل MPLS باعث بی اثر شدن تمام روش‌های امنیتی پیش بینی شده در پروتکل MPLS-VPN می‌شود. این کار می‌تواند به صورت تصادفی و یا عمدی انجام شود. ممکن است حالت تصادفی آن هیچگاه کشف نشود و با این حال نیز باعث ایجاد مشکل خاصی برای آن VPN خاص نگردد، اما مسلماً حالت عمدی آن پیامدهای غیر قابل جبرانی را به همراه خواهد داشت.

عدم تغییر در کلمه‌های عبور تجهیزات مختلف (مثل تجهیزات مسیریابی یا سرور یا سیستم عامل و یا هر نرم‌افزار یا سخت‌افزار دیگری) را می‌توان به عنوان خطا در پیکربندی محسوب کرد. در این حالت حمله کننده می‌تواند با آگاهی از کلمه‌های عبور پیش فرض که به راحتی از طریق سایت‌های اینترنتی در دسترس قرار می‌گیرد، به نرم‌افزار یا سخت‌افزار مورد نظر خود دست یافته و اقدام به خرابه‌کاری یا دستکاری و یا سوءاستفاده از داده‌ها یا ظرفیت‌های سیستم نماید.

الف-۲- آسیب‌پذیری نیروی انسانی

یکی دیگر از آسیب‌پذیری‌های مهم سیستم‌های رایانه‌ای عدم آشنایی نیروی انسانی با روش‌های آماده سازی فضا برای حمله از سوی حمله‌کنندگان احتمالی می‌باشد. در این حالت حمله‌کننده با استفاده از برقراری ارتباط با نیروی انسانی و فریفتن ایشان از راه‌های مختلف اقدام به جمع‌آوری اطلاعات از سیستم هدف از قبیل نوع کانال‌های ارتباطی، شناسه‌های کاربری و کلمه عبور، آدرس IP، میزبان‌های مهم و یا نوع نرم‌افزار و سخت‌افزارهای موجود در شبکه می‌نماید. این روش مشهور به روش مهندسی اجتماعی (Social Engineering) می‌باشد.

حمله‌کننده در این حالت معمولاً از طریق برقراری تماس تلفنی با افرادی که ممکن است دارای اطلاعاتی در مورد سیستم باشند اقدام می‌نماید. معمولاً زمان تماس به ساعات پایانی هفته یا خارج از ساعت اداری روز موکول می‌شود. حمله‌کننده ممکن است خود را به عنوان مدیر ارشد سازمان، تعمیر کار، فردی که معمولاً به ضرورت کاری خارج از سازمان است و یا حتی یک فرد عادی که جهت انجام فعالیت‌های علمی دست به جمع‌آوری اطلاعات می‌زند معرفی نماید. به‌طور کلی حمله‌کننده ممکن است با توجه به شناختی که از طرف تماس دارد درخواست خود را با تحکم و یا به‌صورت درخواست لطف در حق خودش مطرح کند.

در کلیه حالت‌های فوق حمله‌کننده خود را به عنوان فردی آگاه از وضعیت سیستم معرفی می‌نماید و با مطرح کردن اطلاعات مختصری که از منابع مختلف در مورد شبکه یا سیستم‌های سازمان جمع‌آوری کرده است سعی در جلب اعتماد طرف تماس می‌نماید. همچنین ممکن است تماس‌های متعددی با افراد سازمان برقرار نماید و در هر تماس از اطلاعات جمع‌آوری شده در تماس قبلی سوءاستفاده کند.

روابط غیررسمی در محیط کاری بین کارمندان با یکدیگر و یا ارباب رجوع نیز یکی دیگر از عوامل تهدیدکننده و تشکیل دهنده منبع ریسک می‌باشد. اینگونه روابط ممکن است منجر به اعتماد بیش از حد افراد به یکدیگر گردد و یا با ایجاد تعهدهای مالی یا اخلاقی نسبت به یکدیگر موجب بده بستن‌های نامشروع بین افراد گردد. ریسک ناشی از این گونه موارد در مواردی حتی بیشتر از ریسک مواجه با مهندسی اجتماعی می‌باشد.

ب- انواع حمله‌های رایانه‌ای^{۱۹}

انواع مختلفی از حمله‌های مختلف وجود دارد که برخی از آن‌ها به خوبی شناسایی و دسته‌بندی شده‌اند. در ادامه شرح مختصری در خصوص هر یک از این نوع حمله‌ها و مثال‌هایی در مورد آن‌ها ارائه می‌گردد.

ب-۱- حمله‌های شناسایی

حمله‌های شناسایی عبارت‌اند از حمله‌هایی که جهت جمع‌آوری اطلاعات اولیه در مورد هدف به اجرا در می‌آیند. این نوع حمله‌ها معمولاً دارای آثار جنبی مستقیم نمی‌باشند و باعث اختلال در کار سیستم نمی‌شوند، اما هر چه اطلاعات جمع‌آوری شده در حین این نوع حمله دقیق‌تر باشد آثار حمله‌های بعدی طراحی شده بر اساس آن‌ها مخرب‌تر خواهد بود. انواع این نوع حمله عبارت‌اند از:

شناسایی به روش مهندسی اجتماعی و بر اساس خصوصیات روان شناختی افراد
سعی در دسترسی مستقیم و ورود بدون واسطه به سیستم یا شبکه از طریق ورود بدون شناسه کاربری یا کلمه عبور، حدس شناسه یا کلمه‌های عبور یا استفاده از شناسه یا کلمه‌های عبور پیش فرض تجهیزات یا نرم‌افزارها

آشغال گردی (Dumpster Diving) از طریق جست‌وجوی مواد دور ریخته شده مثل گزارش‌های چاپی، ریون‌ها یا کاربن‌ها، مستندات سیستم، مکاتبات و یا دیسک‌ها، دیسک‌ها یا رسانه‌های ذخیره اطلاعات دور انداخته شده یا خراب و خارج از رده

جست‌وجو در Web به دنبال اطلاعات مفید مثل جست‌وجو در سایت‌های اطلاعاتی مؤسسه (WebSite سازمانی)، استفاده از موتورهای جست‌وجو مثل Google, yahoo, AltaVista و غیره، استفاده از Usenet، استفاده از بانک اطلاعات Whois، استفاده از اطلاعات سایت ARIN جهت تحقیق در مورد آدرس‌های IP سازمان، بررسی DNS

ب-۲- حمله‌های پوش و جست‌وجو در شبکه به دنبال رخنه

پس از جمع‌آوری اطلاعات اولیه در خصوص شبکه هدف، حمله‌کننده سعی در یافتن راه‌های ورود به شبکه یا نفوذ به آن می‌نماید. این مرحله جهت یافتن سرپل عملیاتی در شبکه هدف از سوی حمله‌کننده به اجراء گذاشته می‌شود.

^{۱۹} - در تهیه مطالب این بخش از مطالب کتاب نفوذگری در شبکه و روش‌های مقابله با آن نوشته احسان ملکیان بهره گرفته شده است.

برخی از حمله‌های پویش عبارت‌اند از:

بررسی خطوط تلفنی سازمان مالک شبکه هدف برای یافتن مودم‌ها: در این حالت از دو نوع حمله **War Dialer** جهت جست‌وجو بین تعداد زیادی از شماره‌های تلفن برای یافتن خطوطی که به مودم متصل هستند و **Demon Dialer** برای حمله علیه یک شماره تلفن متصل به مودم جهت یافتن کلمه عبور و نفوذ به ماشین متصل به آن مودم استفاده می‌شود.

توجه: خطوط متصل به مودم به عنوان خطوط وحشی شناخته می‌شوند. در صورت پیکربندی نادرست نرم‌افزارهای مدیریت مودم، تهدید ناشی از حمله به این نوع خطوط بسیار زیاد خواهد بود. توجه: وجود یک مودم متصل به یک ماشین عضو شبکه داخلی ((**LAN**) موجب از بین رفتن تأثیر کلیه ابزارهای پیشرفته امنیتی خواهد شد.

ب-۳- نقشه برداری از شبکه

در صورت شناسایی راه ورود به شبکه، مرحله بعدی شناسایی وضعیت شبکه و نحوه قرار گرفتن ماشین‌ها در آن و یا به عبارت دیگر نقشه برداری از شبکه می‌باشد. این حمله شامل مراحل زیر خواهد بود:

شناسایی ماشین‌های فعال از طریق ارسال بسته‌های **Ping**

شناسایی و تعقیب مسیرها در شبکه یا **Trace Route**

ب-۴- شناسایی پورت باز

در صورت موفق بودن حمله نقشه برداری از شبکه، حمله کننده از توپولوژی واقعی یا تقریبی شبکه آگاهی می‌یابد. در این حالت آدرس ماشین‌های شبکه و محل قرار گرفتن هر ماشین معلوم می‌گردد. (فرض بر آن است که پروتکل شبکه از نوع **TCP/IP** می‌باشد). برای شناسایی نوع وظیفه‌ای که بر عهده هر ماشین می‌باشد و حدس نوع سوءاستفاده‌ای که از آن می‌توان نمود لازم است پورت‌های باز یا فعال **TCP** یا **UDP** هر ماشین و پروسه‌هایی که روی آن اجراء شده‌اند مشخص شوند.

در پروتکل **TCP/IP** هر ماشین می‌تواند حداکثر ۶۵۵۳۵ پورت **TCP** به همین تعداد پورت **UDP** داشته باشد که با توجه به نوع و مأموریت کامپیوتر مربوط، فقط تعداد محدودی از این پورت‌ها باز و فعال می‌باشند.

باز بودن پورت به معنی آن است که در کامپیوتر هدف پروسه‌ای (یا برنامه ای) وجود دارد که بسته‌های رسیده از شبکه به مقصد آن پورت را دریافت کرده و آن‌ها را پردازش می‌نماید. به عنوان

مثال برنامه‌های **Web Browser** بسته‌های ارسال شده به مقصد پورت **TCP 80**، سرویس دهنده **DNS** بسته‌های ارسال شده به پورت **UDP 53** و نرم‌افزارهای پست الکترونیک از پورت‌های **TCP 25** برای ارسال و **TCP 110** برای دریافت استفاده می‌نمایند.

روش‌های مختلف پویش پورت عبارت‌اند از:

مکانیزم پویش مؤدبانه (**Polite Scan**) از طریق سعی در برقراری ارتباط کامل سه مرحله‌ای **TCP**

(به‌جز در سیستم عامل‌های **Windows**)

پویش مخفیانه (**TCP SYN Scan**) از طریق برقراری ارتباط و قطع آن قبل از تکمیل روش سه

مرحله‌ای (به‌جز در سیستم عامل **Windows**)

پویش بر اساس روش نقض پروتکل از طریق ارسال بسته‌های ناکامل جهت برقراری ارتباط

با ارسال بسته‌های بی معنی که در این حالت دریافت پاسخ از طرف مقصد به معنی بسته بودن آن

پورت است. (به‌جز در سیستم عامل **Windows**)

پویش به روش **TCP ACK Scan** که در این حالت نیز عدم دریافت پاسخ به معنی باز بودن

پورت است.

پویش به روش **FTP Bounce Scan** جهت شناسایی پورت‌های باز از طریق امکانات سرویس

دهنده **FTP** بدون فاش کردن هویت یا آدرس **IP** حمله کننده

پویش با استفاده از بسته‌های **UDP** برای اطمینان از بسته بودن پورت **UDP**

ارسال **Ping** بدون بهره گیری از **ICMP** از طریق ارسال بسته‌های **TCP** بی هدف و تشخیص

فعال بودن ماشین به دلیل دریافت هر نوع پاسخ **SYN-ACK** یا **RESET**.

شناسایی برنامه‌های **RPC (Remote Procedure Call)** و سوءاستفاده از نقاط ضعف فراوان

برنامه‌های **RPC** از طریق فروپاشی سیستم و یا **Buffer Overflow**

تنظیم شماره پورت مبدأ ((**Source Port**) جهت افزایش شانس عبور بسته‌های ارسال شده از

طریق حمله کننده از مسیر یاب و دیواره‌های آتش ((**Firewall**) از طریق تنظیم پورت مجاز مثل پورت

TCP 80 برای پورت مبدأ و پورت مورد آزمایش در ماشین مقصد.

شناسایی سیستم عامل ماشین هدف از طریق ارسال بسته‌های غیر متعارف خاص به ماشین

هدف و بررسی پاسخ ارسال شده برای آن

Firewalk علیه **Firewall** جهت شناسایی پورت‌های بازمانده از طریق **Firewall**

ب-۵- حمله به سیستم امنیتی IDS

سیستم تشخیص نفوذ یا IDS^{۲۰} یکی از ابزارهای دفاعی شبکه است که با شناسایی الگوهای حمله بر اساس مدل‌های شناسایی شده و بانک اطلاعاتی خود سعی در تشخیص و در حالت IPS^{۲۱} جلوگیری از نفوذ به شبکه می‌نماید. برخی از حمله‌ها جهت عبور از این نوع مکانیزم دفاعی یا دور زدن آن طراحی شده‌اند. برخی از این نوع حمله‌ها عبارت‌اند از:

حمله به IDS بر اساس ارسال بسته‌های قطعه قطعه شده کوچک و قطعات هم پوشان IP حمله به IDS جهت کشف برنامه‌های CGI آسیب پذیر

ب-۶- نفوذ از طریق حمله به سیستم عامل یا برنامه‌های کاربردی

همه سیستم‌های عامل آسیب پذیرند. همچنین ضعف‌های نرم‌افزاری که قبلاً در مورد آن‌ها صحبت شد باعث ایجاد نقاط آسیب پذیر فراوان در برنامه‌های کاربردی (Application) می‌شود. همچنین بسیاری از ابزارهای سیستم مانند نرم‌افزارهای مدیریت ارتباط، مدیریت دیسک، مدیریت فایل‌های چند رسانه‌ای، نرم‌افزارهای Office و غیره دارای نقاط ضعف و آسیب پذیری فراوان هستند.

برخی از حمله‌های طراحی شده بر اساس آسیب پذیری‌های فوق در زیر فهرست شده‌اند: فروپاشی برنامه کاربردی یا سیستم عامل از طریق سر ریز پشته ((Stack Overflow با استفاده از دستکاری فضای آدرس دهی ساختمان داده اصلی کنترل کننده فعالیت‌های سیستم عامل. به دست گرفتن کنترل ماشین پس از شکسته شدن پشته از طریق هدایت سیستم به اجرای فرمان‌های مورد نظر حمله کننده و دستیابی به کلیه منابع سیستم

حمله علیه کلمه‌های عبور از طریق حدس مستقیم کلمه عبور یا استفاده از نرم‌افزارهای Brute Force شکستن کلمه‌های عبور به روش‌های علمی و بر اساس اصل ذخیره‌سازی کلمه‌های عبور در جایی از سیستم یا تبادل کلمه عبور در مرحله درخواست دسترسی به سیستم و جست‌وجو به دنبال آن.

²⁰ - Intrusion Detection System

²¹ - Intrusion Prevention System

ب-۷- حمله بر علیه Web و برنامه‌های کاربردی آن

با کاربرد روز افزون برنامه‌های تحت Web و وجود آسیب پذیری ذاتی در اینگونه برنامه‌ها و همچنین ضعف‌های نرم‌افزاری در برنامه‌های کاربردی تحت Web به دلیل ضعف در برنامه نویسی، حمله علیه Web گسترش بسیاری یافته است. برخی از این نوع حمله‌ها عبارت‌اند از:

درو کردن حساب‌های کاربردی در Web (Account Harvesting) از طریق شناسایی حساب‌های کاربری Web و تلاش در حدس کلمه‌های عبور و سوءاستفاده از آن‌ها
حمله تعقیب نشست‌های Web (Web Session Tracking) از طریق تعقیب و ربودن نشست‌های Web^{۲۲} که در آن از شناسه نشست (Session ID) تخصیص داده شده از طرف برنامه تحت Web به کاربر متقاضی درخواست خدمات از آن برنامه، سوءاستفاده می‌شود.

حمله به کوکی‌های موقت (Precession Cookies) که در این نوع حمله کوکی‌ها (که عبارت از اطلاعاتی است که از طریق پروتکل HTTP به مرورگر کاربر ارسال شده و حاوی اطلاعات خاصی در مورد نوع ارتباط است) به عنوان هدف تحت حمله قرار گرفته و از آن‌ها سوءاستفاده می‌شود.

ب-۸- حمله به برنامه‌های کاربردی یا تحت Web از طریق دستکاری SQL

در این نوع حمله از طریق دستکاری در شکل Queryهای ارسالی به بانک اطلاعاتی مرتبط با برنامه کاربردی یا برنامه تحت Web، سعی در دریافت مجموعه‌ای از اطلاعات می‌شود. این حمله معمولاً بر اساس استفاده از معنای کاراکترهای خاص برای بانک‌های اطلاعاتی برنامه‌ریزی می‌شود. این کاراکترها عبارت‌اند از:

- کاراکتر ' (Quotation)
- کاراکتر " (Double Quote)
- کاراکتر ، (Comma)
- کاراکتر ; (Semi Colon)

ب-۹- حمله‌های استراق سمع در سطح لایه شبکه

در این نوع حمله ترافیک شبکه (اعم از کل ترافیک شبکه و ترافیک ارسالی به یک ماشین خاص) تحت نظر قرار گرفته و بر اساس تجزیه و تحلیل آن اقدام به شناسایی شبکه و جاسوسی می‌شود. در این حالت تغییری در ترافیک عبوری داده نمی‌شود و به همین دلیل شناسایی آن بسیار

مشکل می‌باشد. حملاتی که منجر به تغییر در داده‌ها یا ترافیک شبکه نمی‌شوند به عنوان حمله‌های غیر فعال (Passive) دسته‌بندی می‌شوند.

برخی از این حمله‌ها به شرح زیر است:

- بو کشیدن یا استراق سمع (Sniffing/ Eavesdropping) که در آن از ابزارهای Sniffer در سطح سخت‌افزار لایه ارتباطی استفاده می‌شود.
- استراق سمع از Hub از طریق نصب نرم‌افزار Sniffer روی یکی از ماشین‌های متصل به یک Hub و دریافت ترافیک کلیه ماشین‌های متصل به آن Hub یا سایر Hub‌های متصل به آن.
- استراق سمع از سوییچ‌های ضعیف یا قدیمی یا مدیریت نشده با استفاده از مکانیزم فوق
- حمله ارسال سیل آسای بسته جهت از کار انداختن سوییچ‌ها از طریق ارسال آدرس مبدأهای تصادفی و سوءاستفاده از نیاز سوییچ‌ها به ذخیره‌سازی آدرس‌های جدید (از طریق پر کردن حافظه و تبدیل سوییچ به Hub)
- گمراه کردن ماشین‌ها با ارسال پیام‌های جعلی ARP از طریق ارسال بسته دروغین و جعلی آدرس فیزیکی نفوذگر به عنوان آدرس پیش فرض مسیریاب و دریافت ترافیک ارسالی به خارج از شبکه محلی

فریب دادن ماشین‌ها با آدرس‌های جعلی IP (جعل IP یا IP Spoofing) از طریق جعل IP حمله کننده از لایه لای فیلتر یا دیواره‌های آتش (Firewall)

ب-۱۰- حمله‌های نوع DoS برای اخلال در سرویس دهی

حمله‌های (Denial of Service) حمله‌هایی هستند که در آن‌ها نفوذگر تلاش می‌کند تا با استفاده از روش‌های عملی یا علمی مانع از سرویس دهی یک سرویس دهنده یا برقراری ارتباط با آن شود. این نوع حمله‌ها معمولاً نیاز به برنامه‌ریزی دقیق و صرف هزینه زیاد جهت به کارگیری خطوط ارتباطی با پهنای باند زیاد دارند، بنابراین معمولاً عمدی و با هدف قبلی انجام می‌شوند.

از دیدگاه فنی حمله‌های DoS به دو دسته تقسیم می‌شوند که عبارت‌اند از:

- حمله‌هایی که مستقیماً منجر به توقف سرویس‌های ماشین می‌شوند.
- حمله‌هایی که منجر به اشباع ظرفیت یک سرویس دهنده و تلف شدن منابع آن شود.

برخی از این روش‌های این نوع حمله در زیر فهرست شده اند:

- متوقف کردن سرویس دهنده از درون:
- در این حالت حمله کننده به سیستم وارد شده و با ایجاد شرایط موردنظر خود به اخلاگری می‌پردازد. در این حالت ممکن است حمله کننده از طریق حمله به کلمه عبور یا استراق سمع موفق به دسترسی به سیستم یا شناسایی پردازش‌ها یا ترافیک‌های آن شود. حمله کننده ممکن است با استفاده از روش‌های قطع پروسه (Process Killing)، تغییر پیکربندی (System Reconfiguration)، فروپاشی پروسه (Process Crashing) یا بمباران درونی (Local bombardment) اقدام به از کار انداختن ماشین تحت نفوذ نماید.
- روش دیگر حمله از درون، حمله اشباع منابع سیستم می‌باشد. در این نوع حمله، از طریق اشباع جدول پروسه سیستم عامل (Process Table)، اشباع فضای ذخیره‌سازی اطلاعات (مثل فضای اشتراکی کاربران شبکه) و ارسال ترافیک بی‌هوده از درون شبکه به بیرون جهت اشغال پهنای باند و قطع یا کندی ارتباط با سایر شبکه‌ها اقدام به اختلال در کار سیستم نماید.
- متوقف کردن سیستم از طریق حمله DoS از بیرون:
- در این نوع حمله با ارسال حجم زیادی از بسته‌های ناقص یا دارای اشکال از یک نقطه در اینترنت در کار سیستم اشکال ایجاد می‌شود. اگر سرویس دهنده هدف دارای آسیب پذیری در مقابل این نوع حمله باشد، قطعاً در هم شکسته و متوقف خواهد شد.

ب-۱۱- حمله‌های DoS از نوع تلف کردن منابع سیستم از راه دور

در این نوع حمله تمام منابع سیستم یا شبکه هدف (مثل حافظه یا پهنای باند) اشغال شده و به همین دلیل کار آن کاملاً مختل یا بسیار کند و غیر قابل تحمل می‌شود. انواع این حمله به شرح زیر است:

- حمله از نوع SYN Flood که در آن سیلابی از درخواست‌های سه مرحله‌ای برقراری ارتباط (3-Way Handshake) ناکامل به سمت میزبان ارسال می‌شود و با اجبار آن به نگهداری اطلاعات ناتمام برقراری ارتباط (ارتباطات نیمه باز و غیر فعال) فضای مجاز تخصیص یافته به نگهداری اطلاعات مربوط به برقراری ارتباط اشغال شده و از ایجاد ارتباطات بعدی جلوگیری می‌شود.

- حمله Smurf که در این نوع حمله بسته‌ای با مقصد فراگیر (Broadcast) در قالب ICMP Echo Request برای تمام ماشین‌های شبکه ارسال می‌شود با این فرض که حمله کننده آدرس ماشین قربانی را به عنوان آدرس مبدا اعلام می‌نماید. در این حالت همه ماشین‌های شبکه اقدام به ارسال بسته ICMP Echo Reply برای ماشین قربانی می‌نمایند که به صورت سیل ویرانگری پهنای باند منتهی به ماشین هدف را اشغال نموده و مانع برقراری ارتباط‌های مفید با آن می‌شوند.
- حمله Fragile این نوع حمله شبیه حمله Smurf است با این تفاوت که به جای بسته ICMP از بسته‌های UDP استفاده می‌شود.

ب-۱۲- حمله‌های توزیع شده (Distributed DoS)

در این نوع حمله، حمله کننده سعی می‌کند با استفاده از ماشین‌هایی که در سراسر اینترنت مستقر هستند به یک هدف در شبکه حمله نماید. در این نوع حمله از ماشین‌هایی به عنوان زامبی ((Zombie استفاده می‌شود. ماشین زامبی رایانه‌ای است که بدون اطلاع صاحب آن به عنوان ابزار حمله مورد سوءاستفاده قرار می‌گیرد. باید توجه کرد که معمولاً نرم‌افزارهایی که رایانه‌ها را تبدیل ماشین زامبی می‌کنند در قالب برنامه‌های رایگان، زیبا و جذاب در اختیار کاربران ناآگاه قرار داده می‌شوند.

ب-۱۳- تسلط بر شبکه از طریق اسب‌های تروا، در پستی ((Root kit و Back Door

مرحله بعدی در برنامه‌ریزی و اجرای یک حمله موفق به شبکه هدف، مستحکم سازی سرپل‌های نفوذ، گسترش نفوذ و تسلط بر شبکه می‌باشد. این کار از طریق نفوذ دادن نرم‌افزارهای آلوده مثل "اسب‌های تروا" ((Trojan Horses یا Root kit انجام می‌شود. در صورت موفقیت حمله کننده به نفوذ دادن این نوع نرم‌افزارها به شبکه هدف، وی می‌تواند از زحمت طاقت فرسای غلبه بر مکانیزم‌های کنترل دسترسی یا شکستن حریم امنیتی شبکه رهایی یابد. انتقال فایل از طریق محیط‌های گفتگوی اینترنتی ((Chat Room، ارسال و دریافت نامه‌های الکترونیکی و ضامم آن‌ها ((Email and Attachments و مراجعه به صفحات Web آلوده به کدهای اجرایی آلوده (مثل فرمان‌های Activex یا اسکریپت‌های خطرناک) راه‌های اصلی نفوذ دادن کدهای مخرب به سیستم یا شبکه‌های هدف می‌باشند.

اسب‌های تروا پس از نفوذ به سیستم به صورت پنهان در سیستم اجرا شده و با باز کردن یک پورت خاص منتظر دریافت فرمان حمله کننده باقی می‌مانند و به محض دریافت فرمان، کنترل ماشین

را در اختیار حمله کننده قرار می‌دهند. این نوع برنامه‌ها معمولاً پس از هر بار ورود کاربر به سیستم فعال می‌شوند اما هیچگونه اختلالی که باعث اطلاع کاربر از وجود آن‌ها شود ایجاد نمی‌کنند.

درهای پشتی ((Back Door به آنگونه از ضعف‌های سیستم عامل گفته می‌شود که باعث می‌شوند حمله کننده بدون نیاز به گذشتن از مکانیزم‌های امنیتی تعبیه شده در سیستم به منابع آن دست یابد. مکانیزم‌های امنیتی ممکن است بسیار پیچیده و غیر قابل نفوذ باشند و حتی از روش‌های رمزنگاری برای مبادله داده‌ها استفاده کنند اما وجود در پشتی باعث بلا اثر شدن این مکانیزم‌ها می‌شود.

Root kitها کدهای جایگزین خطرناکی هستند که جایگزین کدهای اصلی سیستم عامل شده و اصولاً منجر به تغییر خصوصیات سیستم عامل می‌شوند. اسب‌های تروا نرم‌افزارهای مخربی هستند که به سیستم نفوذ داده شده و به عنوان برنامه‌ای جدا از سیستم عامل کار می‌کنند، اما **Root kit**ها برنامه‌های مخربی هستند که جایگزین بخش‌هایی از سیستم عامل شده و کنترل کامل آن را به حمله کننده منتقل می‌کنند. برخی از عملکردهای **Root kit**ها را می‌توان به شرح زیر فهرست کرد:

- توانایی تغییر مسیر اجرا ((Execution Redirection یا اجرای برنامه‌های دیگر به جای برنامه مورد درخواست کاربر
- مخفی نگه داشتن فایل‌ها در سطح هسته جهت پنهان سازی نفوذ
- مخفی نگه داشتن پروسه‌ها در سطح هسته
- مخفی نگه داشتن ارتباطات شبکه‌ای در سطح هسته

ب-۱۴- رد گم کردن و مخفی کاری

هر چه مدت زمان تسلط حمله کننده به سیستم‌ها یا شبکه‌های هدف طولانی‌تر باشد احتمال موفقیت حمله بیشتر خواهد بود. بنابراین حمله کننده در غالب موارد به دنبال مخفی کاری و پاک کردن رد پا و آثار حضور خود در شبکه یا سیستم هدف می‌باشد. این کار از طریق روش‌های زیر امکان پذیر است:

- دستکاری و تغییر فایل‌های ثبت رخدادها (Event Logs) مثل فایل‌های **security.log** یا **system.log** که فایل‌های موقت ثبت رخدادها هستند و یا فایل‌های **secevent.evt** یا **sysevent.evt** که فایل‌های دائمی ثبت رخدادها در سیستم عامل‌های خانواده ویندوز (NT,2000) هستند.

- ایجاد فایل‌ها و شاخه‌های پنهان روی ماشین هدف به منظور ایجاد محلی امن برای پنهان سازی فایل‌های منتقل شده و نفوذ داده شده به ماشین هدف
- ایجاد کانال‌های پنهان جهت پنهان سازی ترافیک داده‌های در حال تبادل بین حمله کننده و ماشین هدف.

آنچه که در این ضمیمه ارائه شده است شرحی کلی بر آسیب پذیری‌ها و روش‌های حمله رایانه‌ای به ماشین‌ها یا شبکه‌های هدف می‌باشد. تمام ماشین‌های متصل به شبکه به طور عام و ماشین‌های متصل به اینترنت به طور خاص در مقابل تهدیدهای فوق آسیب پذیر می‌باشند. لازم است در مرحله ارزیابی ریسک به این تهدیدها نیز توجه شود و حتی الامکان به دقت پتانسیل اجرای آن‌ها علیه سیستم اطلاعاتی و دارایی‌های اطلاعاتی در اختیار سازمان بررسی و ارزیابی گردد.

عملیات ارزیابی ریسک بدون در نظر گرفتن تهدیدات و آسیب پذیری‌های فوق کامل نخواهد

بود.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک
مدیریت و مقابله با ریسک شماره دستورالعمل : ۳-۳-۳	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده است و در اختیار کمیته امنیت اطلاعات می‌باشد. کلیه اسنادی که بر اساس این سند تولید یا گردآوری می‌شوند حداقل دارای طبقه‌بندی **محرمانه** خواهند بود. تصمیم‌گیری در خصوص سطح حداکثری طبقه‌بندی حفاظتی این اسناد به عهده تهیه کننده یا گردآورنده سند می‌باشد.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل سازمان‌دهی عملیات مدیریت و مقابله با ریسک‌های شناسایی شده در مرحله ارزیابی ریسک (بر اساس دستورالعمل ۳-۳-۲) می‌باشد.

مسئولیت:

مسئولیت مدیریت و مقابله با ریسک‌های امنیتی شناخته شده برای هر دارایی اطلاعاتی یا فرآیند به عهده متصدی، تحویل گیرنده یا مالک همان دارایی اطلاعاتی یا فرآیند خواهد بود. به علاوه این مسئولیت بر اساس سلسله مراتب سازمانی به افراد بالا دست منتقل می‌شود، بنابراین مدیران یا مسئولان قسمت‌های مختلف در مقابل عملکرد افرادی که تحت مدیریت ایشان فعالیت می‌نمایند نیز مسئولیت دارند.

مسئولیت نظارت بر اجرای صحیح عملیات مدیریت و مقابله بر ریسک بر عهده واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و یا واحد جانشین آن می‌باشد.

الزامات:

لازم است کلیه ریسک‌های شناسایی شده در مرحله ریسک مورد بررسی قرار گرفته و یکی از تصمیمات زیر در خصوص آن‌ها اتخاذ شود:

الف- اجتناب از ریسک، از طریق تغییر فرآیند یا خودداری از استفاده از دارایی اطلاعاتی مربوط و یا تغییر در روش استفاده از آن به نحوی که عامل ایجاد ریسک از بین رفته و ریسک مربوط حذف گردد. به عنوان مثال می‌توان به جلوگیری از ذخیره‌سازی اطلاعات سری بر روی رسانه‌های الکترونیکی برای حذف ریسک سرقت اطلاعات با استفاده از تجهیزات پردازشی اشاره کرد.

ب- کاهش ریسک به حد قابل قبول، از طریق تغییر در فرآیند یا روش استفاده از دارایی اطلاعاتی به نحوی که مقدار ریسک مربوطه به حد قابل قبولی کاهش یابد. به عنوان مثال می‌توان به جداسازی رایانه‌های حاوی اطلاعات دارای طبقه‌بندی خیلی محرمانه از شبکه LAN سازمان برای کاهش خطر سرقت از طریق شبکه یا دستکاری آن‌ها اشاره کرد.

ج- انتقال ریسک از طریق عقد قرارداد با سایر طرف‌های تجاری برای پذیرفتن یا جبران خسارات ناشی از حوادث رایانه‌ای توسط ایشان، مانند عقد قرارداد بین بانک‌ها با شرکت‌های بیمه در

خصوص پرداخت خسارت‌های احتمالی سرقت‌های رایان‌های از حساب مشتریان توسط شرکت‌های بیمه.

د- پذیرش و پایش ریسک، از طریق پذیرش ریسک استفاده از دارایی اطلاعاتی یا فرآیند ریسک دار و تحت نظر داشتن ریسک‌های پذیرفته شده برای جلوگیری از افزایش مقدار ریسک از حد قابل قبول و تعیین شده توسط مدیریت ارشد سازمان، مانند تحت نظر داشتن گزارش وقایع امنیتی و بررسی آن‌ها برای آگاهی از روند تلاش برای دسترسی غیر مجاز به دارایی‌های اطلاعاتی سازمان از طریق اینترنت (در سازمان‌هایی که به دلیل ضرورت کاری مجبور به پذیرش ریسک موجود اتصال به اینترنت می‌باشند).

پس از تصمیم در خصوص نحوه تعامل با ریسک (شامل اجتناب، کاهش، انتقال و یا پذیرش ریسک) لازم است نحوه تعامل با ریسک به تفکیک هر نوع از ریسک‌های شناسایی شده مستند شده و به صورت گزارشی مکتوب برای اطلاع کمیته امنیت اطلاعات ارسال شود.

- در خصوص ریسک‌های پذیرش شده (اعم از ریسک‌های کاهش یافته به حد قابل قبول و یا پذیرفته شده) لازم است رویه‌های مستند در خصوص چگونگی کنترل آن‌ها نوشته شود. این رویه‌ها باید در راستای مکانیزم‌های کنترلی بیانیه کاربردپذیری (SOA) اختصاصی (موضوع دستورالعمل ۳-۳) سازمان نوشته شوند.

در رویه‌های کنترلی باید به موارد زیر اشاره شود:

الف: چه چیزی تحت حفاظت قرار گیرد.

ب: در مقابل چه چیزی حفاظت انجام شود.

ج: حفاظت چگونه انجام شود.

د: برای حفاظت به چه ابزار و روشی نیاز است.

- لازم است رویه‌های کنترلی به تفکیک دو نوع رویه‌های حفاظت از فرآیندها و رویه‌های حفاظت از دارایی‌های اطلاعاتی تهیه و تدوین شوند.

اولویت تدوین رویه‌های کنترلی بر اساس شاخص اهمیت فرآیند و یا شاخص ریسک جغرافیایی تعیین می‌شود. به این معنی که فرآیندها یا مکان‌های استقرار که دارای اهمیت یا ریسک زیادتری برای سازمان هستند باید در اولویت حفاظت قرار گیرند.

فرآیند مدیریت ریسک

تحلیل ریسک به عنوان اساس و بنیان مدیریت ریسک محسوب می‌شود. لازم است پس از شناسایی و تشریح ریسک به اداره آن پرداخت، می‌توان از ریسک جلوگیری کرد، آن را منتقل نمود، آن را کاهش داد یا آن را پذیرفت. نحوه تصمیم‌گیری به چگونگی روش ارزیابی دارایی و احتمال از دست رفتن آن در مقابل هزینه حفاظت از آن دارایی، بستگی دارد. هنگام انتخاب روش حفاظتی و توجه به جنبه‌های هزینه‌ای آن، بهتر است در مورد قسمت‌هایی از سازمان که لازم است در اولین فرصت تحت حفاظت قرار گیرند نیز بررسی کامل به عمل آید. ممکن است اجرای حفاظت کامل از کلیه دارایی‌هایی اطلاعاتی هزینه بسیار زیادی را به همراه داشته باشد و امکان پذیر نباشد. بنابراین می‌توان براساس فهرست‌های تهیه شده در مرحله ارزیابی ریسک، دارایی‌های بحرانی را تعیین کرده و فعالیت‌های اضطراری را به مورد اجرا گذاشت. پس از انتخاب محل شروع و ترتیب فعالیت‌ها، نوبت به اجرای روش‌های حفاظتی می‌رسد. روش‌های مختلفی وجود دارد. براساس استانداردهای ISO روش‌های زیر قابل اجرا می‌باشند.

- درک وضعیت
- شناسایی ریسک
- ترمیم رخنه
- پیشگیری از نفوذ یا ضربه
- محدودسازی اثر حمله / حادثه
- تصحیح وضعیت
- بازیابی / احیاء سیستم
- دیده بانی

بعضی اوقات می‌توان از روش‌هایی استفاده کرد که می‌تواند فقط "تولید/حساس/امنیت" کند. مثلاً گذاشتن نگهبان‌های قوی هیکل در قسمت ورودی ساختمان به منظور درگیر شدن با افراد نیست، بلکه فقط ظاهر ایشان از ورود بی‌مورد افراد به ساختمان جلوگیری می‌کند. بسته به نوع دارایی‌ها و ارزش ذاتی هر یک، روش‌های مختلفی قابل اجرا است. مکانیزم‌های حفاظتی می‌توانند سازمانی یا تکنیکی باشند. استفاده از هر روش به انتخاب مدیران اجرایی یا تصمیم‌سازان دیگر بستگی دارد.

با توجه به رشد روز افزون فن آوری‌های موجود در حمله و دفاع نمی‌توان در این زمینه نسخه‌ای دائمی پیشنهاد کرد و بسته به موقعیت باید از آخرین فن آوری ممکن استفاده نمود. مثلاً مکانیزم‌های کنترل دسترسی قدیمی براساس استفاده از شناسه کاربر به عنوان کلید ورود به سیستم و کلمه عبور به عنوان تصدیق کننده هویت کاربر طراحی شده‌اند. می‌توان این مکانیزم‌ها را با استفاده از سایر روش‌های نوین مانند استفاده از توکن‌های سخت‌افزاری و یا سنجش پارامترهای حیاتی (اثر انگشت، ساختار مردمک چشم) تقویت کرد.

طی مدیریت ریسک می‌توان ارزش دارایی‌ها را بهتر درک کرده و محیط‌های نا امن را آشکار و راه حل‌هایی برای غلبه بر نقاط ضعف پیش بینی نمود. مرحله بعدی فرآیند امنیت بخشی به سیستم اطلاعاتی برنامه‌ریزی هدف است که بنابراین لازم است همه چیز طبق برنامه و به نحوی عمل شود که دسترسی به محدوده‌های امن به عنوان اصلی ترین هدف انتخاب شود. طبق این هدف لازم است مکانیزم‌هایی طراحی شود که براساس آن از درست کارکردن همه چیز در حد کفایت، اطمینان حاصل نمود.

جدول مدیریت کیفی ریسک

استفاده از جداول و دسته‌بندی کیفی تهدیدها درک بهتر وضعیت و تصمیم‌گیری در مورد انتخاب مکانیزم‌های امنیتی را تسهیل می‌نماید. تهدیدهای مختلف را میتوان به شکل زیر دسته‌بندی کرد:

دسته ۱: تهدیداتی که باعث مرگ انسان‌ها یا تخریب شدید اطلاعات حیاتی، فروپاشی سیستم یا صدمات جبران ناپذیر به محیط زیست می‌شوند.

دسته ۲: تهدیداتی که باعث جراحات بدنی یا تخریب اطلاعات، بیماری‌های همه گیر یا صدمه زیاد به محیط زیست می‌شوند.

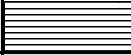
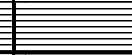
دسته ۳: تهدیداتی که باعث ضرب و جرح، بیماری همه گیر یا لطمه به سیستم یا محیط زیست می‌شوند.

از طرف دیگر دسته‌بندی امکان وقوع تهدیدها به شکل زیر نیز سودمند خواهد بود:

- دسته A: مکرر - حوادثی که احتمال وقوع آنها زیاد است.
- دسته B: محتمل - حوادثی که امکان وقوع آنها وجود دارد.
- دسته C: استثنایی - حوادثی که ممکن است در مواقع خاص بروز کنند.

- دسته **D**: به ندرت- حوادثی که احتمال وقوع آن‌ها وجود ندارد.
- دسته **E**: غیر محتمل- حوادثی که عملاً امکان وقوع آن‌ها وجود ندارد.

بنابر این می‌توان جدول ارزیابی کیفی ریسک زیر را تشکیل داد:

جدول ارزیابی کیفی ریسک					
احتمال وقوع					
E (غیر محتمل)	D (به ندرت)	C (استثنایی)	B (محتمل)	A (مکرر)	
					شدت تهدید بسیار زیاد
					شدت تهدید زیاد
					شدت تهدید متوسط
					شدت تهدید کم

	ریسک نوع ۱ (غیر قابل پذیرش و لازم است فوراً اقدامات تصحیحی انجام پذیرد)
	ریسک نوع ۲ (غیر قابل پذیرش و لازم است اقدامات تصحیحی با کسب اجازه از مدیریت صورت پذیرد)
	ریسک نوع ۳ (تحت نظارت مدیریت قابل پذیرش است)
	ریسک نوع ۴ (قابل پذیرش)

مرجع

این دستورالعمل به شماره □-□ / □-□-□ / □-□ ثبت شده است و سایر دستورالعمل‌های مرتبط

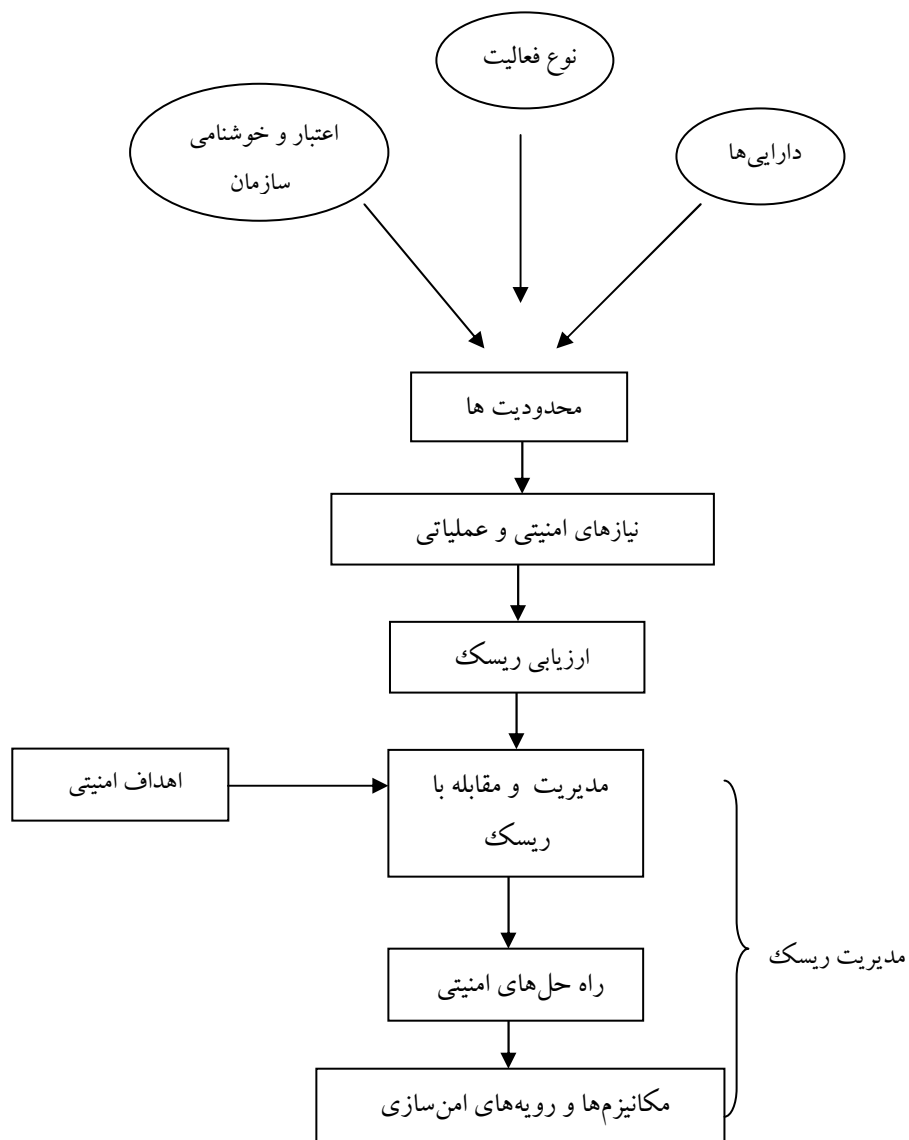
با آن عبارت‌اند از:

دستورالعمل ۲-۳-۳

دستورالعمل ۴-۳-۳

روند نما

روند نمای مدیریت و مقابله با ریسک در نمودار زیر نشان داده شده است.



(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	شناخت سیستم و تحلیل ریسک
بیانیه کاربردپذیری (SOA) اختصاصی شماره دستورالعمل: ۴-۳-۳	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع:

این سند به عنوان سند محرمانه طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات می‌باشد. دسترسی به این سند فقط پس از موافقت کتبی کمیته امنیت اطلاعات امکانپذیر می‌باشد.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات:

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل تبیین ضرورت و چگونگی تنظیم بیانیه کاربردپذیری (SOA^{۲۳}) اختصاصی ((وزارت/ سازمان/ اداره کل/ شرکت /...)) می‌باشد.

توضیح: بیانیه کاربردپذیری اختصاصی عبارت است از فهرست آن دسته از مکانیزم‌های کنترلی لازم از بین فهرست عام مکانیزم‌های کنترلی ارائه شده توسط استاندارد مرجع که قرار است در ((وزارت/ سازمان/ اداره کل/ شرکت /...)) به کار گرفته شوند تا نیل به اهداف پیاده‌سازی نظام امنیت اطلاعات امکانپذیر گردد.

مسئولیت:

مسئولیت تدوین بیانیه کاربردپذیری (انتخاب مکانیزم‌های کنترلی قابل اجرا در ((وزارت/ سازمان/ اداره کل/ شرکت /...)) از بین مکانیزم‌های عام ارائه شده توسط استاندارد مرجع) به عهده کمیته امنیت اطلاعات می‌باشد.

الزامات:

لازم است تک تک بندهای فهرست مکانیزم‌های کنترلی عام ارائه شده توسط استاندارد مرجع توسط کمیته امنیت اطلاعات بررسی شده و آن دسته از مکانیزم‌های کنترلی که لازم است در سازمان به کار گرفته شوند استخراج شده و در فهرست جداگان‌های تحت عنوان بیانیه کاربردپذیری اختصاصی ((وزارت/ سازمان/ اداره کل/ شرکت /...)) تدوین شده و به تصویب کمیته امنیت اطلاعات سازمان برسد. (فهرست مکانیزم‌های کنترلی عام ارائه شده توسط استاندارد ISO-27001 در ضمیمه همین دستورالعمل ارائه شده است).

- لازم است به ازای هر بند از بیانیه کاربردپذیری اختصاصی سازمان که توسط کمیته امنیت اطلاعات تصویب شده است، دستورالعمل‌ها و رویه‌های جداگانه (برحسب نیاز به دستورالعمل یا رویه) برای نیل به اهداف آن بند تنظیم، تدوین، ابلاغ و اجرا شود.
- لازم است در بیانیه کاربردپذیری در مقابل هر بند از مکانیزم‌های کنترلی به نام و شماره مرجع دستورالعمل‌ها و یا رویه‌های مربوط به پیاده‌سازی آن مکانیزم اشاره شود.

²³ Statement of Applicability

- لازم است واحد امنیت اطلاعات یا نهاد جانشین آن، به صورت سالیانه گزارشی از چگونگی و روند اجرای دستورالعمل‌ها یا رویه‌های مرتبط با هر بند از بیانیه کاربرپذیری را به تفکیک هر بند، به اطلاع کمیته امنیت اطلاعات برساند. (دوره گزارش دهی با نظر کمیته امنیت اطلاعات قابل تغییر می‌باشد).

فرآیند

پس از انجام مرحله ارزیابی ریسک و تعیین روش‌های مدیریت ریسک امنیت اطلاعات، فهرستی از فعالیت‌های قابل اجرا برای دستیابی به سطح امنیت مورد نظر سازمان تهیه خواهد شد. این فهرست مبین روش‌های مقابله با ریسک‌های پیش روی سازمان در حوزه امنیت اطلاعات و چگونگی اجرای آن‌ها می‌باشد. برای دسته‌بندی بهتر این روش‌ها و فراهم ساختن امکان و سهولت ممیزی‌های بعدی، تهیه فهرستی خلاصه که در آن کلیه مکانیزم‌های کنترلی در حوزه امنیت اطلاعات مورد مذاقه قرار گرفته‌اند ضروری است.

استانداردهای مختلف که در حوزه‌های مدیریتی یا اجرایی تدوین شده‌اند به همراه خود روش‌های مختلفی را برای کارا تر کردن روش‌های ارزیابی و ممیزی نیل به هدف استاندارد یا ممیزی فعالیت‌ها را معرفی می‌نمایند.

در خصوص استاندارد مدیریت امنیت اطلاعات می‌توان به استاندارد **ISO-27001** اشاره کرد که فهرستی از مکانیزم‌های کنترلی (شامل ۱۳۳ روش کنترلی) را به عنوان مکانیزم‌های کنترلی پایه، معرفی می‌نماید. فهرست این مکانیزم‌ها در ضمیمه همین دستورالعمل درج شده است. از این فهرست می‌توان برای از قلم نیافتادن مکانیزم‌های کنترلی در مرحله انتخاب روش‌های کنترلی استفاده کرد. این فهرست حاوی کلیه جنبه‌های مطرح در حوزه امنیت اطلاعات می‌باشد و می‌توان اطمینان داشت با به کارگیری مکانیزم‌های کنترلی مندرج در آن دستیابی به اهداف امنیت اطلاعات امکانپذیر خواهد بود.

برای دستیابی به بیانیه کاربرپذیری اختصاصی سازمان باید با توجه به نتایج حاصل از مرحله ارزیابی ریسک و روش‌های انتخاب شده بر اساس دستورالعمل مدیریت و مقابله ریسک به فهرست عام مکانیزم‌های کنترلی مراجعه کرده و با مطالعه هر یک از مکانیزم‌های کنترلی مندرج در آن به انتخاب مکانیزم کنترلی مرتبط با فعالیت سازمان پرداخت و فهرست جدیدی از آن که طبقاً زیر مجموعه‌ای از مکانیزم‌های کنترلی عام می‌باشد انتخاب و به عنوان بیانیه کاربرپذیری اختصاصی

سازمان به کار گرفت. (به عنوان مثال ممکن است با توجه به نظر کمیته امنیت اطلاعات از بین ۱۳۳ مکانیزم کنترلی فقط به کارگیری ۱۲۵ یا هر تعداد دیگر از مکانیزم‌ها کافی باشد) تدوین بیانیه کاربردپذیری اختصاصی یکی از مراحل شاخص در پیاده‌سازی سامانه مدیریت امنیت اطلاعات می‌باشد.

می‌توان گفت که با تدوین بیانیه کاربردپذیری راه برای شروع فعالیت‌های مؤثر در زمینه برقراری و حفاظت از امنیت اطلاعات باز می‌شود.

البته می‌توان بدون داشتن این بیانیه نیز به فعالیت‌های امن‌سازی پرداخت، اما باید توجه داشت که در این حالت نمی‌توان تداوم و کارایی این فعالیت‌ها را تضمین نمود.

پس از تدوین بیانیه کاربردپذیری لازم است دستورالعمل‌ها و رویه‌های اجرایی برای پیاده‌سازی مکانیزم‌های کنترلی انتخاب شده را بر اساس اولویت‌های سازمانی آماده و جهت ابلاغ به واحدهای سازمان ارسال نمود. این کار را می‌توان به تدریج و بر اساس بودجه بندی و برنامه‌ریزی مناسب و با توجه به محدودیت‌های سازمان به انجام رساند.

توجه شود که ممکن است بر اساس نتایج حاصل از ارزیابی ریسک و یا طبق سیاست‌گذاری‌های سازمان، اجرای برخی از مکانیزم‌های کنترلی عام ضروری تشخیص داده نشده و آن مکانیزم از فهرست مکانیزم‌های مندرج در بیانیه کاربردپذیری اختصاصی حذف شود. (به عبارت دیگر ممکن است تعداد مکانیزم‌های موجود در بیانیه کاربردپذیری کمتر از ۱۳۳ مکانیزم باشد). این کار بلامانع است اما تصویب کننده بیانیه کاربردپذیری اختصاصی سازمان باید توجیهات لازم و کافی را در خصوص این کار داشته باشد و در هنگام ممیزی آن را در اختیار ممیزان قرار دهد. اصولاً فعالیت‌های ممیزی بر اساس بیانیه کاربردپذیری اختصاصی انجام می‌شود و در صورت عدم ارائه توجیهات کافی در خصوص حذف برخی از مکانیزم‌ها و یا روش‌های اجرایی انتخاب شده برای حفاظت از امنیت دارایی‌های اطلاعاتی، ممکن است از صدور گواهینامه استاندارد خودداری شود.

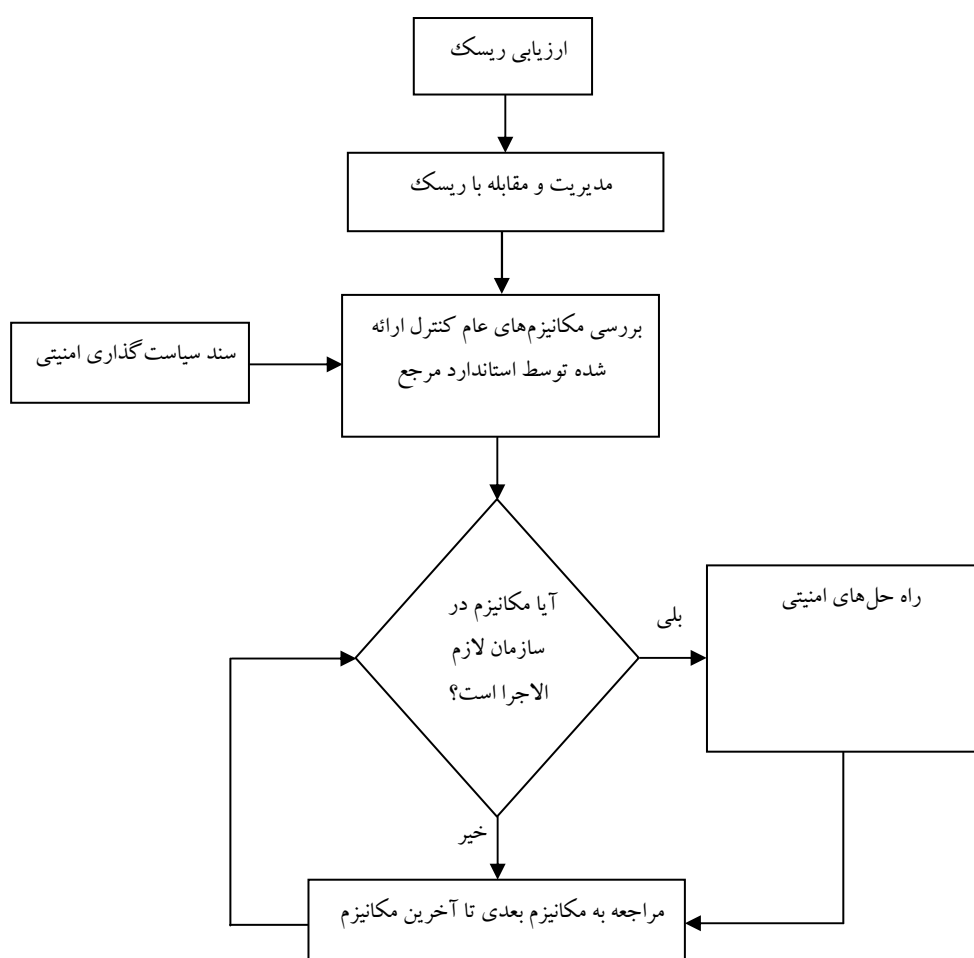
مرجع

این دستورالعمل به شماره □-□/□-۳-۴/□-□ ثبت شده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۱
- دستورالعمل ۲-۳-۳
- دستورالعمل ۳-۳-۳

روند نما

روند نمای تدوین بیانیه کاربردپذیری در نمودار زیر نشان داده شده است.



ضمیمه یک- بیانیه کاربردپذیری

توجه:

- ۱- در صورت نیاز به اجرای هریک از مکانیزم‌های کنترلی، در ستون کاربردپذیری عبارت بلی و در غیر اینصورت عبارت خیر درج شود.
- ۲- لازم است برای کلیه مکانیزم‌های کنترلی لازم الاجرا (کاربردپذیر) که با عبارت بلی در ستون کاربردپذیری مشخص شده اند، در ستون شماره مرجع شماره دستورالعمل یا رویه‌های امن سازی مربوط درج گردد.
- ۳- بیانیه کاربردپذیری اختصاصی سازمان متشکل از کلیه مکانیزم‌های کنترلی از بین مکانیزم‌های جدول زیر خواهد بود که در ستون کاربردپذیری آن‌ها عبارت بلی درج شود.

شماره مرجع	کاربردپذیری (بلی / خیر)	مکانیزم کنترلی	اهداف کنترلی
			Security policy
		A.5.1.1 Information security policy document	Information security Policy
		A.5.1.2 Review of the information Security policy.	
			Organization of information security
		A.6.1.1 Management commitment To information security	Internal organization
		A.6.1.2 Information security Co-ordination	
		A.6.1.3 Allocation of information security responsibilities	
		A.6.1.4 Authorization process for information processing facilities	
		A.6.1.5 Confidentiality agreements	
		A.6.1.6 Contact with authorities	

اهداف کنترلی	مکانیزم کنترلی	کاربردپذیری (پلی / خیر)	شماره مرجع
	A.6.1.7 Contact with specialist Interest groups		
	A.6.1.8 Independent review of information security		
External parties	A.6.2.1 Identification of risks related to external parties		
	A.6.2.2 Addressing security when Dealing with customers		
	A.6.2.3 Addressing security in Third party contracts		
Asset management			
Responsibility of assets	A.7.1.1 Inventory of assets		
	A.7.1.2 Ownership of assets		
	A.7.1.3. Acceptable use of assets		
Information Classification	A.7.2.1 Classification guidelines		
	A.7.2.2 Information labeling and handling		
Human resource security			
Prior to employment	A.8.1.1 Roles and responsibilities		
	A.8.1.2 Screening		
	A.8.1.3 Terms and conditions of employment		
During employment	A.8.2.1 Management responsibilities		
	A.8.2.2 Information security awareness, education and training		
	A.8.2.3 Disciplinary process		
Termination or change of	A.8.3.1 Termination		

اهداف کنترلی	مکانیزم کنترلی	کاربردپذیری (بلی / خیر)	شماره مرجع
employment	responsibilities		
	A.8.3.2 Return of assets		
	A.8.3.3 Removal of asset rights		
Physical and environmental security			
Secure areas	A.9.1.1 Physical Security perimeter		
	A.9.1.2 Physical entry controls		
	A.9.1.3 securing offices, rooms and facilities		
	A.9.1.4 Protecting against external and environmental threats		
	A.9.1.5 Working in secure areas		
	A.9.1.6 Public access, delivery and loading areas		
Equipment security	A.9.2.1 Equipment sitting and protection		
	A.9.2.2 Supporting utilities		
	A.9.2.3 Cabling security		
	A.9.2.4 Equipment maintenance		
	A.9.2.5 Security of equipment off-premises		
	A.9.2.6 Secure disposal or re-use of equipment		
	A.9.2.7 Removal of property		
Communications and operations management			
Operational procedures and responsibilities	A.10.1.1 Documented operating procedures		

اهداف کنترلی	مکانیزم کنترلی	کاربردپذیری (پلی / خیر)	شماره مرجع
	A.10.1.2 Change management		
	A.10.1.3 Segregation of duties		
	A.10.1.4 Separation of development, test and operational facilities		
Third party service delivery management	A.10.2.1 service delivery		
	A.10.2.2 Monitoring and review of third party services		
	A.10.2.3 Managing changes to third party services		
System planning and acceptance	A.10.3.1 Capacity management		
	A.10.3.2 System acceptance		
Protection against malicious and mobile codes	A.10.4.1 Controls against malicious code		
	A.10.4.2 Controls against mobile code		
Back-up	A.10.5.1 Information Back-up		
Network security management	A.10.6.1 Network controls		
	A.10.6.2 security of network services		
Media handling	A.10.7.1 Management of removable media		
	A.10.7.2 Disposal of media		
	A.10.7.3 Information handling procedures		
	A.10.7.4 Security of system documentation		
Exchange of Information	A.10.8.1 Information exchange policies and procedures		

اهداف کنترلی	مکانیزم کنترلی	کاربردپذیری (بلی / خیر)	شماره مرجع
	A.10.8.2 Exchange agreements		
	A.10.8.3 Physical media in transit		
	A.10.8.4 Security of electronic office systems		
	A.10.8.5 Business information systems		
Electronic commerce services	A.10.9.1 Electronic commerce		
	A.10.9.2 On-line transactions		
	A.10.9.3 Publicly available information		
Monitoring	A.10.10.1 Audit logging		
	A.10.10.2 Monitoring system use		
	A.10.10.3 Protection of log Information		
	A.10.10.4 Administrator and operator logs		
	A.10.10.5 Fault logging		
	A.10.10.6 Clock synchronization		
Access control			
Business requirement for access control	A.11.1.1 access control policy		
User access management	A.11.2.1 User registration		
	A.11.2.2 Privilege management		
	A.11.2.3 User password management		
	A.11.2.4 Review of user access rights		
User responsibilities	A.11.3.1 Password use		

اهداف کنترلی	مکانیزم کنترلی	کاربردپذیری (پلی / خیر)	شماره مرجع
	A.11.3.2 Unattended user equipment		
	A.11.3.3 Clear desk and clear screen policy		
Network access control	A.11.4.1 Policy on use of network services		
	A.11.4.2 User authentication for external connections		
	A.11.4.3 Equipment identification in networks		
	A.11.4.4 Remote diagnostic and configuration port protection		
	A.11.4.5 Segregation in networks		
	A.11.4.6 Network connection control		
	A.11.4.7 Network routing control		
Operating system access control	A.11.5.1 Secure log-on procedures		
	A.11.5.2 User identification and authentication		
	A.11.5.3 Password management system		
	A.11.5.4 Use of system utilities		
	A.11.5.5 Session time-out		
	A.11.5.6 Limitation of connection time		
Application and information access control	A.11.6.1 Information access restriction		
	A.11.6.2 Sensitive system isolation		
Mobile computing and teleworking	A.11.7.1 Mobile computing and communications		

اهداف کنترلی	مکانیزم کنترلی	کاربردپذیری (بلی / خیر)	شماره مرجع
	A.11.7.2 Teleworking		
Information systems acquisitions, development and maintenance			
Security requirements of information systems	A.12.1.1 Security requirements analysis and specification		
Correct processing in applications	A.12.2.1 Input data validation		
	A.12.2.2 Control of internal processing		
	A.12.2.3 Message integrity		
	A.12.2.4 Output data validation		
Cryptographic controls	A.12.3.1 Policy on the use of cryptographic controls		
	A.12.3.2 Key management		
Security of system files	A.12.4.1 Control of Operational software		
	A.12.4.2 Protection of system test data		
	A.12.4.3 Access control to source code		
Security in development and support processes	A.12.5.1 Chang control procedures		
	A.12.5.2 Technical review of applications after operating system changes		
	A.12.5.3 Restrictions on changes to software packages		
	A.12.5.4 Information leakage		
	A.12.5.5 Outsourced software development		

اهداف کنترلی	مکانیزم کنترلی	کاربردپذیری (پلی / خیر)	شماره مرجع
Technical vulnerability management	A.12.6.1 Control of technical vulnerabilities		
Information security incident management			
Reporting information security events and weaknesses	A.13.1.1 Reporting security events		
	A.13.1.2 Reporting security weaknesses		
Management of information security incidents and improvements	A.13.2.1 Responsibilities and procedures		
	A.13.2.2 Learning from information security incidents		
	A.13.2.3 Collection of evidence		
Business continuity management			
Information security aspects of business continuity management	A.14.1.1 Including information security in the business continuity management process		
	A.14.1.2 Business continuity and risk assessment		
	A.14.1.3 Developing and implementing continuity plans		
	A.14.1.4 Business continuity and planning framework		
	A.14.1.5 Testing, maintaining and re-assessing business continuity plans		
Compliance			
Compliance with legal requirements	A.15.1.1 Identification of applicable legislation		
	A.15.1.2 Intellectual property rights (IPR)		

اهداف کنترلی	مکانیزم کنترلی	کاربردپذیری (بلی / خیر)	شماره مرجع
	A.15.1.3 Protection of organizational records		
	A.15.1.4 Data protection and privacy of personal information		
	A.15.1.5 Prevention of misuse of information processing facilities		
	A.15.1.6 Regulation of cryptographic controls		
Compliance with security policies and standards, and technical compliance	A.15.2.1 Compliance with security policies and standards		
	A.15.2.2 Technical compliance checking		
Information system audit considerations	A.15.3.1 Information system audit controls		
	A.15.3.2 Protection of information system audit tools		

۳-۴- کنترل دسترسی

این بخش شامل دستورالعمل‌های زیر می‌باشد:

۷- مدیریت دارایی‌های اطلاعاتی		
۱-۷	الزامات حوزه فعالیت در کنترل دسترسی	
۱-۱-۷	سیاست‌گذاری کنترل دسترسی	
۲-۷	مدیریت دسترسی کاربران	
۱-۲-۷	ثبت کاربر	
۲-۲-۷	مدیریت دسترسی‌های ممتاز	
۳-۲-۷	مدیریت کلمه عبور کاربر	
۴-۲-۷	بازنگری حقوق دسترسی کاربران	
۳-۷	مسئولیت پذیری کاربران	
۱-۳-۷	استفاده از کلمه عبور	
۲-۳-۷	تجهیزات کاربری بدون مراقب	
۳-۳-۷	روش مانیتور پاک و میز پاکیزه	
۴-۷	کنترل دسترسی شبکه	
۱-۴-۷	سیاست‌گذاری در استفاده از سرویس‌های شبکه	
۲-۴-۷	احراز صلاحیت کاربر برای اتصال به شبکه‌های خارج از سازمان	
۳-۴-۷	شناسایی تجهیزات در شبکه	
۴-۴-۷	حفاظت از سرویس‌های رفع اشکال از راه دور و پیکربندی درگاه‌ها	
۵-۴-۷	جداسازی شبکه‌ها	
۶-۴-۷	کنترل اتصال‌های شبکه	
۷-۴-۷	کنترل مسیریابی شبکه	
۵-۷	کنترل دسترسی سیستم عامل	
۱-۵-۷	رویه‌های امن آغاز به کار	
۲-۵-۷	شناسایی و احراز صلاحیت (تائید اعتبار) کاربر	

۲- مدیریت دارایی‌های اطلاعاتی		
سیستم مدیریت کلمه عبور		۳-۵-۷
استفاده از ابزارهای سیستم		۴-۵-۷
محدودیت مدت نشست		۵-۵-۷
محدودیت زمان اتصال		۶-۵-۷
کنترل دسترسی برنامه‌های کاربردی و داده‌ها		۶-۷
محدودسازی دسترسی به اطلاعات		۱-۶-۷
جداسازی سامانه (سیستم)های حساس		۲-۶-۷
پردازش همراه و کار از راه دور		۷-۷
پردازش همراه و مخابرات سیار		۱-۷-۷
کار از راه دور		۲-۷-۷

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	الزامات حوزه فعالیت کنترل دسترسی
سیاست‌گذاری کنترل دسترسی شماره دستورالعمل : ۱-۱-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود. کلیه دستورالعمل‌ها و اسناد تهیه شده بر اساس این دستورالعمل حداقل دارای طبقه‌بندی حفاظتی محرمانه خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	دبیر*
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل تبیین و تدوین سیاست‌گذاری کنترل دسترسی منطقی به دارایی‌های اطلاعاتی در اختیار ((وزارت/ سازمان/ اداره کل/ شرکت...)) می‌باشد که در قلمرو پیاده‌سازی سامانه مدیریت امنیت اطلاعات (موضوع دستورالعمل ۱-۱-۳) قرار گرفته‌اند.

مسئولیت:

مسئولیت اجرای این سیاست‌گذاری در خصوص هر یک از دارایی‌های اطلاعاتی، به عهده متصدی یا مالک یا تحویل گیرنده همان دارایی اطلاعاتی می‌باشد. به علاوه این مسئولیت بر اساس سلسله مراتب سازمانی به مسئولین رده بالاتر انتقال می‌یابد.

مسئولیت نظارت بر اجرای این سیاست‌گذاری به عهده واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و یا نهاد جایگزین آن می‌باشد.

الزامات:

- کلیه کارمندان (اعم از رسمی، قراردادی، پیمانکاران، نیروهای خدماتی) و یا سایر افرادی که ضروری است به تعامل با دارایی‌های اطلاعاتی در اختیار ((وزارت/ سازمان/ اداره کل/ شرکت...)) پردازند ملزم به رعایت مفاد این دستورالعمل و پیوست‌های آن می‌باشند.
- در صورت صدور هر گونه قانون، مقررات یا دستورالعمل سازمانی مربوط به حفاظت از اطلاعات یا نحوه دسترسی پذیری به آن لازم است بلافاصله این دستورالعمل بر اساس قانون، مقررات یا دستورالعمل جدید، به هنگام سازی شود.
- صدور اجازه دسترسی به هر متقاضی دسترسی به دارایی‌های اطلاعاتی فقط پس از احراز هویت و صلاحیت متقاضی مجاز خواهد بود.
- در طراحی روش احراز هویت لازم است به عوامل زیر توجه شود:
 - طبقه‌بندی حفاظتی اطلاعات مورد درخواست
 - امکان اعمال مدیریت متمرکز کنترل دسترسی
 - طراحی فرآیند پردازش درخواست دسترسی متناسب با طبقه‌بندی حفاظتی اطلاعات مورد درخواست

- لازم است شناسه‌های کاربری اختصاص داده شده بر اساس موارد زیر تحت کنترل قرار داشته باشند:

- برای هر کاربر شناسه کاربری (User ID) مجزا تخصیص داده شود.
- استفاده اشتراکی از شناسه کاربری یا تخصیص یک شناسه کاربری به چند نفر ممنوع می‌باشد.
- به هر کاربر فقط حق دسترسی به دارایی‌های اطلاعاتی یا اطلاعاتی داده شود که برای انجام کار خود به آن نیاز دارد. دادن حق دسترسی به سایر اطلاعات یا دارایی‌های اطلاعاتی ممنوع است.
- لازم است از Screen Saver برای قفل کردن خودکار صفحه نمایشگر استفاده شود.
- دسترسی کاربران به دارایی‌های اطلاعاتی فقط در ساعات کار رسمی اداری مجاز و در غیر این ساعات ممنوع است، مگر آنکه مجوز کتبی آن قبلاً صادر شده باشد.
- لازم است شناسه‌های کاربری بدون استفاده یا متروک از سیستم حذف شود.
- استفاده از شناسه‌های کاربری عمومی (مثل شناسه‌های کاربری مورد استفاده در اتصال به اینترنت که در مکان‌های عمومی مورد استفاده واقع می‌شود) فقط پس از اثبات دلیل نیاز به استفاده از آن و کسب مجوز کتبی از مقام مسؤول مجاز است.
- در صورت استفاده از شناسه‌های کاربری عمومی لازم است فهرست گیری (Log) از فعالیت‌های انجام شده به نحوی باشد که حتی الامکان در صورت نیاز بتوان به فردی که از آن شناسه استفاده کرده است دست یافت.
- در خصوص استفاده از کلمه‌های عبور باید به نکات زیر توجه شود:
 - کلمه‌های عبور باید به صورت منظم تعویض گردد.
 - کلمه‌های عبور باید به حد کافی مستحکم و پیچیده باشند.
 - استفاده از کلمه عبور مشترک ممنوع است.
 - کلمه‌های عبور مدیریتی (Admin Password) باید به صورت امن نگهداری شوند.
 - کلمه‌های عبور مدیریتی (Admin Password) باید به صورت رمزنگاری شده ذخیره‌سازی شوند.

- لازم است هر کاربر پس از دریافت کلمه عبور خود که توسط مدیر سیستم تعیین شده است فوراً نسبت به تعویض آن اقدام نماید.
- در سازمان‌ها، نهادها یا مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حساس شناسایی شده‌اند، لازم است علاوه بر روش کلمه عبور از روش استفاده از توکن‌های سخت‌افزاری (مثل USB Token و یا Smart Card) استفاده شود.
- در سازمان‌ها، نهادها یا مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حیاتی شناسایی شده‌اند لازم است علاوه بر روش‌های فوق از روش‌های کنترل دسترسی بیومتریک استفاده شود. هنگام استفاده از این روش کنترل دسترسی باید به استحکام روش احراز هویت از طریق شناسایی اثر انگشت (Finger Print)، شناسایی الگوی چهره یا چشم (Facial/Eye Pattern) یا الگوی صدا (Voice Pattern) توجه شود.
- هنگام دسترسی به اطلاعات یا دارایی‌های اطلاعاتی با طبقه‌بندی حفاظتی سری یا بالاتر لازم است از روش احراز صلاحیت دو مرحله‌ای (تائید صلاحیت دسترسی از طرف مقام بالاتر و یا دسترسی به اطلاعات با حضور مسؤول هم رده) استفاده شود.
- لازم است در طراحی روش کنترل دسترسی به عوامل زیر نیز توجه شود:
 - اعمال کنترل‌های اضافی صدور مجوز دسترسی برای افراد ثالث یا اشخاصی که دارای رابطه استخدامی با سازمان نمی‌باشند.
 - مکان استقرار دارایی اطلاعاتی یا مکان دسترسی (دسترسی راه دور یا خارج از محیط سازمان)
 - تشکیل و مدیریت فهرست کنترل دسترسی (Access Control List) یا به عبارت ساده‌تر ACL
 - اعطای دسترسی بر اساس مسؤولیت/ پاسخگویی
 - تعریف دسترسی بر اساس مدل فایل/ دایرکتوری
 - روش ممیزی/ فهرست‌گیری از فعالیت‌ها (Auditing/Logging)
- لازم است کاربرها به دسته‌های زیر تقسیم‌بندی شده و در صورت وجود هر یک از دسته‌ها نسبت به تدوین روش اعطای دسترسی به هر یک تصمیم‌گیری شود:
 - کاربران متقاضی دسترسی ممتاز (Privilege Access)

- کاربران عادی
- بازدید کنندگان
- شرکای تجاری یا همکاران دولتی
- تهیه کنندگان / ارائه کنندگان خدمات / پیمانکاران / کارمندان موقت
- لازم است در دسترسی به شبکه به نکات زیر توجه شود:
 - استفاده از **Active Directory** و یا روش‌های مشابه آن برای احراز هویت / صلاحیت کاربران الزامی است.
 - لازم است جهت کنترل دسترسی به **Port** های **TCP/IP** از **Firewall** استفاده شود.
 - لازم است برای جلوگیری از دسترسی به اطلاعات محدود شده از روش **Packet Filtering** استفاده شود.
 - لازم است برای کنترل دسترسی به برخی از سرویس‌های شبکه مثل **Video Conference** یا **VoIP** یا.... از روش محدودسازی استفاده از پروتکل **(Restricted Use of Protocols)** استفاده شود.
 - دسترسی به سخت‌افزارهای شبکه بر اساس مدل **AAA** (که در ادامه مطالب شرح داده شده است) تحت کنترل قرار گیرد.
- دسترسی به برنامه‌های کاربردی باید بر اساس مدل دسترسی سه سطحی کنترل دسترسی عام، کنترل دسترسی خاص و کنترل دسترسی ممتاز به شرح زیر مدیریت شود: (انتخاب و پیشنهاد نوع مکانیزم یا مکانیزم‌های کنترل دسترسی در هر سطح به عهده واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و یا نهاد جایگزین وی و تصویب آن به عهده ((بالاترین مقام اجرایی سازمان))) خواهد بود.
 - دسترسی به هر برنامه کاربردی جهت مشاهده یا بهره‌برداری اطلاعات فقط پس از طی فرآیند تخصیص دسترسی عام مجاز خواهد بود.
 - دسترسی به هر برنامه کاربردی جهت تغییر در اطلاعات موجود در آن نرم‌افزار یا بانک‌های اطلاعاتی مرتبط با آن فقط پس از طی فرآیند تخصیص دسترسی خاص مجاز خواهد بود.

- دسترسی به هر برنامه کاربردی، بانک اطلاعات، سیستم عامل، تجهیزات پردازشی یا مسیریابی یا ذخیره‌سازی و یا هر گونه دارایی اطلاعاتی دارای طبقه‌بندی حفاظتی خیلی محرمانه یا بالاتر و یا جهت تغییر در پیکربندی آن دارایی اطلاعاتی فقط پس از طی فرآیند تخصیص دسترسی ممتاز مجاز خواهد بود.
- دسترسی به بانک‌های اطلاعاتی به منظور تغییر در محتوای آن فقط پس از طی فرآیند تخصیص دسترسی خاص مجاز خواهد بود.
- دسترسی از خارج از سازمان به اطلاعات درون شبکه سازمان فقط پس از عبور از نقطه امن مجاز خواهد بود. عملکرد و اجزای نقطه امن در پیوست شماره یک همین دستورالعمل شرح داده شده است.
- جهت کنترل دسترسی به اطلاعات حیاتی سازمان لازم است از مکانیزم تعریف نقطه امن استفاده شود. در صورت ضرورت لازم است دارایی‌های اطلاعاتی بسیار حیاتی جدا از شبکه‌های ارتباطی مورد استفاده قرار گیرند.
- علاوه بر الزامات دسترسی از خارج سازمان به اطلاعات درون شبکه لازم است در خصوص استفاده از تجهیزات زیر و کنترل دسترسی به هر یک تصمیم‌گیری شود:
 - تجهیزات پردازش همراه
 - PDA یا تلفن‌های هوشمند
 - تجهیزات یا درایوهای USB و یا لوازم مشابه
 - فلاپی دیسک، CD، DVD و یا تجهیزات مشابه
 - تجهیزات امنی (مثل مودم‌ها، مسیریاب‌ها یا سویچ‌ها، بریج‌ها، تجهیزات ارسال و دریافت ماهواره‌ای و یا سایر تجهیزات متعلق به سرویس دهنده‌های مخابراتی یا پردازشی)
- علاوه بر الزامات فوق لازم است برای جلوگیری از دسترسی‌های ناخواسته و یا ایجاد امکان عبور غیر مجاز از مکانیزم‌های کنترل دسترسی و یا پیشگیری از روش‌های بی اثر کردن روش‌ها و یا جلوگیری از ایجاد فرصت‌های حمله به سیستم ناشی از

حمله‌های مبتنی بر فروپاشی سیستم و دور زدن ابزار کنترل دسترسی به موارد زیر توجه شود:

- فقط سخت‌افزارهای پردازشی یا ارتباطی دارای مجوز به کار گرفته شود و نصب آن‌ها توسط افراد معتمد انجام پذیرد. تصمیم‌گیری در مورد نوع مجوز استفاده (شفاهی، کتبی و یا استعلام از مراجع رسمی) به عهده (((بالاترین مقام اجرایی سازمان))) می‌باشد.
- نصب مودم اعم از مودم کابلی یا بی سیم یا ماهواره ممنوع است مگر آنکه قبلاً مجوز آن توسط واحد امنیت اطلاعات صادر شده باشد.
- نصب مستقیم مودم به شبکه داخلی سازمان ممنوع است و لازم است مودم‌های مجاز از طریق مکانیزم نقطه امن و یا از طریق لایه حفاظتی مناسب (مثل DMZ) به شبکه متصل شوند.
- از طریق اعمال کنترل دسترسی ممتاز، دسترسی به فایل‌های پیکربندی نرم‌افزارها و سخت‌افزارها باید تحت کنترل کامل قرار گیرد.
- استفاده از تجهیزات USB یا حافظه‌های Flash برای جابجایی اطلاعات شبکه داخلی یا سایر اطلاعات دارای طبقه‌بندی حفاظتی ممنوع می‌باشد. در صورت ضرورت استفاده از این نوع تجهیزات لازم است از مکانیزم‌های رمزنگاری اطلاعات استفاده شود.
- در صورت سرقت یا مفقود شدن هر یک از دارایی‌های اطلاعاتی لازم است روش‌های کنترل دسترسی که ممکن است به دلیل دستیابی افراد غیر مجاز به آن دارایی اطلاعاتی افشاء شوند، مورد بازبینی قرار گرفته و در صورت نیاز تغییر یابند.
- لازم است کلیه نرم‌افزارهای اضافی یا غیر ضروری موجود در شبکه داخلی سازمان به خصوص نرم‌افزارهای مدیریتی (مدیریت دسترسی، مدیریت ریسک، مدیریت اطلاعات) و برنامه نویسی حذف گردند.
- دسترسی به نرم‌افزارهای انتقال فایل (مثل TFTP، FTP، RARP و غیره) محدود گردد.

- اجرای دستور در سطح سیستم (مثل دستورهای سیستم عامل) فقط منحصر به افراد خاصی که از طریق اعمال سیاست کنترل دسترسی ممتاز حق دسترسی به سیستم دارند محدود گردد.
- کنترل دسترسی به فایروال، IDS، آنتی ویروس، سیستم احراز هویت یا اعتبارسنجی، کنترل ورود به سیستم ((Active Directory و دیده بانی و مانیتورینگ سیستم باید جزو دسترسی‌های ممتاز محسوب شده و کنترل‌های لازم در مورد آن اعمال گردد.
- هر گونه نقص در عملکرد سیستم‌های کنترل دسترسی یا حمله به آن‌ها به عنوان حادثه‌ای مهم تلقی شده و فوراً مورد رسیدگی قرار گرفته و ترمیم شود.
- در صورت نیاز به سرویس عدم انکار و یا عدم امکان عقد موافقت‌نامه‌های دو یا چند جانبه حفظ محرمانگی لازم است از زیرساخت کلید عمومی ((PKI/CA رسمی کشور و یا اپراتورهای CA مورد وثوق استفاده شود.

الزامات ممیزی کنترل دسترسی:

- هنگام ممیزی روش‌های کنترل دسترسی لازم است ممیزی وضعیت اجرای سیاست‌های کنترل دسترسی در قالب لایه‌های زیر به مورد اجراء گذاشته شود:
- الف- ممیزی مکانیزم‌های کنترلی مدیریتی شامل:
 - سیاست‌گذاری کنترل دسترسی و رویه‌های اجرایی آن
 - کنترل اهتمام افراد و کارکنان به رعایت معیارهای کنترل دسترسی
 - ساختار مدیریتی فعالیت‌های کنترل دسترسی
 - آزمایش مکانیزم‌های کنترل دسترسی (اخطار: آزمایش خود سرانه مکانیزم‌های کنترل دسترسی حتی با فرض یافتن ضعف‌های آن ممنوع است. این کار فقط باید با اطلاع قبلی افراد مسؤول و بر اساس برنامه از پیش تعریف شده و توسط افراد معتمد به عمل آید).
 - ب- ممیزی مکانیزم‌های کنترل دسترسی فیزیکی شامل:
 - جداسازی فیزیکی شبکه‌ها

- امنیت پیرامونی
- کنترل دسترسی فیزیکی به تجهیزات پردازشی
- جداسازی محیط‌های کاری برای جلوگیری از مجاورت‌های غیر ضروری
- دسترسی به اطلاعات **Back up** گرفته شده
- دسترسی به کابل‌ها و زیرساخت ارتباطی
- کنترل تردد
- ج- ممیزی مکانیزم‌های کنترل فنی
 - کنترل دسترسی به سیستم‌ها
 - کفایت معماری شبکه برای پاسخگویی به نیازهای کنترل دسترسی
 - کنترل دسترسی شبکه
 - رمزنگاری و پروتکل‌های استفاده شده
 - ممیزی فعالیت‌های ممیزی

فرآیند:

کنترل دسترسی باید بر اساس نوع و ماهیت دارایی اطلاعاتی موضوع دسترسی، هویت متقاضی دسترسی و صلاحیت وی برای دسترسی انجام پذیرد.

طبقه‌بندی حفاظتی دارایی اطلاعاتی (بر اساس دستورالعمل ۳-۲-۱) تعیین کننده نوع و ماهیت دارایی اطلاعاتی از دیدگاه اعطای حقوق دسترسی و روش کنترل آن می‌باشد. بدیهی است هر چه سطح طبقه‌بندی دارایی اطلاعاتی مورد نظر بالاتر باشد باید اعطای حقوق دسترسی با دقت بیشتری انجام پذیرفته و مکانیزم‌های کنترل آن سخت گیرانه‌تر باشد.

صلاحیت کاربر (اعم از انسان و یا نهاده‌ای که درخواست دسترسی به اطلاعات را دارد) بر اساس نوع و ماهیت دارایی اطلاعاتی تعیین می‌گردد. به عبارت دیگر خصوصیات و قابلیت‌های متقاضی دسترسی جهت دسترسی به هر دسته از دارایی‌های اطلاعاتی باید قبلاً تعیین شود. به عنوان مثال یکی از قواعد دسترسی به فایل‌های پیکربندی تجهیزات مسیریابی را می‌توان به شرح زیر مکتوب کرد.

"دسترسی به فایل پیکربندی مسیریاب اصلی شبکه سازمان الف فقط برای مدیر شبکه سازمان الف و جانشین وی مجاز می‌باشد".

به عبارت دیگر هیچیک از افراد به‌جز دو فرد فوق صلاحیت دسترسی به فایل پیکربندی مسیریاب را ندارند.

بنابر مواد فوق لازم است کلیه افرادی که تقاضای دسترسی به یک دارایی اطلاعاتی تحت حفاظت را دارند اولاً احراز هویت شده و سپس در صورت صلاحیت دسترسی به آن دارایی اطلاعاتی امکان دسترسی به آن را پیدا نمایند.

احراز هویت افراد یا نهاده‌های متقاضی دسترسی بر اساس تشخیص عوامل زیر انجام می‌شود:

- هویتی که ادعا می‌شود (شناسه کاربری)
 - آنچه که اثبات کننده ادعا است (کلمه عبور)
 - آنچه که همراه دارد (توکن سخت‌افزاری)
 - آنچه که هست (اثر انگشت، الگوی عنبیه یا صورت یا سایر پارامترهای بیومتریک)
 - آنکس که گفته وی را تائید می‌کند (مقام بالاتر یا عامل قانونی)
 - استفاده از دو عامل اول در احراز هویت ضروری و اجباری می‌باشد.
- جهت اعمال کنترل‌های بیشتر (در حفاظت از دارایی‌های با طبقه‌بندی حفاظتی بالاتر) لازم است از سایر عوامل یا ترکیبی از عوامل دیگر (بر اساس سطح طبقه‌بندی یا حساسیت دارایی اطلاعاتی) استفاده نمود.

جهت کسب اطلاعات کاملتر در مورد شیوه‌ها و مدل‌های اجرایی کنترل دسترسی به پیوست شماره دو همین دستورالعمل مراجعه شود.

مرجع:

این دستورالعمل به شماره □-□/۱-۷/□-□ به ثبت رسیده است.

روند نما

این دستورالعمل فاقد روند نما می‌باشد.

پیوست یک

مکانیزم نقطه امن ارتباطی

نقطه امن ارتباطی در یک شبکه رایانه‌ای با هدف تامین اهداف زیر تعریف می‌گردد:

- جلوگیری از ورود غیر مجاز به شبکه رایانه‌ای تحت حفاظت از طریق خطوط مخابراتی اعم از کابلی، بی سیم و یا ماهواره‌ای
- جلوگیری از حمله به منابع یا تجهیزات موجود در شبکه
- جلوگیری از خروج غیر مجاز اطلاعات از شبکه
- جلوگیری از حمله از درون شبکه یا با استفاده از منابع شبکه به سایر شبکه‌ها یا اهداف رایانه‌ای
- اطمینان از رمزنگاری اطلاعات در حال انتقال
- اطمینان از هویت و صلاحیت طرف مقابل در دریافت یا ارسال اطلاعات
- جلوگیری از ورود کدهای مخرب مثل ویروس‌ها، اسب‌های تروا یا کرم‌های رایانه‌ای به شبکه تحت حفاظت

اجزای تشکیل دهنده نقطه امن به ترتیب از سمت لایه خارجی به لایه داخلی عبارت‌اند از:

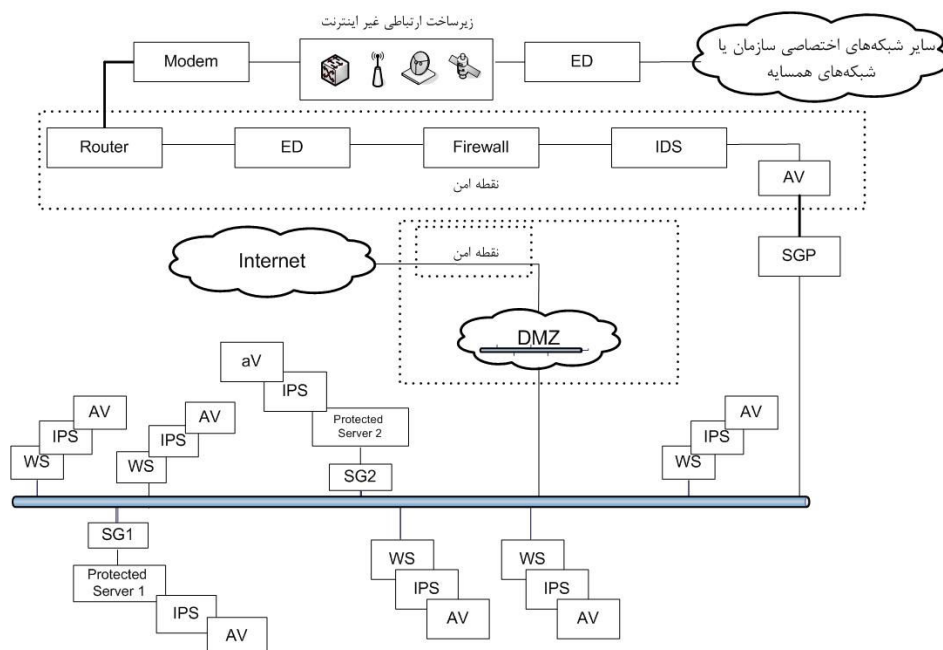
- مودم یا واسطه ارتباطی (جهت برقراری ارتباط با سایر شبکه‌ها)
- مسیریاب (جهت مسیریابی و کنترل بسته‌های ارسالی)
- رمزکننده (جهت رمزگذاری یا رمزگشایی اطلاعات ارسالی / دریافتی)
- فایروال (جهت جلوگیری از حمله‌های شناخته شده و پنهان سازی IPهای داخلی)
- IDS/IPS (جهت جلوگیری از تلاش برای نفوذ در سیستم)
- ضد ویروس (جهت جلوگیری از ورود ویروس....)
- دروازه امنیتی (جهت کنترل دسترسی به نرم‌افزارها یا برنامه‌های کاربردی خاص)

تبصره ۱: در صورت اتصال به شبکه‌های عمومی مثل اینترنت استفاده از رمزکننده ضروری نمی‌باشد، اما اگر هدف از برقراری ارتباط اتصال به یک یا چند شبکه خاص متعلق به سازمان‌ها یا مراکز دارای هویت مستقل باشد، اولاً باید تبادل اطلاعات به صورت رمزگذاری شده باشد و ثانیاً لازم است توافقنامه حفظ محرمانگی (موضوع دستورالعمل ۲-۱-۵) بین طرف‌های تبادل به امضاء برسد.

تبصره ۲: در صورت استفاده از برنامه‌های کاربردی خاص (که حق دسترسی به آن‌ها فقط به افراد معینی داده می‌شود) استفاده از دروازه‌های امنیتی ((Security Gateway مبتنی بر نشانه‌های سخت‌افزاری (Token) مثل قفل USB Key یا Smart Card یا هر نوع شناسه سخت‌افزاری دیگر لازم است. در صورت نیاز می‌توان دروازه امنیتی را در جلو سرورس دهنده ((Server سرورس مورد نظر نصب نمود.

معماری نقطه امن

نحوه قرار گرفتن تجهیزات نقطه امن و اتصال آن به شبکه داخلی و شبکه خارجی در پلان زیر نمایش داده شده است.



توجه : افزاز شبکه داخلی به زیرشبکه‌های مجزا از یکدیگر (بر اساس کاربری و نوع کاربران) کارآیی عملیات امن سازی را به مقدار قابل توجه افزایش خواهد داد.
راهنما:

AV: Anti Virus
IDS: Intrusion Detection System
IPS: Intrusion Prevention System +Host IDS
WS: Work Station
SG: Security Gateway
SGP: Security Gateway (Public)
DMZ: Demilitarized Zone
ED: Encryption Device

توضیحات:

- ۱- قرارداد **SGP** در مرز شبکه داخلی اختیاری می‌باشد و در صورت لزوم به منظور حفاظت از کلیه ایستگاه‌های کاری یا سرویس دهنده‌های موجود در شبکه تعبیه خواهد شد.
- ۲- حتی الامکان لازم است از طریق **NAT** آدرس‌های **IP** شبکه داخلی از دید ناظر خارجی پنهان سازی شود.
- ۳- در صورت استفاده از بستر اینترنت برای اتصال به سایر شبکه‌ها لازم است نقطه امن قبل از **DMZ** نیز ایجاد شود. در این صورت می‌توان به صورت مقتضی معماری نقطه امن و معماری **DMZ** را ترکیب نمود.
- ۴- در صورت نیاز به حفاظت از یک سرویس دهنده (**Server**) خاص و یا محدودسازی افرادی که به آن سرویس دهنده دسترسی دارند لازم است از **SG**‌های اختصاصی برای همان سرویس دهنده استفاده شود.
- ۵- نصب **AV** و **IPS** روی همه ایستگاه‌های کاری و سرویس دهنده‌ها ضروری است.
- ۶- اتصال به سایر شبکه‌ها یا ارائه سرویس راه دور به کاربران بدون عبور از نقطه امن یا ترکیب نقطه امن و **DMZ** ممنوع می‌باشد.
- ۷- در صورتی که تعداد شبکه‌های طرف تعامل یا تعداد و ماهیت کاربران راه دور به نوعی است که امکان عقد موافقت‌نامه‌های حفظ محرمانگی متفی باشد و یا ارائه سرویس عدم انکار (**Non Repudiation**) ضروری باشد لازم است از زیرساخت کلید عمومی (**PKI/CA**) جهت حفاظت از ارتباطات و پیام‌های تبادل شده استفاده شود. در این حالت لازم است **CA** (مرکز صدور گواهی) انتخاب شده، معتبر و دارای پشتیبانی قانونی باشد. (جهت دریافت اطلاعات بیشتر در خصوص مرکز صدور گواهی الکترونیک کشوری و چگونگی بهره‌برداری از خدمات آن با وزارت بازرگانی مکاتبه شود.)

پیوست دو

مبانی کنترل دسترسی

زیر بنای امنیت اطلاعات بر اساس کنترل چگونگی دسترسی به منابعی که باید در مقابل تغییر یا افشای غیر مجاز حفاظت شوند پی ریزی می‌شود.

مکانیزم‌های کنترلی که برای کنترل دسترسی به کار گرفته می‌شوند دارای ماهیت تکنیکی، فیزیکی و مدیریتی می‌باشند.

موضوع‌های اصلی که در کنترل دسترسی باید به آن‌ها پرداخته شود عبارت‌اند از:

- روش‌ها و مکانیزم‌های شناسایی (Identification)
- روش‌ها، مدل‌ها و تکنیک‌های اعتبار سنجی (Authentication)
- مدل‌های مبتنی بر صلاحدید (Discretionary)، اجبار (Mandatory) و احتراز (non Discretionary)
- استمرار پاسخگویی (Accountability)، آشکارسازی یا دیده بانی (Monitoring) و ممیزی (Auditing)
- روش‌های امن‌سازی و تسری آن
- سامانه‌های تشخیص نفوذ (IDS)
- تهدیدهای احتمالی علیه روش‌ها و تکنیک‌های کنترل دسترسی

کنترل دسترسی عبارت است از روشی که طی آن نحوه برقراری ارتباط یا تعامل بین کاربران و سیستم‌ها با سایر سیستم‌ها یا منابع (اعم از اطلاعاتی، پردازشی، ذخیره‌سازی و ارتباطی) کنترل می‌شود. هدف اصلی در کنترل دسترسی جلوگیری از دسترسی غیر مجاز به اطلاعات بوده و همچنین می‌تواند در تعیین حدود حوزه اختیار متقاضی دسترسی ((Authorization به منع مورد نظر (پس از طی موفق مرحله اعتبار سنجی) به کار گرفته شود.

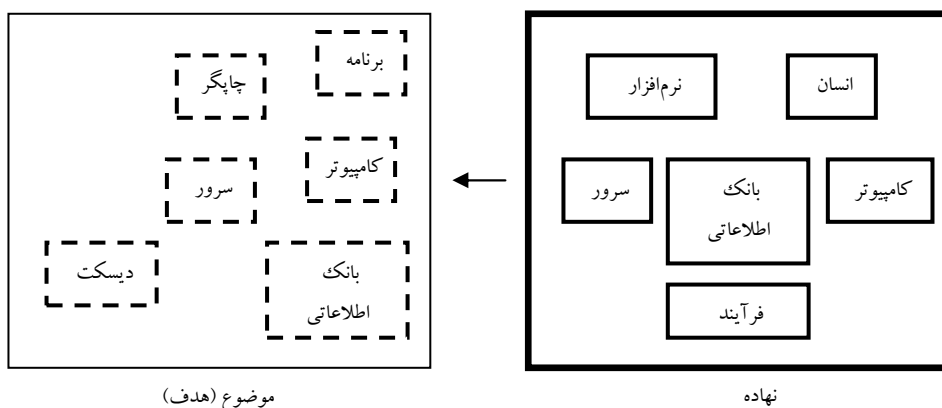
به‌طور معمول به‌جز کاربران که معمولاً از دیدگاه عام موجودیت‌هایی هستند که تقاضای دسترسی به منابع را دارند، انواع دیگری از موجودیت‌ها نیز وجود دارند که متقاضی دسترسی به منابع هدف می‌باشند. بنابراین هنگام بحث در خصوص کنترل دسترسی درک صحیح نهاده ((Subject و موضوع یا هدف ((Object اهمیت فراوانی دارد.

دسترسی عبارت است برقراری جریانی از اطلاعات بین یک هدف و یک نهاده. نهاده ((Subject عبارت است از یک موجودیت کنشگر یا فعال (Active) که خواهان دسترسی به یک موضوع

(Object) و یا داده‌های مرتبط با موضوع یا هدف می‌باشد. نهاده می‌تواند در قالب کاربر، برنامه و یا فرآیندی باشد که برای انجام دادن یک کار یا وظیفه (Task) به موضوع یا هدف مراجعه می‌نماید.

موضوع یا هدف عبارت است از یک موجودیت کنش پذیر یا غیر فعال (Passive) که حاوی اطلاعات یا داده می‌باشد. هدف می‌تواند یک کامپیوتر، بانک اطلاعاتی، فایل برنامه نرم‌افزاری، دایرکتوری و یا فیلد موجود در یک جدول از یک بانک اطلاعاتی باشد.

به عنوان مثال هنگام مراجعه یک برنامه به یک فایل، برنامه در قالب نهاده (Subject) و فایل در قالب موضوع (Object) ظاهر می‌شوند. از سوی دیگر هنگام مراجعه یک کاربر به یک برنامه، کاربر در قالب نهاده و برنامه در قالب موضوع ظاهر می‌شوند.



کنترل دسترسی مهمترین جزء در برقراری امنیت اطلاعات می‌باشد زیرا مکانیزم‌های کنترل دسترسی اولین رده دفاعی در مقابل دسترسی غیر مجاز به دارایی‌های اطلاعاتی تحت حفاظت را تشکیل می‌دهند.

مکانیزم‌های کنترل دسترسی قابلیت کنترل، محدودسازی، آشکارسازی و حفاظت از منابع سازمان در جهت حفظ دسترسی پذیری، جامعیت و محرمانگی را در اختیار استفاده کننده از آن می‌گذارد.

شناسایی، اعتبارسنجی، تفویض اختیار و پاسخگویی

هر نهاده‌ای که بخواهد به یک منبع دسترسی پیدا کند باید ثابت کند که همان کسی است که ادعا می‌کند و دارای شرایط و سندیت لازم می‌باشد و از حق یا امتیاز انجام فعالیتی که می‌خواهد انجام دهد برخوردار است. پس از گذراندن این مرحله آن نهاده می‌تواند به شبکه یا منابع دیگر مورد درخواست خود مراجعه کرده و کار خود را به انجام رساند اما لازم است اولاً کلیه فعالیت‌های وی رهگیری و ثبت شده و ثانیاً وی ملزم به پاسخگویی در مقابل فعالیت‌ها یا عملیات خود باشد.

شناسایی ((Identification عبارت است از اطمینان از این‌که هر نهاده (کاربر، برنامه یا فرآیند) همان موجودیتی است که ادعا می‌شود. ساده ترین راه اثبات ادعا و شناسایی استفاده از شناسه کاربری و کلمه عبور می‌باشد.

برای تکمیل اعتبارسنجی و اعتباردهی به نهاده، لازم است متقاضی که قبلاً از طریق شناسه کاربری و کلمه عبور شناسایی شده است مدرک یا مدارک بیشتری را ارائه نماید. این نوع مدارک می‌تواند یکی یا مجموعه‌ای از مواد زیر باشد:

- کلمه عبور
- رمز عبور چند پاره‌ای
- کلید رمزنگاری
- شماره شناسایی شخصی (PIN)
- مشخصه‌های آناتومی
- نشانه‌های سخت‌افزاری (Token)

مشخصه‌های مواد فوق که از طرف متقاضی ارائه می‌شوند با مشخصه‌های از پیش ذخیره شده نزد موضوع مقایسه می‌شوند تا مرحله اعتبارسنجی تکمیل شود.

اما هنوز کار پایان یافته تلقی نمی‌شود. پس از شناسایی و اعتبارسنجی متقاضی، لازم است وجود حق یا امتیاز دسترسی به منابع مورد نظر بررسی شود. این کار توسط موضوع و بدون دخالت نهاده متقاضی انجام می‌شود.

در صورت بررسی و اثبات وجود حق یا امتیاز دسترسی به منبع یا منابع مورد نظر بر اساس بررسی اطلاعات موجود نزد موضوع، اختیار دسترسی به نهاده تفویض می‌شود این مرحله تفویض اختیار (Authorization) نام دارد.

توجه: در صورتی‌که به هر دلیل مرحله تفویض اختیار قبل از تکمیل اعتبارسنجی به اجراء گذاشته و تکمیل شود، مکانیزم کنترل دسترسی در معرض تهدید و فروپاشی قرار می‌گیرد. این وضعیت ممکن است به دلیل بروز شرایط رقابتی ((Race Condition حادث شود. این حالت وقتی پیش می‌آید که بیش از یک فرآیند به طور همزمان درخواست استفاده از منبع اشتراکی را داشته باشند. در چنین حالتی ممکن است نتایج استفاده از منبع وقتی فرآیند ۱ قبل از فرآیند ۲ از منبع بهره‌برداری کند متفاوت با حالتی باشد که فرآیند ۱ بعد از فرآیند ۲ از منبع بهره‌برداری نماید.

این حالت به عنوان مثال می‌تواند برای فرآیندهای اعتبارسنجی و تفویض اختیار حادث شود. اگر هر دوی این پروسه برای تکمیل نیاز به مراجعه به یک منبع، مثلاً استخراج اطلاعات از بانک کاربران داشته باشند، ممکن است حالت شرایط رقابتی پیش آمده و نتایج اجرای فرآیند تفویض

اختیار ((Authorization متفاوت از حالت عادی باشد که به معنای خطا در ((Authorization است و ممکن است به دسترسی غیر مجاز به منابع منتهی شود.

برای مطالعه بیشتر در خصوص نقض شرایط رقابتی به مطلب زیر مراجعه شود:

"What is Race Condition and Dead locks" Microsoft Knowledge Base Article 317723
<http://support.microsoft.com/kb/317723>

بنابراین لازم است مراحل کنترل دسترسی به ترتیب زیر به مورد اجرا گذاشته شود.

- شناسایی
- اعتبارسنجی
- تفویض اختیار
- استفاده از منبع و ثبت مراحل کار
- پاسخگویی

سلسله مراتب کنترل، ثبت و ممیزی دسترسی

آنچه که در ادامه مطرح خواهد شد ناظر بر کنترل دسترسی منطقی می‌باشد. کنترل دسترسی فیزیکی به‌طور جداگانه و تحت سرفصل امنیت فیزیکی مورد بحث قرار خواهد گرفت.

شناسایی و اعتبارسنجی

پس از شناسایی کاربر از طریق شناسه کاربری ((USER ID نوبت به اعتبارسنجی می‌رسد. اعتبارسنجی بر اساس سه فاکتور عمومی زیر انجام می‌پذیرد:

- آنچه که مدعی می‌داند (کلمه عبور، PIN،)
 - آنچه که همراه دارد (کلید USB، قفل سخت‌افزاری، کارت هوشمند)
 - آنچه که هست (خصوصیات بیومتریک مثل اثر انگشت، الگوی چهره...)
- که معمولاً به آن اعتبارسنجی بر اساس آگاهی، اعتبارسنجی بر اساس مالکیت و اعتبارسنجی بر اساس خصوصیات فردی گفته می‌شود.
- برای اطمینان از کفایت روش اعتبارسنجی استفاده از بیش از یک فاکتور از بین سه فاکتور فوق ضروری است.

توجه: هنگام انتخاب عوامل شناسایی توجه به نکات زیر ضروری است:

- هر عامل شناسایی یا شناسه باید یکتا باشد که بتوان بر اساس آن پاسخگویی استفاده کننده را تضمین نمود.

- روش انتخاب شناسه کاربری باید یکسان و استاندارد باشد.
- عامل شناسایی یا شناسه نباید مبین موقعیت سازمانی (پست) یا وظیفه استفاده کننده باشد.
- نباید از شناسه به صورت اشتراکی استفاده شود.

مدیریت شناسه‌های کاربری

- هنگام تصمیم در خصوص اعطای دسترسی لازم است به موارد زیر توجه شود:
- هر یک از کاربران نیاز به دسترسی به کدام منبع دارند؟
 - چه کسی نیاز به دسترسی را تأیید کرده و اجازه آن را صادر می‌کند؟
 - چگونه تصمیم در مورد دسترسی‌ها با سیاست‌گذاری امنیتی سازمان منطبق می‌شود؟
 - آیا کاربران قبلی هنوز دسترسی دارند؟
 - فرآیند سلب دسترسی چگونه است؟
 - آیا کنترل و آشکارسازی دسترسی به صورت متمرکز انجام می‌شود و چگونه؟
 - آیا کاربران نیاز به حفظ کلمه‌های عبور متعدد دارند؟
 - در صورت استفاده از محیط‌های دسترسی که دارای نیازهای دسترسی گوناگون هستند آیا امکان متمرکز کردن سیستم کنترل دسترسی وجود دارد؟
 - روش‌های کنترل دسترسی برای کاربران سازمان، مشتریان و یا شرکای تجاری چه تفاوتی با هم دارند؟
 - چگونه می‌توان مطمئن بود که قوانین و مقررات دولتی مربوط به کنترل دسترسی رعایت شده اند؟
 - ثبت کاربر چگونه انجام می‌شود؟
- روش‌های مدیریت شناسه‌های کاربری فعلی معمولاً به صورت دستی و با استفاده از تنظیم دستی مجوزهای دسترسی به دایرکتوری‌ها، فهرست‌های کنترل دسترسی (ACLs) و پروفایل‌های سیستم اجراء می‌شوند. این گونه روش‌ها ممکن است در سازمان‌های کوچک قابل اجرا باشند اما در سازمان‌های بزرگ و به خصوص در مقابل تقاضای روز افزون برای بهره‌برداری از خدمات الکترونیک ناکارا می‌باشند.

برای پاسخگویی به این چالش استفاده از روش‌های خودکار مدیریت شناسه (**Identity Management**) یا به طور خلاصه **IdM** ضروری است.

روش‌های **IdM** با استفاده از فناوری‌های زیر قابل به‌کارگیری است:

- **Directories**
- **Web Access Management**
- **Password Management**
- **Legacy Single Sing-on**
- **Account Management**
- **Profile Update**

هر یک از فناوری‌های فوق به طور خلاصه در ادامه معرفی شده‌اند.

Directoryها

بسیاری از سازمان‌های بزرگ اقدام به تشکیل نوعی **Directory** (فهرست راهنما) نموده‌اند که حاوی اطلاعات مربوط به منابع و کاربران شبکه تحت اختیار ایشان می‌باشد. بیشتر این **Directoryها** فرمت سلسله مراتبی ((**hierarchical** داشته و بر اساس استاندارد **X.500** فرمت بندی شده‌اند و از پروتکل **LDAP (Light weight Directory Access Protocol)** برای تعامل بین نهاده‌ها و برنامه‌های کاربردی با **Directory** استفاده می‌کنند. در این حالت برنامه‌های کاربردی می‌توانند با استفاده از یک درخواست **LDAP** اطلاعات مربوط به یک کاربر خاص را درخواست نمایند. همچنین کاربران می‌توانند درخواست مشابهی را در خصوص یک منبع ((**Resource** خاص ارسال نمایند.

موضوع‌های ((**Objects** موجود در **Directory** توسط **Directory Service** مدیریت می‌شوند. **Directory Service** توانایی پیکربندی و مدیریت چگونگی شناسایی، اعتبارسنجی، تفویض اختیار و کنترل دسترسی درون شبکه را در اختیار مدیر شبکه قرار می‌دهد.

به عنوان مثال هنگام **Login** در **Windows** کاربر به یک کنترل کننده دامنه ((**DC**) متصل می‌شود که حاوی بانک اطلاعاتی سلسله مراتبی **Directory** می‌باشد. بانک اطلاعاتی **Directory Service** (یا همان **Active Directory**) را که حاوی اطلاعات کنترلی منابع شبکه و کنترل دسترسی است به اجرا می‌گذارد.

بنابراین پس از ورود موفق به **DC** منابع خاصی از شبکه (مثل خدمات چاپ، **File Server**، **mail** و مشابه آن) در اختیار کاربر قرار می‌گیرد.

نقش Directory در مدیریت شناسه‌ها (IdM)

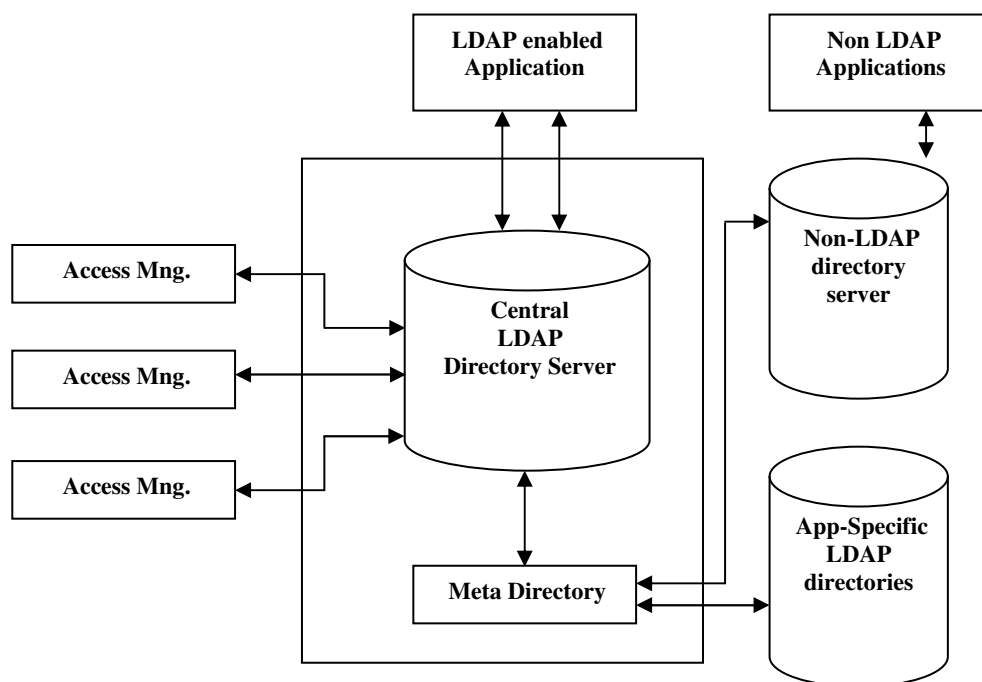
Directory مورد استفاده در **IdM** نرم‌افزار بانک اطلاعاتی مخصوص است که در جهت عملیات جست‌وجو و استخراج اطلاعات بهینه سازی شده است. این عملیات مهمترین بخش از راه حل مدیریت شناسه را تشکیل می‌دهد، زیرا کلیه اطلاعات منابع، مشخصه‌های کاربران، پروفایل‌های تفویض اختیار، نقش و وظائف، سیاست‌های کنترل دسترسی و بسیاری اطلاعات دیگر به صورت یکجا در آن ذخیره می‌شود. هنگامی که سایر نرم‌افزارهای **IdM** برای انجام وظائف محوله به خود (مثل تفویض اختیار، کنترل دسترسی یا تخصیص مجوز) نیاز به اینگونه اطلاعات دارند می‌توانند به این بانک اطلاعاتی متمرکز مراجعه نموده و به اطلاعات موجود در آن دست یابند.

Web Access Management

نرم‌افزارهای مدیریت دسترسی (**Web WAM**) کنترل آنچه که می‌تواند هنگام دسترسی به نرم‌افزارهای تحت **Web** سازمان، در دسترس کاربران قرار گیرد را به عهده دارند. این فناوری به صورت پیوسته توسعه یافته و هر روز از استحکام و توانایی بیشتری برخوردار می‌شود. دلیل آن استفاده روزافزون از تجارت الکترونیک، بانکداری الکترونیک **On-Line**، تولید و ارائه محتوای الکترونیکی، خدمات **Web** و بسیاری فناوری‌های دیگر می‌باشد.

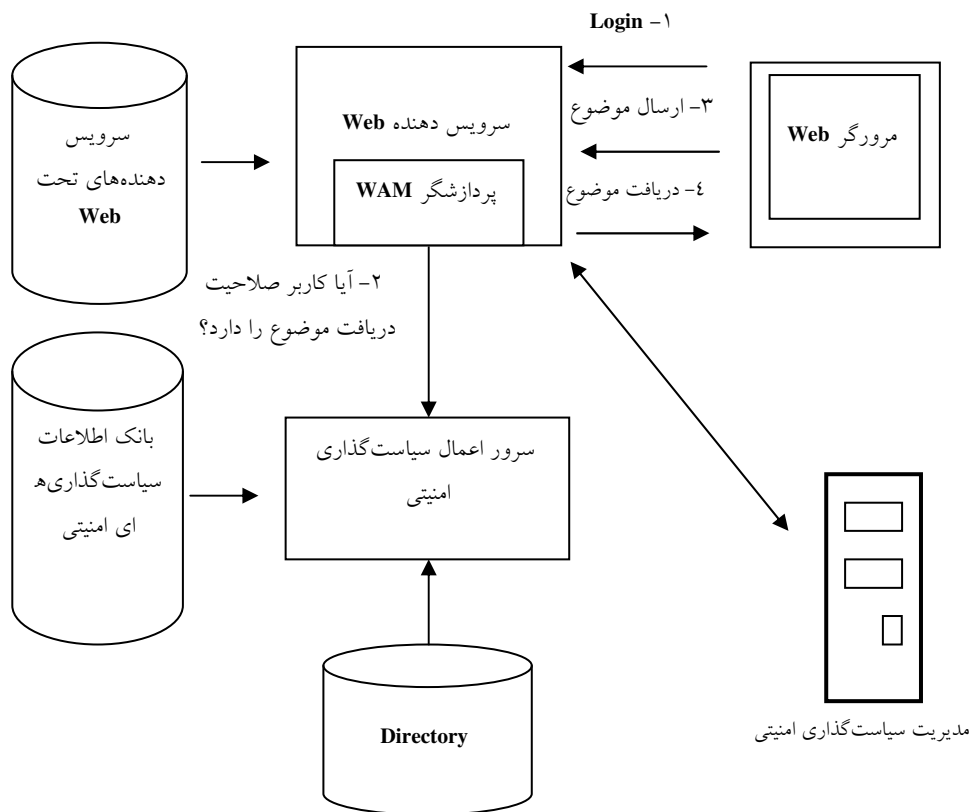
توالی فعالیت‌های اصلی مدیریت کنترل دسترسی **Web** در زیر فهرست شده است:

- کاربر اعتبار نامه خود را به سرویس دهنده **Web** ارسال می‌نماید.
 - سرویس دهنده **Web** اعتبار کاربر را ارزیابی می‌نماید.
 - کاربر درخواست دسترسی به یک منبع خاص (**Object**) را ارسال می‌نماید.
 - سرویس دهنده **Web** بر اساس مدل سیاست‌گذاری امنیتی خود مجاز بودن کاربر برای انجام چنین درخواستی را کنترل می‌نماید.
 - در صورت مجاز بودن کاربر، سرویس دهنده **Web** اجازه دسترسی به منبع مورد درخواست را صادر می‌نماید.
- روابط درونی بین اجزاء درگیر در انجام فرآیندهای فوق در شکل بعدی نمایش داده شده است.



Meta-directory ها اطلاعات را از سایر منابع جمع کرده و برای غنی کردن اطلاعات **IdM** در اختیار آن قرار می‌دهند.

مدل پایه تعامل اجزاء در کنترل دسترسی **web** در شکل زیر نمایش داده شده است.



مدل پایه کنترل دسترسی web

نرم افزار **WAM** دروازه اصلی است که بین کاربران و نرم افزارهای تحت **Web** سازمان قرار می گیرد. هنگامی که کاربر درخواست دسترسی به یک منبع موجود در **Web** را ارسال می کند نرم افزار سرویس دهنده **Web** به **Directory** (که عملکرد آن قبلاً شرح داده شده است)، سرور احراز هویت و احتمالاً بانک اطلاعات حاوی اطلاعات اضافی در خصوص سیاست های امنیتی مراجعه کرده و در صورت انطباق درخواست با الزامات دسترسی، منبع مورد نظر را در اختیار کاربر قرار می دهد. مدیر سیستم (**Administrator**) می تواند با استفاده از کنسول **WAM** اقدام به تنظیم سطوح دسترسی، الزامات احراز هویت و ایجاد حساب های کاربری نموده و همچنین عملیات دیگر مدیریت دسترسی به نرم افزارهای تحت **Web** را کنترل نماید.

مدیریت کلمه عبور

جهت مدیریت کارای انتخاب، تخصیص، استفاده و کنترل کلمه‌های عبور توجه به نکات زیر ضروری است:

- یکسان سازی کلمه‌های عبور ((Password Synchronization، به منظور کاهش اشکال‌های مرتبط با نیاز به حفظ یا نگهداری کلمه‌های عبور متفاوت توسط یک کاربر
- امکان تغییر کلمه عبور توسط کاربر، به منظور کاهش نیاز به مراجعه به مدیر سیستم برای تغییر کلمه‌های عبور به هر دلیل ممکن
- تغییر کلمه عبور بر اساس مدل پرسش و پاسخ، به منظور سهولت در تغییر کلمه‌های عبور فراموش شده بدون ایجاد ریسک آسیب پذیری ناشی از حمله‌های مهندسی اجتماعی

هویت دیجیتال

بسیاری از افراد تصور می‌کنند هویت دیجیتال فقط در قالب شناسه کاربری ((USER ID تخصیص داده شده به یک فرد خلاصه می‌شود. واقعیت این است که هویت دیجیتال باید چیزی فراتر از یک شناسه کاربری ساده باشد.

هویت هر شخص را می‌توان به صورت مجموعه‌ای از مشخصه‌های سازمانی وی (مثل بخشی که در آن کار می‌کند، وظیفه سازمانی وی، مدارک تحصیلی وی و...)، حقوق سازمانی وی (مثل منابعی که در اختیار وی است، حدود اختیارات وی در سازمان و...) و همچنین خصوصیات فیزیکی وی (مثل اطلاعات بیومتریک، قد، وزن، سن، جنس و غیره) تعریف کرد.

بنابراین اگر کاربری درخواست دسترسی به یک بانک اطلاعاتی حاوی اطلاعات حساس را داشته باشد لازم است با استفاده از سیستم IdM اطلاعات هویتی وی استخراج و قبل از اعطای حق دسترسی، صلاحیت وی را مورد بررسی قرار داد. به عنوان مثال می‌توان فرض کرد کاربر تقاضا کننده مدیر ارشد [مشخصه] با مجوز دسترسی محرمانه [مشخصه] باشد و دارای حق دسترسی به بانک اطلاعاتی [حقوق] جهت خواندن یا بازنویسی رکوردهای خاص در ساعات رسمی اداری [مشخصه] باشد.

به عنوان مثالی دیگر می‌توان فرض کرد مقرر شده است سربازی یک اسلحه کلاشینکف را تحویل بگیرد. وی باید عضو یک واحد نظامی خاص [مشخصه] بوده و مشغول خدمت [مشخصه]

محسوب شده و مقام مافوق وی تحویل اسلحه به وی را تأیید [حقوق] نماید و همچنین اندام وی سالم [مشخصه فیزیکی] باشد تا تجهیزات مورد نیاز در اختیار وی قرار گیرد.

کلیه اطلاعات فوق در **Directory** (یا **Meta Directory**) سیستم **IdM** به صورت متمرکز نگهداری شده و در مواقع نیاز به آن مراجعه می‌شود.

ایجاد یک کنترل کننده دامنه ((**Domain Controller**) یا سرور کنترل دسترسی که فقط بر اساس شناسه کاربری و کلمه عبور کار کند را نمی‌توان همیشه به عنوان ایجاد سیستم کنترل دسترسی پذیرفت، بلکه لازم است با توجه به الزامات عملیاتی، درجه حساسیت سازمان بهره‌بردار و همچنین سطح طبقه‌بندی اطلاعات، سیستم مدیریت دسترسی جامعی را بر اساس ترکیبی از عوامل فوق ایجاد نمود.

در این حالت هویت الکترونیک هر کاربر براساس عوامل تعیین شده در سیستم مدیریت دسترسی تعریف شده و به کار گرفته می‌شود.

استفاده از سیستم مدیریت هویت ((**Identity Management**) بر اساس عنصر هویت دیجیتال در سازمان‌ها، نهادها و مراکزی با خصوصیات زیر ضروری است:

- در صورتی که هر کاربر نیاز به کار با بیش از پنج شناسه کاربری (همراه با کلمه عبور) داشته باشد.
- اگر تخصیص و ایجاد حساب کاربری ((**Account**) برای کاربران جدید بیش از یک روز طول بکشد.
- اگر حذف حساب کاربری و کلید دسترسی‌های تخصیص داده شده به یک نفر (به هر دلیل) بیش از یک روز طول بکشد.
- اگر دسترسی به منابع حساس و بحرانی قابل محدودسازی نباشد.
- اگر دیده بانی (آشکارسازی) دسترسی یا ممیزی منابع حساس و بحرانی امکانپذیر نباشد.

برای مطالعه بیشتر در خصوص مدیریت هویت می‌توان به منبع زیر مراجعه کرد:

<http://en.wikipedia.org/wiki/Identity-Management>

<http://www.opengroup.org/Projects/idm/uploads/40/9784/idm-wp.pdf>

روش‌های بیومتری

در روش‌های بیومتری (Biometrics) هویت هر شخص بر اساس تحلیل مشخصه‌ها یا رفتارهای شخصی وی بررسی می‌شود. این روش یکی از کاراترین و دقیق‌ترین روش‌های تشخیص هویت است. روش بیومتری از پیچیدگی و دشواری خاص برخوردار است به همین دلیل معمولاً روش گرانقیمت‌تری نسبت به سایر روش‌های تشخیص هویت است.

در روش بیومتری احراز هویت را می‌توان بر اساس رفتار شخصی و یا الگوی امضای مشخص نیز انجام داد اما بدیهی است که این نوع مشخصه‌ها در طول زمان تغییر پذیر می‌باشند و یا ممکن است به فراموشی سپرده شوند. بنابراین استفاده از روش‌های بیومتری مبتنی بر مشخصه‌های فیزیکی افراد که نوعاً تغییر ناپذیرند (مثل الگوی عنبیه یا شبکه‌ی چشم یا اثر انگشت) دقت بیشتری را به همراه خواهد داشت.

در روش بیومتری مشخصه‌های فیزیکی فرد پویش (Scan شده و اطلاعات حاصل از آن با اطلاعاتی که از قبل در مورد فرد ذخیره شده مقایسه می‌شود. بنابراین لازم است تجهیزات به‌کار گرفته شده برای آن دارای دقت بسیار زیاد باشد.

خطاهای حاصل از این نوع روش تشخیص هویت را می‌توان در قالب دو دسته خطای آماری دسته‌بندی کرد که عبارت‌اند از:

- خطای مثبت که حاصل آن عدم اجازه دسترسی به فرد مجاز است (خطای نوع اول).
 - خطای منفی که حاصل آن اجازه دسترسی به فرد غیر مجاز است (خطای نوع دوم).
- وقوع خطای نوع دوم در کنترل دسترسی بسیار خطرناک است و باید نحوه انتخاب تجهیزات و الگوریتم‌های تشخیص هویت به نحوی باشد که کاملاً از آن اجتناب شود. پارامتری که از آن برای اندازه‌گیری خطا در سیستم‌های بیومتری استفاده می‌شود معروف به نرخ خطای تداخل (Crossover Error Rate) یا به‌طور خلاصه CER می‌باشد. در مقایسه بین دو سامانه تشخیص هویت مبتنی بر روش بیومتری، سامان‌های که عدد CER کمتر داشته باشد دارای دقت بیشتری می‌باشد. برخی اوقات از نام (Equal Error Rate) EER نیز به جای CER استفاده می‌شود.

سیستم‌های بیومتری بر اساس مشخصه‌های فیزیکی یا رفتاری زیر عمل می‌نمایند:

- اثر انگشت
- الگوی کف دست

- هندسه دست
- الگوی شبکیه
- الگوی عنبیه
- حرکات حین امضاء
- حرکات حین تایپ دکمه‌های صفحه کلید
- تن صدا
- الگوی چهره
- مساحی دست

برای مطالعه بیشتر در خصوص روش‌های بیومتری مراجعه به منبع زیر مفید است:

<http://www.biometrics.org>

سیستم مدیریت کلمه عبور

- هر چند مکانیزم کلمه عبور در تشخیص هویت کلمه عبور بیشترین کاربرد را دارد اما این مکانیزم به عنوان ضعیف ترین و ناامن ترین مکانیزم امنیتی شناخته می‌شود. دلایل آن عبارت است:
- معمولاً افراد کلمه‌های عبوری را انتخاب می‌کنند که به آسانی حدس زده می‌شوند.
 - کلمه عبور خود را به افراد دیگر می‌دهند.
 - برای جلوگیری از فراموشی در بسیاری اوقات کلمه‌های عبور نوشته و بدون حفاظت کافی نگهداری می‌شوند.
 - اصولاً توجه به حفظ امنیت در اولویت قرار ندارد و حفاظت از کلمه عبور به عنوان یک مکانیزم امنیتی نیز بدون اهمیت تلقی می‌شود.
- بنابراین لازم است برای جلوگیری از بروز مشکلات ناشی از عدم استفاده صحیح از کلمه عبور، سیستم مدیریت کلمه عبور به اجراء گذاشته شود. هدف از اجرای مدیریت کلمه عبور اطمینان از ایجاد روشی مناسب و قابل اطمینان برای تولید، تغییر و حفظ محرمانگی کلمه عبور می‌باشد.
- در طراحی سیستم مدیریت کلمه عبور توجه به نکات زیر ضروری است:
- در صورت استفاده از روش‌های خودکار تولید کلمه عبور لازم است:
- کلمه عبور تولید شده ساده اما به حد کافی پیچیده باشد به طوری که متشکل از حروف، اعداد و علائم باشد اما بسیار طولانی نباشد.
 - کلمه عبور قابل تلفظ باشد تا بتوان آن را به خاطر سپرد.

- از کلمات موجود در فرهنگ لغات برای تولید آن استفاده نشود تا اجرای حمله **Dictionary** علیه آن غیر ممکن باشد.
- الگوریتم تولید رشته تصادفی به اندازه کافی قدرتمند باشد.
- اگر انتخاب کلمه عبور به کاربر محول شده باشد باید به هنگام انتخاب کلمه عبور کاربر مجبور به رعایت موارد زیر باشد:
- کلمه عبور متشکل از حروف غیرمرتبط با شناسه کاربری ((**USER ID**), حاوی اعداد و علائم، حاوی حروف بزرگ و کوچک و غیر قابل حدس زدن به سادگی باشد.
- امکان استفاده مجدد از کلمه عبورهای قبلی انتخاب شده توسط کاربر وجود نداشته باشد.
- کاربر ملزم به تغییر دوره‌ای کلمه عبور خود باشد.
- هنگام طراحی سیستم مدیریت کلمه عبور لازم است مکانیزمهای حفاظتی مناسبی برای جلوگیری از افشای کلمه عبور انتخاب و تعبیه شود. حمله‌های منجر به افشای کلمه عبور می‌توانند به یکی از شکل‌های زیر به اجراء گذاشته شوند:
- شنود الکترونیکی از طریق کنترل ترافیک شبکه و اطلاعات جاری در آن به‌خصوص هنگامی که یک کاربر کلمه عبور خود را به سرور احراز هویت ارسال می‌کند. در این حالت امکان دستیابی به کلمه‌های عبور رمز نشده و حتی در برخی حالت‌ها کلمه‌های عبور رمز شده وجود دارد.
- دسترسی به فایل حاوی کلمه‌های عبور که معمولاً در سرور احراز هویت نگهداری می‌شود. دسترسی غیرمجاز به این فایل می‌تواند موجب خسارت‌های بسیار شود. بنابراین لازم است این فایل به‌صورت رمزگذاری شده نگهداری شده و دسترسی به آن تحت کنترل کامل باشد.
- حمله‌های سعی مکرر ((**Brute Force**) بر اساس اقدام به ورود به سیستم با استفاده از کلمه‌های عبور ممکن ترکیب شده از حروف، علائم و اعداد مختلف و سعی برای یافتن کلمه عبور مناسب
- حمله‌های فرهنگ لغت ((**Dictionary**) استفاده از کلمه‌های موجود در فرهنگ لغات برای حدس زدن کلمه عبور و ورود به سیستم

- استفاده از جدول‌های رنگین کمانی ((Rainbow tables بر اساس سعی در استفاده از الگوهای بهم ریخته ((hash کلمه‌های عبور ممکن (مثلاً ترکیب‌های **aiA, iAl, Ail, Ali** یا **lai diA**) یا حالت‌های رمز شده کلمه‌های عبور ممکن

کنترل کلمه عبور

برای جلوگیری از حمله‌های فوق می‌توان از نرم‌افزارهای مختلفی استفاده کرد و به عنوان مثال با مقایسه کلمه عبور انتخاب شده توسط کاربر با واژه‌های موجود در فرهنگ لغات، و در صورت وجود آن در فرهنگ لغت اخطار لازم به کاربر داده شود.

رمزنگاری کلمه عبور

برای محافظت از کلمه‌های عبور ذخیره شده باید از روش رمزنگاری استفاده شود. برای این کار می‌توان از الگوریتم‌های استاندارد **MD4** یا **MD5** و یا الگوریتم‌های اختصاصی (در سازمان‌هایی که حفظ محرمانگی برای آن‌ها اهمیت زیاد دارد) استفاده کرد.

توجه : در سازمان‌هایی که از طرف سازمان پدافند غیرعامل به عنوان مراکز مهم، حساس و یا حیاتی شناخته شده‌اند استفاده از الگوریتم‌های رمز خارجی ممنوع است و لازم است از الگوریتم‌های ایرانی استفاده شود. برای کسب اطلاع در مورد الگوریتم‌های ایرانی می‌توان به انجمن رمز ایران مراجعه نمود.

در محیط ویندوز کلمه‌های عبور در بانک اطلاعاتی (**Security Account Management**) **SAM** و به صورت رمزگذاری شده نگهداری می‌شوند. برای حفاظت بهتر می‌توان از ابزار **Syskey** استفاده کرد و بانک اطلاعاتی **SAM** را با استفاده از یک کلید انتخابی رمزنگاری نمود. برای این کار می‌توان در خط فرمان دستور **Syskey** را اجرا کرد.

Syskey در سه حالت قابل استفاده است:

- Mode 1:** کلید سیستم به صورت محلی تولید، رمزگذاری و ذخیره می‌شود. در این حالت کامپیوتر را می‌توان به صورت عادی راه اندازی (**Boot**) کرده و به کار گرفت.
- Mode 2:** کلید سیستم به صورت محلی تولید، رمزگذاری و ذخیره می‌شود اما توسط کلمه عبور حفاظت می‌شود. در این حالت هنگام راه اندازی کامپیوتر لازم است کلمه عبور انتخاب شده برای **Syskey** وارد شود تا بتوان به کار پرداخت.

Mode 3: کلید سیستم تولید، رمزگذاری و بر روی یک دیسک یا CD ذخیره می‌شود. راه اندازی کامپیوتر بدون وجود این دیسکت یا CD غیرممکن است.

در محیط‌های Unix از فایل Password برای نگهداری کلمه‌های عبور رمزگذاری شده استفاده می‌شود.

توکن سخت‌افزاری مولد کلمه عبور

توکن سخت‌افزاری تولید کلمه عبور وسیله‌ای است که دارای یک نمایشگر LCD و احتمالاً یک صفحه کلید کوچک بوده و به راحتی قابل حمل می‌باشد. این وسیله در زمان‌های مختلف کلمه‌های عبور مختلفی را نمایش می‌دهد. اگر این وسیله با سیستم احراز هویت مورد استفاده در سیستم کنترل دسترسی (مثل کنترل دسترسی به یک سرور یا سرویس یا نرم‌افزار خاص) همزمان (Synchronized) شده باشد، آنگاه می‌توان از کلمه‌های عبور تولید شده توسط آن برای دسترسی به منبع مورد نظر استفاده کرد. به عنوان مثال در زمان t کلمه عبور "One time password" هنگام درخواست کاربر توسط نمایشگر توکن نمایش داده می‌شود که این کلمه عبور فقط در همان زمان t از سوی سیستم احراز هویت پذیرفتنی است و در سایر اوقات غیرقابل پذیرش خواهد بود. این نوع توکن را توکن مولد کلمه عبور همزمان شده یا (Synchronous Token Device) می‌نامند.

از توکن‌های مولد کلمه عبور می‌توان به صورت غیر همزمان نیز استفاده کرد. در این حالت اجازه دسترسی بر اساس مدل پرسش/پاسخ ((Challenge/Response صادر می‌شود که در آن هنگام ارسال درخواست دسترسی ابتدا سیستم احراز هویت رشته‌ای از کاراکترها را در اختیار کاربر قرار می‌دهد، سپس کاربر با واردکردن آن رشته به توکن پاسخ توکن را دریافت کرده و به سیستم احراز هویت وارد می‌کند. در صورتی که پاسخ داده شده معتبر باشد اجازه دسترسی به منبع مورد درخواست صادر خواهد شد. این نوع توکن، توکن مولد کلمه عبور غیر همزمان (Asynchronous Token Device) نامیده می‌شود.

SecurID یکی از راه حل‌های توکن همزمان مولد کلمه عبور می‌باشد که توسط شرکت RSA ارائه می‌شود و دارای کاربرد بسیار در سیستم‌ها و سازمان‌های مختلف است. این وسیله کلمه عبور را بر اساس زمان، تاریخ و ID کارت توکن تولید می‌کند. در مدل‌های پیشرفته‌تر برای تولید کلمه عبور لازم است PIN نیز وارد شود.

مدل عملکرد این سیستم در شکل زیر نمایش داده شده است:

- ۴- کاربر پاسخ داده شده را از طریق ایستگاه کاری وارد می‌کند.
- ۵- ایستگاه کاری پاسخ را برای سرور احراز هویت ارسال می‌نماید.
- ۶- اگر پاسخ داده شده همان باشد که سرور انتظار آن را دارد اجازه دسترسی برای کاربر صادر می‌شود. توجه شود که کلمه‌های عبور همزمان را می‌توان با استفاده از نرم‌افزار نیز تولید نمود. در این حالت توکن سخت‌افزاری مورد نیاز نیست و به آن توکن نرم‌افزاری گفته می‌شود.
- برای مطالعه بیشتر در خصوص کلمه‌های عبور یکبار مصرف که در روش‌های فوق مورد استفاده می‌شود می‌توان به منابع زیر مراجعه نمود:

RFC 2289-A One-Time Password System: <http://www.faqs.org/rfcs/rfc2289.html>

RFC 2444-The One-Time Password SASL Mechanism: <http://www.faqs.org/rfcs/rfc2444.html>

One-Time Password: http://en.wikipedia.org/wiki/one-time_password

توضیح: RFCها مستندات مکتوبی هستند که کلیه تبادلات و عملیات اینترنت بر اساس آن‌ها انجام می‌شود. تاکنون بیش از چهار هزار RFC منتشر شده است که در آن‌ها به کلیه ابعاد ارتباطات اینترنتی اعم از آدرس دهی، مسیریابی، تبادل پیام، رمزنگاری، احراز هویت، کنترل دسترسی و... پرداخته شده است. RFC خلاصه عبارت Request For Comments می‌باشد و عدد نشان داده شده در مقابل آن نشان دهنده ترتیب انتشار آن سند می‌باشد. دسترسی به متن کلیه RFCها از طریق آدرس www.faqs.org/rfcs امکانپذیر است.

کلیدهای رمزنگاری

راه دیگر اثبات هویت افراد استفاده از کلیدهای خصوصی متعلق به ایشان به منظور تولید امضای الکترونیک می‌باشد. از امضای الکترونیک می‌توان به جای کلمه عبور استفاده کرد. در مواردی که نیاز به حفاظت و امنیت بیشتر در احراز هویت می‌باشد استفاده از امضای الکترونیک پسندیده‌تر است.

کلید خصوصی عبارت است از داده‌ای سری که فقط و فقط در اختیار یک مرجع باشد. کلید خصوصی نباید نزد افراد دیگر افشاء شود. امضای الکترونیک روشی است که با استفاده از آن می‌توان محتوی یک پیام را (که قبلاً با استفاده از روش‌های مربوط تغییر شکل یافته است) با استفاده از کلید خصوصی رمزنگاری نمود. به این کار تحلیل پیام ((Message Digest گفته می‌شود. عمل رمزگذاری متن تغییر شکل یافته را امضای الکترونیکی پیام ((Digitally Signing می‌گویند. امضای الکترونیک الصاق شده به یک پیام اثبات کننده ارسال پیام از یک منبع شناخته شده است و همچنین با استفاده از آن می‌توان مطمئن بود متن پیام در مرحله انتقال از مبداء به مقصد تغییر نیافته است.

می‌توان یک کلید عمومی را برای جلوگیری از افشای کلید خصوصی افراد در کنار آن به کار گرفت. با استفاده از کلید خصوصی، کلید عمومی، امضای الکترونیک و مدل زیرساخت کلید عمومی (PKI) که جداگانه شرح داده خواهد شد، احراز هویت، حفاظت از پیام و عدم انکار ارسال یا دریافت آن امکان‌پذیر می‌شود. به‌طور کلی می‌توان گفت کلید خصوصی و امضای الکترونیک مکانیزم‌های مناسبی برای احراز هویت می‌باشند.

کارت‌های الکترونیکی

کارت‌های الکترونیکی مثل کارت‌های مغناطیسی، کارت‌های حافظه و یا کارت‌های هوشمند (Smart Card) نوع دیگری از ابزار احراز هویت هستند. استفاده از کارت‌های هوشمند امنیت بیشتری را به‌دنبال دارد.

مبحث امنیت کارت‌های هوشمند مبحث پیچیده‌ای است. انواع مختلفی از حمله علیه این مکانیزم کنترل دسترسی وجود دارد که عبارت‌اند از:

- حمله **fault generation**: استفاده از خطا در عملکرد کارت به دلیل تغییر در ولتاژ ورودی، فرکانس ساعت یا تنش حرارتی
- حمله **Side-Channel**: مطالعه عملکرد کارت شامل ولتاژهای مختلف مدار در حین کار، میدان‌های مغناطیسی ناشی از عملیات کارت، زمان انجام عملیات و...
- حمله‌های نرم‌افزاری: بررسی نرم‌افزارهای داخلی یا ترکیبی مورد استفاده برای احراز هویت توسط کارت هوشمند.

برای ایجاد امکان پذیرش کارت‌های هوشمند صادر شده یک سازمان به وسیله سازمان‌های دیگر (مثل پذیرش کارت هوشمند صادر شده توسط بانک A در دستگاه ATM بانک B) استاندارد ISO/IEC 14443 به شرح زیر تدوین شده است:

- ISO/IEC 14443-1 مشخصه‌های فیزیکی
- ISO/IEC 14443-2 فرمت بندی و اجتناب از تداخل
- ISO/IEC 14443-1 پروتکل‌های تبادل

برای مطالعه بیشتر در خصوص کارت‌های هوشمند می‌توان به منبع زیر مراجعه نمود:

Smart Card Alliance home page: www.smartcardalliance.org

تقویض اختیار (احراز صلاحیت)

پس از احراز هویت متقاضی دسترسی نوبت به بررسی حدود اختیارات وی می‌رسد. این مرحله به منظور تعیین منابع و نوع دسترسی کاربر به آن‌ها می‌باشد.

حدود دسترسی

عواملی را که می‌توان در تعیین حدود دسترسی مورد استفاده قرار داد می‌توان به شرح زیر فهرست کرد:

- گروه یا رده سازمانی که کاربر به آن وابستگی دارد.
- محل فیزیکی یا منطقی کاربر متقاضی دسترسی
- زمان درخواست دسترسی
- نوع تبادل یا فرآیندی که تقاضا از طریق آن ارسال شده است.
- تنظیم مقدار اولیه در حالت No Access
- تحدید دسترسی به "آنچه که لازم است (Need to know)"
- استفاده از Thin Client به جای PC برای حذف فلاپی، CD، پورت USB و غیره.

مدل‌های کنترل دسترسی

مدل‌های کنترل دسترسی مورد استفاده در خصوص تصمیم‌نهایی اعطای دسترسی به یک منبع خاص برای یک کاربر احراز هویت شده را می‌توان در قالب سه مدل زیر دسته‌بندی کرد:

- ۱- Discretionary Access Control (DAC) که در آن مالک اطلاعات در خصوص اعطای دسترسی به متقاضی تصمیم‌گیری می‌نماید و اینکار را از طریق استفاده از ACL (Access Control List) به انجام می‌رساند.
 - ۲- Mandatory Access Control (MAC) که در آن سیستم عامل با استفاده از جدول‌های امنیت، سیاست‌گذاری امنیتی را اعمال می‌نماید.
 - ۳- Role-based Access Control (RBAC) که در آن تصمیم‌گیری در مورد اعطای دسترسی بر اساس وظیفه (Role) متقاضی دسترسی و جایگاه سازمانی وی انجام می‌شود. در این مدل هویت متقاضی مورد توجه قرار نمی‌گیرد.
- برای دسترسی به اطلاعات بیشتر در خصوص مدل‌های کنترل دسترسی می‌توان به منبع زیر مراجعه نمود:

Access Control: <http://foundation.bricksfactory.org/deliverables/d353/ar01S06.html>

فهرست‌های کنترل دسترسی

فهرست‌های کنترل دسترسی یا (Access Control Lists) ACLs در بسیاری از سیستم‌های عامل، برنامه‌های کاربردی و مسیریاب‌ها (Routers) به کار گرفته می‌شوند. این فهرست‌ها حاوی لیست نهاده‌ها (Subjects) و موضوع‌ها (Objects) و نوع دسترسی مجاز هر نهاده به هر موضوع می‌باشند. همچنین ممکن است برای تعریف حق دسترسی از نام گروه‌ها به جای نام نهاده‌ها استفاده شود. ACL نگاشت مقادیر ماتریس کنترل دسترسی به ازای هر موضوع می‌باشد. یک نمونه از ماتریس کنترل دسترسی در شکل زیر نمایش داده شده است:

موضوع‌ها (منابع)					
فایل ۴	فایل ۳	فایل ۲	فایل (منبع) ۱	حسن	مدیران بخش‌ها
Full Control	Read	Read, Write	Read	احمد	
Read	No Access	No Access	No Access	بیژن	
Read	Read	Read	Read	نسرين	
Read, Write	Read, Write	Read, Write	Read, Write	مدیران بخش‌ها	
Full Control	Read	Full Control	Full Control		

انواع دسترسی: خواندن Read، نوشتن Write، اجراء execute، حذف Delete، کنترل کامل Full

Control، عدم دسترسی No Access

توانایی (حقوق) هر کاربر: سطر ماتریس

ACL هر منبع: ستون ماتریس

لایه‌های کنترل دسترسی

کنترل دسترسی را از لحاظ اجرایی می‌توان مشتمل بر سه لایه مدیریتی، تکنیکی و فیزیکی دانست. هر لایه دارای مکانیزم‌های کنترلی متفاوتی است که می‌توان به صورت نرم‌افزاری یا سخت‌افزاری به کار گرفت. لازم است اجزای مختلف این سه لایه در هماهنگی کامل با هم باشند تا بتوان امنیت زیرساخت پردازشی و داده‌های جاری در آن را برقرار ساخت. هر لایه دارای اجزای مختلفی به شرح زیر است:

• الف- کنترل‌های مدیریتی

- سیاست‌گذاری و فرآیندهای امنیتی
- کنترل پرسنل

- ساختار نظارتی
- آموزش و اطلاع رسانی امنیتی
- آزمایش وضعیت امنیتی
- ب- کنترل‌های فیزیکی
 - جداسازی شبکه‌ها
 - امنیت پیرامونی
 - کنترل کامپیوترها
 - جداسازی محیط‌های کاری از یکدیگر
 - تهیه نسخه پشتیبان از داده‌ها و اطلاعات
 - امنیت کابل کشی
 - گشت محلی
- ج- کنترل‌های تکنیکی
 - دسترسی سیستم
 - معماری شبکه
 - دسترسی شبکه
 - رمزنگاری و پروتکل‌های ارتباطی
 - ممیزی

مدیریت متمرکز کنترل دسترسی

در سیستم مدیریت متمرکز کنترل دسترسی، به‌طور کلی یک مرجع (بخش یا فرد خاص) مسؤول نظارت بر دسترسی به کلیه منابع موجود در شبکه یا سازمان می‌باشد. این مرجع (مدیر امنیتی) وظایف زیر را به عهده دارد:

- پیکربندی مکانیزم‌های اعمال سیاست‌های کنترل دسترسی
 - اعمال تغییر در پروفایل‌های دسترسی کاربران
 - ابطال حق دسترسی در مواقع نیاز یا حذف کامل آن
- این روش به منظور افزایش کارایی، یکنواخت سازی و تمرکز فعالیت‌های کنترل دسترسی به دلیل سپردن آن به یک مرجع، به کار گرفته می‌شود. به دلیل تمرکز کلیه فعالیت‌ها نزد یک مرجع ممکن است این روش باعث کند شدن سرعت فعالیت‌ها شود.

احراز هویت، احراز صلاحیت، پاسخگویی

AAA²⁴ مدل کنترل دسترسی کامل مبتنی بر سه محور اصلی کنترل دسترسی احراز هویت،

احراز صلاحیت و پاسخگویی در شبکه می‌باشد و دارای عملکرد زیر است:

۱- احراز هویت (تعیین اعتبار)²⁵

در این بخش هویت کاربری که قصد استفاده از منابع شبکه را دارد مورد بررسی قرار می‌گیرد. در ساده ترین و معمولی ترین حالت، ابزار شناسایی شامل کلمه عبور و نام کاربری است. در صورت نیاز می‌توان از عناصر شناسایی دیگر یا به‌طور کلی هویت دیجیتال نیز استفاده کرد که در این صورت نوع سرویس دهنده، بانک‌های اطلاعاتی و در مواردی پروتکل‌ها و استانداردها نیز مطابق تغییرات اعمال شده در نظر گرفته می‌شوند. عموماً در شبکه‌هایی با حجم کم و متوسط عمل تعیین اعتبار توسط مسیریاب‌ها و فایروال‌ها صورت می‌گیرد ولی در شبکه‌های بزرگ و پیچیده معمولاً سرویس دهنده مجزایی برای این منظور در نظر گرفته می‌شود که از استانداردها و پروتکل‌هایی مانند TACACS+ و RADIUS که در ادامه شرح داده خواهند شد استفاده می‌کنند.

برای استفاده از این ویژگی نیاز به فعال کردن **Authentication** روی تجهیزات مورد استفاده در

شبکه است که عموماً در چهار مرحله صورت می‌گیرد:

- فعال کردن AAA روی سخت‌افزارهای مورد نظر
- ایجاد بانک اطلاعاتی حاوی کلمه عبور و نام کاربران یا تجهیزات شبکه
- ایجاد فهرست‌هایی برای تعیین روش مورد نظر در تعیین اعتبار
- اعمال فهرست‌های ایجاد شده در مرحله قبل

۲- احراز صلاحیت (اعطای مجوز)²⁶

Authorization فرآیندی است که طی آن به کاربران و یا تجهیزات متقاضی دسترسی به منابع،

امکان استفاده از منبع یا منابع مستقر در شبکه داده می‌شود. به عبارت دیگر این عمل برای مدیران

²⁴ - AAA (Authentication, Authorization, Accounting)

²⁵ - Authentication

²⁶ - Authorization

شبکه امکان تعیین نوع دسترسی به هر یک از منابع شبکه را برای تک تک متقاضیان دسترسی و یا گروهی از آن‌ها فراهم می‌کند.

از سوی دیگر، عمل اعطای آدرس‌های شناخته شده و از پیش تعیین شده به کاربران یا تجهیزات، مانند افرادی که با استفاده از پروتکل PPP به شبکه متصل می‌شوند را انجام می‌دهد. اگر این ویژگی تجهیزات شبکه فعال باشد سرویس دهنده درخواست‌های کاربر برای دسترسی به منابع و تجهیزات شبکه را با اطلاعات ثبت شده در بانک اطلاعاتی مقایسه می‌کند و مطابق با مجوزهای تعیین شده برای هر کاربر دسترسی وی به منابع و تجهیزات شبکه را فراهم می‌کند و یا مانع از دسترسی وی به آن منابع می‌شود.

برای استفاده از این ویژگی باید عامل **Authentication** فعال شده باشد. مرحله‌ای که باید صورت گیرد عبارت‌اند از:

- فعال کردن AAA روی تجهیزات و فعال کردن **Authentication**
- ایجاد فهرست‌هایی مبنی بر روش انجام **Authorization**
- اعمال فهرست‌های ایجاد شده

۳- پاسخگویی (تهیه گزارش عملکرد کاربر)^{۲۷}

آخرین بخش از فرآیند AAA، تهیه گزارش از عملکرد کاربران یا سخت‌افزارهایی است که هویت آن‌ها در مراحل قبلی تأیید شده است. پیام‌های **Accounting** به شکل رکوردهای اطلاعاتی، میان تجهیزاتی که از طریق آن‌ها دسترسی متقاضی درخواست شده و پایگاه‌های داده‌ای کنترل دسترسی از قبیل **RADIUS** یا **TACACS+** تبادل می‌شود. فرآیند استفاده از این ویژگی شبیه مرحله **Authorization** است.

²⁷ - Accounting

دستورات AAA در سیستم‌ها و تجهیزات CISCO

به عنوان نمونه‌ای از روش اعمال AAA می‌توان به مواد زیر توجه کرد:

۱- دستورات Accounting

ساختار کلی دستور :

```
aaa accounting {auth-proxy | system | network | exec | connection | commands level} {default | list-name} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] group group-name
```

```
no aaa accounting {auth-proxy | system | network | exec | connection | commands level} {default | list-name} [vrf vrf-name] [broadcast] group group-name
```

در جدول‌های زیر نیز پارامترهای مربوط به دستورها شرح داده شده‌اند.

(جدول ۱)

کلمات کلیدی و پارامترها	توضیح
Auth-proxy	ارائه اطلاعاتی در مورد تمام رویدادهای مربوط به کاربران تعیین اعتبار شده.
System	اجرای Accounting برای تمام رویدادهای سطح سیستمی که به کاربران وابسته نیستند (مانند دستور Reload در روتر).
Network	اجرای Accounting برای تمام درخواست‌های مربوط به سرویس‌های شبکه مانند ARAP, PPP, SLIP
Exec	اجرای Accounting برای نشست‌های EXEC shell
Connection	ارائه اطلاعاتی در مورد کلیه ارتباطات خارجی که از سوی Access Server ایجاد می‌شود مانند Telnet, R Login و...
Command level	اجرای Accounting برای تمام دستورات در سطح ممتاز. سطح مجاز عددی بین صفر تا ۱۵ است که سطح دسترسی و اجرای دستورات روی سیستم توسط کاربر را مشخص می‌کند.
Default list-name	استفاده از روش‌های Accounting لیست شده که آرگومان List-name نام این لیست را مشخص می‌کند. (جدول شماره ۲)
vrf vrf-name	(اختیاری) تعیین مسیر مجازی برای ارسال. (فقط در Accounting استفاده می‌شود).
Start-stop	پیغامی مبنی بر آغاز یا پایان Accounting راهنگام آغاز یا پایان فرآیند ارسال

توضیح	کلمات کلیدی و پارامترها
می‌کند.	
پیغامی مبنی بر پایان Accounting هنگام پایان فرآیند ارسال می‌کند.	Stop- only
سرویس Accounting را روی یک خط یا کارت واسط شبکه غیر فعال می‌کند.	None
(اختیاری) امکان ارسال رکوردهای اطلاعاتی مربوط به Accounting را برای چند سرور AAA فراهم می‌کند. به طور همزمان رکوردهای Accounting به اولین سرور هر گروه فرستاده می‌شود. اگر اولین سرور قابل دسترس نباشد می‌توان از سرور پشتیبان استفاده کرد.	Broad cast
حداقل یکی از کلمات کلیدی که در جدول ۲ آمده است در این قسمت تنظیم می‌شود.	Group group-name
توجه: AAA Accounting به طور پیش فرض غیر فعال است.	

(جدول ۲)

توضیح	کلمات کلیدی و پارامترها
استفاده از تمام سرورهای RADIUS برای تعیین اعتبار که توسط دستور زیر تعریف شده است: aaa group server radius	Group radius
استفاده از تمام سرورهای TACACS+ برای تعیین اعتبار که توسط دستور زیر تعریف شده اند: aaa group server TACACS+	Group TACACS+
استفاده از یک زیر مجموعه از سرورهای RADIUS یا TACACS+ که توسط group-name تعیین می‌شوند.	Group group-name
توجه: در صورتی که تنها یک سرور وجود داشته باشد از دستورات زیر استفاده می‌شود: Radius-server host TACACS-server host	

نکته - از دستور زیر برای فعال کردن **AAA** روی سیستم‌ها استفاده می‌شود :

aaa new-model

۲- دستورات Authentication

(جدول ۳)

دستور	توضیح
aaa authentication attempts login number of attempts	با این دستور تعداد دفعاتی که روتر امکان وارد کردن نام و کلمه عبور کاربر را قبل از قطع نشست فراهم می‌کند مشخص می‌شود.
aaa authentication banner string	برای نمایش یک پیغام در هنگام ورود کاربر به سیستم از این دستورات استفاده می‌شود.
aaa authentication enable default method 1 [method2...]	از این دستور برای ایجاد روش‌های تعیین اعتبار که امکان دسترسی کاربر به دستورات سطح ممتاز را فراهم می‌کند استفاده می‌شود. (این روش‌ها در جدول شماره ۴ مشخص شده است)
aaa authentication fail-message string	از این دستور برای نمایش یک پیغام در هنگام عدم موفقیت کاربر برای ورود به سیستم استفاده می‌شود.
aaa authentication login {default list-name} method1 [method2...]	از این دستور برای تنظیم AAA برای Login به سیستم استفاده می‌شود. با استفاده از کلمه Default، روش‌های تعیین اعتبار که در لیست تعیین شده‌اند مورد استفاده قرار می‌گیرند. برای Method هم باید حداقل یکی از کلمات کلیدی که در جدول شماره ۵ آمده است مورد استفاده قرار گیرد.
aaa authentication password-prompt text- string	برای تغییر متن نمایش داده شده در هنگام تلاش کاربر برای وارد کردن کلمه عبور.
aaa authentication username-prompt text- string	برای تغییر متن نمایش داده شده در هنگام تلاش کاربر برای وارد کردن نام کاربری.
aaa authentication ppp {default list-name} method1 [method2...]	برای تعیین روش‌های تعیین اعتبار برای کاربرانی که به وسیله پروتکل PPP به سیستم وارد می‌شوند. روش‌ها در جدول شماره ۶ مشخص شده‌اند.

(جدول ۴)

روش‌های تعیین اعتبار (enable methods)

توضیح	کلمات کلیدی
استفاده از کلمه عبور برای ورود به سطح ممتاز ((Privilege mode	Enable
برای استفاده از کلمه عبور تعیین شده برای Line به منظور تعیین اعتبار	Line
عدم استفاده از تعیین اعتبار	None
استفاده از تمام سرورهای تعیین شده در لیست سرورهای RADIUS نکته: روش Radius برپایه تک کاربری کار نمی‌کند.	group radius
استفاده از تمام سرورهای تعیین شده در لیست سرورهای TACACS+	group TACACS+
استفاده از یک زیر مجموعه از سرورهای Radius یا TACACS+ برای تعیین اعتبار که به وسیله دستورات زیر تعیین می‌شوند. aaa group server Radius aaa group server TACACS+	group group-name

(جدول ۵)

روش‌های تعیین اعتبار (login methods)

توضیح	کلمات کلیدی
استفاده از کلمه عبور تعیین شده برای ورود به سطح ممتاز	Enable
استفاده از پروتکل Kerberos5 برای تعیین اعتبار	Krb5
استفاده از پروتکل Kerberos5 برای تعیین اعتبار کاربرانی که از طریق Telnet به روتر وصل می‌شوند.	Krb5-telnet
استفاده از کلمه عبور تعیین شده برای Line به منظور تعیین اعتبار	Line
استفاده از نام‌های کاربری موجود در بانک اطلاعاتی محلی روی سیستم برای تعیین اعتبار	Local
استفاده از نام‌های کاربری محلی که نسبت به بزرگ و کوچک بودن حروف حساس هستند.	Local-case
عدم استفاده از روش‌های تعیین اعتبار	None
استفاده از سرورهای موجود در لیست سرورهای Radius	Group Radius
استفاده از سرورهای موجود در لیست سرورهای TACACS+	Group Tcacacs+
استفاده از یک زیر مجموعه از سرورهای Radius یا TACACS+ برای تعیین اعتبار کاربران	Group group-name

(جدول ۶)

روش‌های تعیین اعتبار (ppp methods)

کلمه کلیدی	توضیح
If-needed	اگر کاربر قبلاً روی یک خط tty تعیین اعتبار شده باشد دیگر تعیین اعتبار نمی‌شود.
Krb5	استفاده از kerberos5 برای تعیین اعتبار (فقط برای تعیین اعتبار کلمات عبور (PAP) استفاده می‌شود.
Local	استفاده از نام کاربر محلی برای تعیین اعتبار
Local-case	استفاده از نام کاربر محلی که نسبت به بزرگ و کوچک بودن حروف حساس هستند.
None	عدم استفاده از تعیین اعتبار
Group Radius	استفاده از سرورهای موجود در لیست سرورهای Radius
Group TACACS+	استفاده از سرورهای موجود در لیست سرورهای TACACS+
Group group-name	استفاده از یک زیر مجموعه از سرورهای Radius یا TACACS+ برای تعیین اعتبار کاربران

۳- دستورات Authorization

ساختار کلی دستور:

```
aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} method1 [method2...]
```

```
no aaa authorization {network | exec | commands level | reverse-access | configuration | default | list-name}
```

(جدول ۷)

کلمات کلیدی و پارامترها	توضیح
Network	اجرای فرآیند Authorization برای تمام سرویس‌های درخواستی مرتبط با شبکه مانند PPP, SLIP, ...
Exec	اجرای فرآیند Authorization برای تعیین این‌که آیا کاربر مجاز به اجرای exec Shell روی سیستم هست یا خیر؟
Commands	اجرای Authorization برای تمام دستورات در سطح ممتاز

توضیح	کلمات کلیدی و پارامترها
تعیین سطح دسترسی که مجاز هستند	<i>Level</i>
اجرای Authorization برای ارتباط دسترسی معکوس مانند یک Telnet معکوس	<i>Reverse-access</i>
برای کپی کردن پیکربندی از یک سرور AAA	<i>Configuration</i>
استفاده از روش‌های اعطای مجوز که در یک لیست مشخص شده است.	<i>Default</i>
نام لیست حاوی روش‌های اعطای مجوز	<i>List-name</i>
یکی از کلمات کلیدی که در جدول شماره ۷ آمده است.	<i>Method 1 [method 2...]</i>

(جدول ۸)

توضیح	کلمات کلیدی و پارامترها
استفاده از زیر مجموعه‌ای از سرورهای Radius و TACACS+ برای تعیین اعتبار کاربران.	<i>Group group-name</i>
به کاربرانی که تعیین اعتبار شده باشند اجازه دسترسی به فعالیت‌های درخواستی را می‌دهد.	<i>If-authenticated</i>
استفاده از نمونه تعریف شده به وسیله دستور Kerberos instance map.	<i>Krb5-instance</i>
استفاده از بانک اطلاعاتی محلی برای تعیین مجوزها.	<i>Local</i>
هیچ فرآیند تعیین مجوزی صورت نمی‌گیرد.	<i>None</i>

سایر دستورهای مهم Authorization

توضیح	دستور
برای اعمال فرآیند تعیین مجوز برای ارتباطاتی که از طریق کنسول صورت می‌گیرد.	aaa authorization console
برای پیکربندی یک سرور دسترسی به شبکه (NAS) برای درخواست اطلاعات پیکربندی از یک سرور امنیتی قبل از این‌که به کاربران اجازه برقراری یک نشست Telnet به صورت معکوس داده شود. نکته: یک نشست Telnet معکوس در جهت مخالف از داخل شبکه به یک سرور NAS در محدوده شبکه برای دسترسی به مودم‌ها یا سایر ابزار مرتبط با NAS برقرار می‌شود.	aaa authorization reverse-access {group radius group TACACS+}
از این دستور برای تعیین یک نام کاربری غیر از نام روتر و کلمه عبوری مطمئن‌تر از مقدار پیش فرض آن (Cisco) استفاده می‌شود. عدد صفر کلمه عبور را رمزگذاری نمی‌کند ولی عدد ۷ آن را رمزگذاری می‌کند.	aaa configuration route username username [password [0 7] password]

کربروس (Kerberos)

کربروس یک پروتکل احراز هویت است که در سالهای میانی دهه ۸۰ میلادی به عنوان بخشی از پروژه آتن دانشگاه MIT طراحی شده است. این مکانیزم بر اساس مدل Client/Server عمل کرده و مبتنی بر رمزنگار کلید متقارن می‌باشد. مدت مدیدی است که از این پروتکل در سیستم‌های Unix استفاده شده است و هم اکنون نیز به عنوان روش پیش فرض احراز هویت در سیستم عامل‌های Windows 2000 و Windows 2003 مورد استفاده قرار می‌گیرد.

کربروس را می‌توان به عنوان مثالی از مدل Single-Sign-On در محیط‌های توزیع شده معرفی کرد. این متد قابلیت‌های توسعه پذیری ((Scalability، شفافیت ((Transparency، پایایی ((Reliability و امنیت را فراهم می‌آورد.

پروتکل Kerberos یکی از پروتکل‌های بسیار مطمئن و امن برای تعیین اعتبار در شبکه به شمار می‌رود. این پروتکل برخلاف سایر پروتکل‌ها (مانند NTLM) که تنها سرویس گیرنده را تعیین اعتبار می‌نماید، اعتبار سنجی دو طرفه را برای سرورها و سرویس گیرنده‌ها فراهم می‌نماید. این پروتکل بر اساس استانداردهای موجود در بحث تعیین اعتبار پیاده‌سازی شده است. بنابراین محدود به یک Platform و سیستم عامل خاص نیست. این پروتکل برای انجام اعتبار سنجی از کلید رمزنگاری متقارن که بین کاربر و کامپیوتر به اشتراک گذاشته می‌شود استفاده می‌کند. در مکانیزم رمزنگاری متقارن تنها از یک کلید سری مشترک برای رمزنگاری و رمزگشایی اطلاعات استفاده می‌شود. (الگوریتم مورد استفاده DES می‌باشد)

مرکز انتشار کلید^{۲۸}

تکنولوژی Kerberos از سه بخش تشکیل شده است:

- سرویس گیرنده
- سرور
- مرجع معتبر انتشار کلید (KDC)

KDC پایگاه داده‌ای از کلیه اطلاعات مربوط به نهاده‌ها در قلمرو Kerberos را نگهداری می‌نماید. این نهاده‌ها دارای اسامی منحصر به فردی در ارتباطات شبکه هستند.

²⁸ - Key Distribution Center

از آنجایی که سیستمی که سرویس KDC را اجرا می‌کند دارای پایگاه داده‌ای با اطلاعات مهم (Account) امنیتی می‌باشد، باید از نظر فیزیکی ایمن باشد. بخشی از این اطلاعات امنیتی، کلید سری است که بین یک نهاد و KDC مشترک است. هر نهاد، کلید سری مربوط به خود را دارد که بسیار مستحکم است. به همین دلیل به این کلید، کلید دراز مدت نیز می‌گویند. کلیدی که بریک نهاد مانند کاربر استوار باشد، از کلمه عبور کاربر مشتق می‌شود. این کلید متقارن است. کلید دیگری که به همراه KDC مورد استفاده قرار می‌گیرد، کلید نشست است که وقتی یک نهاد می‌خواهد با نهاد دیگر ارتباط برقرار کند KDC آن را صادر می‌کند.

به عنوان مثال وقتی یک سرویس گیرنده بخواهد با یک سرور ارتباط برقرار کند، درخواست خود را به KDC می‌فرستد و KDC کلید نشست صادر می‌کند تا سرور و سرویس گیرنده بتوانند هویت یکدیگر را تأیید کنند. این کلید طول عمر محدودی دارد و به این دلیل برای یک نشست Login (ورود به سیستم) مناسب است. پس از پایان نشست Login کلید نشست دیگر معتبر نیست و برای برقراری مجدد باید کلید نشست جدیدی ایجاد شود.

مراحل فرآیند تعیین اعتبار با استفاده از پروتکل Kerberos

پروتکل کربروس علاوه بر سرور تشخیص هویت از سرور دیگری تحت عنوان سرور اعطا کننده بلیت (TGS)^{۲۹} استفاده می‌کند. سرور تشخیص هویت (AS)^{۳۰}، هویت کاربری که وارد شبکه شده است را تشخیص می‌دهد و تا زمانی که از شبکه خارج نشده این تشخیص هویت اعتبار دارد. در ادامه برای استفاده از یک سرور خاص، کاربر از TGS درخواست بلیت می‌کند و دیگر نیازی به وارد کردن رمز عبور ندارد. روند عملیات ارتباط بین سرویس گیرنده، سرور (AS) و سرور TGS شامل مراحل زیر است:

مرحله اول :

در این مرحله دو پیام بین سرویس گیرنده و سرور (AS) تبادل می‌شود که طی آن هویت کاربر توسط سرور شناسایی و بلیتی جهت استفاده از TGS صادر می‌شود. در پیام اول سرویس گیرنده

^{۲۹} - Ticket Granting Server

^{۳۰} - Authentication Server

درخواست صدور بلیت جهت استفاده از TGS را می‌نماید، در واقع کاربر هنگام ورود به شبکه با وارد کردن رمز عبور خود این درخواست را از سرور تشخیص هویت (AS) می‌نماید.

در این پیام کاربر شناسه خود (ID)، شناسه سرور اعطا کننده بلیت (TGS) که قصد گرفتن بلیت جهت استفاده از آن را دارد به همراه یک Time stamp به سرور AS ارسال می‌کند، AS نیز پیامی رمز شده با استفاده از کلید استخراج شده از کلمه عبور کاربر برای سرویس گیرنده ارسال می‌کند.

این پیام حاوی اطلاعات زیر است:

- کلید نشست برای ارتباط بین سرویس گیرنده و سرور (TGS) که داده‌های ارسالی بین آن‌ها با استفاده از این کلید به رمز می‌شود. این کلید تا زمانی که کاربر در شبکه حضور داشته باشد معتبر است و به صورت کاملاً امن به دست سرویس گیرنده می‌رسد.
- شناسه TGS که بلیت برای استفاده از آن صادر شده است. این شناسه در مواردی مفید است که در شبکه چندین AS و TGS وجود داشته باشد و از طریق آن می‌توان تشخیص داد که بلیت برای کدام TGS صادر شده است.
- یک Time stamp که مدت زمان اعتبار کل پیام دوم را مشخص می‌کند.
- یک Time stamp دیگر که مدت اعتبار بلیتی که برای استفاده از TGS صادر شده است را مشخص می‌کند.
- بلیتی که برای استفاده از TGS توسط AS صادر شده است. خود این بلیت توسط کلیدی که قبلاً به صورت امن بین سرور AS و TGS به اشتراک گذاشته شده است رمز می‌شود. در نتیجه سرویس گیرنده قادر به تغییر محتویات بلیت نخواهد بود.

محتویات بلیت Kerberos عبارت‌اند از :

- کلید نشست که در پیام نیز قرار داده شده است. این کلید در اختیار سرور TGS نیز قرار می‌گیرد. چراکه در نهایت بلیت به TGS ارسال می‌شود.
- شناسه کاربری که بلیت برای وی صادر شده است.
- آدرس شبکه سیستمی که کاربر از طریق آن درخواست خود را به سرور AS ارسال کرده است.

- شناسه سرور TGS، با استفاده از این شناسه سرور مطمئن می‌شود که بلیت برای اوست و به درستی آن را از حالت رمز خارج کرده است.
- یک Time stamp برای تعیین مدت زمان اعتبار پیام درخواست بلیت.
- مقداری که طول عمر بلیت را مشخص می‌کند.

نکته قابل توجه در مرحله اول این است که در تبادل دو پیام رد و بدل شده، کلمه عبور کاربر در شبکه منتقل نمی‌شود و امکان شناسایی آن به حداقل می‌رسد و این مسأله از نظر امنیتی بسیار قابل توجه است.

مرحله دوم:

در این مرحله دو پیام بین سرویس گیرنده و سرور TGS رد و بدل می‌شود. وقتی سرویس گیرنده‌ای می‌خواهد برای اولین بار از سروری استفاده نماید این دو پیام تبادل می‌شود و طی آن بلیتی برای استفاده از یک سرور به سرویس گیرنده اعطا می‌شود.

در مراجعات بعدی نیازی به چالش مجدد جهت تعیین اعتبار نیست، مگر این‌که طول عمر بلیت تمام شده باشد. روال کار به این صورت است که سرویس گیرنده بلیتی را که از AS گرفته به TGS می‌فرستد و بلیت سرور خاصی را از TGS درخواست می‌کند و TGS هم پس از انجام ارزیابی‌های لازم و اطمینان از هویت کاربر و مجاز بودن وی جهت دسترسی به سرور مورد نظر، بلیت را صادر می‌کند.

در پیام اول این مرحله سرویس گیرنده شناسه سرور مقصد را جهت صدور بلیت به TGS ارسال می‌کند و همراه آن بلیتی را که در مرحله قبل از سرور تشخیص هویت (AS) دریافت کرده به‌همراه یک بسته اطلاعاتی تحت عنوان Authenticator (رمز شده با کلید نشست اخذ شده در مرحله قبل از سرور AS) ارسال می‌کند.

این بسته اطلاعاتی حاوی شناسه کاربر، آدرس شبکه‌ای سرویس گیرنده و یک Time stamp می‌باشد.

Time stamp مربوط به Authenticator بر خلاف بلیت‌ها بگونه‌ای است که فقط یک بار می‌توان از آن استفاده کرد و در صورتی که سرویس گیرنده نیازمند ارسال مجدد Authenticator باشد لازم است Time stamp آن عوض شود. سرور TGS بعد از دریافت اطلاعات، بلیت را با استفاده از کلیدی که قبلاً بین TGS و AS به اشتراک گذاشته شده از رمز خارج می‌کند.

در ادامه هم با کلید نشستی که داخل بلیت است بسته اطلاعاتی **Authenticator** را از رمز خارج می‌کند و سپس شناسه کاربر، آدرس شبکه‌ای سرویس گیرنده را با داده‌های معادل در بلیت و همچنین با آدرس فرستنده پیام به منظور تطابق مقایسه می‌کند. ضمناً اعتبار زمانی بلیت و **Authenticator** را نیز کنترل می‌کند. در نهایت کنترل می‌کند که بلیت برای استفاده از این **TGS** صادر شده باشد.

در صورت صحت تمام موارد و وجود مجوز استفاده از سرور مورد نظر سرویس گیرنده، در پیامی دیگر سرور **TGS** بلیتی به منظور برقراری ارتباط با سرور به سرویس گیرنده ارسال می‌کند. این پیام به وسیله کلید نشستی که در مرحله قبل بین **TGS** و سرویس گیرنده به اشتراک گذاشته شده به رمز در می‌آید. این پیام شبیه پیام دوم در مرحله اول است با این تفاوت که در آن بلیت و کلید نشستی جهت استفاده از سرور مورد نظر به سرویس گیرنده ارسال می‌شود. این بار بلیت ارسالی به سرویس گیرنده توسط کلیدی که قبلاً بین **TGS** و سرور به صورت امن به اشتراک گذاشته شده رمز می‌شود و لذا باز هم سرویس گیرنده قادر به تغییر دادن محتویات بلیت نیست و فقط آن را جهت استفاده دریافت می‌کند.

مرحله سوم :

این مرحله در هر بار اتصال سرویس گیرنده و سرور انجام می‌شود و طی آن سرویس گیرنده، بلیت و بسته اطلاعاتی **Authenticator** را به سرور ارسال می‌کند ولی این بار **Authenticator** با استفاده از کلید نشستی که طی مرحله قبل به دست سرویس گیرنده رسیده رمز می‌شود (این کلید داخل بلیت برای سرور هم ارسال می‌شود). سرور بعد از دریافت پیام و کنترل صحت و سقم آن در پیامی دیگر هویت خود را به سرویس گیرنده اثبات می‌کند.

سرویس‌های ارائه شده توسط KDC

وظایف خود را بین دو سرویس تقسیم می‌کند. یکی از آن‌ها سرویس تعیین اعتبار (**AS**) است که برای انتشار بلیت اعطای بلیت (**TGT**)^{۳۱} به کار می‌رود و سرویس اعطای بلیت (**TGS**) که برای صادر کردن بلیت‌های نشست به کار می‌رود.

³¹ - **Ticket Granting Ticket**

در واقع سرویس گیرنده برای اولین بار که با KDC تماس برقرار می‌کند با AS در ارتباط است و وقتی که نیاز داشته باشد که با سروری خاص ارتباط برقرار کند، بلیت اعطای بلیت که توسط AS صادر شده به سوی TGS می‌فرستد تا بتواند یک بلیت نشست برای برقراری ارتباطات با سرور خاص دریافت کند.

زیر پروتکل‌های Kerberos

- **Kerberos**، سه زیر پروتکل دارد که **Exchange** (تبادل) نیز نامیده می‌شوند و عبارت‌اند از:
Authentication Service (AS) Exchange: این زیر پروتکل برای صادر کردن یک کلید نشست **Logon** و **TGT** برای سرویس گیرنده مورد استفاده قرار می‌گیرد.
- **TGS Exchange**: این زیر پروتکل برای صادر کردن یک کلید نشست سرور و یک بلیت نشست مربوط به سرور برای سرویس گیرنده مورد استفاده قرار می‌گیرد.
- **CS Exchange**: این زیر پروتکل هنگامی که سرویس گیرنده بلیت نشست را به سرور می‌فرستد به کار می‌رود.

بلیت‌ها

بلیت‌ها، قلب سیستم اعتبارسنجی **Kerberos** هستند. پیام‌های مختلفی برای درخواست کردن و فرستادن بلیت بین نهاده‌ها به کار می‌روند. محتوای این بلیت‌ها در جدول زیر درج شده است.

جدول محتویات بلیت Kerberos

نام فیلد	محتویات فیلد
Ticket Version	شماره نسخه بلیت
Realm Name	اسم محدوده عملکرد پروتکل Kerberos
Server Name	اسم سرور هدف
Flags	گزینه‌هایی برای بلیت
Key	کلید نشست
Client Realm	محدوده اولیه‌ای که اعتبارسنجی را انجام داده است
Client Name	نام سرویس گیرنده

نام فیلد	محتویات فیلد
Transited	اسم محدوده‌هایی که بلیت از آن عبور کرده است
Authentication Time	زمان ایجاد بلیت
Start Time	زمان شروع اعتبار بلیت
End Time	زمان انقضای بلیت
Renew Till Time	زمانی که بلیت مطلقاً منقضی می‌شود
Client Address	آدرس‌های معتبر برای سرویس گیرنده
Authentication Data	داده‌های مجوز دهی برای سرویس گیرنده
Extensions	فیلد اختیاری برای استفاده از داده‌های خاص برنامه

ضعف‌های کربروس

با توجه به اینکه کربروس به عنوان روش پیش فرض احراز هویت در سیستم عامل‌های پر استفاده خانواده Windows مورد استفاده قرار می‌گیرد، آگاهی از ضعف‌های این روش ضروری است.

برخی از آسیب پذیری‌های شناخته شده روش کربروس در زیر شرح داده شده است:

- اگر KDC از سرویس خارج شود دسترسی به منابع حفاظت شده توسط کربروس غیر ممکن می‌شود. بنابراین لازم است از طریق ایجاد Redundancy با این وضع مقابله شود.
- لازم است KDC به نحوی پیکربندی شود که بتواند پاسخگوی حجم درخواست‌های دریافت شده باشد. پاسخگویی باید در زمان قابل قبول ارائه شود.
- کلیدهای سری به صورت موقت روی ایستگاه کاری کاربر ذخیره می‌شوند که به معنی آن است که نفوذگر احتمالی می‌تواند به کلیدهای رمزنگاری دست پیدا کند.
- کلیدهای نشست رمزگشایی شده و در ایستگاه‌های کاری کاربران به صورت Cache یا در جدول کلیدها (Key table) ایجاد می‌شوند. در این حالت نیز نفوذ کننده احتمالی می‌تواند به آن‌ها دست یابد.

- کربروس در مقابل حُدس کلمه عبور آسیب پذیر است. KDC توانایی تشخیص وقوع حمله فرهنگ لغت (Dictionary Attack) را ندارد.
- اگر رمزنگاری ترافیک شبکه فعال نباشد، کربروس نمی‌تواند کاری برای حفاظت از ترافیک شبکه انجام دهد.
- اگر طول کلیدها کم باشد، در مقابل حمله‌های سعی مکرر^{۳۲} (Brute Force) آسیب پذیر خواهد بود.

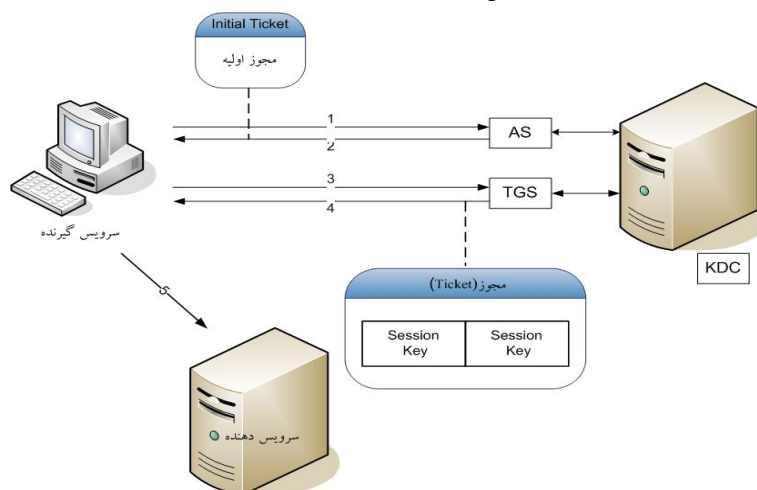
برای مطالعه بیشتر در مورد روش کربروس می‌توان به منابع زیر مراجعه نمود:

<http://www.logicalsecurity.com>

<http://www.mit.edu/afs/athena.mit.edu/astaff/project/Kerberos/www/papers.html>

(کربروس در اساطیر یونانی نام سنگ نگهبان سه سر دنیای زیر زمین بوده است)

مدل عملکرد روش کربروس در شکل زیر نمایش داده شده است.



- ۱- کاربر از طرف AS احراز هویت می‌شود.
- ۲- AS یک مجوز اولیه برای کاربر ارسال می‌کند.
- ۳- کاربر درخواست دسترسی به سرویس دهنده را ارسال می‌نماید.
- ۴- TGS یک مجوز جدید همراه با کلید نشست را صادر می‌نماید.
- ۵- کاربر یک کلید نشست را استخراج کرده و مجوز را برای سرویس دهنده ارسال می‌نماید.

۳۲- زورگیری

رادیوس (RADIUS)

(Remote Authentication Dial-in User Service) RADIUS یک پروتکل احراز هویت است که

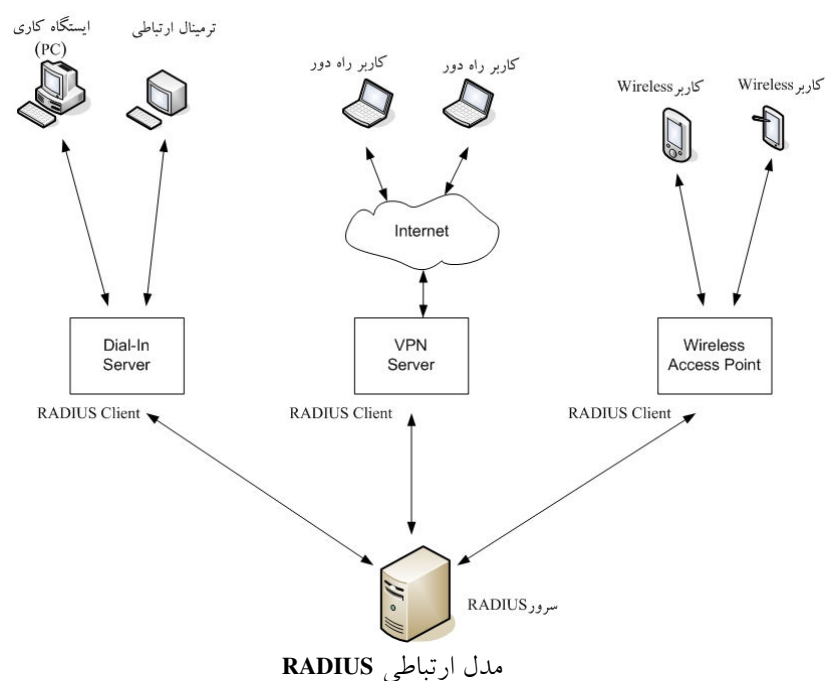
برای احراز صلاحیت کاربران راه دور به کار گرفته می‌شود.

در یک شبکه مفروض کاربران راه دور می‌توانند از طریق **Access Server**، آرایه مودم‌ها و یا خطوط **DSL**، **ISDN** و **T1** به آن متصل شده و از منابع موجود استفاده نمایند. **Access Server** دلایل اعتبار را از کاربر راه دور درخواست کرده و به سرور **RADIUS** که حاوی شناسه‌های کاربری و کلمه‌های عبور است تحویل می‌دهد. در این حالت کاربر راه دور به عنوان یک **Client** به **Access Server** مراجعه می‌کند و **Access Server** نیز به نوبه خود به عنوان **Client** به سرور **RADIUS** مراجعه می‌نماید.

در بسیاری از مراکز ارائه خدمات اینترنت (**ISP**) از **RADIUS** برای احراز هویت مشتریان (قبل از صدور مجوز اتصال به اینترنت برای ایشان) استفاده می‌نمایند. سرور کنترل دسترسی **Access Server** و نرم‌افزار سمت کاربر با یکدیگر تبادل اولیه اطلاعات کرده و بر سر استفاده از یک پروتکل احراز هویت مشترک (از قبیل **PAP**، **CHAP** و یا **EAP**) به توافق می‌رسند. سپس کاربر شناسه کاربری و کلمه عبور خود را برای سرور کنترل دسترسی ارسال می‌نماید. این ارتباط از طریق اتصال **PPP** برقرار می‌شود. سرور کنترل دسترسی **Access Server** و سرور **RADIUS** نیز با استفاده از پروتکل **RADIUS** با یکدیگر ارتباط برقرار می‌نمایند. اگر برقراری ارتباط موفقیت آمیز باشد، یک **IP** اختصاصی به کاربر تخصیص داده شده و همراه با برقراری ارتباط وی با اینترنت پارامترهای اتصال نیز برای وی ارسال می‌شود. همچنین برای استفاده‌های حسابداری زمان شروع و پایان اتصال کاربر از سوی **Access Server** برای **RADIUS** ارسال می‌شود به علاوه از **RADIUS** برای برقراری ارتباط کاربران راه دور یا ایستگاه‌های کاری سیار با شبکه سازمان متبوع ایشان استفاده می‌شود. با استفاده از **RADIUS** می‌توان پروفایل‌های دسترسی کاربران به منابع مختلف شبکه را برای هر کاربر تنظیم کرده و پس از احراز هویت موفق کاربر راه دور، دسترسی تحت کنترل وی به شبکه را امکانپذیر نمود. پروفایل‌های دسترسی کاربران در یک بانک اطلاعاتی مرکزی ذخیره می‌شود و به همین دلیل می‌توان عملیات رهگیری فعالیت‌های کاربران راه دور را به صورت متمرکز به اجراء گذاشت.

خصوصیات RADIUS طی RFC 2138 و RFC 2139 منتشر شده است. این به آن معنی است که این پروتکل یک پروتکل آزاد ((Open Protocol می‌باشد و می‌توان آن را به شکل تقریباً دلخواه پیاده‌سازی کرد.

فرمت و پیکربندی ابزارهای اثبات هویت کاربری را می‌توان از طریق سرویس دهنده LDAP، بانک‌های اطلاعاتی مختلف و یا فایل‌های متنی ((Text file نگهداری نمود. شکل زیر نشان دهنده چگونگی ارتباط کاربران مختلف با سرور RADIUS می‌باشد:



TACACS

TACACS (Terminal Access Controller Access Control System) دارای نسل‌های سه گانه

زیر است:

- الف- TACACS که فرآیندهای احراز هویت و احراز صلاحیت را با یکدیگر ترکیب می‌نماید.
- ب- Extended TACACS (XTACACS) که فرآیندهای احراز هویت، احراز صلاحیت و ممیزی را به صورت جداگانه به مورد اجراء می‌گذارد.
- ج- TACACS+ که XTACACS را با روش احراز هویت دو عاملی ترکیب می‌نماید.

TACACS از روش کلمه عبور ثابت (**Fixed Password**) استفاده می‌نماید در حالی که **TACACS** + امکان استفاده از کلمه‌های عبور پویا (**Dynamic Password**) را برای کاربران فراهم می‌آورد. البته از آن‌جا که **TACACS+** از پروتکل متفاوتی استفاده می‌کند با مدل‌های **TACACS** و **XTACACS** سازگار نمی‌باشد.

TACACS+ اصولاً عملکردی مشابه **RADIUS** را (البته با تعدادی تفاوت) ارائه می‌نماید. تفاوت‌های این دو پروتکل در ادامه شرح داده شده اند:

- **TACACS+** از پروتکل **TCP** به عنوان پروتکل انتقال استفاده می‌کند در صورتی‌که **RADIUS** از پروتکل **UDP** بهره می‌برد.

- **RADIUS** فقط در مرحله شروع ارتباط کلمه عبور کاربر را رمز کرده و از **RADIUS Client** به **RADIUS Server** ارسال می‌نماید و سایر اطلاعات از قبیل شناسه کاربری اطلاعات **Accounting** و خدمات تخصیص داده شده به وی به صورت رمز نشده (کشف) و متن واضح ارسال می‌گردد. این وضعیت جولانگاه بلامنازع را برای حمله کننده‌های احتمالی فراهم می‌آورد. بنابراین لازم است از مکانیزم‌های امنیتی مناسب برای ترمیم این نقطه ضعف استفاده شود. در پروتکل **TACACS+** کلیه اطلاعات فوق رمزنگاری شده و بنابراین آسیب پذیری فوق ترمیم شده است.

- پروتکل **RADIUS** عملکردهای احراز هویت و احراز صلاحیت را با یکدیگر ترکیب می‌نماید. اما در **TACACS+** از مدل کامل معماری **AAA** استفاده می‌شود که در آن مراحل مختلف احراز هویت، احراز صلاحیت و پاسخگویی از یکدیگر تفکیک شده‌اند.

- **RADIUS** فقط در محیط‌هایی که از مدل احراز هویت و احراز صلاحیت برای تصمیم‌گیری جهت صدور مجوز ورود کاربر به سیستم تحت حفاظت استفاده می‌شود کاربرد دارد، در حالی‌که از **TACACS+** می‌توان برای کنترل دسترسی کاربر احراز صلاحیت شده به بخش‌ها و منابع مختلف شبکه هدف استفاده کرد.

تفاوت‌های اصلی پروتکل‌های **RADIUS** و **TACACS+** در جدول زیر خلاصه شده است:

تفاوت‌های پروتکل‌های کنترل دسترسی RADIUS و TACACS+

پروتکل			
TACACS+	RADIUS		
TCP	UDP	ارسال بسته ها	تفاوت‌ها
کلیه ترافیک بین Client و سرور رمزنگاری می‌شود.	فقط کلمه عبور بین RADIUS و سرور رمزنگاری می‌شود.	رمزنگاری بسته ها	
معماری AAA مورد استفاده واقع می‌شود.	احراز هویت و احراز اصالت به صورت ترکیبی انجام می‌شود.	پشتیبانی AAA	
پروتکل‌های مختلف مثل Apple Net BIOS، Talk و IPX را پشتیبانی می‌نماید.	بر اساس پروتکل PPP عمل می‌کند.	پشتیبانی پروتکل ها	
از مدل چند مرحله‌ای پرسش پاسخ برای هر یک از مراحل AAA استفاده می‌نماید. هر مرحله از AAA باید به صورت مجزا اعتبارسنجی شود.	از مدل تعامل ساده پرسش- پاسخ ((Challenge-Response در زمان احراز هویت کاربر استفاده می‌کند که در تمام مراحل AAA به کار گرفته می‌شود.	تعامل ((Response	
دسترسی خاص به تک تک سرویس‌ها و منابع موجود در شبکه	دسترسی عام به شبکه	کنترل	

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	مدیریت دسترسی کاربران
ثبت کاربر شماره دستورالعمل : ۱-۲-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات
خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

این دستورالعمل مبین روش، الزامات و خصوصیات اسناد، مکاتبات و فرآیند ثبت کاربر در سیستم‌های کنترل دسترسی مبتنی بر نظام مدیریت امنیت اطلاعات جهت دسترسی به دارایی‌های اطلاعاتی موجود در فهرست دارایی‌های اطلاعاتی (موضوع دستورالعمل ۱-۳-۱) می‌باشد.

مسئولیت:

- مسئولیت درخواست ایجاد حساب کاربری به عهده مسئول مستقیم کاربری است که تقاضای دسترسی به دارایی‌های اطلاعاتی را دارد.
- مسئولیت تأیید یا رد درخواست دسترسی به عهده متصدی دارایی‌های اطلاعاتی (موضوع دستورالعمل ۱-۳-۲) مورد درخواست می‌باشد.
- مسئولیت بررسی و انطباق شرایط کاربر با معیارهای امنیتی ((وزارت/ سازمان/ اداره کل/ شرکت...)) و تصویب یا عدم تصویب آن به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن (مثل مرکز حراست فناوری اطلاعات) می‌باشد.
- مسئولیت انتخاب مکانیزم دسترسی به هر دارایی اطلاعاتی از بین مکانیزم‌های تصویب شده به عهده متصدی یا تحویل گیرنده یا مالک همان دارایی اطلاعاتی می‌باشد.

الزامات:

- هرکاربر باید دارای یک هویت واحد و منحصر به فرد باشد و بر همان اساس شناسایی شود.
- این هویت می‌تواند بر اساس دیدگاه سیستم مدیریت امنیت هر سازمان به صورت استاندارد تدوین گردد.
- در صورت شناسایی سازمان از طرف سازمان پدافند غیرعامل به عنوان سازمان حساس یا حیاتی لازم است روش استفاده از هویت دیجیتال (شرح داده شده در پیوست دستورالعمل ۱-۳-۷) به کار گرفته شود.
- در هر صورت لازم است مشخصات و اطلاعات کاربر متقاضی دسترسی به طور کامل ثبت شود.
- لازم است هنگام استخدام افراد یا عقد هر گونه قرارداد همکاری منجر به استفاده کاربر از دارایی‌های اطلاعاتی، الزامات کنترل دسترسی عام سازمان به اطلاع کاربر رسانده شده و سند تعهد به رعایت آن‌ها به امضای متقاضی برسد.

- لازم است هنگام اعطای حق دسترسی به هر یک از دارایی‌های اطلاعاتی تحت اختیار سازمان الزامات کنترل دسترسی خاص مربوط به همان دارایی اطلاعاتی به اطلاع کاربر رسانده شده و سند مربوط به رعایت آن‌ها به امضای وی برسد.
- لازم است حقوق دسترسی کاربر و ابزارهای دسترسی وی به دارایی اطلاعاتی مورد تقاضا به شکل امن و غیر قابل انکار به صورت مکتوب به وی اطلاع داده شود.
- لازم است کاربر بر اساس دستورالعمل ۷-۲-۳ نسبت به دریافت و استفاده از کلمه عبور خود اقدام نماید.
- لازم است مستندات و مکاتبات مربوط به اعطای حقوق دسترسی به صورت امن نگهداری شوند.
- در صورت قطع رابطه کاری یا استخدای کاربر به هر دلیل ممکن، لازم است این موضوع فوراً به اطلاع افراد مربوط رسیده و سریعاً نسبت به قطع حقوق دسترسی وی تصمیم‌گیری شود.
- هنگام ایجاد شناسه کاربری (User ID) و تخصیص دسترسی نکات زیر باید مورد توجه قرار گیرد:
 - قبل از تأیید دریافت کلمه عبور، باید ابزارهای دسترسی ایجاد شده و تخصیص داده شده به وی غیر فعال باشند.
 - باید مکانیزم قفل شدن شناسه کاربری پس از تعداد معینی سعی ناموفق برای ورود به سیستم فعال شده و اخطارهای لازم به متصدی دارایی اطلاعاتی و مدیر امنیت ارسال شود.
 - کلمه عبور باید دارای پیچیدگی کافی متناسب با سطح طبقه‌بندی حفاظتی دارایی اطلاعاتی مورد مراجعه باشد.
 - لازم است شناسه کاربری از طریق اعمال مقررات محدودیت زمان نشست (موضوع دستورالعمل ۷-۵-۵) و محدودیت زمان اتصال (موضوع دستورالعمل ۷-۶-۵) تحت کنترل قرار داشته باشد.

فرآیند:

جهت اطمینان از رعایت الزامات و حفظ شرایط امنیت اطلاعات در ثبت کاربر طی فرآیند زیر برای ثبت کاربر ضروری است:

۱- مسئول مستقیم کاربر درخواستی مبنی بر ثبت کاربر تنظیم و به متصدی دارایی اطلاعاتی ارائه می‌نماید.

۲- متصدی دارایی اطلاعاتی پس از بررسی درخواست و لحاظ کردن الزامات دسترسی به دارایی تحت اختیار خود و در صورت تائید، درخواست را جهت تصویب به مسئول واحد امنیت اطلاعات ارجاع می‌دهد.

تبصره: در صورت درخواست اعطای حق دسترسی ممتاز در سازمان‌ها یا مراکزی که از سوی سازمان پدافند غیرعامل به عنوان سازمان حساس یا حیاتی شناسایی شده‌اند لازم است تائید ارگان حراستی مربوط نیز اخذ گردد.

۳- واحد امنیت اطلاعات پس از بررسی و انطباق شرایط کاربر با معیارهای مدیریت امنیت اطلاعات نسبت به ثبت کاربر اقدام می‌نماید.

۴- پس از ثبت کاربر نسبت به درج مشخصات کاربری در لیست دسترسی‌ها (موضوع دستورالعمل ۷-۳-۴) اقدام و سوابق مربوط ثبت می‌گردد.

۵- ثبت کاربر و تخصیص دسترسی به صورت کتبی به اطلاع کاربر رسانده می‌شود.

۶- پس از تائید صحت دریافت کلمه عبور اولیه توسط کاربر سایر ابزارهای دسترسی به وی تحویل و حقوق دسترسی به وی اعطا می‌شود.

ضمن اجرای مراحل فوق لازم است موارد زیر نیز مورد توجه قرار گیرد:

- مراحل و فرآیند ثبت کاربر و اعطای دسترسی باید به گونه‌ای باشد که از تداخل در مسئولیت‌ها، دوباره کاری و یا سوءتعبیر در اعطای دسترسی عام، خاص یا ممتاز جلوگیری شود.
- باید تمام دسترسی‌ها و شناسه‌های کاربری تا زمانی که کاربر اعلام نکرده است که شناسه کاربری کلمه عبور و یا ابزارهای اثبات هویت سخت‌افزاری را به صورت امن دریافت کرده، غیر فعال باقی بمانند تا سوء استفاده احتمالی از آن‌ها امکان ناپذیر باشد.

رویه:

به عنوان مثال رویه ثبت کاربر در سیستم عامل ویندوز از طریق **Domain Controller** به شرح زیر است:

۱. **Control Panel→Administrative Tools→Active Directory Users and Computers**
۲. به بخش مورد نظر (**Organization Unit** مربوط) که نیاز است کاربر در آن‌جا ایجاد گردد مراجعه شود.
۳. با کلیک راست **New→User** انتخاب شود.
۴. اطلاعات لازم وارد و ثبت ((**Next**) شود.
۵. کلمه عبور اولیه (**Password**) درج گردد. این کلمه عبور باید به اطلاع کاربر رسانده شود.
۶. گزینه‌های کنترلی به شرح زیر تنظیم شود:
 - ☒ **User must Change Password**
 - ☐ **User Can not Change Password**
 - ☐ **Password Never expires**
 - ☒ **Account is Disable**
۷. پس از ایجاد کاربر سایر اطلاعات مربوط از قبیل شماره تلفن، آدرس پست الکترونیک، آدرس پستی و غیره به طور کامل درج گردد.
۸. مشخصات و دسترسی‌های کاربر در لیست کاربران و دسترسی‌ها ثبت گردد.
۹. دسترسی کاربر و کلمه عبور طبق دستورالعمل ۷-۲-۳ و به صورت مکتوب و امن به اطلاع وی رسانده شود.

ابزار مورد نیاز:

فرم ثبت کاربر ابزار اصلی ثبت کاربر می‌باشد و باید با همکاری واحدهای مربوط مثل اداره تشکیلات و روش‌ها و واحد امنیت اطلاعات و بخش‌های بهره‌بردار سیستم‌های اطلاعاتی تهیه گردد.

مرجع:

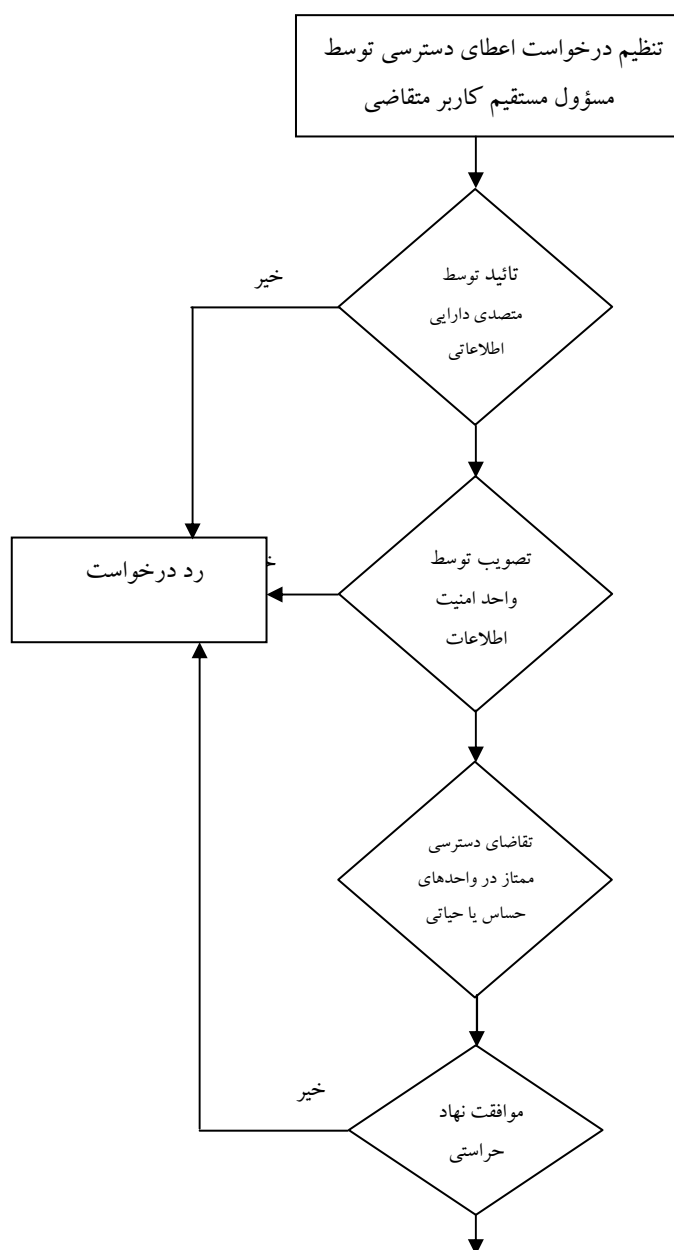
این دستورالعمل به شماره □-□/۱-۲-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های

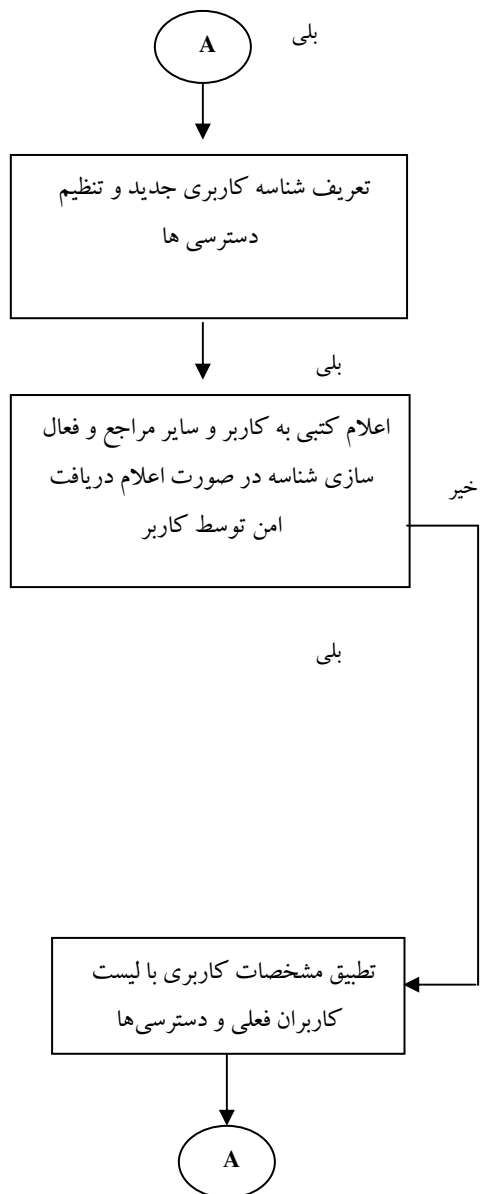
مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۳
- دستورالعمل ۲-۱-۳
- دستورالعمل ۱-۱-۷
- دستورالعمل ۳-۲-۷
- دستورالعمل ۵-۵-۷
- دستورالعمل ۶-۵-۷

روندنما:

روندنمای ثبت کاربر در شکل زیر نمایش داده شده است:





(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	مدیریت دسترسی کاربران
مدیریت دسترسی‌های ممتاز شماره دستورالعمل: ۲-۲-۷	

محرمانه

تائیدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع:

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:		
نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

[illegible]

هدف:

این دستورالعمل مبین روش‌ها، الزامات و خصوصیات اسناد، مکاتبات و فرآیندهایی است که جهت مدیریت دسترسی‌های ممتاز سیستم‌های اطلاعاتی بر اساس نظام مدیریت امنیت اطلاعات جهت دسترسی به دارایی‌های موجود در فهرست دارایی‌های اطلاعاتی (موضوع دستورالعمل ۱-۳-۱) باید به کار گرفته شود.

مسئولیت:

مسئولیت تعیین شرایط و ضوابط تخصیص دسترسی‌های ممتاز به دارایی‌های اطلاعاتی به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن (به عنوان مثال مرکز حراست فناوری اطلاعات) می‌باشد.

الزامات:

- هنگام اعطای حق دسترسی ممتاز باید الزامات دستورالعمل ثبت کاربر (دستورالعمل ۷-۲-۱) به طور کامل رعایت گردد.
- دسترسی ممتاز فقط باید بر اساس نیاز و حسب مورد و یا در مواقع ضرورت که به تأیید مدیر واحد امنیت اطلاعات برسد، اعطاء شود.
- لازم است افرادی که ممکن است نیاز به حق دسترسی ممتاز داشته باشند از قبل شناسایی شده و دلایل نیاز ایشان به دسترسی ممتاز مورد تحقیق قرار گیرد. تعداد این افراد باید محدود باشد.
- روش‌های تولید نرم‌افزار و همچنین اجرای عادی نرم‌افزارهای کاربردی باید به نحوی باشد که هیچ کاربری نیاز به استفاده از دسترسی ممتاز نداشته باشد.
- برای حفظ یکپارچگی روش اعطای دسترسی ممتاز و به حداقل رساندن خطای انسانی از چک لیست‌ها و فرآیندهای از پیش طراحی شده برای پردازش فرآیند تخصیص دسترسی ممتاز استفاده شود.
- حتی الامکان باید از مدل **OTP (One Time Password)** جهت اختصاص دسترسی ممتاز استفاده شود.
- در سیستم‌هایی که حقوق دسترسی ممتاز به صورت پیش فرض تخصیص داده می‌شود، لازم است نام کاربری پیش فرض تغییر داده شود (به عنوان مثال در سیستم عامل ویندوز نام کاربری پیش فرض **Administrator** به نامی دیگر تغییر داده شود).

- به‌طور کلی استفاده از نام‌های کاربری پیش فرض ممنوع است.
- در سیستم‌هایی که نیاز به حق دسترسی ممتاز دارند باید حداقل دو کاربر با دسترسی ممتاز ایجاد شود که یکی از آن‌ها در مواقع اضطراری به عنوان پشتیبان به کار گرفته شود.
- لازم است حقوق دسترسی ممتاز به‌صورت دوره‌ای (حداقل هر ۶ ماه یکبار) مورد بازنگری قرار گیرد.
- لازم است اجرای دستورالعمل‌های ۱-۲-۷، ۳-۲-۷، ۴-۲-۷ و ۱-۳-۷ در خصوص بهره‌برداری از شناسه‌های کاربری و کلمه عبور کاربران دارای حق دسترسی ممتاز به‌صورت مضاعف مورد کنترل قرار گیرد.

فرآیند:

- مدیریت دسترسی‌های ممتاز باید در سه بخش ایجاد دسترسی ممتاز، تغییر در حدود آن و نگهداری آن به‌اجراء گذاشته شود.
- در ایجاد یا تغییر دسترسی ممتاز باید مراحل زیر طی گردد:
 - بر اساس نیاز مبرم به استفاده و توجه به اصل نیاز به حق دسترسی به‌صورت مورد به‌مورد، مسئول مستقیم کاربر متقاضی حق دسترسی درخواست کتبی مربوط را ارائه نماید.
 - متصدی دارایی اطلاعاتی مورد تقاضا درخواست ارسال شده را بررسی و اعلام نظر می‌نماید.
 - در صورت اعلام نظر موافق متصدی مذکور واحد امنیت اطلاعات آن را بررسی می‌نماید.
 - در صورت اعلام نظر موافق واحد امنیت اطلاعات ارگان حفاظتی یا حراست سازمان مربوط اعطای حق دسترسی را مورد بررسی قرار می‌دهد.
 - در صورت اعلام نظر موافق ارگان حفاظتی مربوط سایر مراحل ثبت کاربر به‌اجراء گذاشته می‌شود.
- جهت نگهداری دسترسی‌های ممتاز لازم است به شرح زیر عمل شود.
- کلیه دسترسی‌های ممتاز پیش فرض و موجود دارایی اطلاعاتی مربوط شناسایی و تحت کنترل قرار می‌گیرد.

- کلیه دسترسی‌های ممتاز پیش فرض حذف گردد.
- دسترسی ممتاز دارایی‌های اطلاعاتی که نیاز به دسترسی ممتاز خارجی (دسترسی ضروری افراد خارج از سازمان مانند پیمانکاران طرف قرارداد با شرط رعایت موافقت‌نامه‌های عدم افشاء) ندارند به حداکثر دو دسترسی محدود گردد.
- نام کاربری دسترسی‌های ممتاز پیش فرض به کلمه یا عبارت‌های نامرتبط با نوع دسترسی یا نام کاربرد یا جایگاه سازمانی کاربر تغییر داده شود.

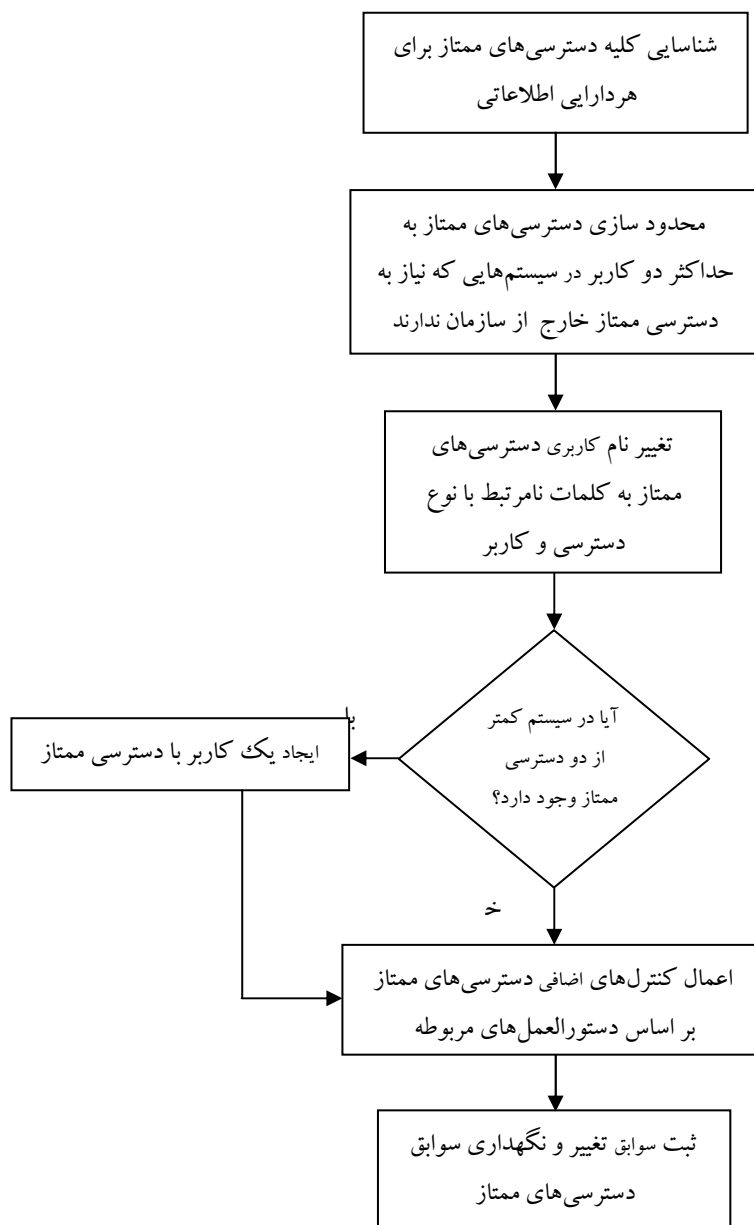
مرجع:

این دستورالعمل به شماره □-□/۲-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۳
- دستورالعمل ۱-۱-۷
- دستورالعمل ۱-۲-۷
- دستورالعمل ۳-۲-۷
- دستورالعمل ۴-۲-۷
- دستورالعمل ۱-۳-۷

روندنما:

روندنمای مدیریت دسترسی‌های ممتاز در شکل زیر نمایش داده شده است:



(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	مدیریت دسترسی کاربران
مدیریت کلمه عبور کاربر شماره دستورالعمل: ۳-۲-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع:

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار ((بالاترین مقام اجرایی سازمان))	رییس
	مسئول ((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات))	*دبیر
	معاون ((اداری، مالی و پشتیبانی))	عضو
	معاون ((برنامه‌ریزی))	عضو
	معاون ((فنی))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات ((معاون پشتیبانی)) سازمان به عنوان دبیر منصوب خواهد شد.

سوابق تغییرات:

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل تبیین ضرورت و روش مدیریت کلمه‌های عبور مورد استفاده در سیستم‌های کنترل دسترسی دارایی‌های اطلاعاتی در اختیار ((وزارت/ سازمان/ اداره کل/ شرکت/...)) می‌باشد.

مسئولیت:

- مسئولیت انتخاب، تخصیص، نگهداری و تغییر کلمه‌های عبور و همچنین استفاده از آن به عهده کاربر متقاضی استفاده از کلمه عبور می‌باشد.
- مسئولیت تعیین ضوابط انتخاب و نوع استفاده از کلمه‌های عبور و نظارت بر اجرای آن‌ها به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن می‌باشد.

الزامات:

- استفاده از کلمه عبور مناسب و محرمانه در کلیه دسترسی‌ها به دارایی‌های اطلاعاتی در اختیار ((وزارت/ سازمان/ اداره کل/ شرکت/...)) الزامی است.
- کاربر استفاده کننده از کلمه عبور باید قبل از استفاده از آن، سند مبنی بر محرمانه نگهداشتن کلمه عبور و استفاده از آن طبق ضوابط را امضاء نماید.
- لازم است کلمه‌های عبور پیش فرض دسترسی به دارایی‌های اطلاعاتی تغییر یابد.
- استفاده از نام کاربری یا کلمه عبور افراد دیگر ممنوع است.
- تخصیص کلمه عبور باید به صورت کتبی و رسمی ثبت گردد.
- اطلاع کلمه عبور به کاربر باید به صورت امن باشد به طوریکه در صورت افشاء کلمه عبور نزد افراد دیگر امکان مطلع شدن از آن وجود داشته باشد.
- لازم است امکان تغییر سریع کلمه عبور در اختیار کاربر گذاشته شود.
- لازم است کلیه اصول و توصیه‌های مندرج در سند سیاست گذاری کنترل دسترسی در خصوص مدیریت کلمه‌های عبور رعایت گردد.
- کلمه‌های عبور مورد استفاده باید به نحوی انتخاب شوند که اولاً دارای پیچیدگی کافی باشند، ثانیاً در مقابل حمله‌های موجود علیه کلمه عبور مقاوم باشند. (مسئولیت تدوین دستورالعمل روش انتخاب کلمه عبور به عهده واحد امنیت اطلاعات یا نهاد جایگزین آن می‌باشد).

فرآیند:

در بسیاری از سازمان‌ها از کلمه عبور به عنوان اصلی‌ترین عامل احراز هویت استفاده می‌شود. حتی در سازمان‌هایی که از مدل هویت دیجیتال برای احراز هویت و احراز صلاحیت استفاده می‌شود، کلمه عبور دارای نقش بسیار پررنگی است. بنابراین مدیریت چگونگی انتخاب، استفاده و نگهداری کلمه عبور دارای اهمیت بسیار است.

در مواقعی که از نرم‌افزارهای مدیریت کلمه عبور جهت سهولت در تولید و استفاده کلمه‌های عبور استفاده می‌شود، باید به نیازها و الزامات امنیتی استفاده از این نوع ابزار توجه نمود.

ممکن است در برخی از موارد درک درستی از لزوم حفظ محرمانگی کلمه عبور وجود نداشته باشد و افراد بدون توجه به پیامدهای خطرناک افشای کلمه عبور نزد افراد دیگر به این کار مبادرت کنند. برای مقابله با این پدیده خطرناک، اطلاع رسانی به افراد و آگاهی بخشی در خصوص تهدیدهای مرتبط با آن و اطمینان از تاثیر این فعالیت‌ها ضروری است. به علاوه لازم است در دوره‌های آموزشی مختلفی که در مورد استفاده از دارایی‌های اطلاعاتی یا امنیت اطلاعات برگزار می‌شود به این موضوع پرداخته شود. همچنین لازم است در مواقع ضروری از اقدامات انضباطی و یا پیگرد قانونی برای مقابله با کوتاهی در زمینه حفظ محرمانگی کلمه عبور استفاده شود. در این صورت لازم است قبلاً آموزش‌های رسمی مربوط در اختیار کاربر قرار داده شده باشد و ثانیاً هنگام تسلیم کلمه عبور به کاربر التزام وی به حفظ محرمانگی آن اخذ شده و پیامدهای نقض آن به اطلاع وی برسد.

مرجع:

این دستورالعمل به شماره □-□/□-۷-۲-۳/□-□ به ثبت رسیده است.

روندها:

این دستورالعمل فاقد روندها می‌باشد.

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	مدیریت دسترسی کاربران
بازنگری حقوق دسترسی کاربران شماره دستورالعمل: ۴-۲-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع:

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:		
نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	دبیر*
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

سوابق تغییرات :	
شرح	تاریخ

هدف:

این دستورالعمل بیان کننده روش و الزامات بازنگری حقوق دسترسی کاربران برای جلوگیری از دسترسی غیر مجاز به اطلاعات به دلیل به هنگام نبودن فهرست های دسترسی یا حقوق دسترسی به دارایی های اطلاعاتی در اختیار (((وزارت/ سازمان/ اداره کل/ شرکت/...))) می باشد.

مسئولیت:

- مسئولیت بازنگری دوره ای حقوق دسترسی کاربران هر دارایی اطلاعاتی به عهده متصدی یا تحویل گیرنده و یا مالک همان دارایی اطلاعاتی (موضوع دستورالعمل ۳-۱-۲) می باشد.
- مسئولیت نظارت بر رعایت مفاد این دستورالعمل به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن می باشد.

الزامات:

- حقوق دسترسی کاربران به دارایی های اطلاعاتی مختلف باید به صورت دوره ای مورد بازنگری قرار گرفته و به هنگام سازی شود.
- زمان دوره بازنگری حقوق دسترسی کاربران دارای حق دسترسی ممتاز نباید بیش از یک سوم زمان بازنگری حقوق دسترسی سایر کاربران باشد.
- در مراکز یا سازمان هایی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حساس یا حیاتی طبقه بندی می شوند دوره زمانی بازنگری حقوق دسترسی کاربران دارای حق دسترسی خاص یا ممتاز نباید بیش از یک سوم دوره زمانی بازنگری حقوق دسترسی کاربران عادی باشد.
- دوره بازنگری حقوق دسترسی کاربران دارایی های اطلاعاتی طبقه بندی شده تحت عنوان خیلی محرمانه یا بالاتر با نظر (((بالاترین مقام اجرایی سازمان))) تعیین می شود و نباید طولانی تر از زمان های مندرج در الزامات فوق باشد.
- حقوق و حدود دسترسی کاربران مختلف باید به صورت امن نگهداری شود و دارای بالاترین طبقه بندی حفاظتی موجود در سازمان باشد.

فرآیند:

فرآیند بازنگری حقوق دسترسی کاربران به شرح زیر خواهد بود. [تغییر در این فرآیند با توجه به نیازهای امنیت اطلاعات سازمان مجاز می‌باشد در هر صورت این فرآیند باید به صورت خاص به تصویب ((بالاترین مقام اجرایی سازمان)) برسد.]

- در بازه زمانی تعیین شده از قبل، مدیر واحد امنیت اطلاعات درخواستی مبتنی بر بررسی و اعلام نظر در خصوص حقوق دسترسی کاربران به تفکیک هر کاربر و حدود دسترسی وی به متصدی دارایی اطلاعاتی ارسال می‌نماید. (فهرست دسترسی هر دارایی اطلاعاتی فقط برای متصدی همان دارایی ارسال خواهد شد و ارسال حدود و فهرست دسترسی به افراد دیگر ممنوع است).
- متصدی دارایی اطلاعاتی پس از بررسی و مطابقت حقوق دسترسی مذکور با فهرست حقوق و حدود دسترسی موجود نزد خود و اعمال شده در سیاست‌های دسترسی دارایی اطلاعاتی موضوع بررسی، مغایرت‌ها را استخراج کرده و پس از تصحیح وضعیت، گزارش عملیات را به مدیر مافوق خود و مدیر واحد امنیت اطلاعات ارسال می‌نماید.
- در صورت عدم استفاده هر کاربر از حقوق دسترسی خود سوابق مذکور ثبت و جهت بررسی دلایل عدم استفاده کاربر از حقوق دسترسی تخصیص داده شده به وی و تصمیم در مورد حذف حقوق به دلیل عدم نیاز کاربر به آن، توسط مدیر واحد امنیت اطلاعات پیگیری می‌شود.
- در صورت وجود مغایرت منجر به نقض حدود دسترسی سوابق مذکور به عنوان حادثه امنیتی ثبت و جهت بررسی آثار ناشی از نقض حدود دسترسی در دستور کار واحد امنیت اطلاعات قرار می‌گیرد.
- در صورت استفاده از ابزارهای خودکار جهت کنترل حدود و حقوق دسترسی لازم است امنیت عملکرد و گزارش‌های ناشی از آن تأمین گردد.
- فرم‌های نمونه درخواست بازنگری و ممیزی حقوق دسترسی در ادامه این دستورالعمل درج شده‌اند.
- فهرست‌های حقوق و حدود دسترسی موجود نزد واحد امنیت اطلاعات پس از هر بازنگری به هنگام سازی خواهد شد.

- لازم است بازنگری حقوق دسترسی کاربران بر اساس چک لیست تهیه شده طبق فهرست دارایی‌های اطلاعاتی انجام شود تا از قلم افتادن برخی دارایی‌های اطلاعاتی جلوگیری شود.
- لازم است پس از بازنگری حقوق دسترسی کاربران، گزارش آن به همراه مغایرت‌ها و اثرات فوری یا آتی آن‌ها توسط واحد امنیت اطلاعات به (((بالاترین مقام اجرایی سازمان))) ارسال گردد.
- گزارش‌های تهیه شده در خصوص بازنگری حقوق دسترسی کاربران دارای طبقه‌بندی حفاظتی باید حداقل یک رده بالاتر از طبقه‌بندی حفاظتی دارایی اطلاعاتی مورد بررسی طبقه‌بندی شود.

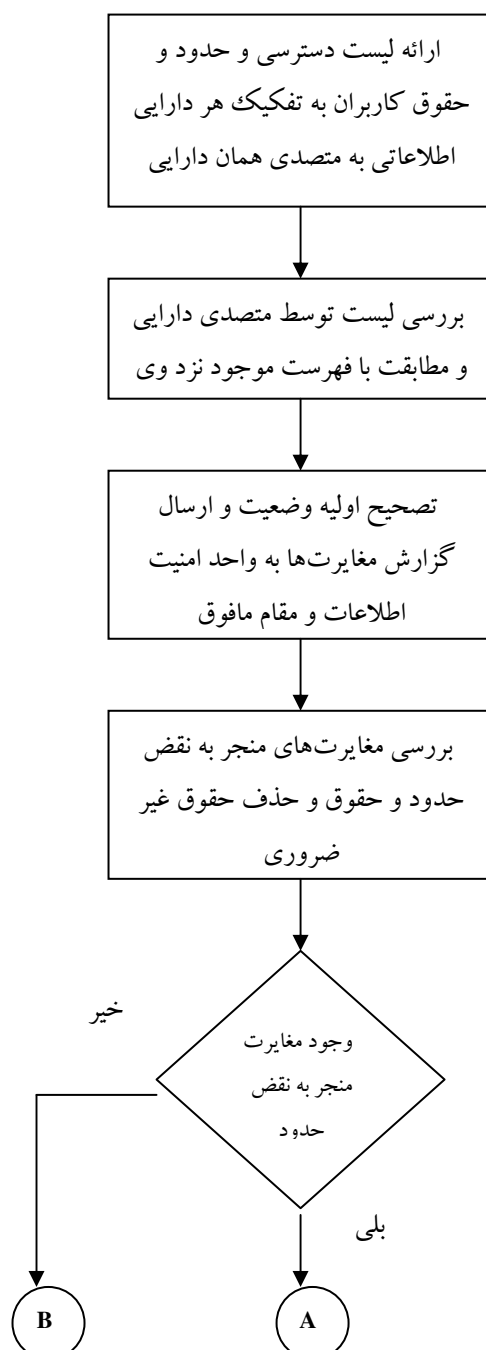
مرجع:

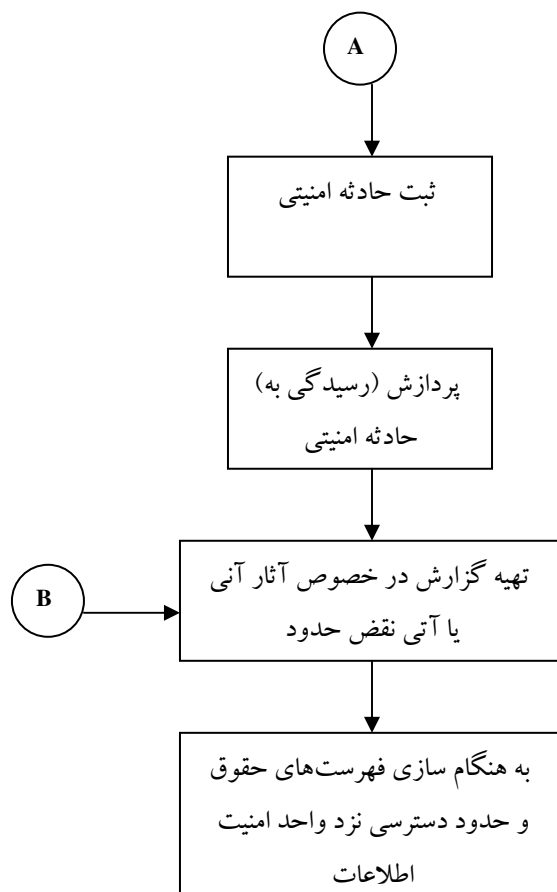
این دستورالعمل به شماره □-□/۴-۲-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۳
- دستورالعمل ۲-۱-۳
- دستورالعمل ۳-۱-۳

روندنما:

روندنمای بازنگری حقوق دسترسی کاربران در نمودار زیر نمایش داده شده است:





فرم نمونه درخواست بازنگری حقوق دسترسی کاربران به تفکیک دارایی‌های اطلاعاتی و کاربران

گیرنده: (((متصدی دارایی اطلاعاتی)))

نام دارایی اطلاعاتی:		شماره برچسب امنیتی:			
نام متصدی (مالک/ تحویل گیرنده):					
محل استقرار دارایی اطلاعاتی:			دوره زمانی بازنگری دارایی اطلاعاتی:		
			تاریخ ارسال:		
فهرست اسامی کاربران:					
نام و نام خانوادگی کاربر	شناسه کاربری	پست سازمانی	سایر اطلاعات پرسنلی	نوع دسترسی	حدود و حقوق دسترسی

نوع دسترسی: دسترسی عام، دسترسی خاص، دسترسی ممتاز

حدود و حقوق دسترسی: خواندن **Read**، تغییر **Write**، حذف **Delete**، اجراء **Execute**، کنترل کامل **Full****Access** بدون دسترسی **No Access**

فرم نمونه بررسی حقوق دسترسی کاربران به تفکیک دارایی‌های اطلاعاتی و کاربران

گیرنده: (((واحد امنیت اطلاعات))) / (((مدیر مافوق متصدی دارایی اطلاعاتی)))

نام بررسی کننده:		تاریخ تکمیل فرم:			
نام دارایی اطلاعاتی:		شماره برچسب امنیتی:			
نام متصدی (مالک/ تحویل گیرنده) امضاء:					
محل استقرار دارایی:		دوره زمانی بازنگری دارایی اطلاعاتی: صحت دوره زمانی اعلام شده: ☐ بلی ☐ خیر			
فهرست و نوع دسترسی کاربران اعلام شده در فرم درخواست بازنگری حقوق دسترسی کاربران					
شناسه کاربری	نوع دسترسی	حدود و حقوق دسترسی	مغایرت حقوق	مغایرت حدود	اثرات احتمالی مغایرت حدود
فهرست و نوع دسترسی کاربران اعلام نشده در فرم درخواست بازنگری حقوق کاربران					
شناسه کاربری	نام و نام خانوادگی کاربر	پست سازمانی	نوع دسترسی	حدود و حقوق دسترسی	مستند تخصیص حقوق

**فرم اعلام دارایی‌های اطلاعاتی فهرست نشده
در مرحله بازنگری حقوق دسترسی کاربران
به تفکیک دارایی‌های اطلاعاتی و کاربران**

گیرنده: (((واحد امنیت اطلاعات))) / (((مدیر مافوق متصدی دارایی)))

نام اعلام کننده:						تاریخ:					
پست سازمانی:											
به اطلاع می‌رساند دارایی اطلاعاتی زیر که فهرست کاربران و حقوق و حدود دسترسی آن‌ها در جدول زیر اعلام شده است در اختیار این جانب بوده اما در مرحله بازنگری حقوق دسترسی کاربران در خصوص آن استعلام نشده است.											
نام دارایی اطلاعاتی:						شماره برچسب:					
کاربرد:						محل نصب:					
اسامی کاربران											
شناسه کاربری	نام و نام خانوادگی کاربر	پست سازمانی	نوع دسترسی	حدود و حقوق دسترسی	مستند تخصیص حقوق						

توضیح: به ازای هر دارایی اطلاعاتی اعلام نشده یک فرم تکمیل و ارسال گردد.

((وزارت/ سازمان/ اداره کل/ شرکت/ ...)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	مسئولیت پذیری کاربران
استفاده از کلمه عبور شماره دستورالعمل: ۱-۳-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: ((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع:

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد

بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی استفاده امن از کلمه‌های عبور تخصیص داده شده به کاربران دارایی‌های اطلاعاتی در اختیار ((وزارت/ سازمان/ اداره کل/ شرکت .../)) اعم از کلمه‌های عبور عادی، یک بار مصرف و یا کلمه‌های عبور تولید شده توسط توکن‌های سخت‌افزاری مربوط می‌باشد.

مسئولیت:

- هر یک از کاربران و یا مراجعه کنندگان به دارایی‌های اطلاعاتی که موظف به استفاده از کلمه عبور جهت دسترسی به دارایی اطلاعاتی مورد درخواست می‌باشند در خصوص رعایت این دستورالعمل دارای مسئولیت می‌باشند.
- مسئولیت اطلاع رسانی در خصوص نحوه استفاده امن از کلمه‌های عبور به عهده مدیر واحد امنیت اطلاعات و یا نهاد جایگزین آن می‌باشد.
- مسئولیت تدوین روش‌ها و مقررات استفاده امن از کلمه عبور به عهده مدیر واحد امنیت اطلاعات و یا نهاد جایگزین آن می‌باشد.

الزامات:

- لازم است اطلاعات و آگاهی لازم جهت استفاده امن از کلمه‌های عبور به کاربران داده شود. این کار باید به صورت عام در هنگام استخدام و به صورت خاص در زمان تحویل کلمه عبور به کاربر انجام شود.
- کلمه عبور باید (حداقل) شرایط زیر را داشته باشد:
- حداقل از شش کاراکتر تشکیل شده باشد.
- ترکیبی از اعداد، حروف و علائم باشد.
- کلمه عبور به اندازه کافی پیچیده باشد و از کلمات معنا دار یا مرتبط با جایگاه کاربر مثل نام، شماره تلفن، شماره شناسنامه، سال تولد، نام اقوام و تشکیل نشده باشد.
- باید در بازه‌های زمانی از پیش تعیین شده نسبت به تغییر کلمه عبور اقدام شود. بازه زمانی تغییر کلمه عبور دسترسی‌های ممتاز نباید بیش از یک سوم بازه زمانی تغییر کلمه عبور دسترسی‌های عادی باشد.
- استفاده از کلمه عبور مشترک با سایر افراد ممنوع است.

- نوشتن کلمه عبور روی کاغذ یا قرار دادن آن زیر صفحه کلید و یا چسباندن آن به مانیتور و یا هر محل غیرقابل حفاظت دیگر ممنوع است.
- هنگام ورود کلمه عبور باید از عدم مشاهده آن توسط افراد دیگر اطمینان حاصل شود.
- استفاده از کلمه‌های عبور پیش فرض ممنوع است.
- استفاده بیش از یک بار از کلمه‌های عبور تولید شده توسط سیستم‌های خودکار ممنوع است.
- در صورتی که کلمه‌های عبور تخصیص داده شده به یک نفر بیش از پنج کلمه عبور باشد ترجیحاً از روش **Single Sign-on** استفاده شود.
- در صورت هر گونه ظن نسبت به افشاء کلمه عبور باید فوراً کلمه عبور تغییر یابد.

فرآیند:

بهترین روش برای اطمینان از آگاهی کاربر نسبت به اهمیت نحوه استفاده از کلمه عبور و یا هر گونه مکانیزم احراز هویت، امضای سند کتبی مبین الزامات استفاده از کلمه عبور پس از مطالعه آن می‌باشد. پس از این کار می‌توان شناسه کاربری و کلمه عبور یا تجهیزات مربوط به احراز هویت را به وی تحویل داد.

همچنین لازم است کاربر دریافت کلمه عبور خود را به متصدی دارای اطلاعاتی اطلاع دهد. در روش‌های خودکار تخصیص کلمه عبور باید کاربر ملزم به تغییر کلمه عبور در اولین مراجعه به دارای اطلاعاتی باشد.

فعال سازی حساب کاربری و اعطای حقوق دسترسی به وی پس از اطمینان از دریافت امن کلمه عبور توسط کاربر مجاز خواهد بود. تغییر کلمه عبور در سیستم‌های تخصیص خودکار کلمه عبور به منزله اعلام دریافت کلمه عبور اولیه توسط کاربر تلقی می‌گردد. به عنوان مثال مراحل انجام این کار در سیستم عامل ویندوز در ادامه شرح داده شده است:

- ابتدا کاربر متن مربوط به آگاهی و تائید وی مبنی بر حفظ محرمانگی کلمه عبور خود را امضاء می‌کند.
- طبق دستورالعمل ۷-۲-۱، نام کاربری و کلمه عبور به شکل کاملاً امن به کاربر اعلام می‌گردد.
- کاربر دریافت کلمه عبور و شناسه کاربری را به اطلاع متصدی دارای اطلاعاتی می‌رساند تا نسبت به فعال سازی حساب کاربری وی اقدام شود.

- هنگام اولین مراجعه کاربر به شبکه (جهت اتصال به سرورها) پیام مبنی بر لزوم تغییر کلمه عبور در اولین ورود به سیستم به وی نمایش داده می‌شود.
- کاربر کلمه عبور جدید خود را وارد و آن را تأیید و ثبت می‌کند.
- در دوره‌های زمانی تعیین شده از طرف مدیر شبکه روند تغییر کلمه عبور مجدداً تکرار می‌شود.

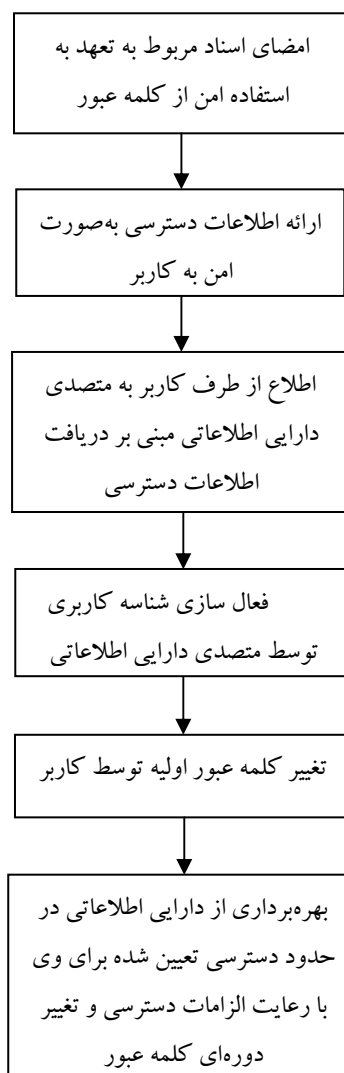
مرجع:

این دستورالعمل به شماره □-□/۱-۳-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۷
- دستورالعمل ۱-۲-۷

روندنما:

روندنمای استفاده از کلمه عبور در نمودار زیر نمایش داده شده است:



(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	مسئولیت پذیری کاربران
تجهیزات و دارایی‌های اطلاعاتی بدون مراقب شماره دستورالعمل : ۲-۳-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی حفظ امنیت دارایی‌های اطلاعاتی است که به دلیل ضرورت در مکان‌های خارج از دسترس و یا خارج از مکان‌های متعلق به ((وزارت/ سازمان/ اداره کل/ شرکت /...)) قرار گرفته یا نصب شده‌اند.

مسئولیت:

- مسئولیت شناسایی دارایی‌های اطلاعاتی بدون مراقب به عهده واحد امنیت اطلاعات می‌باشد.
- کلیه کاربران سیستم‌های اطلاعاتی یا دارایی‌های اطلاعاتی در خصوص گزارش وجود تجهیزات بدون مراقب در حوزه کاری خود به واحد امنیت اطلاعات مسئولیت دارند.

الزامات:

- لازم است تدابیر لازم برای حفظ امنیت دارایی‌های موضوع این دستورالعمل اندیشیده شده و امکانات حفاظتی ویژه‌ای جهت مراقبت از راه دور این تجهیزات در محل نصب گردد. (مثل دوربین‌های نظارتی یا سیستم‌های کنترل نفوذ یا کنترل محیط مثل حسگر دما یا رطوبت)
- جهت کنترل دسترسی فیزیکی تجهیزات بدون مراقب لازم است از سیستم‌های قفل سخت‌افزاری استفاده شود.
- لازم است در تجهیزات مورد استفاده کاربران، محدودیت زمان نشست ((Time Out لحاظ شده و پس از سپری شدن آن سیستم قفل یا دسترسی کاربر قطع گردد.
- در تجهیزات بدون مراقب سرویس دهنده شبکه که در محل خارج از دسترس یا خارج از مکان‌های در اختیار سازمان نصب می‌شوند لازم است علاوه بر نصب تجهیزات امنیتی و تأمین امنیت، تدابیر لازم جهت تأمین انرژی و تهویه مناسب نیز در نظر گرفته شود.
- هنگام بازنگری حقوق دسترسی کاربران لازم است حقوق و حدود دسترسی به تجهیزات بدون مراقب رأساً توسط واحد امنیت اطلاعات مورد بررسی و ممیزی قرار گیرد.
- لازم است واحد امنیت اطلاعات دوره زمانی جست‌وجو به دنبال تجهیزات بدون مراقب را به نحوی تنظیم نماید که زمان آن بیش از فاصله زمانی بین دو دوره بازنگری حقوق دسترسی کاربران عادی نباشد.
- هیچیک از دارایی‌های اطلاعاتی دارای طبقه‌بندی نباید بدون مراقب رها شود.

- هیچیک از دارایی‌های اطلاعاتی متعلق به سازمان‌ها یا مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حساس یا حیاتی شناسایی شده‌اند نباید بدون مراقب رها شوند.
- هنگام صدور مجوز استفاده از تجهیزات (موضوع دستورالعمل ۲-۱-۴) باید در خصوص نوع مراقبت از آن تصمیم‌گیری شود.

فرآیند:

تجهیزات و دارایی‌های اطلاعاتی بدون مراقب بر اساس نوع کاربری به سه دسته تقسیم می‌شوند:

الف- تجهیزاتی که معمولاً در محیط کاری قرار داشته ولی معمولاً کسی با آن‌ها کار

نمی‌کند مثل فایل سرورها یا تجهیزات نصب شده داخل **Rack**‌ها

ب- تجهیزاتی که به وسیله کاربران خاص یا به صورت موردی مورد استفاده واقع می‌شوند مثل چاپگرهای ویژه یا تجهیزاتی که در دوره زمانی خاص مورد استفاده قرار می‌گیرند و در سایر زمان‌ها به آن‌ها مراجعه نمی‌شود.

ج- تجهیزاتی که اصولاً به وسیله کاربران مورد استفاده مستقیم قرار نمی‌گیرند و در واقع جهت ارائه سرویس‌های ارتباطی یا شبکه‌ای به کار گرفته می‌شوند اما در محلی قرار گرفته‌اند که مراقبتی از آن‌ها به عمل نمی‌آید مثل سویچ‌ها، روترها، تکرار کننده‌ها، آنتن‌های مخابراتی، **Access Point**‌ها، تجهیزات مخابرات سلولی،

همان‌طور که هر یک از کاربران یا افراد حاضر در محل مسئولیت حفظ تجهیزات و دارایی‌های اطلاعاتی در اختیار خود را بر عهده دارند، باید از نحوه حفاظت از تجهیزات بدون مراقب نیز آگاه باشند و از آن‌ها مراقبت نمایند.

به‌طور کلی در خصوص این نوع تجهیزات می‌توان از روش‌های زیر برای اعمال حفاظت بهتر

بهره برد:

- پس از پایان هر نشست با این نوع تجهیزات یا در حالت بیکار بودن باید توسط یک مکانیزم حفاظتی خودکار (مثل **Screen Server** و کلمه عبور) از دسترسی به آن‌ها جلوگیری شود.
- پس از تکمیل عملیات روی کامپیوتر (**Minicomputer** یا **Mainframe**) علاوه بر خاموش کردن **PC** یا ترمینال مربوط، به نشست جاری نیز پایان داده شود.

- باید دسترسی فیزیکی به کامپیوتر یا تجهیزات بدون مراقب را با استفاده از قفل و کلید یا قراردادن در محفظه‌های قابل حفاظت محدود نمود.
- همچنین لازم است روش از پیش برنامه‌ریزی شده‌ای جهت جست‌وجو به دنبال تجهیزات بدون مراقب و شناسایی آن‌ها تعریف شده و به صورت دوره‌ای توسط واحد امنیت اطلاعات یا نهاد جایگزین آن به اجراء گذاشته شود.

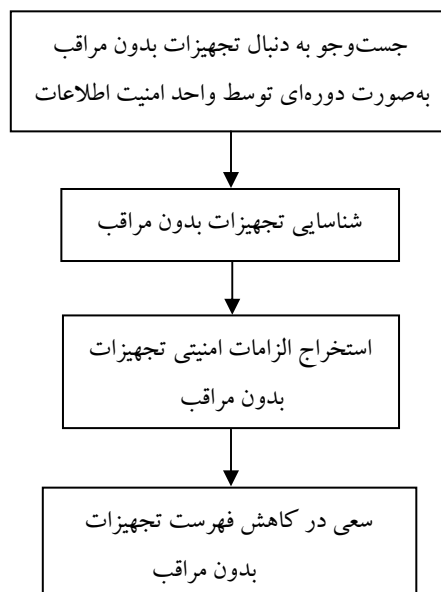
مرجع:

این دستورالعمل به شماره □-□/۲-۳-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۴-۱-۲
- دستورالعمل ۳-۱-۳
- دستورالعمل ۳-۴-۷

روندنما:

روندنمای استفاده از تجهیزات بدون مراقب در شکل زیر نمایش داده شده است:



(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	مسئولیت پذیری کاربران
روش مانیتور پاک و میز پاکیزه شماره دستورالعمل : ۳-۳-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد

بود.

تصویب شده در کمیته توسط:		
نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامهریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

[illegible]

هدف

هدف از تدوین این دستورالعمل جلوگیری از افشای غیر ضروری و ناخود آگاه اطلاعات اعم از اطلاعات محرمانه و غیر محرمانه از طریق اجرای سیاست مانیتور پاک و میز پاکیزه می‌باشد.

مسئولیت

کلیه بهره‌برداران از دارایی‌های اطلاعاتی متعلق به ملزم به رعایت این دستورالعمل می‌باشند. نظارت بر حسن اجرای این دستورالعمل به عهده مدیر نهاد متصدی امنیت اطلاعات و یا نهاد جایگزین آن (مثل مرکز حراست فناوری اطلاعات و ارتباطات) می‌باشد.

الزامات

- لازم است نحوه استفاده از اطلاعات و دارایی‌های اطلاعاتی به نحوی باشد که امکان افشای غیر ضروری و ناخود آگاه اطلاعات به حداقل برسد.
- لازم است نحوه قرار گرفتن صفحه نمایش اطلاعات و یا آرایش میز کار به نحوی باشد که احتمال دیده شدن اطلاعات و داده‌ها به حداقل برسد.
- لازم است صفحه نمایش از طریق نرم‌افزارهای حفاظتی ((**Screen Saver** پشتیبانی شده از طریق کلمه عبور تحت حفاظت قرار گیرد تا در صورت بیکار ماندن سیستم در طول دوره زمانی مشخص (حداکثر سه دقیقه) فعال شده و دسترسی غیر مجاز به سیستم غیر ممکن گردد. توجه: برخی از **Screen Saver**های رایگان به شدت خطرناک بوده و ممکن است به عنوان دروازه دسترسی نفوذگران به سیستم مورد استفاده واقع شوند.
- هنگام انتقال اطلاعات چاپی از نقطه‌ای به نقطه دیگر و یا قرار دادن آن‌ها روی میز کار باید حفاظت لازم با توجه به نوع طبقه‌بندی حفاظتی آن‌ها به مورد اجراء گذاشته شود.

فرآیند:

حتی اگر از پیچیده ترین الگوریتم‌های حفاظتی برای رمزگذاری داده‌ها و اطلاعات یا حفاظت فیزیکی اسناد استفاده شود، هنگام نمایش یا چاپ باید این اطلاعات به صورت رمزگشایی شده نمایش داده شوند تا برای کاربر قابل استفاده باشند.

این وضعیت به خصوص در مورد هر گونه اطلاعات محرمانه یا مربوط به اطلاعات شخصی افراد باعث ایجاد نقاط آسیب پذیر فراوان می‌شود، به طوریکه داده‌ها یا اسناد می‌توانند به صورت اتفاقی یا عمدی در معرض دید افراد غیر مجاز قرار گرفته و احتمالاً مورد سوء استفاده واقع شوند.

بنابراین لازم است سیاست ماینیتور پاک و میز پاکیزه در کلیه بخش‌های ((وزارت/ اداره کل/ سازمان/ شرکت/...)) به کار گرفته شود تا امکان افشای اطلاعات غیر ضروری از طریق صفحه تصویر یا اوراق چاپی موجود روی میزها یا در محل‌های کار جلوگیری شود. اجرای این فرآیند باید به صورت مداوم و از طریق اجرای مکانیزم‌های تشویقی و انضباطی تحت کنترل قرار داشته باشد.

مرجع:

این دستورالعمل به شماره □-□/□-□/□-□ به ثبت رسیده است.

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی شبکه
سیاست‌گذاری استفاده از سرویس‌های شبکه شماره دستورالعمل : ۱-۴-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: ((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از اجرای این دستورالعمل پیشگیری از دسترسی غیرمجاز به سرویس‌های شبکه یا شبکه‌های تحت اختیار یا مالکیت ((وزارت/ اداره کل/ سازمان/ شرکت/...)) و دارایی‌های اطلاعاتی موجود در آن می‌باشد.

مسئولیت‌ها

- همه بهره‌برداران از سرویس‌های شبکه‌ای ارائه شده توسط شبکه‌های در اختیار ((وزارت/ اداره کل/ سازمان/ شرکت/...)) ملزم به رعایت کامل الزامات حفاظت از داده‌ها و دارایی‌های اطلاعاتی می‌باشند. نظارت بر این امر به عهده مدیر ارشد شبکه ((وزارت/ اداره کل/ سازمان/ شرکت/...)) می‌باشد.
- همه کارمندان مرتبط با نقاط ارایه سرویس‌های شبکه و یا محل نصب تجهیزات مربوط موظف‌اند نسبت به حضور افراد ناشناس در اماکن مهم مربوط به ارائه یا تداوم سرویس‌های شبکه حساسیت نشان داده و افراد مسئول را مطلع نمایند.
- مدیر نهاد متصدی امنیت اطلاعات یا نهاد جایگزین آن موظف است بر ترافیک کلیه داده‌های متبادله بین شبکه و مراکز بیرونی و همچنین تعاملات داخلی سرویس‌های شبکه نظارت مداوم داشته باشد.

الزامات

- حوادث امنیتی در سرویس‌های شبکه باید در حداقل فرصت ممکن توسط مدیر امنیت تشخیص داده شده و واکنش مناسب در مقابل آن‌ها اعمال شود. لازم است ابزار مناسب اجرای این الزام در اختیار وی قرار داده شود.
- هرگونه موارد نقض امنیت باید در کوتاهترین زمان ممکن توسط مدیر امنیت رسیدگی شود تا صدمات ناشی از آن مشخص شده و محدود سازی دامنه آسیب پذیری، بازیابی و تعمیرات لازم انجام گیرد و مدارک مربوط به هر یک به طور رسمی ثبت، جمع‌آوری و به مراجع ذیربط گزارش شود.
- طبقه‌بندی حفاظتی اطلاعات مربوط به حوادث امنیتی در سرویس‌های شبکه باید حداقل یک رده سخت گیرانه‌تر از طبقه‌بندی حفاظتی دارایی اطلاعاتی مربوط تلقی شده و فقط در اختیار افراد مسئول قرار گیرد و از افشای آن‌ها میان سایر افراد جلوگیری شود.

- در مراکز و نهادهایی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حیاتی دسته‌بندی می‌شوند لازم است کلیه استانداردها و پروتکل‌های مرتبط با سرویس‌های شبکه به صورت کامل از لحاظ امنیتی ارزیابی و تحلیل شده، رخنه‌پذیر نبودن آن‌ها به تأیید افراد متخصص برسد. مسئولیت اطمینان از صحت و رخنه‌پذیر نبودن پروتکل‌ها بر عهده مدیر نهاد متصدی امنیت اطلاعات است.
- اتصال غیر امن به سرویس‌های شبکه می‌تواند باعث اثرات سوء بر عملکرد کلی سازمان باشد و ممنوع است.
- ارتباط با شبکه‌ها و یا سرویس‌های شبکه‌ای که اتصال به آن‌ها مجاز است باید قبلاً تحلیل ریسک شده و اگر ایجاد ارتباط مستلزم اعطای حق دسترسی اطلاعات غیر عمومی سازمان به کاربران شبکه مقابل اعم از کاربر انسانی یا ماشین باشد، لازم است از طریق عقد توافق‌نامه‌های حفظ محرمانگی (موضوع دستورالعمل ۲-۱-۵) یا موافقت‌نامه‌های عدم افشاء و رعایت الزامات امنیتی متقابل پشتیبانی شود.
- لازم است فقط در صورت شناسایی کامل و پس از اطمینان از داشتن حقوق دسترسی خاص، اجازه استفاده مستقیم از خدمات به کاربر داده شود.
- کنترل موارد فوق به خصوص در زمان اتصال به نرم‌افزارهای حساس و یا اطلاعات مهم سازمان، دارای اهمیت بسیار است و باید از طریق اعمال سیاست‌های سخت گیرانه کنترل دسترسی (موضوع پیوست‌های دستورالعمل ۷-۱-۱) مدیریت شود.
- لازم است طبق زمانبندی منظم سیاست‌گذاری امنیتی سرویس‌های شبکه مرور و بازبینی شود.
- لازم است که نقشه توپولوژی سرویس‌های شبکه تهیه شود و صحت آن در بازبینی‌های دوره‌ای بررسی شود.
- لازم است وقایع مربوط به دسترسی به فایل‌ها و دایرکتوری‌های حساس ثبت شود.
- لازم است یک مدل محرمانه تخصیص IP به سرویس‌های مختلف شبکه، طراحی و پیاده‌سازی شود.
- لازم است اطمینان حاصل شود که اطلاعات محرمانه سرویس‌های مختلف شبکه به نحو صحیح و فقط برای کاربران مجاز توزیع شده است.

- لازم است اطمینان حاصل شود که برای کاربران مجاز درمورد امنیت سرویس‌های مختلف شبکه، دسترسی به فایل و غیره، آموزش مناسب ارائه شده است.
- لازم است اطمینان حاصل شود که برای مدیران سرویس‌های مختلف شبکه آموزش‌های مناسب گذاشته شده و آن‌ها گواهی نامه‌های لازم را اخذ کرده‌اند.
- لازم است درباره توانمندی‌های امنیتی سخت‌افزارهای سرویس‌های شبکه که خریداری شده‌اند یا قرارست خریداری شوند تحقیق و بررسی کامل انجام شود.
- اطمینان حاصل شود که ارتباط سخت‌افزاری بین سرویس‌های مختلف شبکه از نظر امنیتی بررسی شده است.
- لازم است به‌طورمنظم، وقایع نگاریهای ثبت شده به منظور شناسایی تلاش برای دسترسی غیرمجاز به دایرکتوری‌ها و فایل‌های محرمانه بررسی شود.
- تجهیزات تولید سرویس‌های شبکه باید در محل‌هایی مستقر شوند که از دسترسی افراد غیرمجاز در امان باشند.
- کلیه اطلاعات دارای طبقه‌بندی، تنها در صورتی می‌توانند از طریق شبکه یا رسانه‌های قابل حمل نظیر CD، حافظه flash، فلاپی دیسک و ... منتقل گردند که از امنیت حین تبادل آن‌ها اطمینان حاصل گردد.
- لازم است سناریوهای حمله به شبکه و مکانیزم‌های کنترل دسترسی آن قبلاً بررسی شده و روش دفاعی متناسب با آن طراحی و آزمایش گردد.

فرآیند

جهت سیاست گذاری و اعمال روش‌های کنترل دسترسی شبکه فرایند زیر به اجراء گذاشته می‌شود:

- شناسایی شبکه‌ها و یا سرویس‌های شبکه‌ای که اتصال به آن‌ها مجاز است.
- تعیین رویکرد مجوزدهی به کاربران (اعم از انسانی و ماشین) و این‌که چه کسی اجازه دارد به کدام یک از شبکه‌ها و یا کدام یک از سرویس‌های شبکه‌ای دسترسی داشته باشد.
- تعیین رویکرد کنترل دسترسی جهت حفاظت از دسترسی به شبکه‌ها یا سرویس‌های شبکه‌ای.
- طراحی و تهیه نقشه توپولوژی سرویس‌های شبکه.

- آماده سازی طرح پشتیبانی و محدود سازی حوزه آسیب برای شرایطی که شبکه یا سرویس‌های شبکه دچار مشکل و خرابی شده است.
- آماده سازی طرح بازیابی برای شرایطی که سرویس‌های شبکه دچار مشکل و خرابی شده است.
- ایجاد یک فرآیند خاص برای تعیین نوع سرویس‌های شبکه که به کارت‌های شبکه متناسب (bind) شده‌اند.
- ایجاد یک فرآیند خاص ثبت و جلوگیری از دسترسی‌های غیرمجاز.
- ارزیابی و بازنگری طرح پشتیبان برای سطوح امنیتی مناسب شامل کنترل دسترسی، کنترل پیام‌ها و داده‌ها، نیازهای سخت‌افزاری و...

روش‌های اجرایی و رویه‌ها

- نرم‌افزار امنیتی برای محافظت از سرویس‌های ارائه شده انتخاب شود.
- اطلاعاتی که لازم نیست بین سرورها به اشتراک گذاشته شوند از دسترسی خارج شوند.
- ابزارهای مدیریت ترافیک سرویس‌های شبکه انتخاب شود.
- یک نقشه از وضعیت کاربران شبکه برای شرح کامل دسترسی به سرویس‌های شبکه تهیه و دسترسی غیرمجاز شناسایی و حذف شوند.
- ابزار مانیتورینگ و سرورهای مربوط به مدیریت سرویس‌های شبکه در محیطی کاملاً امن و دارای مکانیزم‌های امنیتی بیشتر نگهداری شوند.
- سخت‌افزارهای مربوط به سرویس‌های شبکه به منظور جلوگیری از دسترسی غیرمجاز در مکان امن نگهداری شوند.
- سرویس‌های شبکه که لازم است دسترسی‌های عمومی آن‌ها از بقیه جدا شوند به هاب یا روتر جداگانه وصل شوند.
- برای جداسازی سرویس‌های شبکه از دسترسی‌های غیرمجاز ممکن، باید روترها بدرستی پیکربندی شوند (به عنوان مثال از طریق اجازه دادن به آدرس‌های IP مخصوص).
- برای تجهیزات و رسانه‌های سرویس‌های شبکه محافظت‌های فیزیکی در حد کفایت اعمال شود.

- در سخت‌افزارها، از مکانیزم‌های کنترلی امنیتی و دسترسی مناسب به منظور ممانعت از پیکربندی غیرمجاز تجهیزات استفاده شود.
- پورت‌هایی که برای دسترسی‌های خارجی استفاده می‌شود با محافظت از طریق کلمه عبور کنترل شوند.
- اطمینان حاصل شود که کاربران در زمان دسترسی به شبکه از طریق مودم و با کمک نرم‌افزارهای امنیتی مناسب، باید بهنگام ورود مراحل کنترل دسترسی را (بر اساس مدل AAA) طی نمایند.
- اطمینان حاصل شود که در مورد کاربرانی که از طریق مودم به سرویس‌های شبکه دسترسی دارند از محافظت‌های اضافی مانند افزایش تعداد سطوح تأیید اعتبار استفاده می‌شود.
- اطمینان حاصل شود که اطلاعات مخصوص هر سرویس شبکه مانند نام، مکان و کارکرد سرویس شبکه (مانند سرویس شبکه **FTP** و...) درجایی ثبت و نگهداری می‌شود و به صورت دوره‌ای کنترل می‌گردد.
- سایر روش‌های دفاعی مانند دیوارهای آتش، رمزنگاری، محدودیت دسترسی کاربران، پشتیبان‌گیری و ... پیاده‌سازی شود.
- فایل مربوط به سرویس نام دامنه (**DNS**) به منظور محدود کردن دسترسی به سرویس، بررسی شود.
- با کمک فیلترینگ **IP** یک لیست دسترسی بروی سرویس‌های شبکه تعریف کرده تا از دسترسی کاربران غیرمجاز جلوگیری شود.
- همه سرویس‌های شبکه که بروی سرور در حال اجرا هستند بررسی شوند تا اطمینان حاصل شود که فقط سرویس‌های مجاز در حال اجرا هستند (سرویس‌هایی که در فایل **inetd.conf** هستند).
- در صورت استفاده از فیلترینگ **IP** از **TCP wrappers** به منظور مشخص کردن دسترسی غیرمجاز استفاده شود.
- اطمینان حاصل شود که ماشین‌های مجری سرویس‌های شبکه از نظر فیزیکی براحتی قابل دسترسی و جابجایی نیستند

- روش‌های امنیتی که در سطح BIOS اعمال می‌شوند برای همه ماشین‌های مجری سرویس‌های شبکه پیاده‌سازی شوند.
- پشتیبان‌گیری‌ها و آزمایش بازیابی‌ها در فواصل زمانی معین انجام شود.
- پشتیبان‌گیری‌ها و بازیابی‌ها به‌منظور اطمینان از جامعیت فرآیند اجرایی انتخاب شده آزمایش شوند.
- به‌طور مرتب فایل‌های startup برای تشخیص نرم‌افزارهای هک بررسی شوند.
- IP routing غیرفعال شود.
- دسترسی به تمامی پورت‌های TCP/IP ثبت و به صورت قاعده مند بررسی شود.
- گروه Everyone را برای همه سرورها حذف کرده و یا در صورت عدم حذف حداقل مجوزهای این گروه Deny شوند.
- همه برنامه‌های کاربردی و ابزارهای توسعه (development tools) از روی سرورهای مرتبط به وب حذف شوند.
- محیط اجراء طوری تنظیم شود که همه سرویس‌ها در chroot محدود و یا در محیط تحت کنترل، قابل اجرا باشد تا تاثیر حفره‌های امنیتی بالقوه محدود گردد.
- همه سرویس‌های غیرضروری مانند FTP یا SNMP غیرفعال شوند.
- هنگام نصب نرم‌افزار روی سرورهای مرتبط به وب، دایرکتوری پیش فرض انتخاب نشود.
- سرور مرتبط به وب در یک مکان از نظر فیزیکی مجزا نگهداری شود.
- از مجوزهای سطح URL برای محدود کردن دسترسی به سرور وب استفاده شود.
- هرگونه موارد نقض امنیت باید در کوتاهترین زمان ممکن به مدیر نهاد متصدی امنیت گزارش شود تا صدمات ناشی از آن مشخص شده و بازیابی و تعمیرات لازم انجام گیرد و مدارک مربوط به هر حادثه به طور رسمی ثبت، جمع‌آوری و به مراجع ذیربط گزارش شود.
- دلایل و مدارک قانونی علیه فرد یا افراد حمله کننده به سرویس‌های شبکه به نحوی جمع‌آوری شود که بتوان این افراد را به صورت رسمی و قانونی تحت پیگرد قرار داد.
- به منظور کاهش حملات ناشی از افراد درون سازمانی به سرویس‌های شبکه، باید دستورالعمل‌های کنترل دسترسی، طبقه‌بندی اطلاعات، و رویدادنگاری به طور منظم و

- دوره‌ای توسط مدیر واحد امنیت اطلاعات بازبینی شوند و اجرای دستورالعمل‌ها مورد بازرسی قرار گیرد.
- به منظور همگامی بخش‌های مختلف شبکه و استمرار فعالیت و تعامل آن‌ها توجه به تنظیم پروتکل‌ها و اجرای استانداردهای فنی ضروری است.
 - با سطح بندی مناسب درسیاست‌های ممیزی، دسترسی‌های غیرمجاز ثبت و از آن جلوگیری شود.
 - گزارش ابزارهای ردیابی فرآیندها (**Process Tracking**) مورد بررسی قرار گرفته تا از موفقیت و یا شکست به کارگیری ابزارسیاست‌گذاری امنیتی اطلاع حاصل شود.
 - هر یک از بهره‌برداران سرویس‌های شبکه، خود ملزم به مراعات کامل الزامات قانونی حفاظت از داده‌ها و اطلاعات در اختیار خود در سرویس‌های شبکه هستند و باید تعهدنامه امنیتی مربوط را امضاء نمایند.
 - مدیر سیستم باید دونام کاربری و کلمه عبور متفاوت داشته باشد. یکی برای دسترسی‌های امن و محدود و دیگری برای استفاده عادی.
 - حقوق کاربری مورد بررسی قرار گیرد تا از شکست یا ضعف ابزار اعمال سیاست‌گذاری امنیتی اطلاع حاصل شود.
 - سیاست‌گذاری حق دسترسی کاربران به اطلاعات طبقه‌بندی شده به صورت منظم مورد بررسی قرار گیرد.
 - اطمینان حاصل شود که مدیر سرویس‌های شبکه، صلاحیت مورد نیاز برای مدیریت شبکه را داراست.

مرجع:

این دستورالعمل به شماره □-□/۴-۵-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۷
- دستورالعمل ۵-۱-۲

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی شبکه
احراز هویت کاربر برای اتصال به شبکه‌های خارج از سازمان شماره دستورالعمل : ۲-۴-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: ((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

کسب اطمینان از تعلق اطلاعات هویتی ارائه شده به مدعی آن هویت (اعم از کاربر انسانی و یا برنامه) و اطمینان از مجاز بودن اتصال کاربر به شبکه‌های خارج از کنترل ((وزارت/اداره کل/ سازمان/ شرکت/...)).

مسئولیت‌ها

- کلیه کاربران شبکه باید خود را در مقابل حفظ امنیت فضای تبادل اطلاعات و ارتباطات و دارایی‌های اطلاعاتی کاملاً پاسخگو و مسئول بدانند و به طریق رسمی عهده‌دار حفظ محرمانگی، جامعیت اطلاعات و پیوستگی خدمات پردازشی سازمان باشند.
- به منظور حفاظت از داده‌های فضای تبادل اطلاعات، مدیر نهاد متصدی امنیت اطلاعات موظف است بر ترافیک کلیه داده‌های متبادله بین شبکه و مراکز بیرونی و همچنین تعاملات داخل شبکه نظارت مداوم داشته باشد.
- به منظور حفاظت از دارایی‌های اطلاعاتی، مدیر ارشد شبکه موظف است بر ترافیک کلیه داده‌های متبادله بین شبکه و مراکز بیرونی و همچنین تعاملات داخل شبکه نظارت مداوم داشته باشد.

الزامات

- سطح دسترسی کارکنان باید در زمان‌های مقتضی بر اساس دستورالعمل ۷-۲-۴ مورد بازبینی قرار گرفته و در صورت نیاز تغییر پیدا کند.
- دسترسی به داده‌ها و سیستم‌ها صرفاً منحصر به کاربران احراز هویت شده و از طریق ایستگاه (های) کاری مشخص و تعیین شده مجاز خواهد بود. کنترل اعمال این خط مشی باید به‌طور خودکار در درون سیستم‌ها و تجهیزات پیاده‌سازی و نظارت شود. رعایت این الزامات در دسترسی به شبکه‌های خارج از کنترل سازمان نیز ضروری است.
- تمامی دسترسی‌ها در سطح شبکه باید توسط راهکارهای اعلام شده از سوی مدیر امنیت یا مدیر ارشد شبکه، احراز هویت شده و ضمن ثبت دسترسی، امکان ادامه فعالیت برای شخص (یا برنامه) فراهم شود. راهکار پایه و اولیه احراز هویت کاربران، استفاده از کلمه عبور (طبق دستورالعمل ۷-۳-۱) پیچیده است و راهکارهای تکمیلی مطابق با دستورات

مدیر امنیت اطلاعات و بر اساس سیاست گذاری کنترل دسترسی (دستورالعمل ۷-۱-۱) خواهد بود.

- وجود مکانیزم‌های مناسب احراز هویت در شبکه و ثبت فعالیت‌های دسترسی به شبکه‌های خارجی الزامی است.
- لازم است قبل از اعطای مجوز دسترسی به شبکه خارج از سازمان دلایل و ریسک‌های مرتبط با آن بررسی شوند.
- تمامی دسترسی‌ها در سطح شبکه باید احراز هویت شده و ضمن ثبت دسترسی، امکان ادامه فعالیت برای شخص (یا برنامه) فراهم شود.
- لازم است تکنولوژی‌ها و پروتکل‌های دسترسی به شبکه‌های خارج از سازمان، دلایل استفاده و ریسک‌های مرتبط با آن بررسی شوند.
- استفاده از تجهیزات خاص احراز هویت مثل تجهیزات رمزنگاری یا توکن‌های سخت‌افزاری برای گروه‌هایی از کاربران که دسترسی آن‌ها مستلزم ایجاد مسئولیت حقوقی برای سازمان باشد ضروری است.
- کلیه فعالیت‌های دسترسی به شبکه‌های خارج از سازمان باید به نحو مناسب **log** برداری شود. این موضوع باید به اطلاع کاربران رسانده شود.
- لازم است تمامی **log** های ثبت شده در دیواره آتش یا سایر تجهیزات وقایع نگاری به صورت دوره‌ای مرور و بازبینی می‌شوند.
- لازم است ورود و خروج کاربران شبکه و دسترسی‌های آن‌ها به سایر سیستم‌ها و اطلاعات در سطح شبکه ثبت و پیگیری شود.
- تمامی ورودی و خروجی‌های کاربران به شبکه به همراه زمان و رایانه مورد استفاده باید ثبت شود.
- تمامی ورودی و خروجی‌های کاربران نرم‌افزارهای کاربردی (**Application**) ها مثل سیستم‌های عام مانند حسابداری، حقوق و دستمزد، کنترل پروژه، مدیریت منابع و غیره و یا سیستم‌های خاص که در جهت انجام ماموریت‌های سازمانی به کار گرفته می‌شوند) اعم نرم‌افزارهای کاربردی که به صورت بسته‌های نرم‌افزاری آماده (**Package**) خریداری

- می‌شوند و یا نرم‌افزارهایی که به سفارش سازمان تولید می‌شوند، باید به وسیله‌ی خود نرم‌افزارها ثبت، به صورت امن نگهداری و به شکل قاعده مند بازبینی شود.
- تمامی ترافیک اینترنت باید در دیواره آتش اختصاص داده شده برای آن ثبت شود.
- سطح دسترسی کارکنان باید در زمان‌های مقتضی (ارتقاء و یا نزول جایگاه سازمانی، توبیخ‌های امنیتی، منقضی شدن مدت زمان دسترسی، و یا...) مورد بازبینی قرار گرفته و در صورت نیاز تغییر پیدا کند.
- انجام فعالیت‌های لازم برای پیشگیری از تبدیل شبکه یا شبکه‌های تحت کنترل به منبع یا عامل یا سرپل حمله به شبکه‌ها یا تجهیزات پردازشی دیگر

فرآیند

- در احراز هویت کاربر برای اتصال به شبکه‌های خارج از سازمان توجه به نکات زیر ضروری است:
- شناسایی و سطح بندی کلیه کاربران متصل به شبکه‌های خارج از سازمان
- رویکرد مجازشناسی، تطبیق اختیارات کاربر احراز هویت شده (و یا ناشناس) در دسترسی به منابع
- رویکرد انکارناپذیری (Non Repudiation)، تضمین تعلق پیام ارسالی به فرستنده و یا تعلق پیام دریافتی به گیرنده
- ایجاد و اجرای روند استاندارد ثبت تمامی ورودی و خروجیهای کاربران به شبکه
- ایجاد و اجرای روند استاندارد کنترل دسترسی و احراز هویت کاربران به فایل‌ها و پوشه‌ها و نوع فعل و انفعالات صورت گرفته
- ایجاد و اجرای روند استاندارد ثبت ترافیک شبکه عبور کننده از سویچها و مسیریابها
- مانیتورینگ و نمایش تمامی ارتباطات متصل به شبکه‌های خارج از سازمان کاربران روی سرور متصل به شبکه سازمان
- مانیتورینگ و نمایش تمامی کاربرانی که در شبکه مشغول فعالیت هستند (login نموده‌اند)
- ارزیابی و بازنگری سطح دسترسی کاربران متصل به شبکه‌های خارج از سازمان
- بازنگری درسیاست کنترل دسترسی و احراز هویت بالحاظ نمودن فناوری‌های مورد استفاده در اجرای فرآیندهای فوق از طریق به‌کارگیری رویه‌های زیر امکانپذیر می‌شود:

- استفاده از کلمه عبور پیچیده به عنوان راه کار پایه و اولیه احراز هویت کاربران و استفاده از راه کارهای تکمیلی مطابق با دستورالعمل‌های منتشر شده توسط نهاد متصدی مدیریت امنیت اطلاعات
- انتخاب و استفاده از کلمات عبور به عنوان راه کار احراز هویت با رعایت ملاحظات امنیتی مربوط
- رویدادنگاری وقایع در سطح OS شبکه و نرم افزارها
- استفاده از ساعت مشترک و استاندارد در شبکه از طریق پیکربندی و راه اندازی NTP (Network Time Protocol)
- تعریف Privilege برای کاربران شبکه با توجه به اصل تخصیص حداقل دسترسی‌ها
- اجرای پورت امن (port security) و اختصاص آدرس MAC ثابت
- پیکربندی syslog برای کلیه سیستم‌ها
- تهیه log از پروسسها، کاربران، Applicationها و معماری سیستم جامع (log Audit)

مرجع:

این دستورالعمل به شماره □-□/□-۷-۴-۲/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۷
- دستورالعمل ۴-۲-۷
- دستورالعمل ۱-۳-۷

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی شبکه
شناسایی تجهیزات شبکه شماره دستورالعمل : ۳-۴-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد

بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام‌الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

تأمین امنیت کانال‌های ارتباطی و دارایی‌های اطلاعاتی موجود در شبکه‌های متعلق به ((وزارت/ اداره کل /سازمان/ شرکت/...))) از طریق شناسایی تجهیزات موجود در شبکه و استفاده از روش مسیرهای از پیش تعیین شده برای جلوگیری از استفاده کاربر از مسیرهایی که وی حق استفاده از آن را ندارد.

مسئولیت‌ها

- مسئولیت شناسایی، مدیریت و پیکربندی تجهیزات مسیریابی، راه‌گزینی و سایر تجهیزات شبکه و پیکربندی آن‌ها به عهده مدیر ارشد شبکه می‌باشد.
- همه کارمندان و افراد مرتبط به شبکه موظف‌اند نسبت به حضور افراد ناشناس در اماکن مهم مربوط به فضای تبادل اطلاعات شبکه حساسیت نشان داده و افراد مسؤول را مطلع نمایند.
- مدیر ارشد شبکه موظف است که معماری امنیتی و هم‌بندی (Topology) آخرین وضعیت شبکه‌های متعلق به ((وزارت/ اداره کل /سازمان/ شرکت/...))) را به منظور اطمینان از مفاد این خط مشی تهیه و بروز نگه دارد.
- مدیر نهاد متصدی امنیت اطلاعات موظف است که معماری امنیتی و هم‌بندی (Topology) آخرین وضعیت شبکه‌های مرتبط را به منظور اطمینان از رعایت مفاد این خط مشی تهیه و بروز نگه دارد.

الزامات

- لازم است تمامی سیستم‌های موجود در شبکه به همراه کاربرانی که در شبکه مشغول فعالیت هستند (login نموده‌اند) به همراه تجهیزاتی که روی آن login نموده‌اند به صورت on-line روی سرور Monitoring نمایش داده شوند.
- تمامی ارتباطات اینترنتی کاربران یا ارتباط با سایر شبکه‌ها در شبکه باید در سرور Monitoring خاص متصل به شبکه اینترنت نمایش داده شوند.
- لازم است تمامی ترافیک عبوری شبکه روی سویچ‌ها و مسیریاب‌ها مانیتور شوند و ارتباطات گره‌ها (Node) با هم به همراه پروتکل‌های آن‌ها نمایش داده شوند.
- لازم است از جابجایی نامحدود کاربران و تجهیزات در شبکه جلوگیری شود.

- لازم است تمامی ترافیک شبکه عبور کننده از سویچها و مسیریابها، به خصوص تجهیزات ثبت و نگهداری شود.
- باید در هنگام نصب تجهیزات یا سیستم‌های جدید (نرم‌افزاری یا سخت‌افزاری) در شبکه سازمان، دستورالعمل‌های امنیتی مرتبط با این تجهیزات برای افرادی که با آنها کار می‌کنند تهیه شود تا از عملکرد بهینه و امن کاربران آنها اطمینان حاصل گردد.
- لازم است شبکه (های) در اختیار ((وزارت/ اداره کل/ سازمان/ شرکت/...)) به‌طور منظم و به منظور کشف کامپیوترهای شخصی یا تجهیزات ناشناس و نقاط دسترسی (access point) غیرمجاز پوشش شود.
- لازم است ارتباطات فیزیکی مابین تجهیزات ارتباطات راه دور و تجهیزات پردازش داده‌ها با استفاده از نمودارهای شبکه مستندسازی شود.
- لازم است محل تجهیزات بدقت با نمودارهای شبکه و اسناد مربوط به فهرست موجودی دارایی‌های اطلاعاتی (موضوع دستورالعمل ۳-۱-۱) دارای مقایسه شده و مغایرت‌های آن مورد رسیدگی قرار گیرند.
- نمودارهای شبکه باید در یک محل امن با دسترسی محدود نگهداری شوند.
- لازم است افزودن یا تغییر در تجهیزات جدید، حذف تجهیزات و یا هر تغییری در شبکه از طریق یک فرایند مکتوب انجام شود.
- وضعیت تجهیزات قدیمی باید به صورت دوره‌ای (حداقل هر دو سال یکبار) چک شود.
- تمامی تجهیزات سخت‌افزاری شبکه باید قبل از انتقال به محیط عملیاتی واقعی به صورت کامل و قابل قبول، زیر نظر مدیر نهاد متصدی امنیت اطلاعات یا نماینده وی آزمایش شده و رسماً به متصدیان راهبری آنها تحویل داده شود.

فرآیند

- شناسایی تجهیزات شبکه را میتوان در قالب زیر انجام داد:
- شناسایی خودکار تجهیزات شبکه شامل تمامی رایانه‌ها، سویچها و مسیریابها، پیکربندی TCP/IP، سرورهای شبکه
- شناسایی تجهیزات خاص احراز هویت برای گروه‌های مختلف از کاربران عادی و دارای حق دسترسی ممتاز

- مستند سازی پیکربندی سویچ‌ها و مسیریاب‌ها.
- مستند سازی ارتباطات فیزیکی در سویچ‌ها و مسیریاب‌ها.
- مستند سازی پیکربندی TCP/IP در تمامی رایانه‌ها.
- مستند سازی روند ثبت ترافیک شبکه عبور کننده از سویچ‌ها و مسیریاب‌ها
- مانیتورینگ و نمایش تمامی ترافیک شبکه در سویچ‌ها و مسیریاب‌ها
- مانیتورینگ تمامی ارتباطات سویچ‌ها و وضعیت پورت‌های آن‌ها
- بازننگری و اعمال تغییرات مورد نیاز روی پیکربندی سویچ‌ها و مسیریاب‌ها، پیکربندی TCP/IP در تمامی رایانه‌ها و ارتباطات فیزیکی در سویچ‌ها.

روش‌های اجرایی و رویه‌ها

- تمامی دسترسی‌های کاربران به نرم‌افزارهای کاربردی باید به شکل مناسب در سرور Monitoring مانیتور شوند. چنانچه این امر نیاز به تغییرات در سطح نرم‌افزاری داشته باشد باید توسط مدیر واحد امنیت پیگیری شود.
- لازم است تمامی پروسه‌های خاص (به جر پروسه‌های اختصاصی windows) که در سیستم‌های کاربران اجرا شده‌اند در سرور مرکزی Monitoring مانیتور شوند.
- برای مانیتورینگ تحت وب، تمامی ارتباطات سویچ‌ها و وضعیت پورت‌های آن‌ها می‌توان از ابزارهای ذیل کمک گرفت:
- Microsoft ISA Server 2004
- نرم‌افزار مانیتورینگ ارائه شده از سوی پیمانکار
- Interface‌های سویچ‌ها نیز باید از طریق خود صفحات تحت وب هر سویچ مانیتور شوند).

مرجع:

این دستورالعمل به شماره □-□/□-۷-۴-۳/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۳

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی شبکه
حفاظت از سرویس های رفع اشکال از راه دور و پیکربندی درگاه ها شماره دستورالعمل : ۷-۴-۴	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه بندی شده و در اختیار کمیته امنیت اطلاعات خواهد

بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

کنترل دسترسی فیزیکی و منطقی به ابزار، نرم‌افزارها و درگاه‌های تشخیص وضعیت و عیب یابی در شبکه‌های تحت اختیار یا متعلق به ((وزارت/ اداره کل /سازمان/ شرکت/...)) برای جلوگیری از تهدیدهای حاصل از به‌کارگیری خارج از کنترل آن‌ها.

مسئولیت‌ها

- مسئولیت جلوگیری از استفاده بدون مجوز از ابزار، نرم‌افزارها و درگاه‌های تشخیص وضعیت و عیب یابی در شبکه‌های تحت اختیار یا متعلق به ((وزارت/ اداره کل /سازمان/ شرکت/...)) به عهده مدیر ارشد شبکه می‌باشد.
- مسئولیت بررسی دوره‌ای شبکه برای اطمینان از عدم وجود ابزار، نرم‌افزارها و درگاه‌های تشخیص وضعیت و عیب یابی بدون مجوز به عهده مدیر نهاد متصدی امنیت اطلاعات یا نهاد جایگزین وی می‌باشد.

الزامات

- فقط در مواقع ضروری و با حصول اجازه از مدیر امنیت اطلاعات و با اخذ تضمین‌های امنیتی لازم، استفاده از ابزارهای مناسب، دسترسی فیزیکی و منطقی به درگاه‌های تشخیص وضعیت و عیب یابی (به صورت مقطعی یا موردی) مجاز خواهد بود.
- ورود مستقیم به سرورهای موجود در شبکه از راه دور به منظور پیکربندی و یا تنظیم سیستم و یا هر گونه بهره‌برداری دیگر از طرف هر یک از راهبران و بهره‌برداران شبکه ممنوع می‌باشد.
- تمامی ارتباطات سویچ‌ها و وضعیت پورت‌های آن‌ها نیز باید به صورت کامل مانیتور شوند.
- لازم است تمامی ترافیک عبوری شبکه از سویچ‌ها و مسیریاب‌ها مانیتور شوند و ارتباطات گره‌ها با هم به همراه پروتکل‌های آن‌ها نمایش داده شوند و به محض کشف پروتکل‌های دسترسی، خطایابی و رفع اشکال از راه دور، اخطار امنیتی مناسب صادر شده و در صورت عدم تایید به موقع، علاوه بر قطع پروسه مربوط وضعیت پیش آمده به عنوان حادثه امنیتی ثبت و پیگیری شود.
- تمامی ترافیک شبکه عبور کننده از سویچ‌ها و مسیریاب‌ها باید ثبت و نگهداری شده و در بازبینی‌های دوره‌ای از لحاظ کشف تبادلهای مربوط به شناسایی، خطایابی و رفع اشکال از

راه دور نیز مورد بررسی قرار گیرد.

- لازم است پورت **telnet** تجهیزات مسیریابی در مواقع غیر ضروری بسته باقی بماند.
- لازم است پورت‌های خدمات ویژه مثل خدمات مدیریت راه دور در مواقع غیر ضروری بسته باقی بمانند.

فرآیند

برای نگهداری و رفع اشکال بسیاری از کامپیوترها و سیستم‌های ارتباطی از درگاه‌های خاصی استفاده می‌شود که می‌توان از راه دور و با استفاده از خطوط تلفن یا سایر خطوط ارتباطی به آن‌ها متصل شد. هر یک از دستگاه‌هایی که برای برقراری ارتباط خودکار با کاربران راه دور مورد استفاده قرار می‌گیرند را می‌توان به عنوان دروازه‌ای برای دسترسی غیرمجاز به اطلاعات به شمار آورد. در صورتی که دسترسی به تجهیزات مسیریابی و کنترل ارتباطات از طریق پورت‌ها و پروتکل‌های رفع اشکال از راه دور ایجاد شود شدت تهدیدات امنیتی ناشی از آن بسیار زیاد خواهد بود. برای جلوگیری از ایجاد این نوع تهدید لازم است از طریق به‌کارگیری فرآیند زیر این نوع فعالیت‌ها تحت کنترل کامل قرار گیرد:

- شناسایی سرویس‌های رفع اشکال از راه دور و درگاه‌ها
 - ایجاد وجاری سازی روندی استاندارد برای ثبت تمامی ورودی و خروجیهای کاربران به شبکه
 - ایجاد وجاری سازی روندی استاندارد برای کنترل دسترسی فیزیکی و منطقی به درگاه‌های تشخیص وضعیت و عیب‌یابی
 - ایجاد وجاری سازی روندی استاندارد برای ثبت ترافیک شبکه عبور کننده از سویچ‌ها و مسیریاب‌ها
 - مانیتورینگ و نمایش تمامی سویچ‌ها و وضعیت پورت‌های آن‌ها
 - مانیتورینگ و نمایش تمامی کاربرانی که در شبکه مشغول فعالیت هستند (**login** نموده‌اند)
 - ارزیابی و بازنگری سطح دسترسی کاربران متصل به شبکه‌های خارج از سازمان
 - بازنگری دوره‌ای درسیاست کنترل دسترسی فیزیکی و منطقی به درگاه‌های تشخیص وضعیت و عیب‌یابی
- اعمال روش‌های اجرایی فرآیند فوق به شرح زیر امکانپذیر است :

- تدوین روال و دستورالعمل گرفتن نسخه پشتیبان برای هر تغییر در پیکربندی به‌طور منظم (به عنوان مثال هر یک ماه یک بار)
- طراحی توپولوژی امن شبکه و اجرای آن
- جداسازی شبکه با VLAN و Sub netting
- محدود سازی IP اتصال به روتر جهت پیکربندی مدیریتی همچنین برای DSLAM
- Shutdown کردن پورت Auxiliary
- غیرفعال نمودن سرویس‌های غیر ضروری و مخاطره آفرین چون Telnet, Bootp, TFTP, Auto loading و استفاده از سرویس‌های SSH و FTP به عنوان جایگزین.
- محدودسازی زمان اتصال: Timeout برای کنسول و خط VTY
- طرح جامع مانیتورینگ در لایه‌های شبکه روی تجهیزات شبکه به‌علاوه در صورت امکان:
- IPsec Policy Agent برای جلوگیری از تغییر غیر مجاز در پیکربندی پروتکل IPsec غیرفعال شود.
- Licensing Logging Service غیرفعال شود.
- Logical Disk Manager Admin Service غیرفعال شود.
- Remote Registry Service برای جلوگیری از تغییر غیر مجاز در Registry (از راه دور) غیرفعال شود.
- Removal Storage غیرفعال شود.
- اجرای برنامه‌ها در قالب سرویس (Run a Service) غیرفعال شود.
- Server Service برای جلوگیری از تغییر غیرمجاز در پیکربندی سرور غیرفعال شود.
- Task Scheduler برای جلوگیری از اجرای خارج از کنترل برنامه‌ها یا کدهای مخرب غیرفعال شود.
- Telephony Service برای جلوگیری از اتصال به سرویس دهنده‌های Telephony غیرمجاز غیرفعال شود.
- Windows Installer غیرفعال شود.
- Windows Time غیرفعال شود.

- **WorkStation Service** برای جلوگیری از امکان اجرای برنامه‌ها از راه دور غیرفعال شود.
- **Computer Browser** برای جلوگیری از امکان مشاهده سایر کامپیوترهای همسایه و منابع به اشتراک گذاشته شده توسط آن‌ها غیرفعال شود.
- **Directory Browsing** در کلیه وب‌سایت‌ها و دایرکتوری‌های مجازی غیرفعال شود.
- **Network Monitor Agent** برای جلوگیری از دستیابی به ترافیک سایر زیرشبکه‌های متصل غیرفعال شود.
- **RPC Locator** برای جلوگیری از یافتن برنامه‌های قابل اجرای موجود در میزبان‌های دیگر غیرفعال شود.
- **Spooler** به منظور محدود کردن دسترسی به پرینتر از طریق وب سرور غیرفعال شود.
- **TCP/IP Net Bios Helper** غیرفعال شود.
- دسترسی به تمامی پورت‌های **TCP/IP** ثبت و بررسی شود.
- کنترل دسترسی از طریق **VPN** به عنوان یک اقدام پیشگیرانه قبل از **FTP login** قرار گیرد.
- اقدامات پیشگیرانه به منظور اطمینان از اینکه از سرور **FTP** به منظور دسترسی به سیستم فایل شبکه شرکت استفاده نمی‌شود، انجام شود.
- در صورت استفاده از مدل آدرس دهی ایستا، **DHCP Client** غیرفعال شود.

مرجع:

این دستورالعمل به شماره □-□/□-۷-۴-□-□ به ثبت رسیده است.

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	کنترل دسترسی شبکه
جداسازی شبکه‌ها شماره دستورالعمل : ۵-۴-۷	

محرمانه

تائیدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد

بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام‌الاختیار ((بالاترین مقام اجرایی سازمان))	رئیس
	مسئول ((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات))	*دبیر
	معاون ((اداری، مالی و پشتیبانی))	عضو
	معاون ((برنامه‌ریزی))	عضو
	معاون ((فنی))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات ((معاون پشتیبانی)) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

هدف از تدوین این دستورالعمل بیان ضرورت جداسازی شبکه‌های مختلف از یکدیگر برای جلوگیری از آسیب‌های ناشی از دسترسی به اطلاعات موجود در یک شبکه از طریق شبکه دیگر است.

مسئولیت:

- مسئولیت تعریف حدود هر شبکه رایانه‌ای یا مخابراتی به عهده ((بالاترین مقام اجرایی)) سازمان می‌باشد.
- مسئولیت جداسازی شبکه‌های رایانه‌ای تعریف شده در یک سازمان و یا جداسازی شبکه‌های سازمانی از یکدیگر و یا از سایر شبکه‌های دیگر به عهده مدیر ارشد شبکه ((وزارت/ سازمان/ اداره کل/ شرکت...)) می‌باشد.
- مسئولیت نظارت بر اجرای این دستورالعمل به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین وی می‌باشد.

الزامات:

- لازم است شبکه‌های تحت مالکیت ((وزارت/ سازمان/ اداره کل/ شرکت...)) با توجه به نوع اطلاعات جاری در آن‌ها و سطح طبقه‌بندی حفاظتی با استفاده از روش‌های مناسب به‌صورت منطقی یا فیزیکی از یکدیگر و از شبکه‌های بیگانه جداسازی شوند.
- جداسازی شبکه‌ها باید در دو سطح منطقی (با استفاده از تعریف منطقی شبکه‌های مجزا از یکدیگر و به کارگیری مکانیزم‌های کنترل دسترسی برای برقراری ارتباط بین آن‌ها) و یا سطح فیزیکی (با استفاده از قطع اتصال‌های کابلی و بی سیم بین شبکه تحت حفاظت از سایر شبکه‌ها) انجام شود.
- به‌طور کلی لازم است شبکه‌ها به دو دسته شبکه داخلی (شامل LANها و DMZ) و خارجی (شامل کلیه شبکه‌های خارج از کنترل سازمان) دسته‌بندی شوند.
- اتصال بین شبکه‌های داخلی و شبکه خارجی عمومی باید از طریق DMZ انجام شود.
- اگر از شبکه‌های خارجی عمومی برای اتصال بین دو شبکه داخلی سازمان استفاده می‌شود لازم است همراه با DMZ از مکانیزم نقطه امن نیز برای جداسازی شبکه‌ها از یکدیگر استفاده شود.
- به‌طور کلی لازم است جهت جداسازی شبکه‌های داخلی متفاوت از لحاظ طبقه‌بندی حفاظتی از مکانیزم نقطه امن استفاده شود.

- شبکه‌هایی که اطلاعات جاری در آن‌ها دارای طبقه‌بندی حفاظتی بالاتر از خیلی محرمانه است باید به صورت فیزیکی از سایر شبکه‌ها جداسازی شوند.

فرآیند:

شبکه‌های رایانه‌ای به صورت روز افزون گسترش یافته و مرزهای سازمانی را پشت سر می‌گذارند. نیاز به استفاده از منابع مشترک اطلاعاتی و یا به اشتراک گذاشتن منابع با سایر مراجع موجب بروز چنین حالتی شده است. این گسترش ممکن است باعث افزایش ریسک دسترسی غیر مجاز به اطلاعاتی شود که دارای حساسیت زیاد بوده و یا نیازی به اشتراک گذاشتن آن‌ها وجود ندارد.

در چنین حالتی ایجاد روش‌های کنترلی شبکه‌ای برای جداسازی گروه‌های مختلف کاربران، سیستم‌های اطلاعاتی و خدمات پردازشی - مخابراتی از یکدیگر ضروری خواهد بود. یکی از روش‌های کنترل امنیت شبکه‌های بزرگ یا نسبتاً بزرگ تقسیم کردن این شبکه‌ها به دو محدوده عام شبکه داخلی سازمان و شبکه خارجی سازمان می‌باشد. شبکه داخلی شبکه‌ای است که متشکل از ایستگاه‌های کاری، تجهیزات پردازشی و مخابراتی و منابعی است که به کاربران داخلی سازمان سرویس دهی می‌نمایند و شبکه خارجی سازمان نیز عبارت است از منابع، تجهیزات پردازشی و مخابراتی که به مشتریان یا کاربران غیر وابسته به سازمان (و یا کاربران وابسته به سازمان که از راه دور به شبکه داخلی متصل می‌شوند) سرویس می‌دهند. لازم است ترافیک بین دو محدوده تعریف شده فوق از طریق مکانیزم نقطه امن که در پیوست دستورالعمل ۱-۷-۱ شرح داده شده است تحت کنترل قرار گیرد. استفاده از فایروال بهترین روش برای جداسازی منطقی بین دو شبکه می‌باشد، همچنین در شبکه داخلی می‌توان از روش‌های ایجاد VPN یا VLAN برای جداسازی بخش‌های مختلف شبکه‌ها از یکدیگر استفاده نمود.

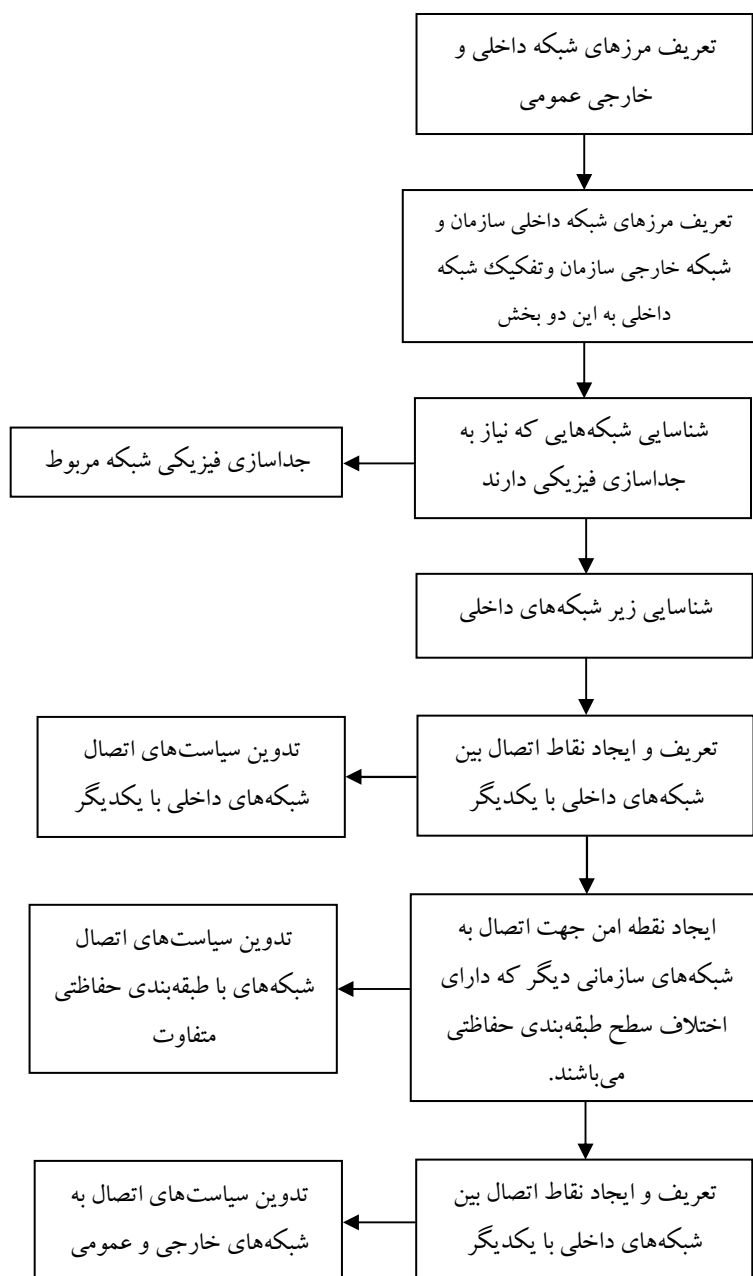
مرجع:

این دستورالعمل به شماره □-□/۵-۴-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۷-۱
- دستورالعمل ۲-۴-۷

روندنما:

روندنمای جداسازی شبکه‌ها در شکل زیر نمایش داده شده است:



(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	کنترل دسترسی شبکه
کنترل اتصال‌های شبکه شماره دستورالعمل : ۶-۴-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد

بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام‌الاختیار ((بالاترین مقام اجرایی سازمان))	رئیس
	مسئول ((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات))	*دبیر
	معاون ((اداری، مالی و پشتیبانی))	عضو
	معاون ((برنامه‌ریزی))	عضو
	معاون ((فنی))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات ((معاون پشتیبانی)) سازمان به‌عنوان دبیر منصوب

خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

محدود سازی توانایی اتصال کاربران به شبکه تحت اختیار ((وزارت/ سازمان/ اداره کل/ شرکت /...)) به خصوص اتصال کاربران راه دور و اطمینان از اعمال سیاست گذاری کنترل دسترسی در خصوص اتصال کاربران به شبکه

مسئولیت:

- مسئولیت تدوین و ایجاد روش‌های محدود سازی به عهده مدیر ارشد شبکه ((وزارت/ سازمان/ اداره کل/ شرکت /...)) می‌باشد.
- مسئولیت نظارت بر اجرای روش‌های تدوین شده محدود سازی اتصال به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن می‌باشد.

الزامات:

- لازم است نقاط اتصال شبکه به صورت مداوم و در بازه‌های زمانی از پیش تعیین شده از لحاظ عدم وجود اتصال‌های فیزیکی غیر مجاز (اعم از کابلی یا بی سیم) بازبینی شود.
- لازم است مستندات نحوه اتصال فیزیکی و مسیرهای عبوری در نقاط اتصال شبکه به صورت کاملاً شفاف و به روز تهیه و نگهداری شده تا در صورت به روز مشکل بتوان از آن‌ها استفاده کرد.
- لازم است ترافیک عبوری از نقاط ارتباطی شبکه در بخش‌های مختلف به صورت منظم و خودکار مانیتور و Log برداری گردد (برای این کار باید از نرم‌افزارهای مانیتورینگ تائید شده استفاده شود. برخی از نرم‌افزارهای مانیتورینگ به صورت عامل شوند و جاسوسی عمل می‌کنند).
- لازم است در مواقع لزوم از مکانیزم‌های امنیتی مناسب مثل Access List ها (ACLs) و یا محدود کننده‌های ترافیک و یا مکانیزم‌های اولویت بندی و دسته‌بندی ترافیک (QoS³³ و CoS³⁴) بر اساس مشخصات مبداء و مقصد از جمله آدرس IP و آدرس فیزیکی مبداء و مقصد استفاده شود.
- در نقاط ارتباط شبکه با شبکه‌های خارجی عمومی باید از فایروال استفاده شده و تمام فعالیت کاربران توسط مکانیزم‌های AAA³⁵ تحت کنترل قرار گیرد.

³³ Quality of Service³⁴ Class of Service³⁵ Authentication, Authorization, Accounting

- لازم است در نقاط اتصال با شبکه‌های دیگر و یا در ایستگاه‌های کاری حساس از مکانیزم‌های **IDS** و **IPS** برای تشخیص و جلوگیری از نفوذ استفاده شود.
- تخطی از سیاست‌گذاری کنترل دسترسی، کنترل اتصال‌های شبکه یا کشف ترافیک ناشناس یا غیر مجاز باید به عنوان حادثه امنیتی ثبت و مورد رسیدگی قرار گیرد.

فرآیند:

بر اساس نیازهای سیاست‌گذاری کنترل دسترسی (موضوع دستورالعمل ۷-۱-۱) در شبکه‌های به اشتراک گذاشته شده، به‌خصوص شبکه‌هایی که فراتر از محدوده تحت کنترل ((وزارت/ سازمان/ اداره کل/ شرکت/...)) گسترش یافته اند، در مواردی لازم است تدابیر خاصی برای جلوگیری از اتصال برخی کاربران از راه دور (اعم از کاربران سازمانی یا سایر کاربران) در نظر گرفته شود. این کار با استفاده از کنترل نقاط اتصال فیزیکی (برای شناسایی اتصال‌های غیر مجاز) و کنترل ترافیک عبوری نقاط اتصال بر اساس جداول و قواعد مسیریابی امکانپذیر می‌باشد. محدودیت‌ها باید بر اساس سیاست‌گذاری امنیتی و نیازهای نرم‌افزاری و سخت‌افزاری برنامه‌های کاربردی و سیستم‌های اطلاعاتی سازمانی تعریف شده و به‌صورت مرتب بازبینی و به‌هنگام شوند. برخی از کاربردهایی که باید از طریق اعمال محدودیت کنترل شوند عبارت‌اند از:

- پست الکترونیک
- ارسال فایل یک طرفه
- ارسال فایل دو طرفه
- دسترسی ممتاز
- دسترسی به روال‌های شبکه‌ای تولید و کنترل ساعت و تاریخ شبکه و یا ایستگاه‌های کاری

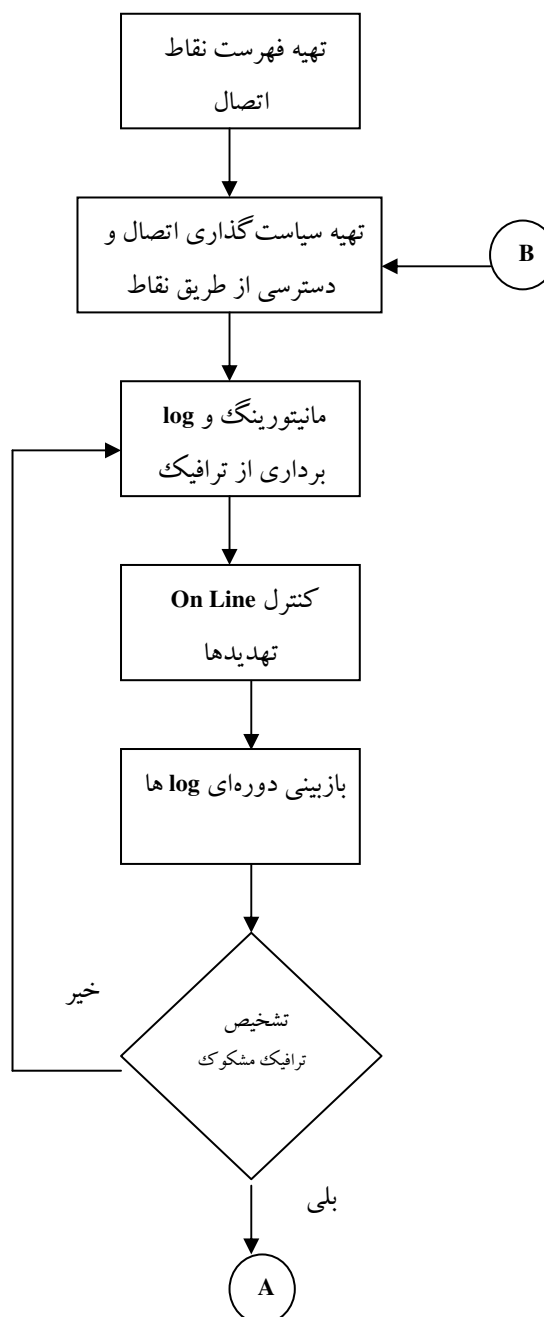
فرم‌های ضمیمه شده به این دستورالعمل را می‌توان به عنوان فرم‌های نمونه در کنترل ترافیک نقاط اتصال به‌کار گرفت.

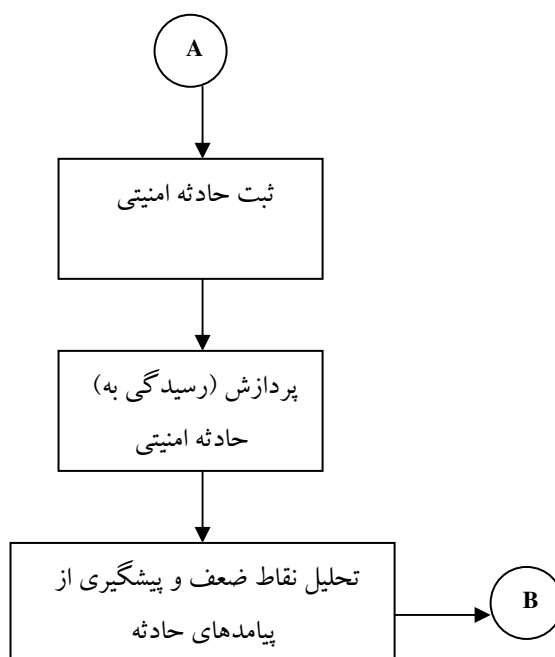
مرجع:

- این دستورالعمل به شماره □-□/۶-۴-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:
- دستورالعمل ۷-۱-۱

روندنما:

روندنمای کنترل اتصال‌های شبکه در شکل زیر نمایش داده شده است:





فرم ثبت ترافیک از تا
(نمونه)

نام نقطه ارتباطی	میانگین ترافیک ورودی	میانگین ترافیک خروجی	مجموع ترافیک ورودی	مجموع ترافیک خروجی	رفتار طبیعی یا غیر طبیعی	توضیحات

فرم گزارش ترافیک غیر طبیعی
(نمونه)

نام نقطه ارتباطی:			
آدرس	Port:	IP:	MAC:
زمان:	روز:	ساعت:	دقیقه:
آدرس منشاء	Port:	IP:	MAC:
نوع ترافیک:			
تهدید احتمالی:			
عملکرد:			

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	کنترل دسترسی شبکه
کنترل مسیریابی	
شماره دستورالعمل : ۷-۴-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	ریس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	دبیر*
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

پیشگیری از ایجاد شرایط رخنه از طریق ارتباط کاربران با برنامه‌های کاربردی و یا برقراری ارتباط راه دور بین شبکه‌های رایانه‌ای به دلیل سوءاستفاده از خصوصیات یا عملکرد الگوریتم‌های مسیریابی

مسئولیت

- مسئولیت امن‌سازی شبکه‌های رایانه‌ای تحت اختیار ((وزارت/ سازمان/ اداره کل/ شرکت...)) به عهده مدیر ارشد شبکه سازمان می‌باشد.
- مسئولیت امن‌سازی پروتکل‌ها و تجهیزات مسیریابی مورد استفاده در شبکه‌های رایانه‌ای تحت اختیار به عهده مدیر ارشد شبکه سازمان می‌باشد.
- مسئولیت نظارت بر امن‌سازی روش‌ها، پروتکل‌ها و تجهیزات مسیریابی به عهده مدیر واحد امنیت اطلاعات و یا نهاد جایگزین آن می‌باشد.

الزامات

- لازم است پروتکل‌ها و تجهیزات مسیریابی شبکه از طریق شناسایی آدرس‌های مبدا و مقصد بسته‌های اطلاعاتی و بررسی مجاز بودن ارسال آن‌ها تحت کنترل قرار گیرد.
- حتی الامکان باید از مکانیزم تبدیل آدرس‌های شبکه (NAT) در نقاط اتصال شبکه‌های داخلی و خارج از سازمان و یا برای جداسازی و حفاظت از بخش‌های خاص شبکه استفاده شود.
- حتی الامکان باید از پروتکل‌های مسیریابی ایستا (Static) جهت مسیریابی شبکه به خصوص در لایه‌های مرزی استفاده شود.
- در صورت استفاده از الگوریتم‌های مسیریابی دینامیک داخلی یا خارجی (Dynamic Routing) باید از مکانیزم‌های تشخیص هویت جهت امن‌سازی تبادل اطلاعات مسیریابی استفاده شود.
- لازم است امکانات اتصال مستقیم به مسیریاب یا سویچ‌های شبکه‌ای مثل پورت Console یا Aux تحت کنترل کامل قرار داشته باشد تا از سوء استفاده از این امکانات برای دخالت در مسیریابی جلوگیری شود.
- پیکربندی، راه اندازی و یا نصب مجدد مسیریاب باید توسط افراد معتمد انجام شود.

- در صورت استفاده از الگوریتم‌های مسیریابی دینامیک لازم است از مکانیزم‌های **Route Filtering** برای جلوگیری از انتشار اطلاعات مسیریابی داخلی به شبکه‌های خارجی استفاده شود.
- لازم است مکانیزم‌های **Source Routing** و **Direct Broadcast** مسیریاب‌ها غیر فعال گردند.

مرجع:

این دستورالعمل به شماره □-□/۷-۴-۷/□-□ به ثبت رسیده است.

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت / ...)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی سیستم عامل
سیاست گذاری امن سازی، کنترل دسترسی سیستم عامل و رویه‌های امن آغاز به کار شماره دستورالعمل : ۷-۵-۱	

عادی

تأییدیه نهایی

نام و نام خانوادگی: ((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: ((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:		
نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامهریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

سوابق تغییرات :	
تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل بیان ضرورت پیشگیری از دسترسی غیر مجاز به سیستم‌های عامل و کنترل دسترسی به سیستم‌های عامل نصب شده بر روی تجهیزات پردازشی اعم از سیستم عامل‌های عام و خاص می‌باشد.

مسئولیت‌ها

- مسئولیت تنظیم سیاست‌های کنترل دسترسی به سیستم‌های عامل مورد استفاده در سرورهای شبکه و کلیه ایستگاه‌های کاری متصل به آن و سیستم عامل‌های خاص تجهیزات مسیریابی به عهده مدیر ارشد شبکه می‌باشد.
- مسئولیت تنظیم سیاست‌های کنترل دسترسی به سیستم‌های عامل مورد استفاده در سرورهای دارای کاربرد امنیتی و کلیه ایستگاه‌های کاری مربوط به مانیتورینگ و سیستم عامل‌های خاص تجهیزات امنیتی از قبیل فایروال، سامانه‌های تشخیص نفوذ (IDS) به عهده مدیر نهاد متصدی امنیت اطلاعات می‌باشد.
- مسئولیت نظارت بر اجرای سیاست‌های کنترل دسترسی در حوزه سیستم عامل به عهده مدیر نهاد متصدی امنیت اطلاعات می‌باشد.

الزامات

- - لازم است با استفاده از امکانات امنیتی در سطح سیستم عامل، از دسترسی غیر مجاز به دارایی‌های اطلاعاتی به وسیله تجهیزات کامپیوتری جلوگیری کرد. این امکانات باید توانایی انجام فعالیت‌های زیر را ایجاد نمایند:
 - الف) شناسایی و بررسی هویت و در صورت ضرورت پایانه یا مکان هر یک از کاربران مجاز
 - ب) ثبت اقدامات موفق یا غیر موفق ورود به سیستم
 - پ) فراهم آوری امکانات مناسب برای تصدیق هویت (در صورتی که روش مدیریت کلمه عبور مورد استفاده قرار می‌گیرد، باید از کفایت این روش اطمینان حاصل شود)
 - ت) محدود ساختن زمان‌های ارتباط کاربران
- لازم است دسترسی به خدمات اطلاعاتی از طریق یک فرآیند امن شروع به کار، امکان پذیر باشد. رویه ی شروع به کار و ورود به هر سیستم رایان‌های یا دسترسی به هر دارایی

اطلاعاتی باید به نحوی طراحی شود که هرگونه فرصت دسترسی غیرمجاز را به حداقل برساند.

- لازم است رویه ورود به سیستم، حاوی حداقل اطلاعات مربوط به سیستم باشد تا از ارائه اطلاعاتی که ممکن است منجر به شناسایی سیستم توسط افرادی شود که قصد ورود غیرمجاز به آن را دارند جلوگیری به عمل آید. هر رویه ورود مناسب باید :

- الف) قبل از تکمیل موفقیت آمیز رویه ورود، هیچ شناسه‌ای از سیستم یا برنامه‌های کاربردی آن را نمایش ندهد.
- ب) هنگام ورود یک اخطار عام در مورد این که فقط افراد مجاز اجازه استفاده از سیستم دارند را نمایش دهد.
- پ) هیچ گونه پیام‌های کمکی را که اطلاعات مندرج در آن بتواند در شناسایی سیستم، مورد استفاده کاربران غیرمجاز قرارگیرد نمایش ندهد.
- ت) فقط پس از ورود کامل اطلاعات احراز هویت، مراحل ارزیابی را انجام دهد و در صورت بروز اشکال نباید محل و دلیل وقوع آن را نمایش داده و یا صحیح بودن یا نبودن هر قسمت از اطلاعات را گزارش کند.
- ث) تعداد دفعات ورود ناموفق را به حداکثر سه بار محدود نماید و :

- ۱- کوشش‌های ناموفق را ثبت کند.
- ۲- در صورت وقوع یک تلاش ناموفق، (برای جلوگیری از اجرای حمله‌های فرهنگ لغت یا حدس کلمه عبور) تاخیر زمانی مناسب برای تلاش بعدی ایجاد شود و یا نیاز به تصدیق هویت خاصی الزامی باشد.
- ۳- در صورت مشکوک بودن درخواست دسترسی، خط ارتباطی مربوط قطع شود.

- ج) حداقل و حداکثر زمان صرف شده برای اجرای رویه ورود را محدود نماید و در صورت تجاوز از این محدوده خط ارتباطی قطع شود.
- چ) پس از موفقیت آمیز بودن اجرای رویه ورود، اطلاعات زیر نمایش داده شود:
 - - تاریخ و زمان آخرین ورود موفقیت آمیز قبلی
 - - جزئیات کلیه تلاش‌های ناموفق ورود از زمان آخرین ورود موفق

- برای هر یک از سه سطح کاربران عادی، کاربران دارای حق دسترسی ممتاز و مدیران شبکه با توجه به نیازمندیهای امنیتی آنها باید سیستم‌های عامل مناسب به صورت مستدل انتخاب شود و پیکربندی امنیتی آنها با عنایت به دستورالعمل‌های منتشر شده از سوی مدیر ارشد شبکه یا مدیر امنیت اطلاعات انجام شود.
- ارتقاء در سطح سیستم‌های عامل مورد استفاده در سازمان باید با پیشنهاد مدیر ارشد شبکه و تأیید مدیر نهاد متصدی امنیت اطلاعات صورت گیرد.
- نصب آخرین وصله‌های امنیتی (Security Patches) الزامی می‌باشد.
- رویدادهای امنیتی رخ داده در هنگام آغاز به کار سیستم‌های عامل باید به عنوان حادثه امنیتی ثبت و گزارش شود.

فرآیند

- فرآیند کنترل دسترسی سیستم عامل و اجرای رویه‌های امن آغاز به کار شامل طیف گسترده‌ای از اقدامات امنیتی است که بخش اعظمی از فعالیت‌های مدیریت امنیت اطلاعات را تشکیل می‌دهد. فهرست اقدامات امنیتی که مرتبط با این حوزه می‌باشد در ادامه درج شده است. بدیهی است که برای اجرای بخش عمده‌ای از این اقدامات نیاز به برنامه ریزی گسترده و تهیه مستندات مدیریتی می‌باشد. البته باید توجه داشت که حد به کارگیری این اقدامات بر اساس ماهیت و محیط عملیاتی سامانه‌های تحت حفاظت و بر اساس تصمیم مدیر نهاد متصدی امنیت اطلاعات تعیین خواهد شد. جهت امن سازی مدل‌های کنترل دسترسی به سیستم عامل لازم است قدم‌های زیر طی شود:
- یک سیاست کلی برای کنترل دسترسی سیستم‌ها تهیه شود که در آن فرایندهای دسترسی، مدیریت، بروزرسانی، خصوصیات لازم برای حسابهای کاربری، کلمه عبور، پشتیبان‌گیری و... با جزییات لازم شرح داده شود.
 - مستندات مربوط به برنامه زمانبندی پشتیبان‌گیری، بروزرسانی و نصب وصله‌های امنیتی که به‌طور مقرر انجام می‌شود تهیه و به اجراء گذاشته شود.
 - اطمینان حاصل شود که صلاحیت و کفایت خدمات پشتیبانی تهیه کنندگان سیستم‌های عامل براساس اطلاعات گذشته، فعلی و آینده راجع به امنیت سیستم عامل به‌طور منظم مورد بررسی قرار می‌گیرند.
 - سیاست‌گذاری کنترل دسترسی برنامه‌های کاربردی نیز مورد بررسی قرار گیرد.

- مستنداتی برای شرح سیستم عامل‌های متفاوت و نسخه‌های متفاوت سیستم عامل‌ها تهیه شود.
- اطمینان حاصل شود که کلمه عبورهای مدیریتی متفاوت به‌منظور جداسازی دسترسی به سیستم عامل از سایر دسترسی‌هایی که نیاز به حقوق مدیریتی دارند وجود دارد.
- رسانه‌های مورد استفاده برای نصب به نحوی مناسب در یک محیط امن ذخیره شود.
- رسانه‌های مورد استفاده برای پشتیبان‌گیری از سیستم عامل در یک محیط امن ذخیره شود.
- فهرست کامل فرآیندهای صحیح و بروز شده برای نصب یا نصب مجدد سیستم عامل شامل تمامی وصله‌های بروزرسانی شده و دانه‌های مورد نیاز تهیه شود.
- طرح‌های آزمایش شده برگشت به قبل برای وقتی که برنامه بروزرسانی سیستم عامل با خطا مواجه می‌شود تدوین گردد.
- اطمینان حاصل شود که وقایع نگاری (log برداری) مناسبی به‌منظور ضبط رخداد‌های مربوط به سیستم عامل، به خصوص آغاز به کار و کنترل دسترسی وجود دارد.
- وقایع نگاری‌های ثبت شده مربوط به رخداد‌های سیستم عامل به‌طور مرتب مورد بررسی قرار گیرد.
- در نظر داشته باشید که فایل‌های سیستم عاملی روی یک پارتیشن، دیسک و یا سرور مجزا قرار گیرد.
- در طرح‌های بازیابی بهنگام حادثه (DRP^{۳۶})، طرحی خاص برای بازیابی سیستم عامل شامل مدیریت بازیابی، طرح گام به گام نصب و راه اندازی، جایگاه نرم‌افزارهای پشتیبان‌گیری، نصب مجدد وصله‌ها و... آماده شود.
- اطمینان حاصل شود که دسترسی به فایل‌های سیستم عامل، بدرستی محدود شده است.
- پشتیبان‌گیری مرتب فایل‌های سیستم عاملی طبق زمانبندی از پیش تعیین شده عمل شود.
- اگر یک سیستم پشتیبان‌گیری وجود دارد، صحت عملکرد آن آزمایش شود.
- برنامه زمانبندی شده‌ای برای بررسی منظم وصله‌ها و دانه‌های لازم برای سیستم عامل ترتیب داده شود.

³⁶ - Disaster Recovery Plan

- اطمینان حاصل شود که کاربرانی که مجوزهای مدیریتی دارند، برخوردار از سابقه حرفه‌ای مناسب و آموزش‌های لازم براساس نیازمندیهای شغلی هستند
- نرم‌افزارهایی که روی سیستم عامل بار می‌شود به طور کامل بررسی و تاثیرات آن بر روی محیط سیستم عامل کنترل گردد.
- روال‌هایی برای رسیدگی و پیگیری به دسترسی‌های غیرمجاز به محیط و فایل‌های سیستم عامل تهیه شود.
- پروفایل‌های مربوط به گروه‌ها و کاربران به منظور اطمینان از اینکه هیچ دسترسی غیرمجازی، مجاز نشده باشد بررسی شود.
- در صورت کنترل دسترسی از طریق سرویس دهنده‌های AAA به فایل‌های سیستمی و شبکه، اطمینان حاصل شود که سطح امنیتی مناسبی برای دسترسی به آن در نظر گرفته شده است.
- اطمینان حاصل شود که تغییرات امنیتی، خطاها و آسیب پذیریه‌های کشف شده مربوط به سرویس‌های سرویس AAA، ثبت، مکاتبه و به‌طور مناسبی با آن برخورد می‌شود
- اطمینان حاصل شود که برای سرویس‌های کنترل دسترسی مهم، اقدامات پیشگیرانه امنیتی مناسب برای ارتباطات شبکه ای، نقاط دسترسی و کامپیوترهای میزبان آن‌ها اعمال شده است.
- مدیر سیستم باید دو نام کاربری و کلمه عبور متفاوت داشته باشد. یکی برای دسترسی‌های امن و محدود و دیگری برای استفاده عادی از کامپیوتر.
- تاثیر پروفایل امنیتی بروی کارایی سیستم عامل برای برنامه‌های کاربردی مانند Oracle, Sybase و... بررسی شود.
- اطمینان حاصل شود که در صورت ایجاد تغییرات در مجوزهای پیش فرض فایل‌ها و شاخه‌ها در نتیجه اعمال تنظیمات موقتی، در پایان کار مجوزها به حالت قبل برمیگردند.

روش‌های اجرایی و رویه‌ها

- در سیستم عامل خانواده Windows NT، Windows 2000 و Windows 2003 علاوه بر رعایت توصیه‌های مندرج در پیوست یک مراحل زیر به اجرا گذاشته شود:
- سیاست‌های اتخاذ شده برای اجراء توسط کاربر محلی با توانایی‌های خاصی که کاربر باید داشته باشد تا بتواند آن‌ها را اجراء کند (پشتیبان‌گیری، مدیریت، خاموش کردن و ...) مقایسه شود.

- برای هرکار تاثیرگذار بر عملکرد شبکه از قبیل مدیریت، خاموش کردن، پشتیبان‌گیری، مدیریت وقایع نگاریها و... دسترسی‌های مجازشده برای گروهها و کاربران مختلف، تاثیرات جنبی آن بررسی شود.
- با سطح بندی مناسب در سیاست‌های ممیزی، دسترسیهای غیرمجاز ثبت و از آن جلوگیری شود.
- اطمینان حاصل شود که وقایع نگاری درمورد رخدادها، سیستم‌ها، برنامه‌های کاربردی انجام می‌شود.
- اطمینان حاصل شود که میزان فضای اختصاص داده شده به وقایع نگاری‌های رخدادها، سیستم و برنامه‌ها (log برداری) کافی است.
- اطمینان حاصل کنید که روزانه از اطلاعات وضعیت سیستم کنترل دامنه (DC) پشتیبان‌گیری می‌شود.
- استفاده از مکانیزم sharing در سیستم‌عامل‌های خانواده‌ی windows به صورت پیش‌فرض ممنوع می‌باشد. موارد خاص این زمینه باید به صورت تقاضای مکتوب به مدیر امنیت اطلاعات ارائه شوند. مدیر امنیت اطلاعات در این زمینه مجوز لازم را برای افراد نیازمند آن اطلاعات و برای مدت محدود (مثلا نیم الی سه ساعت) صادر خواهد نمود.
- حق دسترسی به کامپیوتر از طریق شبکه (Access This Computer Over Network) از روی سرور وب به طور کامل تحت کنترل قرار گیرد.
- با انجام تست اطمینان حاصل شود که درهنگام ایجاد مشکل برای کنترل کننده دامنه اصلی، کنترل کننده دامنه ثانویه میتواند نقش جایگزین را بخوبی انجام دهد.
- اطمینان حاصل شود که ریسک‌های مرتبط به زمان‌های تعمیر اضطراری بررسی شده و تحت کنترل است.
- اطمینان حاصل شود که بوت شدن سروربه ترتیب از هارد سپس از فلاپی و یا CD-ROM انجام می‌شود (ترتیب بوت شدن در BIOS سیستم تنظیم می‌شود).
- اطمینان حاصل شود که برای ورود به BIOS نیاز به کلمه عبور مناسب باشد تا ترتیب بوت شدن و سایر تنظیمات BIOS از تغییر مصون نگهداری شود.
- در صورت امکان سوء استفاده از فلاپی درایو برای ایجاد مشکل در سیستم و یا ویروسی شدن سیستم به علت نصب نرم‌افزار از طریق فلاپی، فلاپی درایو غیرفعال شود.
- حساب کاربری مهمان تا زمانی که به آن نیاز نیست غیرفعال شود.

- سرور دسترسی از راه دور (**Remote Access Server**) در صورت عدم نیاز غیرفعال شود.
- گزینه **Run** بروی منو فایل برای ایستگاه‌های کاری مخصوص کاربران غیرفعال شود.
- **Logoff** و **Logon** مورد بازرسی قرار گیرد تا از موفقیت و یا شکست به کارگیری ابزار سیاست‌گذاری امنیتی اطلاع حاصل شود.
- دسترسی به اشیا و فایل‌ها مورد بازرسی قرار گیرد تا از موفقیت و یا شکست به کارگیری ابزار سیاست‌گذاری امنیتی اطلاع حاصل شود.
- مدیریت گروه و کاربر مورد بازرسی قرار گیرد تا از موفقیت و یا شکست به کارگیری ابزار سیاست‌گذاری امنیتی اطلاع حاصل شود.
- تغییرات سیاست‌گذاری امنیتی مورد بازرسی قرار گیرد تا از موفقیت و یا شکست به کارگیری ابزار سیاست‌گذاری امنیتی اطلاع حاصل شود.
- **System Restart** و **System Shutdown** مورد بازرسی قرار گیرد تا از موفقیت و یا شکست به کارگیری ابزار سیاست‌گذاری امنیتی اطلاع حاصل شود.
- ردیابی فرایندها (**Process Tracking**) مورد بازرسی قرار گیرد تا از موفقیت و یا شکست به کارگیری ابزار سیاست‌گذاری امنیتی اطلاع حاصل شود.
- دسترسی به فایل‌های سیستمی باید فقط از طریق مجوزهای مناسب انجام شود.
- دسترسی به **REGEDIT32.EXE** فقط از طریق دسترسی‌های مجاز انجام شود.
- **REGEDIT32.EXE** از روی همه ایستگاه‌های کاری حذف شود تا سیستم عامل ایستگاه‌های کاری از آسیب مصون بماند.
- برای پشتیبان‌گیری از **Registry** و اطلاعات مرتبط به امنیت که از آن‌ها بروی دیسک‌های تعمیر اضطراری پشتیبان گرفته نشده است، از نرم‌افزارهای لازم استفاده شود.
- اطمینان حاصل شود که **Additional Restrictions for Anonymous Connections** بروی **None Rely on Default Permissions** تنظیم شده است.
- **Allow Server Operator to Schedule Tasks** غیرفعال شود.
- **Allow System to be Shutdown without Having to Log On** غیرفعال شود.
- اطمینان حاصل شود که مجوزهای گروه **Allowed to Eject Removable NTFS Media** به‌طور مناسبی اختصاص داده شده است.

- اطمینان حاصل شود که **Amount of Idle Time Required Before Disconnecting Session** به‌طور معقول و قابل قبولی تنظیم شده است.
- برای **Automatically Log Off Local Users When Logon Time Expires** زمان مناسبی تنظیم شود.
- **Clear Virtual Memory Pagefile When System Shuts Down** فعال شود.
- **Digitally sign client communications** فعال شود.
- **Digitally sign server communications** فعال شود.
- اگر بعضی از کاربران از نسخه‌های سطح پایین ویندوز استفاده می‌کنند، اطمینان حاصل شود:
 - **LAN Manager Authentication Level** حداقل روی **NTLMv2** تنظیم شده باشد.
 - اگر همه کاربران از **Win2K** استفاده می‌کنند اطمینان حاصل شود که کنترل کننده‌های دامنه طوری تنظیم شده‌اند که سایر روش‌های تعیین اعتبار را نپذیرند.
- اطمینان حاصل شود از **Message Text and Title for Users Attempting to Logon** استفاده شده است.
- اطمینان حاصل شود **Number of Previous Logons to Cache (If Domain Controller is Not Available)** بر روی صفر تنظیم شده است.
- اطمینان حاصل شود **Prevent System Maintenance of Computer Account Password** برای کامپیوترها و سرورهایی که عضو دامنه هستند، غیرفعال شده است.
- اطمینان حاصل شود **Prevent users from installing print drivers** فعال است.
- اطمینان حاصل شود **Recovery Console: Allow Automatic Administrative Logon** غیرفعال است.
- اطمینان حاصل شود **Recovery Console: Allow Floppy Copy and Access to All Drives and Folders** غیرفعال است.
- اطمینان حاصل شود **Send Unencrypted Password to Connect to Third-Party SMB Servers** غیرفعال است.
- اطمینان حاصل شود **Digitally encrypt secure channel data** فعال است.
- اطمینان حاصل شود **Digitally sign secure channel data** فعال است.

- اطمینان حاصل شود **Shutdown System Immediately If Unable to Log Security Audits** فعال است.
- اطمینان حاصل شود **Strengthen Default Permissions of Global System Objects** فعال است.
- دسترسی فقط خواندنی برای حسابهای کاربری غیرمدیریتی اختصاص داده شود.
- اگر **Simple Network Management Protocol (SNMP)** بر روی کنترل کننده‌های دامنه (**Domain Controllers**) نصب شده است، بررسی شود که کنترل‌های مناسب برقرار بمانند.
- اطمینان حاصل شود که جلوی استفاده غیرمجاز از **FLOPLOCK.EXE** که یک برنامه سودمند برای استفاده از درایو فلاپی می‌باشد، بر روی سرور گرفته شده است. این برنامه دسترسی به درایو فلاپی را محدود به مدیریت می‌کند.
- بررسی شود که **OS/2** و زیرسیستم‌های **PoSix** از روی سیستم‌هایی که مستقیماً به اینترنت متصل‌اند، حذف شده باشند.
- اطمینان حاصل شود که **Unsigned driver installation behavior** بنحو مناسبی تنظیم شده است.
- از آنجایی که **Internet Information Services 5.0 (IIS 5)** به صورت پیشفرض بر روی همه سرورهای **Win2K** وجود دارد، آنرا از روی سرورهای غیروب از حالت نصب خارج (**uninstall**) کنید.
- با بررسی اعضای مدیریت شمای^{۳۷} **Active Directory**؛ اطمینان حاصل شود که از تغییرات غیر مجاز بر روی شمای **Active Directory** جلوگیری می‌شود.
- در سیستم عامل **UNIX** علاوه بر رعایت اقدامات زیر به مطالب مطرح شده در پیوست‌های دو و سه توجه شود:
- اطمینان حاصل شود کلمه عبور کاربر **superuser** به‌طور منظم تغییر داده می‌شود.
- یک نقشه از دسترسی گروههای کاربری به دایرکتوریهای سیستم عامل تهیه شود.
- فایل **/etc/passwd** بررسی شود تا اطمینان حاصل شود کاربران به گروههای درست و مسیر **home** پیش فرض اختصاص داده شدند.
- فایل‌ها و دایرکتوریها به‌منظور تشخیص دسترسی غیرمجاز گروهها و کاربران به طور منظم بررسی شوند.

- مجوزهای دایرکتوریهای سیستمی (/etc, /bin, /usr, /tmp, /dev, /root, /sbin) بررسی شوند.
- با کمک دستور cron برای انجام کارها با زمانبندی منظم، فایل‌های وقایع نگاری امنیتی به یک مکان جداگانه برای انجام بررسیهای لازم کپی شود.
- اطمینان حاصل شود که همه کلمه‌های عبور shadow فعال شده‌اند تا کلمه عبورهای hash خارج از /etc/passwd ذخیره شوند.
- اطمینان حاصل شود که برای رمزنگاری کلمه عبورهای کاربری از روش MD5 استفاده می‌شود.
- اطمینان حاصل شود که مکانیزمی مناسب برای محدود کردن تعداد منابعی که یک کاربر میتواند بدون قطع پروسه‌های دیگر مصرف کند، وجود دارد.
- مجموعه روال‌های لازم برای بیشتر وسختگیرانه‌تر کردن امنیت سیستم عامل نسبت به شرایط پیش فرض پس از نصب، تنظیم شود.
- از propertyهای موجود برای بهبود امنیت در نسخه Unix، علاوه بر تنظیمات و اعمال پایه‌ای ایجاد امنیت در سیستم عامل‌ها استفاده شود.
- امکانات امنیتی اضافی که در نسخه Unix مورد استفاده وجود دارد برای تامین امنیت بیشتر تنظیم شود. (به عنوان مثال ارزشهای متفاوت securelevel در BSD)
- علاوه بر بررسی‌های رسمی دوره ای، اسکریپتهای cron برای بررسی صحت (جامعیت) ورودیها در /etc/passwd همچنین چک کردن مجوزهای سلسله مراتب سیستم فایل به اجرا گذاشته شوند.
- اگر مجوزهای کاربر superuser به طور موقتی برای دسترسی به فایل‌ها و دایرکتوریها نیاز بود اطمینان حاصل شود که پس از رفع نیاز به این دسترسیها، مجوزها حذف میشوند.

مرجع:

این دستورالعمل به شماره □-□/۱-۵-۷/□-□ به ثبت رسیده است.

روندنا

این دستورالعمل فاقد روندنا می‌باشد.

ضمیمه یک :**کنترل دسترسی و امن سازی سیستم عامل (ویندوز ۲۰۰۰ و ۲۰۰۳)****سیستم ممیزی****۱- تنظیمات ممیزی****Audit Setting**

Microsoft Solution for security (Windows 2000 Server)

منبع**نقطه آسیب پذیری**

اگر هیچ سیاست ممیزی روی سرور تنظیم نشود شناسایی تهدیدات رویدادهای امنیتی (Security Event) سخت و گاهی غیر ممکن است.

تهدیدات

عدم امکان پیگیری و شناسایی رویدادهایی که خطرات امنیتی در سیستم ایجاد می‌کنند.

پیامدها

هیچ مدرکی برای تحلیل گر امنیتی و مدیر شبکه جهت پیگیری و شناسایی رویدادهای امنیتی وجود نخواهد داشت. در صورتی که تعداد زیادی Audit فعال شود فهرست‌ها و گزارشات امنیتی (Security Log) مملو از ورودی‌ها و داده‌های بی معنی و زاید می‌شوند.

راه حل امنیتی

راه حل مناسب، تنظیم صحیح روش ممیزی رویدادها (Event Audit) است که در شناسایی تهدیدات امنیتی موثرند.

روش

پیکربندی ممیزی (Audit Setting) در سیاست‌های گروهی (Group Policy) ذیلأ درج شده است.

Computer Configuration> Windows Setting>Security Setting>
Audit Policy

Local Policies>

در windows 2003 :

Start> Local Security Policy> Security Setting>

واژه ها:

رویداد: Event
فهرست و گزارش: Log
ممیزی : Audit
سیاست‌های گروهی : Group Policy

۲- حداکثر سائز فهرست‌های امنیتی، سیستم و برنامه‌ها.

Maximum Size for Security, System and Application Logs

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

اگر تعداد گزینه‌هایی که برای ممیزی تعیین می‌شوند زیاد باشد امکان پر شدن ظرفیت فهرست‌های امنیتی بیشتر می‌شود و این امر باعث غیرفعال شدن سیستم خواهد شد.

تهدیدات

نفوذگران می‌توانند با پیکربندی سیستم برای تولید گزارش‌های ممیزی بیش از حد و پر کردن ظرفیت فهرست‌ها (Log) باعث غیرفعال شدن سرورها و عدم سرویس دهی به کاربران شوند.

پیامدها

عدم تنظیم صحیح سائز فهرست‌های ممیزی- امنیتی می‌تواند باعث پر شدن فهرست‌ها و در نتیجه جایگزین شدن فهرست‌ها و گزارش‌های جدید به جای فهرست‌های قدیمی‌تر شود. در این صورت نفوذگران می‌توانند با تولید فهرست‌های ممیزی متعدد، گزارش‌های ثبت شده مربوط به حملاتشان را از بین ببرند و ضمناً باعث از کارافتادن سرور شوند.

راه حل امنیتی

تنظیم صحیح حداکثر سائز این فهرست‌ها، به شکلی که قابلیت دسترسی به فهرست‌های قدیمی‌تر برای مدت زمان مناسبی امکان پذیر باشد.

روش

در مسیر زیر می‌توان حداکثر سائز را برای هر کدام از انواع Logها تعیین کرد.

Computer Configuration> Windows Setting> Security Setting> Local Policies> Audit Policy
در windows 2003 :

Start> Local Security Policy> Security Setting>

واژه‌ها:

فهرست امنیتی: Security Log ممیزی: Audit

۳- روش نگهداری فهرست‌های ممیزی

Retention Method for Application, Security and System Logs

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

با افزایش گزینه‌های ممیزی خطر پر شدن فهرست‌ها (Logs) افزایش می‌یابد و تا زمان پاک شدن فهرست‌ها توسط مدیر سیستم سرور غیر فعال می‌ماند.

تهدیدات

نفوذگران می‌توانند با پر کردن فهرست‌ها، سرورها را غیر فعال کنند.

پیامدها

اگر این گزینه را طوری تنظیم کنیم که رویدادهای ممیزی (Audit Events) به صورت روزانه جایگزین شوند، ممکن است رویدادهای مهمی که اخیراً روی داده و از نظر امنیتی مهم هستند ثبت و نگهداری نشود و نفوذگران می‌توانند این فهرست‌ها را پر کنند تا اثری از فعالیت‌ها و حملات آن‌ها باقی نماند.

راه حل امنیتی

راه حل مناسب تنظیم این گزینه به صورتی است که رویدادهای ممیزی شده در صورت نیاز جایگزین شوند. ضمناً ارسال فهرست‌ها به یک سرور آگاهی دهنده یا سایر ابزار آگاهی دهنده و نگهداری در یک بانک اطلاعاتی برای استفاده طولانی مدت نیز یک راه حل امنیتی مناسب دیگر است.

روش

تنظیماتی که برای این گزینه می‌توان انجام داد شامل یکی از موارد زیر است:

- جایگزینی رویدادها به صورت روزانه (Over Write Events By Days)
- جایگزینی رویدادها در صورت نیاز (Over Write Events As Needed)
- عدم جایگزینی رویدادها (Don't Over Write Events)
- بدون تعریف (Not Defined)

Computer Configuration> Windows Setting> Local Policies> Security Settings> Audit Policy
Retention Method for Application Log
Retention Method for System Log
Retention Method for Security Log

در windows 2003 گزینه‌های فوق وجود ندارد و می‌توان از طریق Audit System Event عمل نمود.

واژه‌ها:

Server Monitoring: سرور آگاهی دهنده

Audit Event: رویدادهای ممیزی

بیکربندی حقوق انتسابی به کاربران

User Rights Assignment Configuration

۴- رفع اشکال برنامه‌ها

Debug Programs

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

اعطای حق رفع اشکال برنامه‌ها به کاربران می‌تواند باعث دستیابی به اطلاعات حساس سیستم از طریق خواندن اطلاعات درون حافظه شود.

تهدیدات

برخی ابزار حمله وجود دارد که نفوذگران می‌توانند به وسیله آن‌ها و با استفاده از این نوع دسترسی کلمه‌های عبور کاربران را که رمزگذاری نیز شده‌اند و سایر اطلاعات امنیتی را، به دست آورند و در نتیجه امکان دستیابی به منابع برای آن‌ها فراهم می‌شود.

پیامدها

نفوذگران با استفاده از کلمه عبور کاربران می‌توانند به منابع سیستم دسترسی پیدا کنند و با دستیابی به اطلاعات حیاتی سیستم اشکالات و اختلالاتی در ارائه سرویس ایجاد کنند. ضمن این‌که گرفتن حقوق از کاربران مجاز امکان اشکال زدایی برنامه‌ها در موارد لزوم را از آن‌ها می‌گیرد.

راه حل امنیتی

راه حل مناسب اعطای این حقوق به مدیران سیستم و در صورت لزوم برخی از کاربران مجاز است.

روش

در مسیر زیر در تنظیم سیاست‌های گروهی (Group Policy) می‌توان این نوع دسترسی را به کاربران مجاز اعطا کرد.

Computer Configuration> Windows Setting> Security Setting> Local Policies> User Rights Assignment

واژه‌ها:

رفع اشکال: Debug

۵- خاموش کردن سیستم در صورت پر شدن فهرست‌های ممیزی**Shutdown the Computer When the Security Audit Log is Full****منبع**

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

با پر شدن فهرست‌های امنیتی ممیزی که حاوی اطلاعات حیاتی در مورد امنیت سرور هستند، امکان تاثیر این رویدادها روی تمام سیستم‌های وابسته به سرور وجود دارد و می‌تواند در ارائه سرویس از سوی سرور اختلالاتی ایجاد کند.

تهدیدات

نفوذگران می‌توانند با پر کردن فهرست‌ها باعث غیر فعال شدن سرور شوند.

پیامدها

با فعال کردن این گزینه به محض پر شدن فهرست‌های امنیتی ممیزی (Audit Security Log)، سیستم خاموش شده و امکان سرویس دهی سرور وجود نخواهد داشت.

راه حل امنیتی

با غیر فعال کردن این گزینه هنگام پر شدن فهرست‌های ممیزی مربوط به رویدادهای امنیتی (Security Event)، سرور خاموش نمی‌شود. با این کار می‌توان مانع از حملات نفوذگران به سرور شد.

روش

این گزینه را می‌توان به صورت فعال (Enable) یا غیرفعال (Disable) یا بدون تعریف (Not Defined) تنظیم کرد. این گزینه در مسیر زیر قابل دسترسی است

Computer Configuration> Windows Setting> Security Settings> Local Policies> Audit Policy

در windows 2003 :

Start> Local Security Policy> Security Setting>

واژه‌ها:

رویداد: Event

فهرست ممیزی: Audit Log

گزینه‌های امنیتی (Security Options)

۶- محدودیت برای اتصالات بی نام

Additional Restrictions for Anonymous Connections

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

امکان دست یابی به نام Accountها در Domain و منابع اشتراکی شبکه بدون تعیین اعتبار کاربر.

تهدیدات

دست یابی افراد به منابع و اطلاعات روی سرور راه دور بدون این که تعیین اعتبار شوند.

پیامدها

دسترسی غیرمجاز افراد به منابع شبکه.

راه حل امنیتی

بیکربندی سیستم برای جلوگیری از این نوع دسترسی

روش

این تنظیم به دو صورت امکان پذیر است:

۱- از طریق رجیستری : که در مسیر زیر یکی از مقادیر 0 و 1 و 2 وارد می شود.

HKLM\System\Current Control set\Control\LSA

مقدار صفر به معنی دادن اجازه برقراری اتصالات بی نام است.

مقدار یک به معنی عدم اجازه برقراری اتصالات بی نام است.

مقدار دو به معنی عدم امکان دسترسی بدون دادن مجوزهای صریح بی نام.

در windows 2003 :

HKEY-CURRENT-CONFIG\system\current content set\content\

۲- از طریق سیاست‌های گروهی (Group Policy) و در مسیر زیر:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Option

در windows 2003 گزینه‌ای در مسیر متناظر برای تنظیم سیاست‌های گروهی وجود ندارد.

۷- اجازه خاموش کردن سیستم بدون نیاز به ورود به سیستم

Allow System to be Shutdown Without Having to Log on

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کاربرانی که امکان دسترسی به سیستم به صورت محلی داشته باشند بدون نیاز به وارد شدن به سیستم می‌توانند سیستم را خاموش کنند.

تهدیدات

نفوذگران و کاربران غیر مجاز بدون این‌که شناخته شوند می‌توانند سیستم را خاموش کنند و در نتیجه سرویس‌ها و برنامه‌هایی که روی سرور اجرا می‌شوند غیر قابل دسترس خواهند بود.

پیامدها

دسترسی افراد غیر مجاز به سرور و خاموش کردن آن و در نتیجه عدم امکان دسترسی به سرویس‌هایی که سرور ارائه می‌دهد.

راه حل امنیتی

غیرفعال کردن این گزینه

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting>

۸- اجازه خارج کردن رسانه‌های قابل حمل

Allow to Eject Removable NTFS Media

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کاربرانی که دارای چنین اجازه‌ای باشند می‌توانند با انتقال این رسانه‌ها به سیستم‌هایی که روی آن‌ها دارای حقوق مدیریتی هستند، به اطلاعات آن‌ها دسترسی پیدا کنند.

تهدیدات

دسترسی کاربران غیر مجاز به اطلاعاتی که اجازه دسترسی به آن‌ها را ندارند و تغییر مالکیت فایل‌ها و ایجاد تغییر در آن‌ها.

پیامدها

دسترسی غیر مجاز به اطلاعات و ایجاد تغییر در آن‌ها توسط کاربران غیر مجاز.

راه حل امنیتی

راه حل امنیتی مناسب در این مورد اعطای انحصاری این حق به مدیران سیستم است.

روش

تنظیم این گزینه از طریق سایت‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting>

(گزینه به **Allowed to Format and Eject Removeable Media** تغییر یافته است)

واژه‌ها:

سیاست گروهی: Group Policy

رسانه: Media

۹- مدت زمان بیکاری مورد نیاز قبل از قطع نشست**Amount of Idle Time Required Before Disconnecting Session****منبع**

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

هر نشست (Session) مربوط به SMB، منابع سرور را مصرف می‌کند که در صورت برقراری یک نشست طولانی Null سرعت سرور کاهش یافته و احتمالاً از ادامه سرویس دهی باز می‌ماند.

تهدیدات

یک نفوذگر می‌تواند به طور مداوم یک Null Session طولانی ایجاد کند و این امر را تا زمانی که سرور از فعالیت بایستد، ادامه دهد.

پیامدها

در صورت برقراری یک نشست طولانی Null سرور از ادامه فعالیت باز می‌ماند و امکان سرویس دهی به کاربران وجود نخواهد داشت.

راه حل امنیتی

با تعیین یک مقدار مناسب مثل زمان ۱۵ دقیقه می‌توان مانع از وقوع رویدادهای امنیتی مانند از کارافتادن سرور شد. این مدت زمان تاثیر کمی روی نشست SMB می‌گذارد. چون این نشست به صورت اتوماتیک برقرار می‌شود، در صورت برقراری مجدد ارتباط از سوی Client مشکلی ایجاد نمی‌شود.

روش

تنظیم این گزینه در مسیر زیر امکان پذیر است.

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting>

(گزینه به Amount of Idle Time Required Befor Suspending Session تغییر یافته است)

واژه ها:

SMB: Server Message Block

نشست: Session

۱۰- ممیزی دسترسی به Object های عمومی سیستم

Audit The Access of Global System Objects

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

با فعال کردن این گزینه، دسترسی به Object های سیستم از قبیل Semaphore ها و رویدادها، قابل ممیزی (Audit) هستند. از طرف دیگر فعال کردن این گزینه باعث ایجاد حجم زیادی گزارش ممیزی (Audit Log) می‌شود و این باعث کند شدن سرویس دهی سرور و یا از کار افتادن آن می‌شود.

تهدیدات

تولید زیاد فهرست‌های ممیزی و کاهش کارایی و سرعت سرور در سرویس دهی و در نهایت از کار افتادن سرور.

پیامدها

باعث تولید زیاد فهرست‌های ممیزی روی سرورهای بسیار فعال شبکه مانند کنترل کننده‌های Domain و یا Application Server ها شده و سرعت این سرورها را در ارائه سرویس به کاربران، کاهش می‌دهد و گاهی باعث از کار افتادن سرورها می‌شود.

راه حل امنیتی

با غیرفعال کردن این گزینه می‌توان مانع از پرشدن فهرست‌های ممیزی (Audit Log) روی سرورها شد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر امکان پذیر است.

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting>

واژه ها:

Semaphore:

تکنیکی جهت کنترل استفاده چند فرآیند از یک ناحیه اشتراکی در حافظه

گزینه‌های مربوط به تنظیم کلمه‌های عبور : Password Policy

۱۱- حداکثر طول عمر کلمه عبور

Maximum Password Age

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

هر کلمه عبوری با صرف مدت زمان مشخصی قابل Crack شدن است و با توجه به میزان پیچیدگی آن، این زمان متغیر است.

تهدیدات

اگر حداکثر مدت اعتبار یک کلمه عبور به صورت مناسب تنظیم نشود، با در نظر گرفتن میزان پیچیدگی آن، در یک زمان مشخص قابل Crack شدن است.

پیامدها

احتمالاً نفوذگران می‌توانند در مدت زمانی کمتر از حداکثر طول عمر کلمه عبور، به آن دسترسی پیدا کنند.

راه حل امنیتی

با تنظیم مقدار مناسب برای این گزینه، دسترسی به کلمه عبور در یک دوره زمانی معقول بسیار دشوار خواهد بود.

روش

تنظیم این گزینه در Group Policy و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Setting> Account Policies> Password Policy

در windows 2003 :

Start> Local Security Policy> Security Setting>

واژه‌ها:

کلمه عبور: Password

۱۲- حداقل طول کلمه عبور

Minimum password length

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کلمات عبوری که طول کوتاه تری داشته باشند راحت تر و در مدت زمان کوتاه تری قابل Crack شدن هستند.

تهدیدات

دسترسی نفوذگران به کلمات عبور کاربران در مدت زمان کوتاه و با روش‌های ساده تر.

پیامدها

دسترسی کاربران غیر مجاز به منابع و اطلاعات شبکه.

راه حل امنیتی

انتخاب حداقل طول مناسب برای کلمات عبور کاربران جهت افزایش سطح امنیتی آنها

روش

تنظیم این گزینه در **Group Policy** قسمت زیر صورت می‌گیرد.

Computer Configuration>Windows Setting> Security Setting> Account Policies> Password Policy

در windows 2003 :

Start> Local Security Policy> Security Setting>

۱۳- کلمات عبور با ساختار پیچیده

Password must meet complexity requirements

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کلمات عبوری که تنها شامل حروف و یا اعداد باشند به سادگی قابل دسترسی توسط نفوذگران هستند.

تهدیدات

کلمات عبور با ساختار ساده خیلی راحت و در مدت زمان کوتاهی قابل دسترسی توسط کاربران غیر مجاز و نفوذگران می‌باشند.

پیامدها

دسترسی آسان نفوذگران به کلمات عبور کاربران و دسترسی به منابع و اطلاعات شبکه.

راه حل امنیتی

استفاده از کلمات عبور با ساختار ترکیبی از حروف و اعداد.

روش

تنظیم این گزینه در Group Policy در قسمت زیر صورت می‌گیرد :

Computer Configuration> Windows Setting> Security Setting> Account Policies>
Password Policy

در windows 2003 :

Start> Local Security Policy> Security Setting>

۱۴- استفاده از کلمات عبور بدون رمزگذاری برای تمام کاربران دامنه

Store password using reversible Encryption for all Users in the Domain

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

استفاده از کلمات عبور بدون رمزگذاری خطر دسترسی نفوذگران به آن‌ها را افزایش می‌دهد.

تهدیدات

دسترسی آسان نفوذگران به کلمات عبور کاربران

پیامدها

دسترسی نفوذگران به منابع و اطلاعات شبکه با استفاده از کلمات عبور کاربران مجاز.

راه حل امنیتی

غیرفعال کردن این گزینه

روش

تنظیم این گزینه از طریق Group Policy در مسیر زیر صورت می‌گیرد :

Computer Configuration> Windows Setting> Security Setting> Account Policies>
Password Policy

در windows 2003 :

Start> Local Security Policy> Security Setting>

واژه‌ها:

رمزگذاری: Encryption

گزینه‌های مربوط به غیر فعال کردن Account ها : (Account Lockout Policy)

۱۵- مدت زمان غیر فعال شدن Account

Account Lockout Duration

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

یک کاربر غیر مجاز می‌تواند با وارد کردن کلمات عبور اشتباه به صورت عمدی بعد از تعداد دفعات مشخصی، Account مربوط به کاربران مجاز را برای مدت زمان تعیین شده در این گزینه، غیر فعال کند.

تهدیدات

یک کاربر عمداً با وارد کردن کلمات عبور اشتباه باعث غیر فعال شدن Account سایر کاربران می‌شود.

پیامدها

غیر فعال شدن Account کاربران مجاز و عدم امکان دسترسی به سیستم برای یک مدت زمان مشخص.

راه حل امنیتی

تنظیم این گزینه با یک مقدار مناسب، تا بعد از چند بار تلاش کاربر غیرمجاز برای ورود به سیستم، Account مورد نظر برای مدت مشخص غیر فعال شود. ضمناً این مدت زمان نباید طولانی باشد، تا در صورت غیر فعال شدن Account کاربران مجاز توسط سایرین، بتوان سریع‌تر آن را فعال کرد.

روش

تنظیم این گزینه از طریق Group Policy و در قسمت زیر انجام می‌شود:

Computer Configuration> Windows Setting> Security Setting> Account Policies> Account Lockout Policy

در windows 2003 :

Start> Local Security Policy> Security Setting>

۱۶- تعداد دفعات تلاش برای ورود به سیستم قبل از غیرفعال شدن Account Account Lockout Threshold

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

نفوذگران می‌توانند با استفاده از روش هایی، تعداد زیادی کلمات عبور را برای ورود به سیستم مورد آزمایش قرار دهند تا در نهایت، کلمه عبور مناسب را پیدا کنند.

تهدیدات

تلاش نفوذگران برای به دست آوردن کلمه عبور مناسب با تست تعدادی کلمه عبور.

پیامدها

یافتن کلمه عبور مناسب توسط نفوذگران و ورود و دسترسی به منابع و اطلاعات سیستم.

راه حل امنیتی

تنظیم این گزینه با مقدار مناسب، برای محدود کردن تعداد دفعات تلاش نفوذگران برای ورود به سیستم.

روش

تنظیم این گزینه از طریق Group Policy ها و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Account Policies>
Account Lock Out Policy

در windows 2003 :

Start> Local Security Policy> Security Setting>

واژه ها:

غیرفعال کردن: Lockout

حد- زمان آستانه: Threshold

۱۷- قطع ارتباط خودکار (Log Off) کاربران بعد از انقضاء زمان Log On

Automatically Log Off Users When Log On Time Expire

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

فعال کردن این گزینه باعث قطع نشست (Session) کاربران و سرور SMB به محض انقضای زمان Log On آن‌ها می‌شود.

تهدیدات

قطع ارتباط کاربر با سیستم و از دست رفتن اطلاعات ذخیره نشده.

پیامدها

پایان یافتن نشست SMB (Session) روی سرور و قطع ارتباط کاربر با سرور.

راه حل امنیتی

برای حفاظت از سرورها در مواردی که کاربر ممکن است فراموش کند عملیات Log Off را انجام دهد، این گزینه فعال می‌شود.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر امکان پذیر است:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 چنین تنظیمی در این بخش موجود نیست.

واژه‌ها:

SMB: Server Message Block

۱۸- پاک کردن فایل مربوط به حافظه مجازی به هنگام خاموش شدن سیستم Clear Virtual Memory Page File When System Shutdown

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

اطلاعات مهمی که در حافظه مجازی و روی دیسک ذخیره می‌شوند در دسترس نفوذگرانی که دسترسی فیزیکی به سرور دارند قرار می‌گیرند.

تهدیدات

نفوذگران می‌توانند بعد از خاموش کردن سرور، دیسک سرور را به یک کامپیوتر دیگر منتقل کرده و محتویات **Page File** را مشاهده کنند.

پیامدها

نفوذگران به اطلاعات ذخیره شده در **Page File** دسترسی پیدا می‌کنند.

راه حل امنیتی

راه حل، فعال کردن این گزینه است. البته با توجه به سایز **Page File**ها این امر ممکن است در مدت زمان خاموش شدن و فعالیت مجدد سرور تاثیر بسزایی بگذارد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی (**Group Policy**) و در مسیر زیر صورت می‌گیرد:

Computer Configuration > Windows Setting > Security Setting > Local Policies > Security Options

در windows 2003 :

Start > Local Security Policy > Security Setting >

(گزینه مذکور به صورت **clear virtual memory page file** است.)

۱۹- امضای دیجیتالی ارتباطات بین Client و Server

Digitally Sign Client and Server Communications

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

ارتباطات نا امن بین Client و سرور می‌تواند خطر دسترسی نفوذگران به اطلاعات ارسالی بین آن‌ها را افزایش دهد.

تهدیدات

نفوذگران می‌توانند به بسته‌های (Packet) اطلاعاتی SMB فاقد امضای دیجیتالی، دسترسی پیدا کرده و بعد از اعمال تغییرات، مجدداً آن‌ها را روی شبکه ارسال کنند.

پیامدها

صحت و درستی بسته‌های اطلاعاتی که مبادله می‌شوند مشخص نیست و ممکن است این بسته‌ها توسط نفوذگران تغییر کرده باشند.

راه حل امنیتی

با فعال کردن این گزینه می‌توان مانع از دسترسی نفوذگران به بسته‌های اطلاعاتی ارسالی بین Client و سرور شد. البته فعال کردن این گزینه می‌تواند روی کارایی و سرعت سرورهای فعال شبکه تاثیر منفی بگذارد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting>

در مسیر متناظر windows 2003 دو گزینه مجزا برای امضای الکترونیکی بین Server و Client به

شکل زیر وجود دارد:

- 1- Digitally sing communications (if client agrees)
- 2- Digitally sing communications (if server agrees)

واژه‌ها:

بسته: Packet

۲۰- غیر فعال کردن Ctrl+ Alt+ Del برای ورود به سیستم

Disable Ctrl+Alt+Del Requirement for Log On

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

نفوذگر می‌تواند برنامه اسب تروا (Trojan Horse) روی سیستم نصب کند که شبیه پنجره Log On باشد و به این طریق کلمه عبور کاربران را ثبت کند.

تهدیدات

نفوذگران می‌توانند به کلمه عبور کاربران دسترسی پیدا کنند.

پیامدها

استفاده نفوذگران از برنامه‌هایی جهت Capture کردن کلمه عبور کاربران و دسترسی به منابع و اطلاعات سیستم.

راه حل امنیتی

با غیرفعال کردن این گزینه کاربران مجبور به استفاده از کلیدهای Ctrl+Alt+Del به هنگام ورود به سیستم هستند.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی (Group Policy) و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

(در windows 2003 تحت عنوان interactive logon به صورت do not require Ctr+Alt+Del

آمده است).

۲۱- عدم نمایش نام آخرین کاربر در صفحه Log On

Don't Display Last User Name in Log On Screen

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

نفوذگران می‌توانند با حدس زدن کلمه عبور کاربر به سیستم دسترسی پیدا کنند.

تهدیدات

نفوذگران با دیدن نام کاربر و تنها با استفاده از ابزار و برنامه‌هایی جهت کشف کلمه عبور وی، می‌توانند به سیستم وارد شوند.

پیامدها

مشخص شدن نام کاربران برای نفوذگران، که با حدس زدن کلمه عبور می‌توانند به منابع سیستم دسترسی پیدا کنند.

راه حل امنیتی

با فعال کردن این گزینه می‌توان مانع از نمایش نام آخرین کاربری شد که به سیستم وارد شده است.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد :

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy>Security Setting>

۲۲- سطح تعیین اعتبار LAN Manager

LAN Manager Authentication Level

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

تعیین اعتبار از طریق LM در Client های ۹۸ و NT به دلیل امنیت پایین (عدم پشتیبانی از Kerberos Version 5) در امر ارسال اطلاعات در سطح شبکه، خطر دسترسی به این اطلاعات توسط نفوذگران را افزایش می‌دهد.

تهدیدات

با استفاده از پروتکل‌های تعیین اعتبار LM یا NTLM، نفوذگران می‌توانند با گوش دادن به خطوط ارسال اطلاعات در شبکه به این اطلاعات دسترسی پیدا کنند.

پیامدها

دسترسی آسان نفوذگران به کلمه عبور کاربران و در نتیجه نفوذ به سیستم و دسترسی به منابع آن.

راه حل امنیتی

راه حل مناسب استفاده از پروتکل NTLMV2 است که از سطح امنیتی بالاتری نسبت به LM و NTLM برخوردار است.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy>Security Setting>

واژه‌ها:

تعیین اعتبار: Authentication

۲۲- تعداد Log On های Cache شده

Number of Previous Log On to Cache
In Case Domain Controller is not all available))

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

نفوذگران که به سرور دسترسی دارند می‌توانند از این اطلاعات Cache شده، جهت به دست آوردن کلمه عبور کاربران استفاده کنند.

تهدیدات

نفوذگران با دسترسی به اطلاعات Cache شده می‌توانند با استفاده از روش‌ها و ابزارهای خاص کلمه عبور کاربران را شناسایی کنند.

پیامدها

دسترسی نفوذگران به کلمه عبور کاربران، نفوذ به سیستم و دسترسی به منابع سرور.

راه حل امنیتی

برای اطمینان از این‌که کاربران مجاز حتی در صورت در دسترس نبودن Controller Domain ها، می‌توانند به شبکه وصل شوند، تعداد Log On های قابل Cache روی تعداد مناسبی مثل 10 تنظیم می‌شود.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy>Security Setting>

۲۴- جلوگیری از تغییر خودکار کلمه عبور Account کامپیوترها

Prevent System Maintenance of Computer Account Password

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

همه کامپیوترهای عضودامنه ویندوز ۲۰۰۰ به صورت پیش فرض، هر هفت روز یکبار باید کلمه عبور خود را تغییر دهند. با غیرفعال کردن این گزینه، کلمه عبور بدون تغییر باقی می‌ماند و تغییر در کلمه عبور به صورت اتوماتیک از جانب کنترل کننده دامنه درخواست نمی‌شود.

تهدیدات

نفوذگران می‌توانند برای این دسته از کامپیوترهای عضو Domain کلمه عبور تعیین کنند.

پیامدها

تغییر کلمه عبور مربوط به Domain Account کامپیوترها توسط نفوذگران و امکان نفوذ به آن کامپیوترها.

راه حل امنیتی

غیرفعال کردن این گزینه

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 تنظیماتی به این شکل وجود ندارد.

۲۵- جلوگیری از نصب درایور چاپگر توسط کاربران

Prevent Users from Installing Printer Drivers

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

نصب درایورهای نامناسب توسط کاربران که می‌تواند باعث آسیب رسیدن به سرور شود.

تهدیدات

نصب درایورهای نامناسب توسط کاربرانی که مقاصد خرابه‌کارانه دارند، می‌تواند باعث آسیب رسیدن به سرورهای شبکه شود.

پیامدها

بروز اختلال در سرویس دهی سرورها.

راه حل امنیتی

فعال کردن این گزینه مانع از نصب درایور چاپگر توسط کاربران می‌شود.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting> ...

۲۶- غیرفعال سازی سرورهای مجازی

Deleting Additional Virtual Servers

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

در حالت نصب پیش فرض IIS، Web سایت، ftp سایت و وب سایت مدیریت ایجاد می‌شود که این سایت‌ها اغلب حاوی کدهای نمونه می‌باشند و همین امر باعث ایجاد نقطه‌ای آسیب پذیر روی سرور می‌شود.

تهدیدات

نفوذگر می‌تواند از ضعف امنیتی موجود در کدها و برنامه‌های درون این سایت‌ها استفاده کرده و وب سرور را مورد نفوذ قرار دهد.

پیامدها

دسترسی نفوذگران به محتویات وب سرور و کنترل از راه دور آن.

راه حل امنیتی

حذف این سایت‌ها از وب سرور

روش

از طریق کنسول مدیریتی IIS می‌توان این سایت‌ها را حذف کرد. به وسیله ابزار IIS Lockdown هم می‌توان این کار را انجام داد. در windows 2003 این تنظیمات از طریق IIS در دسترس است.

۲۷- آگاه سازی کاربران جهت تغییر کلمه عبور قبل از انقضای آن**Prompt User to Change Password before Expiration****منبع**

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کاربران تا زمانی که کلمه عبورشان منقضی نشود متوجه این امر نخواهند شد. بنابراین دسترسی کاربران مجاز به یکباره قطع خواهد شد.

تهدیدات

عدم امکان دسترسی کاربران به شبکه.

پیامدها

کاربران نمی‌توانند هم به صورت محلی (Locally) و هم از طریق Dial-Up یا VPN به شبکه وصل شوند.

راه حل امنیتی

تنظیم این گزینه با یک مقدار مناسب، هنگامی که زمان باقی مانده تا انقضای کلمه عبور به این حد رسید، کاربر مطلع شود.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting> ...

واژه‌ها:

انقضای: Expiration

۲۸- اجازه ورود اتوماتیک به Recovery Console با حقوق مدیریتی

Recovery Console: Allow Automatic Administrative Log On

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کاربران می‌توانند با **Restart** کردن سرور، وارد وضعیت **Recovery Console** شده و دسترسی کاملی به سرور داشته باشند.

تهدیدات

دسترسی کاربران معمولی به **Recovery Console** با مجوز **Full Control** مربوط به مدیر سیستم.

پیامدها

امکان فعال و غیرفعال کردن سرویس‌ها و درایورها توسط این کاربران از طریق **Recovery Console** و ایجاد اختلال در سرویس دهی سرورها.

راه حل امنیتی

با غیرفعال کردن این گزینه مانع از ورود کاربران معمولی به این وضعیت می‌شویم.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting> ...

۲۹- کانال امن : رمزگذاری یا امضای دیجیتالی کانال امن داده**Secure Channel: Digitally Encrypt or Sign Secure Channel Data****منبع**

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

وقتی که کامپیوتر ویندوز ۲۰۰۰ به Domain وصل می‌شود یک Account برای آن ایجاد می‌شود و از کلمه عبور برای ایجاد کانال امن با کنترل کننده دامنه استفاده می‌کند. کلیه درخواست‌های ارسالی روی این کانال، تعیین اعتبار می‌شوند و اطلاعات حساس مثل کلمات عبور نیز رمزگذاری می‌شوند.

تهدیدات

اگر تنظیم این گزینه به صورتی باشد که رمزگذاری کانال امن برای کل ترافیک داده‌ای باشد، در آن صورت اگر کنترل کننده دامنه قادر به رمزگذاری نباشد ارتباط با آن برقرار نمی‌شود.

پیامدها

عدم امکان برقراری ارتباط ویندوزهای قدیمی مثل ویندوز ۹۸ با کنترل کننده دامنه جهت تعیین اعتبار و اتصال به دامنه .

راه حل امنیتی

اگر این گزینه را به صورتی تنظیم کنیم که در صورت امکان، رمزگذاری داده‌ها صورت گیرد، در این صورت ایجاد کانال امن و رمزگذاری تنها در صورتی که از سوی دو طرف یعنی Client و سرور پشتیبانی شود امکان پذیر است.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد :

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting> ...

(همچنین عنوان Secure channel به Domain member تغییر یافته است)

واژه‌ها:

رمزنگاری: Encrypt

۳۰- ارسال کلمات عبور بدون رمزگذاری برای ارتباط با سرورهای SMB

غیرمایکروسافتی.

Send Unencrypted Password to Connect to Third-Party SMB Servers

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

با فعال کردن این گزینه، سرور کلمات عبور را به صورت رمزگذاری نشده به سایر سیستم‌هایی که سرویس SMB را ارائه می‌دهند ارسال می‌کند. این سیستم‌ها ممکن است قادر به استفاده از مکانیزم‌های امنیتی مربوط به SMB که در ویندوز ۲۰۰۰ وجود دارد نباشند.

تهدیدات

اطلاعات مهم و حساس مثل کلمات عبور بدون رمزنگاری ارسال می‌شوند و نفوذگران می‌توانند با گوش دادن به شبکه (Sniff) به این اطلاعات دسترسی پیدا کنند.

پیامد

دسترسی نفوذگران به اطلاعات حساس مثل کلمات عبور.

راه حل امنیتی

غیرفعال کردن این گزینه

روش

این گزینه را می‌توان از طریق سیاست‌های گروهی و در مسیر زیر تنظیم کرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 :

Start> Local Security Policy> Security Setting> ...

واژه‌ها:

برنامه‌های غیر مایکروسافتی : Third-Party

بو کشیدن: Sniff

SMB: Server Message Block

۳۱- خاموش شدن فوری سیستم در صورتی که قادر به Log برداری و ثبت گزارشات ممیزی امنیتی نباشد.

Shutdown System Immediately If Unable To Log Security Audits

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

این تنظیم در صورتی که سیستم قادر به ثبت گزارشات امنیتی و ممیزی نباشد، رفتار سیستم را در مورد ادامه فعالیت یا عدم فعالیت تعیین می‌کند.

تهدیدات

فعال کردن این گزینه وقتی ظرفیت گزارشات امنیتی پر می‌شود و سیستم قادر به Log برداری نیست می‌تواند، شرایط حملات DoS را فراهم کند.

پیامدها

نفوذگران برای از کار انداختن سرور می‌توانند از حمله DoS استفاده کنند و با پر کردن ظرفیت Security Log باعث خاموش شدن و از کار افتادن سرور شوند.

راه حل امنیتی

غیرفعال کردن این گزینه راه حل مناسبی برای جلوگیری از خطر حمله DoS است.

روش

این گزینه را می‌توان از طریق سیاست‌های گروهی و در مسیر زیر تنظیم کرد.

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security .
Options

در windows 2003 :

Start> Local Security Policy> Security Setting> ...

۳۲- نوع رفتار سیستم موقع خروج Smart Card

Smart Card Removal Behavior

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

در صورتی که از Smart Card جهت تعیین اعتبار استفاده شود، باید کامپیوتر بعد از خروج آن به صورت اتوماتیک قفل (Lock) شود تا در صورتی که کاربر فراموش کرد به صورت دستی این عمل را انجام دهد، مشکلی ایجاد نشود.

تهدیدات

در صورت تنظیم نکردن صحیح این گزینه ممکن است کاربر فراموش کند به صورت دستی سیستم را قفل کند و در این حالت کاربران غیرمجاز می‌توانند به سیستم دسترسی پیدا کنند.

پیامدها

دسترسی به اطلاعات سیستم توسط کاربران غیرمجاز.

راه حل امنیتی

راه حل مناسب در این زمینه تنظیم این گزینه، به صورتی است که بعد از خروج Smart Card از دستگاه، سیستم به صورت اتوماتیک قفل شود.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> Local Policies> Security .

Options

در windows 2003 :

Start> Local Security Policy> Security Setting> ...
Service Configuration

۳۳- سرویس SNMP

SNMP Services

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

در بسیاری از موارد، مدیریت برنامه‌ها نیازمند عاملی است که باید روی سرور نصب شود. این عامل‌ها از پروتکل SNMP برای فرستادن اعلام خطرهای (Alert) به سرور مدیریت مرکزی استفاده می‌کنند.

تهدیدات

فعال کردن سرویس SNMP باعث می‌شود که علاوه بر امکان خواندن اطلاعات از سرور امکان ایجاد تغییر در آن‌ها نیز فراهم شود. ضمناً این اطلاعات به صورت رمزگذاری نشده ارسال می‌شوند.

پیامدها

نفوذگر با گوش دادن به ترافیک شبکه (Sniff) می‌تواند بسته‌های اطلاعاتی SNMP را مشاهده کند.

راه حل امنیتی

در صورت وجود سرور MoM در شبکه، این سرویس به صورت اتوماتیک تنظیم می‌شود. در غیر این صورت باید آن را غیرفعال کرد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد:

Computer Configuration> Windows Setting> Security Setting> System Services

در windows 2003 این مسیر وجود ندارد.

واژه‌ها:

SNMP: Simple Network Management Protocol
MoM: Microsoft Operation Manager

۳۴- ترمینال ارتباطی

Terminal Services

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

مدیریت از راه دور سرورها می‌تواند در صرفه جویی زمان و هزینه موثر باشد و امکان اجرای وظایف و عملیات مدیریتی روی سرورها را از راه دور، برای مدیران شبکه فراهم کند.

تهدیدات

اگر نفوذگر بتواند به پورت ۳۳۸۹ مربوط به این سرویس وصل شود و به نام کاربری (User Name) و کلمه عبور (Password) کاربر مجاز نیز دسترسی داشته باشد می‌تواند ارتباط راه دور با سرور برقرار کند.

پیامدها

دسترسی نفوذگران به منابع و اطلاعات روی سرورها و امکان اجرای عملیات مدیریتی روی آنها.

راه حل امنیتی

در صورت نیاز می‌توان این سرویس را به صورت اتوماتیک روی سروری که از راه دور مدیریت می‌شود، فعال نمود. درغیراین صورت باید همیشه غیرفعال باشد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Setting> System Services

در windows 2003 این مسیر وجود ندارد.

۳۵- سرویس Windows Management Instrumentation (WMI)

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

این سرویس جهت مدیریت دیسک‌های منطقی (Logical Disk) روی سیستم، ضروری است و بسیاری از برنامه‌ها و ابزارهای سیستم از این سرویس استفاده می‌کنند.

تهدیدات

اگر این سرویس فعال باشد نفوذگری که به سیستم دسترسی دارد ممکن است از این ویژگی جهت به دست آوردن اطلاعاتی در مورد سخت‌افزارها و نرم‌افزارهای نصب شده روی سرور استفاده کند.

پیامدها

دسترسی نفوذگران به اطلاعاتی در مورد سخت‌افزارها و برنامه‌های نصب شده روی سرور.

راه حل امنیتی

اگر سرورها نیاز به مدیریت از طریق WMI داشته باشند باید این سرویس را به صورت اتوماتیک تنظیم کرد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Setting> System Service

در windows 2003 این مسیر وجود ندارد.

واژه‌ها:

WMI: Windows Management Instrumentation

تنظیمات رجیستری : Registry Setting

۳۶- پیکربندی نام‌های NetBIOS

Configure Net BIOS Name Release Security

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

اسامی NetBIOS روی پروتکل TCP/IP جهت تعیین اعتبار، کاربردی ندارند و به همین دلیل می‌توانند باعث ایجاد آسیب پذیری در سیستم شوند.

تهدیدات

کاربری با اهداف خرابه‌کارانه می‌تواند از پروتکلی غیر معتبر جهت ارسال نام به کامپیوتر مقصد استفاده کند که این باعث چشم پوشی و عدم پاسخ به درخواست ارسالی می‌شود.

پیامدها

مانع از وصل شدن به دامنه، استفاده از دستور Net Send و Network Neighborhood می‌شود.

راه حل امنیتی

ایجاد کلیدی در رجیستری تا سرورها، در خواست‌های رسیده از کامپیوترها جهت Name Resolution را نپذیرند.

روش

برای تنظیم این گزینه در رجیستری و در مسیر زیر کلیدی با مشخصات زیر وارد می‌شود.

HKLM\System\Current Control Set\Services\Net BT\Parameters

Registry Key: No Name Release on Demand

Format: DWORD

Value (Decimal):1

در windows 2003 :

HKEY-CURRENT-CONFIG\Current Control Set

۳۷- غیر فعال سازی تولید خودکار نام فایل با قالب 8.3**Disable Auto Generation of 8.3 File Names****منبع**

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

ویندوز ۲۰۰۰ از اسامی فایل با فرمت 8.3 برای سازگاری با برنامه‌های ۱۶ بیتی پشتیبانی می‌کند. بر این اساس امکان استفاده از اسامی با طول بیشتر از ۸ کاراکتر وجود دارد.

تهدیدات

نفوذگر می‌تواند تنها با استفاده از ۸ کاراکتر به فایل‌هایی با طول بیشتر دسترسی پیدا کند.

پیامدها

دسترسی نفوذگران به فایل‌های داده‌ای و برنامه‌ها با اسامی بیش از ۸ کاراکتر با استفاده از اسامی کوتاه.

راه حل امنیتی

ایجاد یک Entry در رجیستری، تا امکان استفاده از فایل‌هایی با اسامی بزرگتر از 8 کاراکتر برای برنامه‌های ۱۶ بیتی مجاز نباشد.

روش

برای تنظیم این گزینه در رجیستری و در مسیر زیر کلیدی با مشخصات زیر وارد می‌شود.

HKLM\System\Current Control Set\Control\FileSystem

Registry Key: NTFS Disable 8 dot 3 Name Creation

Format: DWORD

Value: 1

در windows 2003 :

HKEY\ CURRENT-CONFIG\Current Control Set

۳۸- غیرفعال سازی Auto Run

Disable Auto Run

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

ویژگی Auto Run امکان خواندن اطلاعات از درایو، به محض قرار دادن دیسک در آن را فراهم می‌کند که این می‌تواند شامل فایل نصب برنامه نیز باشد.

تهدیدات

نفوذگر با امکان دستیابی فیزیکی به سیستم می‌تواند با قراردادن CD با قابلیت Auto Run در درایو مربوطه باعث اجرای برنامه مخرب روی سرور شود.

پیامدها

نصب و اجرای اتوماتیک برنامه‌هایی با کدهای مخرب که باعث ایجاد اختلال در سرویس دهی سرور می‌شوند.

راه حل امنیتی

غیرفعال کردن این گزینه از طریق ایجاد کلیدی در رجیستری

روش

برای تنظیم این گزینه در رجیستری و در مسیر زیر کلیدی با مشخصات زیر وارد می‌شود.

HKLM\Software\Microsoft\Windows\Current Version\Policies\Explorer

Registry Value Entry: No Drive Type Auto Run

Format: DWORD

Value (Hex): 0XFF

در windows 2003 :

HKEY\ CURRENT-CONFIG\ Software\Microsoft\Windows\Current Version\Policies\Explorer

Registry Value Entry: No Drive Type Auto Run

Format: DWORD

Value (Hex): 0XFF

۳۹- حذف زیرسیستم‌های Os/2 و PoSix

Removing Os/2 and POSIX Subsystems

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

زیر سیستم های Os/2 در مواردی که سرور نیاز به ارتباط قابل توجهی با Client های Os/2 داشته باشد، کاربرد دارند.

تهدیدات

زیر سیستم‌های Os/2 خطری امنیتی برای پروسس‌هایی است که توسط کاربر شروع شده و خاتمه نیافته‌اند. در این صورت کاربر بعدی که به سیستم Login می‌کند قادر به دسترسی به آن پروسس‌هاست و حتی توانایی استفاده از دسترسی‌های کاربر قبلی را نیز دارد.

پیامدها

دسترسی کاربر به پروسسی که توسط یک کاربر دیگر آغاز شده و خاتمه نیافته است.

راه حل امنیتی

برای تنظیم این گزینه در رجیستری، چند کلید حذف می‌شود .

روش

برای تنظیم این گزینه از طریق رجیستری و در مسیر زیر کلیدهایی با مشخصات ذیل حذف می‌شود .

HKLM\System\Current Control Set\Control\Session Manager\Sub Systems
Registry Key: -Optional

- OS/2
- PoSix

در windows 2003 :

HKLM\System\Current Control Set\Control

واژه‌ها:

PoSix: Portable Operating System Interface for UNIX

۴۰- فعال سازی فوری محافظ صفحه نمایش با کلمه عبور

Make Screen Saver Password Protection Immediate

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

مقدار پیش فرض برای این گزینه، به معنی در معرض خطر قرار دادن سیستم است. چون بر طبق این مقدار، نفوذگر قبل از فرا رسیدن زمان قفل شدن سیستم می‌تواند به سیستم وارد شود.

تهدیدات

نفوذگر می‌تواند مدتی بعد از فعال شدن Screen Saver و قبل از قفل شدن سیستم به سیستم وارد شود.

پیامدها

دسترسی به منابع سیستم توسط نفوذگران.

راه حل امنیتی

تنظیم این گزینه به صورتی که به محض فعال شدن Screen Saver سیستم قفل شود.

روش

برای تنظیم این گزینه در رجیستری و در مسیر زیر کلیدی با مشخصات زیر وارد می‌شود.

HKLM\Software\Microsoft\Windows NT\Current Version\Win Log On\Screen Saver

Green Period

Registry Value Entry: Screen Saver Green Period

Format: String

Value (Decimal): 0

در windows 2003 مسیر فوق تا Win Log On به شکل زیر وجود دارد اما پیکربندی Screen Saver

وجود ندارد:

HKEY-LOCAL-MACHIN\Software\Microsoft\Windows NT\Current Version\Win Log On

۴۱- محدودسازی دسترسی به نشست‌های Null

Restrict Null Session Access

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

Null Session ها، ضعف محسوب می‌شوند چون امکان دسترسی به منابع Share شده روی سیستم را به کاربران، بدون تعیین اعتبار آن‌ها می‌دهند.

تهدیدات

کاربران می‌توانند بدون این‌که تعیین اعتبار شوند به منابع Share شده روی سیستم دسترسی پیدا کنند.

پیامدها

دسترسی کاربران غیرمجاز به منابع سیستم.

راه حل امنیتی

تنظیم این گزینه از طریق رجیستری به گونه‌ای که مانع از دسترسی کاربران به منابع از طریق Null Session ها شود.

روش

جهت تنظیم، در رجیستری و در مسیر زیر کلیدی با مشخصات زیر وارد می‌شود.

HKLM\System\Current Control Set\Services\LAN Man Server\Parameters

Registry Value Entry: Restrict Null Sess Access

Format: DWORD

Value (Decimal):1

واژه‌ها:

نشست: Session

۴۲- مقید کردن آزاد سازی دسترسی کنسول به احراز هویت از طریق DC Requiring Domain Controller Authentication to Unlock the Console

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کامپیوتر اعتبارنامه کاربرانی که تعیین اعتبار شده‌اند را به صورت محلی در حافظه Cache می‌کند و هنگام Unlock کردن سیستم، از این اعتبارنامه استفاده می‌کند. در این حالت هر تغییری که اخیراً در مورد حقوق کاربری یا گزینه‌های امنیتی مربوط به Account و Password کاربران ایجاد شود، در این پروسه تعیین اعتبار تاثیری نمی‌گذارد. بنابراین حقوق کاربر به روز (Update) نمی‌شود و از همه مهمتر این‌که با وجود غیرفعال شدن یک Account هنوز امکان Unlock کردن سیستم با آن Account وجود دارد.

تهدیدات

با وجود غیرفعال شدن یک Account غیر معتبر و Hack شده، هنوز امکان ورود به سیستم وجود دارد.

پیامدها

Unlock شدن سیستم به وسیله یک Account غیرفعال شده و دسترسی نفوذگران به منابع سیستم.

راه حل امنیتی

تنظیم این گزینه در رجیستری به گونه‌ای که هر تغییری در مورد Account فوراً روی آن اعمال شود. بنابراین نیاز است که کامپیوتر هر بار که تلاشی جهت Unlock کردن سیستم صورت گرفت، از ابتدا عملیات تعیین اعتبار Account را انجام دهد.

روش

برای تنظیم این گزینه در رجیستری و در مسیر زیر کلیدی با مشخصات زیر وارد می‌شود.

HKLM\Software\Microsoft\Windows NT\Current Version\Win Log On
Registry value Entry: Force Unlock Log On
Format: DWORD
Value: 1

در windows 2003 به همین شکل آمده است.

امنیت کنترل کننده دامنه – Securing Domain Controller

حقوق انتسابی به کاربران – User Rights Assignment

۴۳- ورود به سیستم به صورت محلی Log On Locally

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

هر Account با داشتن این امتیاز می‌تواند به صورت محلی به سرور وارد شده و اطلاعات روی آن را مشاهده کند.

تهدیدات

کاربران با داشتن این امتیاز می‌توانند به صورت محلی به سرور وارد شده و به اطلاعات آن دسترسی پیدا کنند.

پیامدها

دسترسی کاربران غیرمجاز به اطلاعات روی سرور.

راه حل امنیتی

تنها اعضای گروه Administrators، Back Up Operators و Server Operators می‌توانند اجازه ورود به صورت محلی به سرور را داشته باشند و سایر کاربران نباید دارای چنین امتیازی باشند.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی مربوط به سرورهای کنترل کننده Domain و در مسیر زیر صورت می‌گیرد.

Computer Configuration>Windows Setting>Security Setting> Local Policies> User Right Assignment

در windows 2003 به همین شکل آمده است.

واژه‌ها:

کنترل کننده Domain : Domain Controller

۴۴- خاموش کردن سیستم Shutdown the System

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کاربران با داشتن این امتیاز می‌توانند سرور کنترل کننده Domain را خاموش کنند.

تهدیدات

کاربرانی که دارای این امتیاز باشند می‌توانند با خاموش کردن سرور مانع از ادامه سرویس دهی آن شوند.

پیامدها

با غیرفعال شدن این سرور اجرای فرآیندهایی مانند ورود به Domain، اعمال سیاست‌های گروهی و جست‌وجو در Active Directory متوقف می‌شود.

راه حل امنیتی

اعطای این حق به تعداد محدودی از مدیران قابل اعتماد شبکه.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی مربوط به سرورهای کنترل کننده Domain و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Setting> Local Policies> User Right Assignment

در windows 2003 به همین شکل آمده است.

۴۵- اجازه زمان بندی فعالیت‌ها توسط گروه Server Operators

Allow Server Operators to Schedule Tasks
(Domain Controllers Only)

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

کاربران عضو گروه Server Operators می‌توانند فعالیت‌ها را روی این دسته از سرورها زمان بندی کنند.

تهدیدات

نفوذگران می‌توانند با عضویت در گروه Server Operators این مجوز را به دست آورند.

پیامدها

نفوذگرانی که صاحب این مجوز باشند می‌توانند فرآیندی را زمان بندی کنند که طی آن Account کاربری آن‌ها در گروه Domain Administrators اضافه شود. در نتیجه می‌توانند با به دست آوردن مجوزهای این گروه، کنترل کاملی روی سرور داشته باشند.

راه حل امنیتی

غیرفعال کردن این گزینه

روش

تنظیم این گزینه از طریق سیاست‌های گروهی مربوط به این دسته از سرورها و در مسیر زیر صورت می‌گیرد.

Computer Configuration>Windows Setting> Security Setting> Local Policies> Security Options

در windows 2003 به همین شکل آمده است.

پیکربندی سرویس‌ها : Services Configuration

۴۶- سرویس DNS Server

Microsoft Solution for Security (Windows 2000 Server)

منبع

نقطه آسیب پذیری

سرویس DNS Server در مواردی که می‌خواهیم از سرویس Active Directory- Integrated DNS روی کنترل کننده Domain استفاده کنیم، مورد نیاز است. فعال بودن هر سرویس یا برنامه می‌تواند به عنوان نقطه‌ای آسیب پذیر جهت نفوذ به سیستم محسوب شود.

تهدیدات

نفوذگر می‌تواند از سرویس فعال روی سرور برای نفوذ و حمله به آن استفاده کند.

پیامدها

دسترسی نفوذگران به منابع روی سرور و اجرای فرآیندهای مخرب جهت اختلال در سرویس‌دهی سرور.

راه حل امنیتی

چنانچه DNS سرور روی کنترل کننده دامنه نصب شود این سرویس باید فعال باشد در غیر این صورت باید آن را غیر فعال کرد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی مربوط به کنترل کننده دامنه و در مسیر زیر صورت می‌گیرد.

Computer Configuration>Windows Setting> Security Settings> System Services

در windows 2003 مسیر فوق از Security Settings به بعد وجود ندارد.

توجه: برای دسترسی به بخش پیکربندی System Services در windows 2003 از طریق زیر عمل شود:

- کلیک راست روی My Computer
- انتخاب گزینه Manage
- انتخاب گزینه Services and Applications
- انتخاب گزینه Services

بنابراین در ادامه این مستند تمام مسیرهایی که دارای گزینه System Services هستند را باید از طریق فوق جست‌وجو کرد.

۴۷- سرویس Inter Site Messaging

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

این سرویس برای KCC ضروری است. ضمناً برای پشتیبانی از عملیات **Directory Active Replication** بین سایت‌ها (با استفاده از پروتکل SMTP) در دامنه مورد استفاده قرار می‌گیرد.

تهدیدات

هر سرویس فعال، یک نقطه آسیب پذیر بالقوه برای حمله و نفوذ به سیستم به شمار می‌آید.

پیامدها

نفوذ افراد غیرمجاز به سرور، دسترسی به منابع آن و انجام فرآیندهای مخرب روی سرور جهت ایجاد اختلال در سرویس دهی.

راه حل امنیتی

تنها در مواردی که به KCC برای محاسبه و کنترل توپولوژی ارتباطی بین کنترل کننده‌های دامنه (به منظور انجام Replication) نیاز باشد، می‌توان آن را فعال کرد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی مربوط به کنترل کننده‌های دامنه و در مسیر زیر صورت می‌گیرد.

Computer Configuration>Windows Setting> Security Setting> System Services

در windows 2003 مسیر فوق از Security Settings به بعد وجود ندارد. به روش گفته شده در

ابتدای این مدخل عمل شود.

واژه‌ها:

Replication: تکرار

KCC: Knowledge Consistency Checker

۴۸- راهبری IIS

IIS Admin Service

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

اگر سرویس SMTP فعال شود سرویس IIS Admin نیز باید فعال شود و این امر باعث ایجاد نقطه‌ای آسیب پذیر روی سرور می‌شود.

تهدیدات

از آنجایی که فعال بودن هر سرویس نقطه‌ای آسیب پذیر محسوب می‌شود، نفوذگران می‌توانند جهت نفوذ به سرور از آن استفاده کنند.

پیامدها

دسترسی نفوذگران به منابع سرور و ایجاد اختلال در سرویس دهی آن.

راه حل امنیتی

اگر از پروتکل SMTP جهت Replication بین سایت‌ها استفاده شود، این سرویس باید به صورت Automatic فعال شود.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting>Security Setting>System Services

در windows 2003 مسیر فوق از Security Settings به بعد وجود ندارد. به روش گفته شده در

ابتدای این مدخل عمل شود.

واژه‌ها:

SMTP: Simple Mail Transport Protocol

۴۹- سرویس NTLM Security Support Provider

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

این سرویس برای پشتیبانی از امنیت پیام‌های RPC مربوط به برنامه‌های RPC مورد نیاز است. با استفاده از این سرویس، این برنامه‌ها جهت تعیین اعتبار از پروتکل‌های LM و NTLM استفاده می‌کنند.

تهدیدات

فعال کردن این سرویس باعث می‌شود که پروتکل‌های NTLM و LM که پروتکل‌هایی ضعیف جهت تعیین اعتبار هستند، مورد استفاده قرار گیرند.

پیامدها

با توجه به ضعف امنیتی موجود در پروتکل‌های NTLM و LM جهت تعیین اعتبار، نفوذگران می‌توانند از این ضعف جهت دسترسی به اطلاعات، هنگام تعیین اعتبار برنامه‌ها، به وسیله سرور کنترل کننده دامنه استفاده کنند.

راه حل امنیتی

در برخی موارد برای سازگاری برنامه‌های قدیمی که تحت ویندوز ۲۰۰۰ اجرا می‌شوند، فعال کردن این سرویس به صورت اتوماتیک ضروری است. در غیراین صورت باید آن را غیر فعال کرد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Setting> System Services

در windows 2003 مسیر فوق از Security Settings به بعد وجود ندارد. در این نسخه در مسیر

Administrative tools گزینه مستقلی به نام Services وجود دارد که در آن گزینه NTLM Security

موجود است، لذا مسیر دسترسی به پیکربندی فوق به شرح زیر است:

Start> Administrative tools> Services> NTLM Security

واژه‌ها:

فراخوانی زیر برنامه‌های راه دور RPC :Remote Procedure Call

۵۰- سرویس Simple Mail Transport Protocol (SMTP)

Microsoft Solution for Security (Windows 2000 Server)

منبع

نقطه آسیب پذیری

سرویس SMTP روی کنترل کننده‌های دامنه برای انجام Replication بین سایت‌ها مورد نیاز است. این سرویس دو نقطه آسیب پذیری ایجاد می‌کند:

۱- به وسیله داده‌هایی که برای این سرویس ارسال می‌شود، امکان سرریز شدن بافر و غیرفعال شدن این سرویس وجود دارد.

۲- سرور SMTP می‌تواند درخواست‌هایی که به وسیله کاربران عضو دامنه ارسال می‌شوند را تعیین اعتبار کند. این سرور معمولاً تنظیمات مربوط به غیرفعال کردن Account‌هایی که به وسیله سیاست‌های گروهی تنظیم می‌شوند را اعمال نمی‌کند. در نتیجه نفوذگران می‌توانند بدون هیچ مشکلی کلمات عبور مختلف را جهت ورود به سیستم امتحان کنند.

تهدیدات

سرریز شدن بافر و تلاش نفوذگران جهت دسترسی به کلمات عبور کاربران مجاز

پیامدها

با سرریز شدن بافر فعالیت سرور دچار اختلال می‌شود. ضمناً نفوذگران با دسترسی به کلمات عبور کاربران مجاز می‌توانند به سیستم وارد شده و به منابع و اطلاعات روی آن دسترسی پیدا کنند.

راه حل امنیتی

در صورتی که به Replication بر پایه سرویس SMTP نیازی نباشد این سرویس را باید غیرفعال کرد.

روش

تنظیم این گزینه از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration > Windows Setting > Security Setting > System Services

در windows 2003 مسیر فوق از Security Settings به بعد وجود ندارد. به روش گفته شده در

ابتدای این مدخل عمل شود.

توجه: با توجه به شیوه دسترسی جدید به System services در windows 2003 گزینه Simple

Mail Transfer Porotocol از جمله گزینه‌هایی است که به صورت پیش فرض فعال نیست و

می‌توان از طریق Control Panel > Add/Remove Program > Add/Remove Windows Component

آن را اضافه کرد.

۵۱- لیست‌های کنترل دسترسی فایل

File Access Control Lists

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

به صورت پیش فرض تمام کاربران دارای مجوز **Full Control** روی فایل‌های موجود در سیستم هستند، این امر نقطه‌ای آسیب پذیر و خطرناک محسوب می‌شود.

تهدیدات

با توجه به مجوز پیش فرض، تمام کاربران روی تمام فایل‌ها از جمله اطلاعات درون **Active Directory**، گزارشات **DNS** و غیره دارای مجوز **Full Control** هستند.

پیامدها

نفوذگران می‌توانند به محتویات درون **Active Directory** و سایر اطلاعات و منابع سیستمی دسترسی داشته باشند و در آن‌ها تغییر ایجاد کنند.

راه حل امنیتی

در مورد مجوزهای دسترسی روی سرور کنترل کننده دامنه، مجوز **Full Control** روی تمام پارتیشن‌ها تنها باید به گروه **Administrator**، **Creator/Owner** و **System** داده شود.

روش

تنظیم مجوزها روی پارتیشن سیستمی (معمولاً درایو C) از طریق سیاست‌های گروهی مربوط به کنترل کننده‌های دامنه صورت می‌گیرد و برای سایر پارتیشن‌ها باید از دستور **CacIs** به صورت زیر در **Command** استفاده شود.

CacIs e: \t/g Administrators: F System: F Create or /Owner: F

در **windows 2003** نیز به همین شیوه است.

سایر پیکربندی‌های امنیتی کنترل کننده‌های Domain

۵۲- غیر فعال کردن تنظیمات LM Hash روی سرورهای کنترل کننده دامنه

Disabling the NoLmHash Setting on Domain Controllers

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

با این تنظیم می‌توان آسیب پذیری مربوط به ذخیره‌سازی LM Hash ها درون بانک اطلاعاتی Account ها را کاهش داد و مانع استفاده از پروتکل LM جهت تعیین اعتبار شد. البته اگر در دامنه، سرویس گیرنده‌های ویندوز ۹۸ وجود داشته باشد، استفاده از LM برای تعیین اعتبار آن‌ها به وسیله کنترل کننده دامنه ضروری است.

تهدیدات

اگر LM Hash را غیر فعال نکنیم مقادیر LM Hash که نمایانگر کلمات عبور کاربران هستند، در Active Directory ذخیره می‌شوند و نفوذگران با دسترسی به این مقادیر می‌توانند به کلمات عبور کاربران دسترسی پیدا کنند. البته دسترسی به این مقادیر در سرور کنترل کننده دامنه به دلیل ساختار بسیار امن Active Directory نسبت به سایر سرورها مشکل‌تر است. ضمناً امکان استفاده از پروتکل LM جهت تعیین اعتبار فراهم می‌شود.

پیامدها

استفاده از پروتکل ضعیف LM جهت تعیین اعتبار و دسترسی نفوذگران به اطلاعات حساس مثل کلمات عبور کاربران.

راه حل امنیتی

باید کلید رجیستری با نام nolm hash را در مسیر HKLM\System\Current Control Set\Lsa روی سرورهای کنترل کننده دامنه حذف کرد.

در windows 2003 برای غیرفعال کردن lmhash در Registry مسیر زیر دنبال شود:

HKEY-LOCAL-MACHINE\system\current content set\control\lsa\nolmhash

واژه ها:

الگوریتمی جهت رمزگذاری کلمات عبور کاربران: LM Hash

۵۳- جابجایی داده‌های ذخیره شده در Active Directory و فایل گزارشات Data Relocation-Active Directory Database and Log Files

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

وقتی سرویس **Directory** روی سرور فعال باشد، فایل‌های مرتبط با آن مانند **NTDS.dit** و **EDB.log** و **TEMP.edb** قفل می‌شوند و این فایل‌ها به طور مستقیم قابل خواندن و نوشتن نیستند. البته این احتمال هست که نفوذگر با دسترسی به فرآیند **Lsass.exe** که عملیات قفل گذاری روی این فایل‌ها را انجام می‌دهد بتواند به این فایل‌ها دسترسی پیدا کند و تغییراتی در آن‌ها ایجاد نماید.

تهدیدات

نفوذگران با دسترسی به فایل‌های مربوط به سرویس **Directory** می‌توانند اختلالاتی در ارائه سرویس توسط **Domain Controller** در شبکه ایجاد کنند.

پیامدها

دسترسی نفوذگران به فایل‌های مربوط به **Active Directory** و ایجاد اختلال در ارائه سرویس به کاربران عضو دامنه.

راه حل امنیتی

راه حل مناسب، قراردادن فایل‌های مربوط به **Active Directory** در یک درایو غیر سیستمی، به منظور جلوگیری از حملات پیمایش دایرکتوری توسط نفوذگران و اعمال مجوزهای دسترسی روی این فایل‌ها است.

روش

هنگام نصب کنترل کننده‌های دامنه می‌توان محل ذخیره فایل **Ntds.dit** و **Log** فایل‌ها را مشخص کرد. بعد از نصب سرور نیز می‌توان جای این فایل‌ها را با استفاده از دستور **NtdsUtil** تغییر داد. البته سرور نباید در حالت سرویس دهی به شبکه باشد.

(مسیر ذخیره این فایل‌ها است %s) %s (

Move Log to %s

در windows 2003 نیز میتوان با استفاده از Command همین کار را انجام داد.

۵۴- بستن پورت‌ها با فیلترهای IPSec

Blocking Ports with IPSec Filers

منبع

(Microsoft Solution for Security (Windows 2000 Server

نقطه آسیب پذیری

هر پورت باز روی سرور می‌تواند به عنوان یک نقطه آسیب پذیر به شمار آید.

تهدیدات

نفوذگر می‌تواند با استفاده از اسب تروا یا Worm، برنامه‌ای را روی سرور نصب کند که با اختصاص تعدادی از پورت‌های غیرمجاز به این برنامه، امکان اجرای یک سری دستورات روی سرور فراهم شود.

پیامدها

امکان اجرای دستورات و برنامه‌های مخرب روی سرور و ایجاد اختلال در سرویس دهی آن توسط نفوذگران فراهم می‌شود.

راه حل امنیتی

روی هر نوع سرور تنها باید پورت‌های مرتبط با سرویس‌های فعال و مورد نیاز باز باشد و سایر پورت‌ها را باید بست.

روش

تنظیم این فیلترها از طریق سیاست‌های گروهی و در مسیر زیر صورت می‌گیرد.

Computer Configuration> Windows Setting> Security Settings> IP Security Policies

این مسیر در windows 2003 همراه با پیکربندی لازم جهت Block کردن وجود دارد.

۵۵- پیکربندی فهرست گزارشات در DHCP

Configure Logging In DHCP

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

اطلاعاتی که در فهرست رویدادها **Event Log** ذخیره می‌شوند براساس نام کامپیوترها می‌باشد. به همین دلیل ثبت گزارشات مربوط به سرویس گیرنده‌های **DHCP** مشکل است.

تهدیدات

نفوذگر می‌تواند بدون این‌که اثری از مشخصات منبع حمله در فهرست رویدادها باقی بماند به سرور نفوذ کند.

پیامدها

هیچ رکورد اطلاعاتی در مورد مشخصات منبع حمله ثبت نمی‌شود و نفوذگران می‌توانند به راحتی و بدون برجای ماندن اثری از حملات آن‌ها در فهرست رویدادها در سرویس دهی سرورها اختلال ایجاد کنند.

راه حل امنیتی

با فعال کردن ثبت گزارشات **DHCP** می‌توان منبع حملات داخلی و یا فعالیت‌های غیرعمدی در شبکه را ردیابی کرد.

روش

تنظیم این گزینه از طریق کنسول تنظیمات **DHCP** سرور و در مسیر زیر صورت می‌گیرد.

Property> General> Enable Audit Log

در **windows 2003** این تنظیمات وجود ندارد.

۵۶- محافظت در برابر حملات DoS در سرور DHCP

Protect Against Denial Of service Attacks on DHCP

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

DHCP سرور به عنوان منبع مرکزی برای پخش IP در بین Client های شبکه، می تواند به عنوان یک هدف جهت حمله توسط نفوذگران مطرح باشد. با غیرفعال شدن این سرور در شبکه، DHCP Client ها قادر به دریافت IP، اتصال به شبکه و دسترسی به منابع آن نیستند.

تهدیدات

نفوذگران می توانند با استفاده از حملات DoS مانند پر کردن بافر، درخواست IP از DHCP یا درخواست تمام IP ها توسط یک Client عملاً سرور را از سرویس دهی باز دارند.

پیامدها

امکان دریافت IP از سرور توسط Client ها و دسترسی آن ها به منابع شبکه وجود ندارد.

راه حل امنیتی

یک راه حل مناسب به کار بردن دو یا چند DHCP سرور و تقسیم Range IP ها بین آن ها است. راه حل دیگر افزایش زمان اختصاصی IP به یک سرویس گیرنده است تا در صورت غیرفعال شدن سرور امکان دسترسی به شبکه برای سرویس گیرنده وجود داشته باشد.

روش

تغییر مدت زمان اختصاص IP در کنسول DHCP و در مسیر زیر صورت می گیرد.

Properties> General> Lease Duration for DHCP Clients

واژه ها:

DoS: Denial of Service

۵۷- غیرفعال سازی نگاشت‌های Script در سرور IIS

Disabling Script Mappings in IIS Server

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

Script Mapping ها از ابزارهای مهم و کاربردی در IIS هستند، که البته باعث کاهش امنیت روی وب سرور می‌شوند.

تهدیدات

از جمله تهدیداتی که سرور در معرض آن‌ها قرار دارد، دسترسی کامل نفوذگر به سرور، اجرای اسکریپت‌ها و کدها روی سرور توسط نفوذگران و امکان دسترسی به Source Code مربوط به صفحات ASP می‌باشد.

پیامدها

کنترل سرور توسط نفوذگران، اجرای کدهای مخرب روی سرور و دسترسی به کد برنامه‌های ASP روی سرور.

راه حل امنیتی

تمام isapi Filter و Script Mapping های غیر ضروری روی سرور باید غیر فعال شوند.

روش

با استفاده از ابزار IIS Lockdown می‌توان این تنظیمات را انجام داد.
در windows 2003 نیز از همین طریق عمل می‌شود.

۵۸- چاپ از طریق اینترنت

Internet Printing

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

با استفاده از این ویژگی می‌توان از طریق اینترنت و صفحات وب از چاپگر متصل به سرور استفاده و حتی از این طریق آن‌ها را مدیریت کرد. فعال بودن این ویژگی سطح آسیب پذیری روی سرور را افزایش می‌دهد.

تهدیدات

نفوذگر از طریق این ویژگی می‌تواند به سرور دسترسی پیدا کند و اختلالاتی در سرویس دهی آن ایجاد کند.

راه حل امنیتی

غیرفعال کردن این ویژگی.

روش

به دو طریق می‌توان این گزینه را تنظیم کرد:

۱- از طریق سیاست‌های گروهی و در مسیر زیر:

Computer Configuration>Administrative Templates> Printers

۲- از طریق کنسول مدیریت IIS

در windows 2003 برای تنظیم از طریق اول به شکل زیر عمل شود:

Start> Administrative tools> Service management>printers

همچنین می‌توان از طریق IIS نیز عمل کرد.

۵۹- حذف دایرکتوری‌های مجازی و برنامه‌های نمونه**Virtual Directory and Sample Applications Removable****منبع**

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

در IIS5.0 برنامه‌های نمونه‌ای وجود دارد که در حالت نصب کامل IIS نصب میشوند و درون تعدادی دایرکتوری مجازی قرار می‌گیرند. این برنامه‌ها به عنوان نقطه آسیب پذیری وب سرور محسوب می‌شوند.

تهدیدات

برنامه‌های نمونه دارای نقاط ضعف امنیتی هستند که نفوذگران می‌توانند از این ضعف‌ها جهت نفوذ به سرور استفاده کنند. این ضعف‌ها شامل دایرکتوری‌های مجازی نیز می‌شود.

پیامدها

نفوذگران با استفاده از ضعف‌های امنیتی موجود در این برنامه‌ها می‌توانند به محتویات وب سایت‌ها دسترسی پیدا کنند و کنترل وب سرور را در اختیار بگیرند.

راه حل امنیتی

راه حل مناسب حذف این برنامه‌ها و دایرکتوری‌های مجازی محتوی آنها است.

روش

به دو روش می‌توان این برنامه‌ها و دایرکتوری‌های مجازی را از وب سرور حذف کرد.

۱- از طریق کنسول مدیریت IIS

۲- به وسیله ابزار IIS Lockdown

در windows 2003 نیز به همین شکل است.

واژه‌ها:

دایرکتوری‌های مجازی: Virtual Directory

۶۰- محدود کردن مجوزهای دسترسی برای کاربران IIS

File Permissions Lockdown of IIS Users

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

پس از دسترسی غیرمجاز نفوذگر به سیستم، این احتمال وجود دارد که او دستوراتی را جهت مشاهده داده‌ها و یا اجرای فعالیت‌های خاص روی وب سرور راه دور، اجرا کند.

تهدیدات

نفوذگر می‌تواند برنامه یا کد اجرایی را روی وب سرور Upload و اجرا کند که این کار می‌تواند شامل برنامه و یا کد مخرب باشد.

پیامدها

اجرای برنامه‌ها و کدهای مخرب توسط نفوذگران روی وب سرور و ایجاد اختلال در سرویس دهی سرور.

راه حل امنیتی

باید لیست کنترل دسترسی (ACL) برای تمام فایل‌های اجرایی درون دایرکتوری WINNT و دایرکتوری‌های درون آن ایجاد کرد به‌طوری‌که اجازه اجرای این فایل‌ها به کاربران بی‌نام داده نشود. ضمناً باید لیست کنترل دسترسی هم، برای فایل‌ها و فولدرهایی که به وسیله دایرکتوری‌های مجازی به آن‌ها رجوع می‌شود ایجاد نمود، به نحوی که اجازه نوشتن درون آن‌ها را به این دسته از کاربران ندهد.

روش

استفاده از ابزار IIS Lockdown با این روش می‌توان لیست‌های کنترل دسترسی را تنظیم کرد.

در windows 2003 نیز به همین شکل است.

واژه‌ها:

ACL: Access Control List

۶۱- غیرفعال سازی Web DAV

Disable Web DAV

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

نقطه آسیب پذیر مربوط به Web Dav این است که نفوذگران می‌توانند در شبکه داخلی جست‌وجو کرده و به اطلاعاتی که دسترسی به آن‌ها محدود شده است و تنها از طریق Account مربوط به سرویس Web Dav قابل دسترسی هستند، دسترسی پیدا کنند.

تهدیدات

نفوذگران می‌توانند به اطلاعاتی که دسترسی به آن‌ها غیر مجاز است، دسترسی پیدا کنند.

پیامدها

دسترسی غیرمجاز نفوذگران به اطلاعات روی سرور.

راه حل امنیتی

غیر فعال کردن ویژگی Web DAV، تنظیم لیست کنترل دسترسی روی DLL مربوط به اجرای Web DAV (Httpext.DLL) جهت جلوگیری از Load شدن آن هنگام اجرای فرآیندهای IIS.

روش

این تنظیم از طریق ابزار IIS Lockdown صورت می‌گیرد.

در windows 2003 نیز به همین شکل است.

واژه‌ها:

Web DAV : Web Distributed Authoring and Versioning

۶۲- تغییر مکان دایرکتوری‌های ذخیره محتوای وب

Relocating the Web Content Directories

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

نصب پیش فرض IIS خطر پیمایش دایرکتوری‌ها را افزایش می‌دهد. پیمایش دایرکتوری وقتی رخ می‌دهد که نفوذگر به دایرکتوری ریشه وب دسترسی پیدا کند و فایل‌هایی خارج از این دایرکتوری را درخواست یا Upload نماید.

در نصب پیش فرض IIS اجازه دسترسی به فایل‌های روی پارتیشن سیستم عامل به همه کاربران داده می‌شود، این امر شامل دسترسی به بسیاری از دستورات سیستمی می‌باشد.

تهدیدات

پیمایش دایرکتوری‌های روی پارتیشن سیستم عامل توسط نفوذگران و اجرای دستورات مختلف روی سرور.

پیامدها

دسترسی نفوذگران به اطلاعات روی سرور و اجرای دستورات مختلف روی آن به منظور اختلال در سرویس دهی.

راه حل امنیتی

راه حل مناسب قراردادن دایرکتوری ریشه مربوط به وب سایت روی پارتیشنی غیر از پارتیشن سیستم عامل است.

روش

برای انتقال دایرکتوری ریشه از کنسول مدیریت IIS استفاده می‌شود و بعد از غیرفعال کردن وب سایت مورد نظر در محیط Command دستور زیر وارد خواهد شد.

XCopy C:\inet pub\WWW Root D:\WWW Root /S /I /O

در windows 2003 نیز به همین شکل است.

۶۳- محدود کردن مجوزها روی فایل Metabase

Hardening Metabase Permissions

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

تمام تنظیمات پیکربندی و امنیتی IIS درون فایل Metabase نگهداری می‌شود. مجوزهای پیش فرض مربوط به این فایل به نفوذگران اجازه می‌دهد تا مستقیماً این فایل را ویرایش کنند.

تهدیدات

نفوذگران می‌توانند با ویرایش این فایل تنظیمات امنیتی و پیکربندی IIS را تغییر دهند.

پیامدها

دسترسی نفوذگران به تنظیمات پیکربندی و امنیتی IIS و کنترل عملکرد سرور توسط آن‌ها.

راه حل امنیتی

مجوز Full Control روی این فایل تنها باید به گروه Administrator و System Account داده

شود.

روش

برای تنظیم مجوزهای روی این فایل می‌توان از دستور زیر در محیط Command استفاده کرد.
Calls%System Root%\System 32\Inet SRV\MetaBase.Bin /g Administrator: F System: F
 در windows 2003 نیز به همین شکل است.

۶۴- غیرفعال سازی گزارش محل ذخیره محتوا از طریق Http

Disabling Content Location in Http Response

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

در صفحات HTML امکان بازیابی اطلاعات درون **Header** از طریق پاسخ‌های **Http** وجود دارد. این اطلاعات حاوی **IP** آدرس وب سایت مورد نظر می‌باشد. همین موضوع باعث ایجاد نقطه آسیب پذیر روی سرور می‌شود. چون **IP** آدرس داخلی سرور قابل شناسایی خواهد بود.

تهدیدات

IP آدرس داخلی سرور در اختیار نفوذگران قرار می‌گیرد.

پیامدها

نفوذگران با دسترسی به **IP** آدرس سرور می‌توانند آن را مورد حمله و نفوذ قرار دهند و در فعالیت سرور اختلال ایجاد کنند.

راه حل امنیتی

جلوگیری از نمایش **IP** آدرس سرور در پاسخ‌های **Http**.

روش

برای تنظیم این گزینه باید در فایل **Meta Base** مربوط به **IIS** گزینه **Use Host Name** را طوری تغییر دهیم که به جای نمایش **IP** آدرس سرور، **FQDN** آن ارسال شود. در **windows 2003** نیز به همین شکل است.

واژه ها:

FQDN: Fully Qualified Domain Name

۶۵- غیرفعال کردن نمایش جزئیات در پیغام‌های خطا مربوط به ASP

Disabling Detailed ASP Error Messages

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

به صورت پیش فرض IIS جزئیات مربوط به پیغام‌های خطای ASP را برای Client ارسال می‌کند. از آنجایی که جزئیات مربوط به برنامه‌ها نمایش داده می‌شود، این امر می‌تواند برای یافتن اشکال برنامه‌ها مفید باشد .

تهدیدات

نفوذگر با دریافت این جزئیات اطلاعات مفیدی در مورد برنامه در حال اجرا روی سرور به دست می‌آورد و با شناخت بهتر اقدام به حمله و نفوذ می‌کند.

پیامدها

دسترسی بهتر و راحت‌تر نفوذگران به برنامه‌های در حال اجرا روی وب سرور و ایجاد اختلال در عملکرد آن‌ها.

راه حل امنیتی

غیرفعال کردن گزینه Detailed ASP Error Messages روی وب سرور

روش

این تنظیم از طریق کنسول مدیریتی IIS و در مسیر زیر صورت می‌گیرد.

Properties> Home Directory> Configuration

در windows 2003 نیز به همین شکل است.

۶۶- حذف Front Page 2000

Removing Front Page 2000 Server Extensions

منبع

Microsoft Solution for Security (Windows 2000 Server)

نقطه آسیب پذیری

ویژگی **Front Page 2000 Server Extensions** امکان مدیریت از راه دور وب سایت‌ها را فراهم می‌کند. این ویژگی علاوه بر مزایایی که دارد نقطه آسیب پذیری نیز به شمار می‌رود.

تهدیدات

نفوذگران ماهر می‌توانند در صورت فعال بودن این ویژگی روی وب سرور آن را مورد حمله و نفوذ قرار دهند.

پیامدها

دسترسی به محتویات وب سرور و امکان کنترل از راه دور آن به وسیله نفوذگران.

راه حل امنیتی

حذف این ویژگی روی وب سرور

روش

حذف این ویژگی از مسیر زیر امکان پذیر است.

Add\Remove Programs> Add/Remove Windows Components> Internet Information Services (IIS)> Details

در windows 2003 نیز به همین شکل است.

ممیزی ویندوز

ممیزی و شناسایی ورودی‌های غیرمجاز

- در بسیاری از محیط‌های امن باید حملات و ورودی‌های غیرمجاز را مرتباً کنترل کرد. دلایل اهمیت این امر عبارت‌اند از:
- هر سیستم فعال در شبکه بدون در نظر گرفتن سطح امنیتی اعمال شده به شبکه می‌تواند مورد حمله و نفوذ قرار گیرد.
 - اغلب به همراه حملات موفق یک سری حملات ناموفق نیز صورت می‌گیرد که در صورت عدم کنترل شبکه، شناسایی این دسته از حملات ناموفق، ممکن نخواهد بود.
 - هنگامی که یک حمله موفق رخ می‌دهد، هرچه زودتر این حمله شناسایی شود آسیب‌های ناشی از آن کاهش می‌یابد.
 - برای دفع حملات لازم است آسیب‌های ناشی از آن شناسایی شود.
 - ممیزی و شناسایی ورودی‌های غیرمجاز در شناسایی عامل حمله موثر است.
 - ترکیب ممیزی و شناسایی ورودی‌های غیرمجاز در شناسایی الگوهای حمله موثر است.
 - بررسی و مرور مداوم گزارش‌های امنیتی، در شناسایی تنظیمات نادرست مثل مجوزهای اشتباه یا تنظیمات ضعیف مربوط به غیرفعال کردن **Account**‌ها موثر است.
 - بعد از شناسایی یک حمله، می‌توان از ممیزی در تعیین منابعی که مورد حمله قرار گرفته‌اند کمک گرفت.

ممیزی

بخش مهمی از استراتژی امنیتی، تعیین سطح مناسب ممیزی برای محیط مورد نظر است. ممیزی باید حملات موفق و غیرموفق را شناسایی کند. وقتی برای میزان ممیزی تصمیمی گیری می‌شود، باید به این نکته توجه داشت که هرچه ممیزی‌ها افزایش یابد، گزارش‌های بیشتری در فهرست رویدادها ایجاد و باعث می‌شود که شناسایی رویدادهای مهم و حیاتی دشوارتر گردد.

در این موارد لازم است که از ابزارهای دیگری مثل مدیر عملیات مایکروسافت **Microsoft Operation Manager (MoM)** برای فیلتر کردن رویدادهای مهم‌تر استفاده شود.

رویدادهای ممیزی را می‌توان به دو گروه تقسیم کرد:

۱. رویدادهای موفق
۲. رویدادهای ناموفق

یک رویداد موفق به انجام یک عمل موفق مثل دسترسی یک کاربر به یک منبع اطلاعاتی اشاره می‌کند و رویداد ناموفق به شکست کاربر در دسترسی به یک منبع اشاره دارد.

بررسی رویدادهای ناموفق برای دنبال کردن رد یک حمله و نفوذ، اهمیت دارد. اصولاً الگوی یک رویداد به اندازه نتایج آن رویداد دارای اهمیت است. برای مثال وقتی سلسله‌ای از رویدادهای ناموفق به دنبال یک رویداد موفق صورت می‌گیرد، ممکن است به یک تلاش جهت حمله و نفوذ که سرانجام موفق هم بوده است اشاره کند.

در صورت امکان باید رویدادهای ممیزی را با سایر اطلاعاتی که در مورد کاربران موجود است، مرتبط کرد. برای مثال وقتی یک کاربر به مرخصی می‌رود می‌توان Account مربوط به وی را غیرفعال کرد و بعد از بازگشت دوباره آن را فعال کرد.

چگونگی فعال کردن ممیزی

ممیزی از طریق تنظیمات گروهی (Group Policy) فعال می‌شود. این تنظیمات می‌توانند روی یک کامپیوتر محلی یا در سطح یک دامنه (Domain)، سایت و یا واحد سازمانی (Organization Unit) است.

تعیین تنظیمات فهرست رویدادها

هر رویدادی که به وسیله ممیزی ایجاد می‌شود در کنسول Event Viewer ظاهر می‌شود. در این قسمت می‌توان چگونگی ذخیره فهرست رویدادها را مشخص کرد. این کار از طریق کنسول Event Viewer و کنسول مربوط به تنظیمات گروهی (Group Policy) امکان پذیر است.

رویدادهای قابل ممیزی

ویندوز ۲۰۰۰ چند گروه از رویدادهای امنیتی قابل ممیزی را مشخص کرده است. این گروه‌ها شامل موارد زیر است:

۱. رویدادهای ورود (Event Log)
۲. رویدادهای مربوط به Account کاربران (Account Log On)
۳. رویدادهای دسترسی به Objectها (Object Access)
۴. رویدادهای دسترسی به سرویس دایرکتوری (Directory Service Access)
۵. رویدادهای استفاده از مجوزها (Privilege Use)
۶. رویدادهای پی گیری فرآیندها (Process Tracking)
۷. رویدادهای سیستمی (System Event)
۸. رویدادهای تغییر تنظیمات (Policy Change)

توجه: در windows 2003 از گزینه System Events می‌توان استفاده کرد.

رویدادهای ورود به سیستم Log On Event

این رویدادها هنگام ورود کاربر به سیستم یا خروج از آن روی می‌دهند و می‌توانند برای پیگیری یک حمله و نفوذ مفید باشند. رویدادهای ورود و خروج، هم برای کاربران و هم برای کامپیوترها است. البته کامپیوترهایی که ویندوز ۹۸ دارند دایرکتوری **Account** ندارند. بنابراین برای آن‌ها رویداد ورود و خروج به شبکه درون فهرست رویدادها ایجاد نمی‌شود.

کدهای مورد استفاده و شرح هر رویداد در جدول‌های بعدی نمایش داده شده اند:

جدول رویدادهای ورود (Log On) که در فهرست رویدادهای امنیتی ایجاد می‌شوند

توضیح	شماره رویداد (Event ID)
یک کاربر با موفقیت به سیستم وارد شده است.	528
تلاش برای ورود با یک نام کاربری ناشناخته و یا یک نام کاربری شناخته شده و یک کلمه عبور نامناسب.	529
تلاش برای ورود به سیستم با یک Account کاربری خارج از زمان مجاز.	530
تلاش برای ورود با یک Account غیرفعال.	531
تلاش برای ورود با یک Account منقضی شده.	532
کاربر مجاز به ورود به سیستم نیست.	533
تلاش یک کاربر برای ورود با یک نوع ورود غیرمجاز.	534
کلمه عبور برای یک Account خاص، منقضی شده است.	535
سرویس Net Log On فعال نیست.	536
تلاش برای ورود به سیستم با شکست مواجه شده است.	537
یک کاربر از سیستم خارج شده است.	538
یک Account در هنگام تلاش برای ورود غیرفعال شده است. این امر می‌تواند نشان دهنده نفوذ از طریق تست کلمات عبور توسط نفوذگران باشد.	539
ورود موفقیت آمیز به شبکه.	540
کاربر مجدداً به نشست Terminal Service (Session) قطع شده، وصل شده است.	682
کاربر بدون Log Off یک نشست Terminal Service را قطع کرده است.	683

جدول رویدادهای مربوط به Account

توضیح	شماره رویداد (Event ID)
مجوز مربوط به سرویس تعیین اعتبار (AS) به صورت موفقیت آمیز انتشار یافته و معتبر است.	672
مجوز (TGS) اعطا شده است.	673
قاعده امنیتی، مجوز سرویس تعیین اعتبار (AS) یا (TGS) جدیدی ایجاد کرده است.	674
تعیین اعتبار قبلی با شکست مواجه شده است.	675
درخواست تعیین اعتبار با شکست مواجه شده است.	676
مجوز TGS اعطا نشده است. (Ticket Granting Service)	677
Account به صورت موفقیت آمیز به Domain Account نگاشت شده است.	678
Account برای ورود موفقیت آمیز مورد استفاده قرار گرفته است.	680
تلاش برای ورود از طریق Domain Account صورت گرفته است.	681
Account کاربری ایجاد شده است.	624
نوع Account کاربری تغییر کرده است.	625
Account کاربر، فعال شده است.	626
تلاش جهت تغییر کلمه عبور.	627
تنظیم کلمه عبور کاربر.	628
Account کاربر غیرفعال شده است.	629
Account کاربر پاک شده است.	630
امنیت برای گروه‌های عمومی موجود فعال شده است.	631
امنیت برای اعضای اضافه شده به گروه‌های عمومی، فعال شده است.	632
امنیت برای اعضای حذف شده از گروه‌های عمومی، فعال شده است.	633
امنیت برای گروه‌های عمومی حذف شده، فعال شده است.	634
امنیت برای گروه محلی موجود، غیرفعال شده است.	635
امنیت برای اعضا اضافه شده به گروه محلی، فعال شده است.	636
امنیت برای اعضای حذف شده از گروه محلی، فعال شده است.	637

توضیح	شماره رویداد (Event ID)
امنیت برای گروه محلی حذف شده، فعال شده است.	638
امنیت گروه محلی تغییر کرده است.	639
امنیت گروه عمومی تغییر کرده است.	641
Account کاربر تغییر کرده است.	642
تنظیمات و پیکربندی‌های Domain تغییر کرده است.	643
Account کاربر غیرفعال شده است.	644

نکته اول- رویدادهای مربوط به Accountهای کاربری، هنگام ورود کاربر به دامنه، ایجاد می‌شوند و در سرور کنترل کننده دامنه، در قسمت **Event Viewer** ثبت و نگهداری می‌شوند. این رویدادها وقتی که بسته تعیین اعتبار، یک گواهی مربوط به کاربر را تأیید می‌کند، ایجاد می‌شوند. البته اگر از گواهی‌های درون بانک اطلاعاتی مربوط به مدیریت Accountها (SAM) روی سیستم استفاده شود، این رویدادها روی آن سیستم به صورت محلی ثبت می‌شوند. این رویدادها برای Account کامپیوترهای دامنه نیز ایجاد می‌شوند.

نکته دوم- اگر یک کامپیوتر عضو دامنه، با کنترل کننده دامنه، بیشتر از ۵ دقیقه اختلاف زمانی داشته باشد رویداد شماره ۶۷۵ ایجاد می‌شود.

نکته سوم- ممیزی رویدادهای مربوط به مدیریت Accountها برای تعیین این که چه وقت یک کاربر یا گروه ایجاد، تغییر یافته و یا حذف شده است کاربرد دارد. ضمناً برای تعیین زمان ایجاد یک قاعده امنیتی و فردی که اجرا کننده این عمل بوده است مفید می‌باشد.

جدول رویدادهای دسترسی به Object ها

توضیح	شماره رویداد (Event ID)
مجوز دسترسی به Object موجود اعطا شده است.	560
استفاده از Object خاتمه یافته است.	562
تلاش جهت باز کردن Object به قصد حذف کردن آن صورت گرفته است.	563
Object حفاظت شده حذف شده است.	564
مجوز دسترسی به نوعی Object که از قبل موجود است، اعطا شده است.	565

هر **Object** در سطح شبکه ویندوز ۲۰۰۰ قابل ممیزی است. لیست کنترل دسترسی (**ACL**) شامل لیستی از کاربران، گروه‌ها و نوع دسترسی آن‌ها به **Object**هایی است که قابل ممیزی هستند و شامل فایل‌ها و دایرکتوری‌های روی درایوهای **NTFS**، پریترها و کلیدهای رجیستری است.

سه بخش مهم در لیست کنترل دسترسی وجود دارد:

۱. قواعد امنیتی که قابل ممیزی هستند.
 ۲. انواع دسترسی خاص که قابل ممیزی هستند.
 ۳. نشان‌های که به نوع ممیزی از نظر دسترسی موفقیت آمیز یا ناموفق اشاره می‌کند.
- ویندوز ۲۰۰۰ از زیر سیستم‌هایی امنیتی در **Kernel Mode** استفاده می‌کند که تنها اجازه دسترسی به **Object**ها را از طریق **Kernel** برای برنامه‌ها فراهم می‌کند. این مسأله مانع از دور زدن سیستم امنیتی به وسیله برنامه‌ها می‌شود. از زمانی که فضای حافظه مربوط به **Kernel** از قسمت مربوط به برنامه‌های **User Mode** جدا شده است، برنامه‌ها برای دسترسی به **Object**ها از طریق ساختار داده‌ای (**Handle**) عمل می‌کنند.
- دسترسی به **Object**ها عبارت‌اند از:

۱. کاربر، برنامه را برای دسترسی به **Object** خاص هدایت می‌کند. (برای مثال **File>Open**).
۲. برنامه، از سیستم درخواست **Handle** می‌کند که تعیین کننده نوع دسترسی به **Object** است.
۳. زیر سیستم امنیتی، فهرست کنترل دسترسی (**ACL**) روی **Object**های درخواست شده را بررسی می‌کند تا مشخص شود آیا کاربر یا برنامه درخواست کننده اجازه دسترسی به آن را دارد یا خیر.
۴. سیستم، **ACL** مربوط به **Object**های درخواست شده را بررسی می‌کند و به دنبال **Entry** مطابق با حقوق درخواستی برنامه یا حقوق موثری که به برنامه اختصاص داده می‌شود می‌گردد. اگر دسترسی مورد درخواست مجاز نباشد رویداد ممیزی شکست دسترسی به **Object** ایجاد می‌شود و اگر دسترسی مجاز باشد رویداد ممیزی ایجاد می‌شود.
۵. اگر مجوز دسترسی اعطا شده باشد سیستم **Handle** به برنامه ارسال می‌کند که جهت دسترسی به **Object**، مورد استفاده برنامه قرار می‌گیرد.
۶. نکته مهم این است که وقتی ممیزی صورت می‌گیرد و رویدادی رخ می‌دهد، هیچ اتفاقی در مورد **Object** روی نداده است. این موضوع برای بررسی و تفسیر رویدادهای

ممیزی بسیار مهم است. برای مثال ممیزی نوشتن روی فایل قبل از روی دادن این عمل ایجاد می‌شود و ممیزی خواندن قبل از این که فایل خوانده شود، ایجاد می‌شود. اطلاعات مهم در جزئیات هر رویداد قرار دارد. برای پیدا کردن هر رویداد ویژه باید این جزئیات را مورد بررسی قرار داد. مثلاً برای بررسی دسترسی به یک Object باید رویداد شماره ۵۶۰ را مورد بررسی و تحلیل قرار داد. کارهایی که نیاز است در این زمینه صورت گیرد شامل موارد زیر است:

هدف ممیزی	چگونگی انجام
پیدا کردن فایل، دایرکتوری یا Object مشخص.	در قسمت جزئیات مربوط به رویداد ۵۶۰ مسیر مربوط به فایل یا دایرکتوری که باید مورد بررسی قرار گیرد جست‌وجو می‌شود.
تعیین فعالیت‌های کاربر خاص.	فیلتری که مشخص کننده کاربر خاص باشد تعریف می‌گردد.
تعیین فعالیت‌های مربوط به کامپیوتر خاص.	فیلتر مشخص کننده کامپیوتری که فعالیت مورد نظر روی آن انجام می‌شود، تعریف می‌شود.

دسترسی به سرویس دایرکتوری

Object های Active Directory قابل ممیزی هستند، از جمله Account کاربران و گروه‌ها. Object های درون Active Directory دارای لیست‌های کنترل دسترسی هستند که می‌توان مجوزهای دسترسی را برای آن‌ها تعیین کرد و دسترسی به آن‌ها را با Account Manager مورد ممیزی قرار داد. این ممیزی‌ها می‌تواند در شناسایی نفوذگرانی که تلاش می‌کنند دسترسی غیرمجاز به Object های درون Active Directory داشته باشند، مفید واقع شود. رویداد شماره ۵۶۵ در فهرست گزارشات امنیتی اشاره به دسترسی به Object های درون Active Directory دارد.

حقوق تعریف شده برای کاربران قابل ممیزی است. در این حالت هر گاه کاربری قصد استفاده از یکی از حقوق کاربری خود را داشته باشد، رویداد ممیزی می‌تواند ایجاد شود. البته اگر تمام حقوق کاربران جهت ممیزی تنظیم شود، حقوق کاربری زیر به صورت پیش فرض ممیزی نمی‌شوند:

۱. رفع اشکال برنامه‌ها
۲. ایجاد Object
۳. کنترل مسیرهای میان بر
۴. تولید ممیزی‌های امنیتی
۵. تهیه نسخه پشتیبان از فایل‌ها و دایرکتوری‌ها
۶. بازیابی فایل‌ها و دایرکتوری‌ها
۷. Replace process level token

جدول ممیزی استفاده از حقوق کاربری

توضیح	شماره رویداد (Event ID)
حقوق مشخصی به کاربر اعطا شده است.	576
کاربر سعی در استفاده از سرویس ممتاز سیستم را دارد.	577
حقوق دسترسی ممتاز برای استفاده از Handle باز مربوط به Object حفاظت شده، به کار گرفته شده است.	578

بعضی از گزارش‌های ممیزی که هنگام استفاده کاربر از حقوق کاربری ایجاد می‌شوند، عبارت‌اند از:

- فعالیت به عنوان بخشی از سیستم عامل
- تغییر زمان سیستم
- خاموش کردن از راه دور
- Load یا Unload کردن درایور دستگاه
- مدیریت گزارشات امنیتی و ممیزی
- خاموش کردن سیستم محلی
- در اختیار گرفتن مالکیت فایل یا هر Object دیگر

رهگیری فرآیندها

با استفاده از ممیزی فرآیندها می‌توان اطلاعاتی در مورد آغاز و خاتمه یک فرآیند، ایجاد یک

Handle جهت دسترسی به Objectها و مواردی دیگر کسب کرد.

جدول رهگیری فرآیندها

توضیح	شماره رویداد (Event ID)
فرآیند جدید ایجاد شده است.	592
فرآیند خاتمه یافته است.	593
Handle مربوط به Object تکثیر شده است.	594
دسترسی غیر مستقیم به Object فراهم شده است.	595
ویندوز آغاز به کار کرده است.	512
ویندوز خاتمه یافته است.	513
بسته تعیین اعتبار به وسیله منبع امنیتی محلی Load شده است.	514

توضیح	شماره رویداد (Event ID)
فرآیند ورود معتبر به وسیله منبع امنیتی محلی ثبت شده است.	515
منابع داخلی اختصاص یافته برای صف بندی پیام‌های مربوط به رویدادهای امنیتی تمام شده است. این امر نشان دهنده از بین رفتن برخی از پیام‌های مربوط به رویدادهای امنیتی است.	516
گزارش امنیتی پاک شده است.	517
بسته اخطار به وسیله مدیر Account ها (SAM)، Load شده است.	518

نکته اول- **Shutdown** کردن و **Restart** مجدد سرور ممکن است نشانه تلاش نفوذگر جهت دسترسی به سرور در هنگام شروع مجدد فعالیت سرور باشد.

نکته دوم- تغییر یا پاک کردن گزارش‌های امنیتی می‌تواند نشانه تلاش نفوذگران جهت جلوگیری از ثبت گزارش‌های مربوط به حملات آن‌ها باشد.

ممیزی تغییر پیکربندی سیستم

با استفاده از ممیزی تغییر پیکربندی سیستم می‌توان از تلاش نفوذگران جهت تغییر در پیکربندی‌های سیستم آگاه شد.

جدول ممیزی مربوط به رویدادهای تغییر پیکربندی سیستم

توضیح	شماره رویداد (Event ID)
حقوق کاربری ایجاد شده است.	608
حقوق کاربری از کاربر گرفته شده است.	609
ارتباط معتبر با دامنه دیگر ایجاد شده است.	610
ارتباط معتبر با دامنه دیگر قطع شده است.	611
تنظیم ممیزی تغییر کرده است.	612
تداخل بین Name Space در یک Forest با Name Space در دیگر به وجود آمده است.	768

حفاظت از فهرست رویدادها

برای حفاظت و نگهداری از فهرست رویدادها جهت استفاده در مواقع لزوم مراحل زیر باید اجرا شود:

۱. تعیین پیکربندی مناسب برای فضای ذخیره‌سازی جهت حفظ گزارشات.
 ۲. تعیین نحوه عملکرد سیستم در صورت پر شدن فهرست رویدادها.
 ۳. جلوگیری از دسترسی برخی از کاربران مثل Guest.
 ۴. اطمینان از ممیزی رویدادهای موفق یا ناموفق سیستم.
 ۵. مجبور کردن کاربران به استفاده از کلمات عبور پیچیده یا روش‌های تعیین اعتبار مناسب مانند استفاده از کارت‌های هوشمند جهت ورود و دسترسی به منابع سیستم.
- علاوه بر این برای اطمینان از صحت اطلاعات موجود در فهرست‌ها باید طراحی امنیتی شبکه به گونه‌ای باشد که مانع از دسترسی فیزیکی نفوذگران به منابع سیستمی شود. ضمناً باید از روش‌هایی جهت ذخیره و حفظ گزارشات در محل دیگر استفاده کرد. مانند تهیه پشتیبان از فهرست رویدادها.
- برای استفاده بهتر و موثرتر از فهرست‌های ممیزی می‌توان اقدامات زیر را صورت داد:
۱. **زمان بندی منظم جهت بررسی و مرور گزارش‌ها** : با زمان بندی مناسب، مثلاً بررسی روزانه فهرست‌های ممیزی می‌توان آسیب پذیری‌ها و تهدیدات را سریع‌تر شناسایی و جهت رفع آن‌ها اقدام کرد. ضمناً پس از بررسی منظم گزارش‌ها می‌توان آن‌ها را در محل دیگری جهت استفاده‌های بعدی ذخیره کرد و به این ترتیب مانع از پر شدن فهرست گزارشات ممیزی شد.
 ۲. **بررسی فایل‌های گزارش مربوط به برنامه‌ها**: بررسی این دسته از گزارش‌ها در شناسایی نقاط آسیب پذیر برنامه‌ها بسیار موثر است. مثلاً برنامه‌هایی مانند JSA, IIS و IAS و سایر برنامه‌های غیر مایکروسافتی.
- توجه : ساعت همه کامپیوترهایی که فایل‌های گزارش را نگهداری می‌کنند باید همزمان باشد. این مسأله به مدیران شبکه اجازه می‌دهد تا رویدادهای مابین کامپیوترها و سرویس‌ها را جهت شناسایی تهدیدات با هم مقایسه کنند.

کنترل درایورها و سرویس‌های نصب شده

بسیاری از حملات از طریق سرویس‌های نصب شده روی سیستم یا جایگزین کردن درایور معتبر با درایور مخرب صورت می‌گیرد.

از ابزار زیر جهت بررسی و کنترل سرویس‌ها و درایورهای نصب شده روی سیستم می‌توان استفاده کرد.

۱. کنسول مدیریت و کنترل سرویس‌ها: از طریق این کنسول می‌توان سرویس‌های کامپیوتری محلی یا راه دور را مدیریت و کنترل کرد.

۲. دستور **NetSVC.exe**: این دستور در **Resource Kit** ویندوز ۲۰۰۰ موجود است و جهت مدیریت و کنترل سرویس‌ها از طریق خط فرمان مورد استفاده قرار می‌گیرد.

۳. دستور **SVCMon.exe**: این دستور تغییر وضعیت سرویس (**Start** و **Stop**) را اطلاع می‌دهد. برای این منظور باید سروورها را جهت فهرست برداری از وضعیت سرویس‌ها در فواصل زمانی مشخص و سرویس‌ها را جهت کنترل به وسیله ابزار **Monitoring** تنظیم و پیکربندی کرد.

۴. دستور **Driver.exe**: این ابزار، اطلاعاتی در مورد درایورهای نصب شده روی سیستم ارائه می‌دهد. این اطلاعات شامل نام فایل، اندازه و داده‌هایی است که به درایور مربوط‌اند.

توجه: تمام سرویس‌ها را نمی‌توان **Stop** کرد. چون بعضی از سرویس‌ها به سرویس‌های دیگر وابسته هستند که اگر **Stop** نشوند، سرویس مورد نظر غیرفعال نمی‌شود.

کنترل و بررسی پورت‌های باز روی سیستم

نفوذگران اغلب جهت حمله به سیستم از پورت‌های باز روی آن که نشان دهنده سرویس فعال روی آن سیستم است استفاده می‌کنند. کنترل و بررسی مداوم پورت‌های باز روی سرور در شناسایی تهدیدات و حملات موثر است. برای بررسی وضعیت پورت‌های سیستم باید هم به صورت محلی و هم از طریق سیستم راه دور عملیات کنترل و پیمایش پورت‌ها را انجام داد.

دستور **NetStat.exe** ابزاری جهت بررسی وضعیت پورت‌های باز روی سیستم است.

netstat [-a] [-e] [-n] [-s] [-P Proto] [-r] [Interval]

-a: نمایش تمام اتصالات و پورت‌های باز

-e: نمایش اطلاعاتی در مورد کارت شبکه

-n: نمایش شماره پورت‌ها و آدرس‌ها

نمایش ارتباطات مربوط به پروتکل‌های مشخص: **P Proto**-

نمایش جدول مسیریابی: **r** -

نمایش آماری وضعیت هر پروتکل **TCP-UDP-IP**: **s**-

نمایش مجدد اطلاعات در فواصل زمانی مشخص: **Interval**

اگر پورت‌های بازی وجود داشته باشد که شناخته شده نیستند باید بررسی کرد که آیا این پورت‌ها به سرویس‌های مورد نیاز روی سیستم وابسته هستند یا خیر، اگر وابسته به هیچ سرویس ضروری نباشند، باید سرویس را غیرفعال کرد تا پورت مرتبط با آن بسته شود. در مواردی که شبکه به وسیله فایروال حفاظت می‌شود، حتماً باید از طریق سیستم راه دور عملیات پویش پورت را برای بررسی وضعیت پورت‌ها روی فایروال انجام داد.

کنترل نفوذهای غیرمجاز و رویدادهای امنیتی

شناسایی و کنترل نفوذهای غیرمجاز و رویدادهای امنیتی شامل سلسله‌ای از عملیات فعال و غیرفعال است. بسیاری از نفوذهای غیرمجاز، بعد از وقوع حمله و با بررسی فایل‌های گزارش، قابل شناسایی هستند. این روش شناسایی اغلب به عنوان شناسایی نفوذ غیرفعال (**Passive Intrusion Detection**) نامیده می‌شود.

سایر روش‌ها به عنوان روش شناسایی فعال شناخته می‌شوند، مانند جست‌وجو برای الگوها و دستورات مورد استفاده در حمله و جلوگیری از اجرای آن دستورات.

اهمیت همزمان بودن (Synchronization)

برای بررسی ورودهای غیرمجاز و رویدادهای امنیتی مابین چند کامپیوتر، هم زمانی ساعت آن سیستم‌ها امری ضروری است. این هم زمانی به مدیر سیستم اجازه می‌دهد تا حملاتی که علیه چند کامپیوتر صورت گرفته را بازسازی کند. در صورت همزمان نبودن، تعیین این که یک رویداد مشخص چه وقت اتفاق افتاده دشوار خواهد بود.

روش‌های شناسایی غیرفعال

این روش‌ها شامل بررسی و مرور رویدادها و گزارش مربوط به برنامه‌ها است. ابزارهایی جهت تحلیل و شناسایی الگوهای حمله وجود دارد که به چند مورد از آن‌ها در ذیل اشاره شده است:

۱- مرورگر رویداد (Event Viewer)

از طریق این کنسول در ویندوز ۲۰۰۰ می‌توان گزارش‌های مربوط به رویدادهای مختلف را مشاهده و بررسی کرد. ضمناً می‌توان برای یافتن رویدادهای خاص فیلترهایی را تعیین کرد. این فیلترها براساس موارد زیر تعریف می‌شوند:

- نوع رویداد
- منبع رویداد
- دسته‌بندی رویدادها
- شماره رویداد
- نام کاربر ویژه
- نام کامپیوتر ویژه
- رویدادهای اتفاق افتاده در فاصله زمانی مشخص

۲- ابزار ذخیره ساده گزارش رویدادها (Dumple.exe)

این ابزار جهت استفاده در محیط خط فرمان (Command Line) طراحی شده است و در Resource Kit ویندوز ۲۰۰۰ موجود است. ساختار دستور به شکل زیر است:

`dumple -f File [-S \Server] [-L Log [-m Source]] [-e n1 n2 n3...] [-r][-t][-d X]`

-F File: نام فایل خروجی

-S Server: نام سروری که فایل حاوی گزارش‌ها در آنجا ذخیره می‌شود

-L Log: System, Application, Security تعیین نوع گزارش جهت ذخیره ساده

-m Source: تعیین منبع ثبت رکورد مربوط به گزارش‌ها

-e n1 n2 n3: فیلتری برای شماره رویدادها (حداکثر تا ۱۰ شماره)

در این صورت تنها رکوردهایی از این نوع ذخیره می‌شوند. این پارامتر بدون

پارامتر -m قابل استفاده نیست.

تعیین این که آیا برای منبع یا رکورد خاص فیلتر کردن صورت گیرد یا خیر: -r:

برای تعیین جداسازی رشته‌ها به اندازه کلید Tab: -t:

تعیین تعداد روزهایی که رویدادها باید ذخیره شوند: d x-

تعداد روزها را مشخص می‌کند (x)

(برای دستیابی به اطلاعات بیشتر به راهنماهای مربوط مراجعه شود.)

توجه: این ابزار تنها می‌تواند محتویات فایل‌های گزارش مربوط به رویدادهای **Security**، **System** و **Application** را ثبت و نگهداری کند و توانایی ثبت رویدادهای مربوط به **File Replication Service**، **DNS Service** یا **Directory Service** را ندارد.

Event CombMT: ابزار تهیه و تحلیل گزارش رویدادهای مربوط به چند سرور به صورت هم‌زمان

این ابزار در **Resource Kit** ویندوز ۲۰۰۳ موجود است.

با استفاده از این ابزار می‌توان یک یا چند شماره رویداد یا محدوده‌ای از آن‌ها را جهت جست‌وجو و بررسی مشخص کرد. ضمناً می‌توان جست‌وجو را براساس رویدادهای خاص، نوع پیغام‌ها، منبع تولید رویداد و دوره زمانی مشخص محدود کرد. حتی می‌توان متن مشخصی را مورد جست‌وجو قرار داد. این مسأله می‌تواند در جست‌وجوی کاربر یا گروه خاص مفید باشد. بعد از نصب و اجرای برنامه باید کامپیوترهایی که قرار است مورد جست‌وجو و بررسی قرار گیرند، مشخص شوند. فهرست‌های قابل تهیه عبارت است از:

- تمام سرورهای کنترل کننده دامنه.
- سرور یا ایستگاه کاری (**Work Station**) مشخص.
- تمام سرورهای شبکه و تمام کامپیوترهایی که درون فایل متن، نام آن‌ها مشخص شده است.
- سرورهای کنترل کننده دامنه که سرویس دهنده **Global Catalog** هستند

تعیین نوع رویدادها و گزارش‌ها

بعد از تعیین کامپیوترها می‌توان نوع رویداد و گزارش‌های مورد جست‌وجو را تعیین کرد که شامل موارد زیر است:

- رویدادهای سیستم (**System**)
- رویدادهای مربوط به برنامه‌ها (**Application**)
- رویدادهای امنیتی (**Security**)
- رویدادهای مربوط به **File Replication Service (FRS)**

• رویدادهای سرور DNS

• رویدادهای مربوط به Active Directory

علاوه بر این می‌توان انواع رویدادهای زیر را جهت جست‌وجو و بررسی تعیین کرد:

Error •

Informational •

Warning •

Success Audit •

Failure Audit •

Success •

ابزار Event CombMT امکان ذخیره نتایج جست‌وجو را فراهم می‌کند و شامل فایل خلاصه نتایج و فایل‌های متنی جداگانه برای هر کامپیوتر است.

جمع‌آوری رویدادها (شواهد)

یکی از اهداف مهم ممیزی، شناسایی فعالیت نفوذگران روی شبکه است. بنابراین جمع‌آوری و سازماندهی گزارشات ممیزی می‌تواند در شناسایی بهتر تهدیدات و نقاط آسیب‌پذیری موثر باشد. ابزاری جهت جمع‌آوری و سازماندهی متمرکز گزارش وجود دارد که از این میان می‌توان به اسکریپت‌ها، مدیر فعالیت‌های میکروسافت (MoM) و سایر ابزار غیر مایکروسافتی (Third Party) اشاره کرد.

۱- اسکریپت سازی (Scripting)

با استفاده از اسکریپت‌ها می‌توان گزارش رویدادهای مربوط به کامپیوترهای راه دور را در مکان مشخص به صورت متمرکز ذخیره کرد. ضمناً می‌توان زمان اجرای آن‌ها و نوع عملی را که باید بعد از پایان کپی برداری از گزارشات صورت گیرد، مشخص کرد. در Resource Kit ویندوز ۲۰۰۰ یک اسکریپت به زبان Perl جهت نمایش گزارش رویدادها روی کامپیوتر محلی یا راه دور موجود است. برای استفاده از این اسکریپت باید Active Perl نصب شود.

۲- مدیر فعالیت‌های میکروسافت (Microsoft Operations Manager (MoM))

MoM مجموعه وسیعی از ابزار و امکانات را جهت بررسی و تحلیل گزارش‌های ممیزی، کنترل کارایی سرور و برنامه‌های در حال اجرا روی آن، فراهم می‌کند. MoM اطلاعات

جمع‌آوری شده را در بانک اطلاعاتی **SQL Server** ذخیره می‌کند و متدهایی را جهت بازیابی و تجزیه و تحلیل داده‌های ذخیره شده، ارائه می‌دهد.

۳- ابزار غیر مایکروسافتی (Third-Party)

ابزارهای دیگری جهت جمع‌آوری و بررسی گزارشات ممیزی غیر از ابزار ارائه شده توسط مایکروسافت موجود است. این ابزار دارای قابلیت‌های زیر هستند:

- پشتیبانی از انواع گزارش‌های مربوط به ویندوز ۲۰۰۰
- استفاده از بانک‌های اطلاعاتی جهت ذخیره اطلاعات
- امکان جست‌وجو براساس نوع رویدادها و شرایط تعیین شده
- از جمله این ابزار می‌توان به سه مورد زیر اشاره کرد:

- Event Log Monitor (TNT Software)
- Event Archive (Dorian Software Creations)
- Log Caster (Ripple Tech)

روش‌های شناسایی فعال

سیستم شناسایی فعال ورودهای غیرمجاز، ترافیک ورودی به شبکه را در لایه **Application** مورد تحلیل و بررسی قرار می‌دهد تا روش‌های شناخته شده نفوذ و حمله و داده‌های مشکوک را شناسایی کند. اگر بسته اطلاعاتی مشکوکی دریافت شود، این سیستم مانع ورود آن بسته به شبکه شده و گزارش آن را تهیه می‌کند. بعضی از این سیستم‌ها حتی می‌توانند بعد از شناسایی حمله، مدیر شبکه را آگاه کنند. انواع حملاتی که این سیستم‌ها قادر به شناسایی آن‌ها هستند عبارت‌اند از:

۱- حملات شناسایی: این نوع حملات وقتی رخ می‌دهند که نفوذگری از خارج شبکه، درحال تلاش برای شناسایی نقاط آسیب پذیر شبکه جهت حمله است. از جمله این حملات تکرار عملیات **Ping** به صورت مکرر - (**Ping Sweep**) - انتقال نواحی **DNS (DNS Zone Transfer)** شناسایی **e-mail**، پوشش پورت‌ها (**Scan Port**) و بررسی محتویات وب سایت جهت شناسایی اسکریپت‌ها و صفحات آسیب پذیر است.

۲- حملات استعمار: این نوع حملات زمانی رخ می‌دهند که نفوذگر از ویژگی‌های پنهان و اشکالات سیستم جهت دسترسی به آن استفاده می‌کند. در اغلب موارد نقطه حمله به وسیله حمله استثماری قبلی شناسایی می‌شود.

۳- حملات عدم پذیرش یا رد سرویس (DoS): این حملات زمانی روی می‌دهند که نفوذگر سعی می‌کند با استفاده بیش از اندازه از منابع سیستم، سرویس در حال اجرا را غیرفعال کند. در این حملات شخص مزاحم درصدد دسترسی به اطلاعات و منابع شبکه نیست بلکه سعی می‌کند تا مانع سرویس دهی سرورها شود.

سیستم شناسایی مناسب، سیستمی است که بتواند تمام این نوع حملات را شناسایی کند.

برای شناسایی از دو روش استفاده می‌شود:

۱- شناسایی غیرمعارف: در این روش تمام فعالیت‌های متعارف و قابل قبول روی کامپیوتر در شبکه مورد کنترل و بررسی قرار می‌گیرد و چنانچه فعالیت غیرمعارف روی دهد به عنوان حمله و تهدید در نظر گرفته می‌شود. برای مثال وقتی تلاش‌های مکرری جهت ورود به سیستم در ساعات کم کاری سیستم‌ها صورت می‌گیرد می‌تواند نشانه تلاش جهت ورود غیرمجاز به سیستم توسط نفوذگر است. ویژگی این نوع روش این است که می‌تواند حملات را بدون تشخیص این‌که واقعاً چه حمله‌ای رخ داده است شناسایی کند.

۲- شناسایی اثر حملات: این روش، حملات مبتنی برپایه الگوهای شناخته شده را شناسایی می‌کند. بسیاری از حملات روی وب سرورها از الگوهای عمومی و مشخصی استفاده می‌کنند که به سادگی قابل شناسایی هستند. با مقایسه ترافیک ورودی با یک رشته اثر در بانک اطلاعاتی، می‌توان این حملات را به وسیله سیستم‌های شناسایی حمله تشخیص داد.

اشکال این روش این است که این بانک اطلاعاتی باید مرتباً به روز رسانی (Update) شود.

بعضی از محصولات و ابزار غیرمایکروسافتی جهت تست و گسترش این روش‌ها عبارت‌اند از:

- Block LCE Defender
- Cyber Cop Scanner
- ICEPac Security Suite
- Cisco Secure IDS
- eTrust Intrusion Detection
- Snort
- Trip Wire
- Foundstone Attacker

ارزیابی نقاط آسیب پذیر

علاوه بر شناسایی ورودی‌های غیرمجاز باید به صورت متناوب نقاط آسیب پذیر را مورد ارزیابی قرار داد. این ارزیابی، حمله را روی شبکه شبیه سازی می‌کند و نقاط آسیب پذیر شبکه را قبل از این‌که مورد حمله نفوذگران قرار گیرد، مشخص می‌کند.

در مورد انتخاب ابزاری جهت ارزیابی آسیب پذیری باید به نکات زیر توجه داشت:

۱- این نوع ابزار باید از روش اتوماتیک برای به روز رسانی و تشخیص نقاط آسیب پذیر استفاده کنند.

۲- باید قابلیت فیلتر کردن و جداسازی نتایج غیرقابل قبول و نادرست را داشته باشند تا مدیران امنیتی شبکه وقت خود را صرف بررسی رویدادهای غیر ضروری نکنند.

۳- باید امکان ذخیره و نگهداری نتایج حاصل از بررسی‌ها را فراهم کنند.

۴- اگر نقطه آسیب پذیری شناسایی شد، این ابزار باید روش‌هایی را جهت رفع این آسیب‌ها ارائه کنند و یا اسکریپت‌هایی را جهت مقابله با تهدیدات فراهم نمایند.

از جمله ابزار قابل استفاده در ارزیابی نقاط آسیب پذیر شبکه به موارد زیر می‌توان اشاره کرد:

- Symantec NetReCon 3.5
- BindView Security Advisor
- eEye Digital Security – Retina Network Security Scanner
- Internet Security Systems (ISS) Internet Scanner
- Symantec Enterprise Security Manager 5.5

مدیریت Patch ها در ویندوز

مدیریت Patch

مدیریت patch فرآیندی است که بستگی به حجم و پیچیدگی عملیات جاری سازمان دارد. نکته مهم و اساسی در این فرآیند شناسایی نیازهای امنیتی سازمان و استراتژی مدیریت ریسک و اجرای مراحل فرآیند مدیریت Patch به صورت دقیق و کامل است. برای مثال چنانچه مدیران امنیتی شبکه تصمیم بگیرند که خطرات امنیتی را به حداقل برسانند، می‌توانند از استراتژی غیرفعال کردن سیستم‌هایی که در معرض آسیب پذیری قرار دارند، تا هنگام پوشش نقاط آسیب پذیر استفاده نمایند.

البته فرآیند مدیریت Patch در یک سازمان بزرگ و پیچیده می‌تواند بسیار وقت گیر و پرهزینه باشد. در فرآیند مدیریت Patch نقاط آسیب پذیر، میزان و درجه اهمیت تهدیدات و نحوه پوشش این نقاط آسیب پذیر جهت کاهش تهدیدات باید مشخص شود. قبل از اجرای فرآیند مدیریت امنیتی شبکه باید اطلاعاتی درمورد سیستم‌های موجود در شبکه جمع‌آوری کرد این اطلاعات عبارتند از:

۱- نوع و نسخه سیستم عامل

۲- سطح patch ها ((Service Pack Version

۳- عملکرد سیستم ها

۴- برنامه‌هایی که در شبکه اجرا می‌شوند

۵- اطلاعات پرسنلی اشخاص و گروه‌های مسئول نگهداری از سیستم‌ها

۶- ارزش و اهمیت اطلاعات و منابع شبکه

۷- تهدیدات و فرآیند شناسایی آنها

۸- شناسایی نقاط آسیب پذیری

۹- اقدامات متقابل جهت مقابله با تهدیدات

پس از شناسایی و ارزیابی آسیب پذیری‌ها، نحوه تنظیم و پیکربندی امنیتی و اولویت بندی تهدیدات مشخص می‌شود.

ارتقاء نرم‌افزار (Software Update Service (SUS

در بسیاری از محیط‌ها استفاده از تعدادی کامپیوتر جهت اجرای مراحل مدیریت Patchها روشی مناسب است. این کامپیوترها محل ذخیره ی ابزارهای امنیتی، Patchها، Hot Fixها، Service Packها و اسناد مربوط به آنها هستند. این سیستم‌ها می‌توانند به عنوان یک سرویس دهنده جهت اجرای فرآیندهایی مثل تحلیل، بازیابی و اجرای Patchها در کل شبکه مورد استفاده قرار گیرند. این سیستم‌ها به عنوان سرویس دهنده‌های SUS شناخته می‌شوند. ضمناً باید کاملاً امن و به هنگام باشند و مرتباً آخرین Patchها را از اینترنت دریافت کرده و در اختیار سایر سیستم‌ها قرار دهند.

فرآیند مدیریت Patch

این فرآیند شامل چند بخش می‌باشد:

۱- مرحله تحلیل ((Analyze: در این بخش به بررسی تهدیدات بالقوه و نیازهای امنیتی محیط مورد نظر پرداخته می‌شود و patch های مورد نیاز برای کاهش این تهدیدات شناسایی و تعیین می‌شوند.

۲- مرحله طراحی و برنامه‌ریزی: در این مرحله Patchهایی که باید برای مقابله با تهدیدات و آسیب پذیری‌ها مورد استفاده قرار گیرند تعیین می‌شوند. ضمناً باید فردی که عملیات تست و اجرای این فرآیند را انجام می‌دهد انتخاب کرد.

۳- مرحله تست و آزمایش: بررسی و مرور patchهای در دسترس و دسته‌بندی آنها در این مرحله صورت می‌گیرد. تست تمام Patchها برای اطمینان از این‌که تمام آنها بدون تاثیر منفی در محیط عمل خواهند کرد، ضروری است. در این مرحله نحوه عملکرد و تاثیر Patchها در محیط مورد نظر بررسی می‌شود.

۴- مرحله گسترش و انتشار: در این مرحله بعد از اطمینان از صحت عملکرد و تاثیر مثبت patchها در محیط، به گسترش و انتشار آنها روی سیستم‌ها پرداخته می‌شود.

۵- مرحله کنترل: در این مرحله تمام سیستم‌ها بعد از نصب Patch روی آنها تحت بررسی و کنترل قرار می‌گیرند تا از عدم وجود تاثیرات ناخواسته روی سیستم‌ها اطمینان حاصل شود.

۶- مرحله بازبینی: به عنوان یک فرآیند دائمی، لازم است که به طور مداوم Patchهای جدیدی که ارائه شده‌اند شناسایی شوند و آنهایی که مربوط به سیستم‌های مورد استفاده

هستند مشخص شوند. در صورت پیدا کردن Patch های مورد نیاز باید کل فرآیند مدیریت Patch ها را از ابتدا آغاز کرد.

نکته مهم: اکیدا" توصیه می‌شود که قبل از نصب و اجرای Patch ها روی سیستم‌ها از اطلاعات موجود، نسخه پشتیبان ((Backup تهیه شود.

تحلیل (Analyze): ابزار پایه‌ای مایکروسافت برای تحلیل امنیت

Microsoft Baseline Security Analyzer (MBSA)

MBSA یکی از ابزارهایی است که مایکروسافت برای بررسی و تحلیل سیستم‌ها طراحی کرده است و روی ویندوزهای NT4.0، 2000 و XP قابل اجرا است. به هنگام بودن یکی از نکات مهم در امن کردن سیستم‌ها به وسیله Patch های امنیتی است. شناسایی Patch های مورد نیاز سیستم امری اساسی است. MBSA این کار را با مراجعه به فایل XML که حاوی اطلاعاتی در مورد Patch های ارائه شده توسط مایکروسافت برای محصولاتش می‌باشد، انجام می‌دهد. MBSA عموماً از ابزار HFNetchk برای این منظور استفاده می‌کند.

فایل XML مورد نظر حاوی اطلاعاتی در مورد Hot Fix های ارائه شده برای هر کدام از محصولات مایکروسافت است. ضمناً حاوی نام، عنوان، اطلاعات مختصری در مورد Hot Fix ها، فایل‌های مربوطه، نسخه فایل‌ها، کلیدهای رجیستری که جهت نصب Hot Fix ها مورد استفاده قرار می‌گیرند و اطلاعاتی در مورد این که کدام Patch ها جایگزین Patch های دیگری می‌شوند، می‌باشد. وقتی این ابزار برای اولین بار اجرا می‌شوند باید این فایل XML را از سایت مایکروسافت دریافت کرد. هر بار که برنامه MBSA اجرا می‌شود تلاش می‌کند تا به اینترنت وصل شود تا این فایل را دریافت کند. اگر اتصال به اینترنت وجود نداشته باشد سعی می‌کند این فایل را روی سیستم محلی پیدا کند. برای این که MBSA مشخص کند چه Patch هایی روی یک کامپیوتر مشخص نصب شده‌اند سه آیتم را مورد بررسی قرار می‌دهد:

۱- کلید رجیستری که به وسیله Patch نصب شده است

۲- نسخه فایل

۳- Checksum مربوط به هر فایل که به وسیله Patch نصب شده است

به صورت پیش فرض MBSA جزئیات مربوط به فایل و کلیدهای رجیستری روی کامپیوتر و درون فایل‌های XML را با هم مقایسه می‌کند. اگر جزئیات مربوط به کلید رجیستری و فایل مورد

نظر روی کامپیوتر با اطلاعات روی فایل XML تفاوت داشته باشد، مشخص می‌شود که Patch‌های مربوطه روی سیستم نصب نشده‌اند و نتیجه این امر گزارش می‌شود.

مواردی که MBSA مورد بررسی قرار می‌دهد شامل وضعیت **Guest Account**، نوع سیستم فایل، فایل **Share** شده، اعضای گروه **Administrator** و غیره می‌باشد که در یک گزارش امنیتی نتایج این بررسی‌ها ثبت و اعلام می‌شود. تنها اعضای گروه **Domain Admin** و **Local Admin** اجازه استفاده از ابزار **MBSA** را دارند. این برنامه دارای تعدادی سوییچ در خط فرمان (**Command line**) است. البته واسط گرافیکی برای اجرای آسان‌تر این برنامه نیز وجود دارد.

پارامترهای **MBSA** به شرح جدول زیر است:

معرفی پارامترهای **MBSA**

کاربرد	Switch Name
Scan کامپیوتر با نام مشخص	/C <domain name><Computer name>
Scan کامپیوتر با IP مشخص	/i <xxx.xxx.xxx.xxx>
Scan محدوده‌ای از IP آدرس‌ها	/r <xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx>
Scan کامپیوترهای یک Domain	/d <domain name>
جלוگیری از چک کردن IIS	/N IIS
جلوگیری از چک کردن سیستم عامل	/N OS
جلوگیری از چک کردن Password ها	/N Password
جلوگیری از چک کردن SQL Server	/N SQL
جلوگیری از چک کردن به هنگام سازی‌های امنیتی (Security update)	/N Updates
چک کردن به هنگام سازی‌های امنیتی ((Security up date) از طریق یک سرور مشخص	/SUS <SUS Server>
متوقف کردن ثبت گزارش‌های مربوط به به‌هنگام سازی‌های امنیتی (Security update)	/S1
متوقف کردن ثبت گزارش‌های مربوط به به‌هنگام سازی‌های امنیتی (Security up date) و هشدار	/S2
Check sum های مربوط به فایل‌ها تست نمی‌شوند	/Nosum
تعیین الگوی نام فایل خروجی %Computer name% (%date%)	/O%domain%

کاربرد	Switch Name
فهرست کردن خطاهای مربوط به آخرین پیمایش (Scan)	/e
فهرست کردن تمام گزارش‌ها	/L
فهرست کردن گزارش آخرین پیمایش (Scan)	/LS
نمایش کلیات گزارش	/Lr <report name>
نمایش جزئیات گزارش	/Ld <report name>
Help	/?
عدم نمایش فرآیند	/qp
عدم نمایش لیست خطا	qe
عدم نمایش لیست گزارش‌ها	/qr

پیمایش Scan به روش HFNetchk تمام نتایج حاصل از بررسی سیستم از نظر به‌هنگام سازی‌های امنیتی (Security Up Date) مورد نیاز را در یک فایل متن، در محیط Command ویندوز نمایش می‌دهد.

MBSA Version 1.1 حاوی **Flag** با نام **/hf** می‌باشد که به پیمایش به سبک **HFNetchk** اشاره می‌کند و دارای پارامترهای **MBSA Version 1.1** است که بعد از **/hf** می‌توان از آن‌ها استفاده کرد. توجه: پارامترهایی که مربوط به سبک **MBSA** هستند و به آن‌ها اشاره شد قابل استفاده با **/hf** نیستند.

لیست پارامترهای خط فرمان مربوط به **HFNetchk**

کاربرد	نام پارامتر
پیمایش (Scan) کامپیوتر با تعیین نام Net BIOS آن. برای تعیین چند کامپیوتر می‌توان نام آن‌ها را با یک کاما از هم جداکرد.	-h <host name>
پیمایش (Scan) کامپیوترهایی که نام Net BIOS آن درون فایل متن مشخص شده است. در این فایل نام هر کامپیوتر باید در خط جداگانه نوشته شود و طول آن از ۲۵۶ کاراکتر بیشتر نباشد.	-fh <file name>
پیمایش (Scan) کامپیوتر با تعیین نام IP آن	-i <xxx.xxx.xxx.xxx>
پیمایش (Scan) کامپیوترهایی که IP آدرس آن‌ها درون فایل متن مشخص شده است. حداکثر تعداد آن‌ها می‌تواند ۲۵۶ باشد.	-fip <file name>
تعیین محدوده‌ای از IP آدرس‌ها	-I <xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx>

نام پارامتر	کاربرد
-d <domain name>	تعیین نام دامنه برای پیمایش (Scan)
-n	تعیین این که تمامی کامپیوترهای شبکه محلی باید پیمایش (Scan) شوند. تمام کامپیوترهای مربوط به تمام دامنه‌ها در شبکه مجاور هم باید پیمایش (Scan) شوند.
-sus <sus filename/sus server>	تعیین فایل متن SUS یا URL مربوط به مسیر دسترسی به فایل SUS. اگر فایل یا سرور تعیین نشوند از مقادیر ذخیره شده در رجیستری کامپیوتر محلی استفاده می‌شود.
-b	پیمایش (Scan) کامپیوتر تنها برای بررسی آن دسته از Up Date هایی که توسط خود مایکروسافت به عنوان Up Date های حیاتی مشخص شده‌اند.
-fq <file name>	مشخص کردن نام فایل که شامل Qnumber هایی است که روی خروجی متوقف شده اند Qnumber روی خط قراری گیرد. این پارامتر تنها آن‌هایی را که در فایل خروجی نمایش داده شده‌اند متوقف می‌کند.
-s	پیغام‌های هشدار و تذکر را متوقف می‌کند.
-no sum	عملیات تأیید Checksum مربوط به فایل‌های به هنگام سازی (Security up date) را اجرا نمی‌کند.
-sum	اجرای عملیات پیمایش (Scan) مربوط به Checksum برای پیمایش سیستم‌هایی با زبان غیرانگلیسی. از این پارامتر تنها در مواردی که فایل XML با Checksum هایی با زبان غیرانگلیسی داریم باید استفاده کرد.
-Z	برای تعیین عدم بررسی و کنترل رجیستری
-history	نمایش وضعیت patch های نصب شده
-V	نمایش علت کار نکردن یک تست در مورد پنهان سازی و یا علت دریافت پیغام‌های هشدار
-O	تعیین قالب برای فایل خروجی، دو گزینه زیر با این پارامتر قابل استفاده هستند: (tab), (warp)
-f (file name)	تعیین نام فایل که نتایج در آن ذخیره می‌شود
-t	نمایش تعداد تهدیداتی که برای اجرای عملیات پیمایش می‌شوند. این مقدار می‌تواند بین ۱ تا ۱۲۸ باشد. مقدار پیش فرض ۶۴ است.
-u <user name>	تعیین نام کاربری برای انجام عملیات پیمایش روی کامپیوتر محلی یا راه دور و یا گروهی از کامپیوترها. این پارامتر باید با پارامتر -p به کار برده شود.
-P <password>	برای تعیین کلمه عبور برای کاربری که عملیات پیمایش را اجرا می‌کند.

نام پارامتر	کاربرد
-X	تعیین محل فایل XML که حاوی اطلاعات مربوط به Patch های امنیتی است. اگر این پارامتر استفاده نشود این فایل از سایت مایکروسافت دریافت می‌شود.
-ver	تعیین می‌کند که آیا شما آخرین نسخه MBSA را اجرا می‌کنید یا خیر؟
-trace	جهت تهیه گزارش از روند اجرای کار و اشکالات به وجودآمده استفاده می‌شود و می‌تواند در شناسایی و رفع خطاها مفید باشد. این پارامتر باید در ابتدای دستور و همراه با سایر پارامترها به کار رود.

ابزار MBSA باید به صورت منظم و دائمی برای بررسی وضعیت Patch های مورد نیاز سیستم استفاده شود بنابراین می‌توان آن را برای اجرا در دوره‌های زمانی مشخص تنظیم کرد.

در این بخش به معرفی اسکریپت مدیریت Patch (Patch management Script) جهت مدیریت Patch ها و ابزار بررسی چند سرور برای شناسایی وضعیت Patch ها روی آن‌ها و ثبت نتایج در یک فایل گزارشی پرداخته شده است. این اسکریپت از MBSA جهت پیمایش سرورها استفاده می‌کند.

مراحل نصب و اجرای دستور MBSA Patch Check Cmd روی سرور Software Up Date Service (SUS)

۱- اجرای فایل Securityops.exe برای استخراج اسکریپت ها

۲- دریافت فایل MBSA

۳- اجرای فایل Mssecure.XML از سایت مایکروسافت. این فایل باید در دایرکتوری مربوط به MBSA قرار داده شود.

۴- ایجاد یک فایل متنی حاوی لیست کامپیوترهایی که می‌خواهیم پیمایش کنیم. این لیست حاوی نام NetBios کامپیوترها است.

۵- اجرای دستور زیر در خط فرمان (Command Prompt)

(نام فایل حاوی لیست کامپیوترها) MBSA Patch Check.Cmd Server List.tnt

۶- بررسی فایل گزارش مربوط به فایل Server List جهت شناسایی Patch های مورد نیاز.

استفاده از چندین لیست در شبکه‌هایی با مقیاس بزرگ که انواع مختلف سرورها در آن قرار دارند می‌تواند مفید باشد. چون ممکن است دسته‌ای از سرورها بیشتر از سایرین مورد تحلیل و بررسی قرارگیرند. بنابراین می‌توانیم هر دسته از سرورها را در لیست مجزا قرار داده و عملیات

پیمایش مربوط به هر کدام را برحسب نیاز زمان بندی کنیم. برای زمان بندی این عملیات می‌توان از ابزار **Task Scheduler** ویندوز استفاده کرد.

در مواردی که امکان استفاده از ابزار **MBSA** وجود ندارد می‌توان با بررسی کلید رجیستری زیر مشخص کرد که چه **Hot Fix**هایی نصب شده‌اند.

HKLM\Software\Microsoft\Windows NT\Current prison\Hot Fix

هر **Hot Fix** جدیدی که نصب می‌شود دارای یک **Qnumber** است که به مقاله مرتبط با آن **Hot**

Fix در **Knowledge Base** مایکروسافت اشاره می‌کند. البته این موضوع برای بعضی **Hot Fix**های قدیمی و **Hot Fix**های مربوط به برخی برنامه‌ها، صدق نمی‌کند.

ابزاری جهت جمع‌آوری این اطلاعات موجود است که شامل موارد زیر است:

Qfecheck.exe/v - ۱

این دستور شماره سرویس پک و نسخه **Hot Fix**های نصب شده روی سرورها را مشخص می‌کند. ضمناً در مورد **Patch**هایی که به طور صحیح و مناسب نصب نشده‌اند، نیز اطلاعاتی ارائه می‌دهد.

Hotfix.exe - ۲

این دستور شماره و نسخه **Hot Fix**های نصب شده روی سرور را نشان می‌دهد.

طراحی (Plan) عملیات

هر تهدید و نقطه آسیب پذیر روی سرور به معنای خطر مهم و قابل توجه نیست. در واقع باید بررسی کرد آیا این تهدیدات شامل محیط مورد نظر ما می‌باشد یا خیر.

برای مثال چنانچه سرویس **ftp** روی سرورهای شبکه فعال نشود، تهدیدات و نقاط آسیب پذیر مربوط به این سرویس برای شبکه‌ها خطر امنیتی ایجاد نمی‌کند. پاسخ به تهدیداتی که برای محیط شبکه‌ها خطری ایجاد نمی‌کنند باعث استفاده بدون فایده از منابع با ارزش شبکه می‌شود و روی ثبات و پایداری شبکه تاثیر منفی می‌گذارد. بنابراین شناسایی و بررسی دقیق آسیب پذیری‌ها و تهدیدات، مسئول امنیت را در شناسایی میزان اهمیت خطرانی که محیط شبکه را تهدید می‌کنند یاری می‌رساند و می‌توان اقدامات مناسب را جهت جلوگیری از این خطرات صورت داد.

نکته مهم این است که هنگام ایجاد یک طرح و برنامه جهت گسترش و نصب **Patch**های جدید روی سیستم باید طرح و برنامه‌ای جهت بازگشت به حالت اولیه (قبل از نصب **Patch** ها) ایجاد کرد.

دسته‌بندی Patch ها

هر Patch جدیدی که ارائه می‌شود باید درجه اهمیت آن برای محیط مورد نظر تعیین گردد تا مشخص شود چه زمانی برای نصب و اجرای آن patch مناسب است. مایکروسافت برای هر نوع آسیب پذیری یک سطح خاص تعیین کرده که شامل موارد زیر است:

نوع کامپیوتر	Rating Level		
	بحرانی (Critical))	متوسط (Moderate))	پایین (Low))
Internet Servers	حملات DoS، کنترل کامل روی سرور، تغییر وب سایت	تنظیمات غیرمعمول، تاثیرات کوتاه و زودگذر	تاثیرات محدود مانند افشاء اسکریپت ها
Internal Servers	افشاء داده‌ها، تغییر در داده‌ها، ممیزی دشوار، ترفیع حقوق دسترسی کاربران راه دور	افشاء و تغییر داده‌های فایل ممیزی یا حملات DoS، افزایش حقوق دسترسی کاربران محلی	سرقت داده‌های بدون هدف و پراکنده یا ایجاد تغییر در آن‌ها، حملات محدود DoS، حملات به وب سایت
Client Systems	اجرای کدها بدون دخالت کاربر، ارتقاء حقوق کاربر راه دور	ارتقاء حقوق کاربر محلی، افشاء داده‌های بی هدف یا حملات DoS	سرقت یا تغییر داده‌های پراکنده یا محدود شده، حملات به وب سایت

دسته‌بندی تهدیدات و نقاط آسیب پذیر مطابق با تاثیراتی است که در صورت وقوع این تهدیدات احتمالاً "رخ خواهند داد. از این دسته‌بندی جهت گروه بندی Patch ها می‌توان استفاده کرد.

البته این دسته‌بندی از سوی مایکروسافت برآوردی کلی از تهدیدات بالقوه امنیتی محسوب می‌شود که میلیون‌ها کاربر و مشتری در سرتاسر جهان تحت تاثیر آن‌ها قرار گرفته‌اند. دسته‌بندی کامل و دقیق براساس تجربه قبلی و داوری معقول امکان پذیر است. به همین علت ممکن است این دسته‌بندی‌ها پیش گویی کننده دقیقی در مورد تاثیرات این تهدیدات برای محیط مورد نظر نباشند. نهایتاً باید دسته‌بندی Patch ها را مطابق با شرایط محیطی هر شبکه انجام داد.

آزمایش (Testing the Patches)

Patch‌هایی که برای نرم‌افزارها ارائه می‌شوند ممکن است در هر محیطی درست عمل نکنند. بنابراین به‌طور ایده‌آل باید تمام Patch‌ها قبل از نصب آزمایش شوند. البته بسیاری از Patch‌های امنیتی باید فوراً جهت رفع یکسری مشکلات جدی و خطرناک نصب شوند. در بسیاری موارد باید روال تست Patch‌ها را به عنوان توافقی بین نیاز به حل مشکلات امنیتی و نیاز به اطمینان خاطر از استحکام و صحت عملکرد Patch‌ها در محیط شبکه در نظر گرفت. میزان عملیات تست و آزمایش بستگی به چگونگی دسته‌بندی Patch‌ها دارد. با استفاده از دسته‌بندی مایکروسافت جدول زیر پائین ترین سطح از عملیات تست و آزمایش را که باید برای هر نوع Patch اجرا کرد، نشان می‌دهد. برای اطمینان از صحت عملکرد Patch‌ها و این که هر یک از سرویس‌های شبکه بدون مشکل به سرویس دهی خود ادامه می‌دهند، تست‌هایی انجام می‌شود. مانند بررسی اتصال Client‌ها به سرویس‌های شبکه جهت بررسی وضعیت سرویس دهی به آن‌ها و اجرای سایر تست‌ها برای تأیید و اطمینان از صحت عملکرد سرورها.

نوع Patch	نوع عملیات تست و آزمایش
Patch‌های مهم و حیاتی	ارزیابی Patch‌ها - نصب Patch‌ها در محیط آزمایشی، ارزیابی عملیات‌های سرور (به صورت کامل) - ارزیابی عملکرد برنامه‌ها - بررسی و کنترل روال Uninstall
Patch‌هایی با درجه اهمیت متوسط	ارزیابی Patch‌ها - نصب Patch در محیط آزمایشی - ارزیابی عملیات‌های سرور (به صورت کامل) بررسی و کنترل روال Uninstall
Patch‌های با درجه اهمیت پایین	ارزیابی Patch‌ها - ارزیابی عملیات‌های سرور (به صورت محدود)

به عنوان بخشی از روال مدیریت ریسک باید مشخص کرد چطور هر مرحله به طور کامل اجرا خواهد شد. اگر از برخی مراحل تعیین شده برحسب ضرورت صرف نظر شود، باید در آزمایشگاه Patch، آن‌ها را به طور کامل ادامه داد تا مشکلات بالقوه قبل رخ دادن روی سیستم‌ها، شناسایی شوند.

کلیه عملیات تست باید روی سرورهایی که تا حد امکان از نظر عملکرد شبیه سرورهای اصلی شبکه هستند انجام شوند.

ارزیابی (Assessing the patch)

حداقل مراحل که باید برای ارزیابی Patchها انجام داد شامل موارد زیر است:

۱- شناسایی مسئول نصب Patch: برای تمام Patchها باید متصدی آن شناسایی شود تا مشخص شود چه کسی مسئول ارزیابی Patch می‌باشد.

۲- بررسی تمام اسناد مربوط به Patch: قبل از اجرای هر سرویس پک، Hot Fix یا Security Patch، تمام اسناد مربوط به آن باید مطالعه و ارزیابی شود. فرآیند بررسی اسناد مربوط به Patchها احتمال این که کاربر نکات حیاتی و مهم رادر زمان ارزیابی Patch فراموش کند، کاهش می‌دهد.

۳- بررسی گروه بندی Patchها: بعد از ارزیابی Patch ممکن است نیاز باشد که گروه آن تغییر یابد. این مسأله روی سایر جنبه‌های آزمایش تاثیر می‌گذارد.

هنگامی که اسناد مربوط به Patchها مورد بررسی قرار می‌گیرد باید به دنبال پاسخ‌هایی برای سئوالات زیر بود:

۱- آیا Patch مورد نظر مناسب است و می‌تواند مشکل امنیتی را حل کند.

۲- آیا نیازمندی‌هایی مرتبط با به روز رسانی ها ((Update وجود دارد. برای مثال ممکن است لازم باشد یکسری ویژگی‌ها و خصوصیات ویژه برای موثر بودن عملیات به روز رسانی ((Update، فعال یا غیرفعال شوند.

۳- آیا لازم است قبل از اجرای عملیات به روز رسانی کارهای دیگری انجام شود.

علاوه بر بررسی اسناد مربوط به Patchها باید به صورت مداوم وب سایت مربوط به پشتیبانی محصولات شرکت مایکروسافت را بررسی کرد تا بتوان اطلاعات جدید مربوط به Patchها را دریافت کرد.

نصب (Installation)

برای نصب Patch ها باید از درستی نصب و عملکرد آن‌ها مطمئن شد. آیا یک Patch نیاز به Restart کردن سیستم دارد یا خیر، چه مقدار فضا برای آن لازم است، چه گزینه‌هایی در دسترس هستند و غیره. علاوه بر این باید اطلاعات مربوط به جنبه‌های مثبت و منفی نصب Patch ها را بررسی و ارزیابی کرد.

۱- عملکرد سرورها

وقتی یک Patch نصب می‌شود باید مطمئن شد که سرور به صورت نرمال به فعالیت خود ادامه می‌دهد. ایده مناسب، بررسی فهرست رویدادها برای نتایج غیرمنتظره است. تست عملکرد سرورها یکی از نکات ضروری بعد از نصب Patch ها است. باید مشخص کرد مقدار ریسک قابل تحمل در یک سرور ویژه برای مجموعه‌ای از آسیب‌پذیری‌ها چقدر است و چه مدت زمان باید اجازه داد تا سرور به فعالیت خود ادامه دهد، تا معلوم شود همه چیز به صورت طبیعی اجرا می‌شود.

۲- عملکرد برنامه‌ها

به عنوان بخشی از عملیات تست Patch ها، آزمایش آن‌ها با همراه با هر برنامه‌ای که روی سرور نصب شده است، برای اطمینان از صحت عملکرد برنامه‌ها ضروری است.

۳- Uninstall برنامه‌ها

در مواردی ممکن است با وجود آزمایش Patch ها بعد از نصب آن‌ها مشکلاتی به وجود آید که نیاز به پاک کردن Patch از روی سیستم باشد. بعد از اتمام عملیات Uninstall باید سیستم‌ها را از جهت عملکرد صحیح مورد بررسی دوباره قرارداد.

۴- ایجاد طرح بازگشت

حتی در مواردی که عملیات تست بدون هیچ مشکلی به طور کامل اجرا شود، احتمال دارد مشکلاتی بعد از نصب Patch روی سیستم‌ها به وجود آید. برای این منظور باید عملیاتی جهت بازگشت سیستم به حالت قبل از نصب Patch طراحی و اجرا کرد. برای مثال می‌توان سرور پشتیبان تهیه کرد تا در صورت بروز مشکل بتوان سریعاً نسخه پشتیبان را بازیابی کرد. این عملیات بازگشت قبل از اجرا باید مورد تست و آزمایش قرار گیرد.

انتشار و به‌کارگیری (Deploy the Patches)

بعد از تست و آزمایش و اطمینان از صحت عملکرد Patch ها نوبت به انتشار Patch ها روی تمام سیستم‌های شبکه می‌رسد. به چند روش می‌توان عملیات انتشار Patch ها را انجام داد:

۱- انتشار دستی

۲- پیکربندی گروهی (Group Policy)

۳- اسکریپت‌ها

۱- انتشار به روش دستی

یکی از روش‌های عمومی، نصب Hot Fix ها به صورت دستی است. با اجرای فایل اجرایی مربوط به Hot Fix به سادگی می‌توان آن را نصب کرد. نام اکثر Hot Fix ها اطلاعات مهمی درباره آن‌ها ارائه می‌دهد. برای مثال نام یک Hot Fix به صورت زیر است:

Q292435-W2K-SP3-X86-en.exe

در این مورد:

شماره مقاله مربوط به Hot Fix در سایت مایکروسافت است : Q292435

این Hot Fix برای ویندوز 2000 قابل استفاده است : W2K

شماره Service Pack ای که شامل این Hot Fix است : SP3

معماری پردازنده که این Hot Fix با آن سازگار است : X86

زبانی که Hot Fix تحت آن ارائه شده است : En

توجه: Hot Fix هایی که نام فایل آن‌ها به صورت Qxxxxxx.exe است برای یک سری برنامه‌های خاص مثل Internet Explorer به کار می‌روند.

Hot Fix ها از تعدادی پارامتر در محیط خط فرمان پشتیبانی می‌کنند که به وسیله آن‌ها می‌توان کنترل بهتری روی فرآیند نصب آن‌ها داشت.

جدول پارامترهای Hot Fix ها

نام پارامتر	عملکرد
-y	اجرای عملیات Uninstall
-f	بستن برنامه‌ها در هنگام خاموش شدن سیستم
-n	جلوگیری از ایجاد دایرکتوری Uninstall
-z	جلوگیری از Restart شدن سیستم بعد از کامل شدن عملیات نصب Hot Fix
-q	موجود بودن واسطه کاری

نام پارامتر	عملکرد
-m	نصب اتوماتیک و بدون دخالت کاربر
-I	نمایش لیست Hot Fix های نصب شده

توجه: Hot Fix هایی که نام آن‌ها به صورت Qxxxxxx.exe است از این پارامترها پشتیبانی نمی‌کنند. اگر از اسکریپت‌ها جهت نصب چند Hot Fix استفاده شود بعد از نصب هر کدام سیستم Restart می‌شود. علت این است که فایل‌هایی که در حال استفاده هستند یا قفل شده اند و یا قابل جایگزینی نیستند بنابراین تمام آن‌ها در یک صف قرار داده می‌شوند تا بعد از Restart سیستم جایگزین شوند. QChain ابزاری جهت نصب چند Hot Fix تنها با یک بار Restart کردن سیستم است.

برای استفاده از این ابزار Hot Fix را با پارامتر z- اجرا می‌کنیم تا بعد از نصب Hot Fix سیستم Restart نشود سپس دستور Qchain.exe را اجرا کرده و سیستم را Restart می‌کنیم. اگر اجزای اضافی مانند DNS بعد از نصب و اجرای Service Pack و Patch ها اضافه شوند، لازم است که نصب Service Pack و Patch ها تکرار شود تا اجزای جدید هم تحت تاثیر عملکرد Patch ها قرار گیرند.

۲- انتشار با استفاده از پیکربندی گروهی (Group Policy)

ویندوز ۲۰۰۰ دارای قابلیت انتشار نرم‌افزار با استفاده از تنظیمات گروهی است. Patch ها به صورت طبیعی در قالب بسته‌های نصب از طریق ویندوز (فایل‌های MSI) عرضه نمی‌شوند ولی می‌توان یک فایل Zap برای این منظور تهیه کرد. این فایل متنی حاوی اطلاعاتی درمورد چگونگی نصب یک برنامه، مشخصات برنامه و فایل اجرایی برنامه است. فایل‌های Zap تنها قابل ارجاع دادن به کاربران هستند. یعنی وقتی Hot Fix ها از طریق تنظیمات گروهی انتشار پیدا می‌کنند باید حتماً با Account مربوط به کاربری که فایل Zap به وی ارجاع شده است به سیستم وارد شد تا عملیات نصب Hot Fix انجام گیرد.

۳- انتشار از طریق اسکریپت‌ها

ممکن است عمل انتشار به وسیله اسکریپت‌های Visual Basic یا فایل‌های Batch صورت گیرد. این موضوع می‌تواند شامل اسکریپت‌هایی باشد که در موقع آغاز به کار ویندوز یا ورود کاربر، سیستم را از نظر وضعیت Patch های نصب شده مورد بررسی و ارزیابی قرار داده و Patch های مورد نیاز را روی سیستم نصب می‌کنند.

کنترل و نظارت (Monitoring)

بعد از نصب Patchها باید سرورها را به طور مداوم تحت کنترل و نظارت قرار داد تا بتوان از بروز مشکلات احتمالی روی آنها آگاهی پیدا کرد. بعد از بروز مشکل باید بررسی کرد که آیا این مشکل به دلیل نصب Patchها رخ داده است یا عمل دیگری باعث آن شده است. یک نکته مهم در کنترل و نظارت مداوم، اطمینان از به هنگام بودن سرورهای جدیدی است که به شبکه اضافه می‌شوند.

مرور و بازبینی (Reviewing)

تنها راه اطمینان از صحت عملکرد یک فرآیند، بازبینی و مرور آن است. این مسأله در مورد فرآیند مدیریت Patchها نیز صدق می‌کند. طی این مرحله علاوه بر مرور و بازبینی عملکرد سرورها بعد از نصب Patchها، باید عملیات آنالیز و بررسی سیستم‌ها از نظر تغییرات مورد نیاز صورت پذیرد تا در صورت نیاز، فرآیند مدیریت Patch مجدداً آغاز شود.

سرور مدیریت سیستم‌های مایکروسافت

Microsoft Systems Management Server (SMS)

اگر سرور مدیریت سیستم ((SMS در محیط شبکه مورد استفاده قرار می‌گیرد بسیاری از مراحل ذکر شده از طریق این سرور قابل اجرا است. این سرور کمک می‌کند تا کامپیوترهایی که نیاز به Patchهای امنیتی دارند شناسایی شوند و عملیات نصب و اجرا روی آنها صورت گیرد. در این صورت تمام کامپیوترهایی که سرویس گیرنده SMS روی آنها نصب شده است می‌توانند از امکانات این سرور استفاده کنند. در این مورد لازم است فرد یا افرادی با آگاهی از نحوه ایجاد بسته‌های SMS جهت به روز رسانی کامپیوترهای شبکه از طریق سرور SMS مدیریت و کنترل این سرور را برعهده بگیرند.

ابزار غیر مایکروسافتی Third Party Tools

تعدادی ابزار غیر مایکروسافتی برای مدیریت Patchها در دسترس می‌باشد که دارای قابلیت‌های اضافی نسبت به ابزار مایکروسافتی هستند، مانند دریافت گزارش وضعیت نصب Patchها، گروه بندی کامپیوترها براساس نیازهای امنیتی و به روز رسانی یکسان، استفاده از محیط‌های گرافیکی با قابلیت‌های فراوان و سایر موارد. تعدادی از این ابزارها شامل موارد زیر است:

- Polaris Group Hot Fix/Service Pack Utility
- Shavlik HF Netchkpro
- Bind View Security Advisor
- Pedestal Software's Security Expressions

ضمیمه دو:

کنترل دسترسی سیستم عامل (هسته LINUX)

امنیت Kernel

الف – استفاده از سیستم شناسایی ورودهای غیرمجاز در سیستم عامل لینوکس (LIDS)

دسترسی به سیستم با استفاده از حقوق کاربری **root** (مدیر سیستم) می‌تواند منشاء خطرهای زیادی باشد و مقابله با آسیب‌هایی که از این طریق به سیستم وارد می‌شود بسیار مشکل و زمانبر خواهد بود. در سیستم عامل لینوکس چند زیر سیستم وجود دارد که به صورت پیش فرض حفاظت نشده‌اند. این زیر سیستم‌ها عبارت‌اند از:

- فایل‌های سیستمی: این فایل‌ها بسیار مهم و حیاتی هستند. مثل فایل **/bin/login** که اگر هکر بتواند به این فایل دسترسی پیدا کند می‌تواند در برنامه ورود به سیستم تغییراتی ایجاد نماید. بسیاری از فایل‌های سیستمی نباید تغییر کنند، بنابراین باید امنیت آن‌ها کاملاً حفظ شود.
- فرآیندهای در حال اجرا: بسیاری از فرآیندها با حقوق **root** اجرا می‌شوند، بنابراین در صورت بروز مشکلی مانند سرریز بافر، نفوذ کننده دسترسی کاملی به سیستم پیدا می‌کند.

LIDS امنیت سیستم را به وسیله کاهش قدرت کاربر **root** افزایش می‌دهد. ضمناً **LIDS** یک مدل امنیتی سطح پایین را به منظور رسیدن به اهداف زیر در **Kernel** اجرا می‌کند:

- حفاظت امنیتی
 - تشخیص حوادث و رویدادها
 - قابلیت و توانایی پاسخ دهی به حوادث
- برای مثال **LIDS** می‌تواند موارد امنیتی و حفاظتی زیر را ارائه دهد:
- حفاظت از فایل‌ها و دایرکتوری‌های مهم در برابر دسترسی‌های غیرمجاز بدون توجه به نوع سیستم مدیریت فایل موجود در هارد دیسک.
 - حفاظت از فایل‌های مشخص برای جلوگیری از تغییر آن‌ها توسط کاربر **root** تا فردی با دسترسی به حقوق **root** نتواند به سیستم آسیب وارد کند.

- حفاظت از فرآیندها برای جلوگیری از خاتمه دادن به آن فرآیندها توسط افرادی با حقوق کاربر **root** (این موضوع قابلیت‌ها و توانایی‌های کاربر **root** را کاهش می‌دهد).
- جلوگیری از دسترسی برنامه‌های غیرمجاز به عملیات ورودی و خروجی ناتمام و ناقص
- حفاظت از رکورد اصلی بوت هارد دیسک (**MBR**)

همچنین **LIDS** می‌تواند پویا و بررسی پورت‌های سیستم را تشخیص دهد و مدیر سیستم را از وقوع حوادث مطلع کند. علاوه بر تهیه گزارش از رویدادهای امنیتی و نفوذهای غیرمجاز و ارسال آن‌ها برای مدیر سیستم، **LIDS** می‌تواند نشست ارتباطی فرد مزاحم با سیستم را نیز قطع کند. **LIDS** به عنوان یک **Patch** باید روی سیستم نصب و کامپایل شود و به صورت مناسب پیکر بندی گردد. فایل‌هایی که جهت پیکربندی و تنظیم **LIDS** استفاده می‌شوند عبارت‌اند از:

/etc/lids/lids.conf	این فایل حاوی اطلاعات مربوط به لیست‌های کنترل دسترسی است.
/etc/lids/lids.cap	این فایل شامل قواعد مربوط به قابلیت‌های سیستم عامل است.
/etc/lids/lids.pw	این فایل شامل کلمات عبور رمزگذاری برای سیستم LIDS است.
/etc/lids/lids.net	این فایل شامل تنظیمات e-mail برای مطلع کردن مدیر سیستم از رویدادهای امنیتی است.

یکی از قابلیت‌های مهم **LIDS** استفاده از امکانات سیستم جهت کاهش قدرت کاربر **root** می‌باشد. این قابلیت‌ها در فایل **lids.cap** آمده و قابل تغییر است و می‌توان آن‌ها را فعال یا غیرفعال کرد.

ب- استفاده از libsafe برای حفاظت از پشته‌های (Stack) برنامه‌ها

فرآیند ایجاد پشته‌ها خطر سرریز بافر را به همراه دارد و می‌تواند ریسک‌های امنیتی زیادی برای سیستم ایجاد کند. به وسیله برنامه **libsafe** (کتابخانه‌های با قابلیت بارگذاری خودکار در **Kernel**) می‌توان این مشکل را برطرف کرد. ویژگی‌های این برنامه عبارت است از:

- **libsafe** با برنامه‌های باینری موجود کار می‌کند.
- **libsafe** می‌تواند در سطح سیستم اجرا شده و برای کاربر کاملاً شفاف و روشن باقی بماند.
- **libsafe** به تنظیماتی مانند تغییر در سیستم عامل، دسترسی به کد منبع برنامه‌های ناتمام و کامپایل مجدد نیاز ندارد.
- **libsafe** نسخه‌ای جانشین برای انجام فعالیتی متناظر با عملیات اصلی (**Task**) ایجاد می‌کند ولی این عمل به طریقی صورت می‌گیرد که شامل محافظت در مقابل تمام سرریز بافرها درون پشته فعلی می‌باشد. این روش مانع از دخالت نفوذگران در اجرای برنامه‌ها می‌شود.

• **libsaf** می‌تواند بسیاری از حملات شناخته شده را شناسایی کرده و مانع از بروز آن‌ها شود. البته کاربرد اصلی آن ممانعت از حملات ناشناخته است که آن را با کارایی مناسب انجام می‌دهد. بنابراین در صورتی که برنامه‌ای ناقص باشد استفاده از **libsaf** راه حلی مناسب برای جلوگیری از بروز حوادثی مانند سرریز بافر و حملات از این نوع می‌باشد. برای استفاده از برنامه **libsaf** می‌توان کد منبع آن را از اینترنت پیاده‌سازی کرد و بعد از کامپایل آن را نصب و اجرا نمود.

کلید استفاده بهینه و موثر از **libsaf** تخمین حد بالای اندازه بافر می‌باشد. این تخمین در زمان کامپایل امکان پذیر نیست و بهتر است برای دست یابی به تخمینی مناسب‌تر بعد از شروع توابعی که از بافر استفاده می‌کنند سائز بافر را محاسبه کرد. این روش میتواند در تعیین حداکثر سائز بافر به وسیله جلوگیری از توسعه پشته فعلی موثر باشد و با فعال کردن نسخه‌های جانشین برای توابع مختلف مدت زمان دسترسی آن‌ها به بافر را بدون تجاوز از حد مجاز محدود کرد.

امنیت فایل‌ها و سیستم فایل

الف- مدیریت فایل‌ها، دایرکتوری‌ها و مجوزها

فایل‌ها عنصر اصلی عملیات پردازشی می‌باشند و حفاظت و امنیت آن‌ها از اهمیت بسیار زیادی برخوردار است. اگر فردی غیر مجاز فایلی را ایجاد و یا حذف کند و یا تغییری در آن ایجاد نماید و یا یک کاربر داخلی ناراضی و یا نفوذگری از خارج سازمان بتواند به فایلی خاص دسترسی پیدا کند، احتمالاً مشکلات امنیتی به وجود خواهد آمد. بنابراین آگاهی کامل از مجوز فایل‌ها برای مدیران سیستم و سایر کاربران بسیار با اهمیت است.

در سیستم عامل لینوکس هر فایل مربوط به یک کاربر و یک گروه است. با استفاده از دستور زیر می‌توان وضعیت مجوز فایل‌ها، کاربر و گروه مالک آن فایل‌ها و سایر اطلاعات را به دست آورد.

#ls - L

دستور ورودی

خروجی

```
-rw-rw-r-- 1 root Root 512 Feb 6 21:10 file-name/dir-name
```

جدول مشخصات فایل

نوع اطلاعات	خروجی دستور Ls
مجوز دسترسی فایل یا دایرکتوری	-rw-rw-r--
تعداد ارتباطات با فایل یا دایرکتوری	1
کاربر مالک فایل یا دایرکتوری	root
گروه مالک فایل یا دایرکتوری	Root
سایز فایل یا دایرکتوری	512
تاریخ آخرین تغییر روی فایل یا دایرکتوری	Feb 6
زمان آخرین تغییر روی فایل یا دایرکتوری	21:10
نام فایل یا دایرکتوری	File-name/dir-name

مجوزهای دسترسی به فایل سه نوع است:

- ۱- مجوز خواندن: (r)
- ۲- مجوز نوشتن و تغییر در فایل: (w)
- ۳- مجوز اجرای فایل: (x)
- ۴- تنظیم set-UID یا set-GID : (S)

توجه: با تنظیم مجوز S برای فایل اجرایی، آن فایل با حقوق کاربر یا گروه مالکش اجرا می‌شود. برای هر فایل نه بیت برای تعیین مجوزهای دسترسی در نظر گرفته شده است که سه بیت اول برای تعیین مجوزهای مالک فایل، سه بیت دوم برای تعیین مجوزهای گروه مالک و سه بیت آخر برای سایر کاربران است.

توجه: بیت اول برای تعیین فایل یا دایرکتوری است.

یک کاربر عادی نمی‌تواند مالکیت یک فایل را به شخص دیگری واگذار کند. این مسأله از نظر امنیتی بسیار حائز اهمیت است. تنها مالک فایل می‌تواند مالکیت آن را به شخص دیگری واگذار نماید. به وسیله دستورات **chown** و **chgrp** می‌توان مالک و گروه مالک فایل را تغییر داد.

```
# chown newuser file or directory
# chgrp newgroup file or directory
```

برای تغییر گروه مالک باید کاربر عضو گروه جدید نیز باشد.

به وسیله دستور **chmod** می‌توان مجوزهای دسترسی فایل‌ها را تغییر داد. این کار به دو صورت انجام می‌شود:

۱- در روش اول کاربر مالک فایل با استفاده از اعدادی که برای هر یک از انواع مجوزها در نظر گرفته شده مجوزهای دسترسی به فایل را تعیین می‌کند. (خواندن ۴، نوشتن ۲، اجرا ۱)

مثال: (700 معادل مجوز **rw-r--r--** است).

```
# chmod 700 test.txt
```

۲- در روش دوم مالک فایل از فرم زیر برای تعیین مجوزها استفاده می‌کند:

- u (کاربر مالک)
- g (گروه مالک)
- o (سایر کاربران)
- a (تمام کاربران)

```
# chmod a+rx,u+w test.txt
```

مثال:

اعطای مجوز تغییر فایل به مالک و مجوز خواندن و اجرا به همه کاربران (نکته: / از علائم + و - برای اعطا و یا عدم اعطای مجوزها به کاربران استفاده می‌شود).

ب- کنترل سازگاری و ثبات کاربران و گروه‌ها

مدیران سیستم زمان زیادی را صرف مدیریت کاربران و گروه‌ها می‌کنند. از نظر امنیتی توصیه می‌شود که فایل‌های `/etc/group` و `/etc/passwd` مستقیماً مورد اصلاح و ویرایش قرار نگیرند بلکه برای مدیریت کاربران و گروه‌ها و کلمات عبور آن‌ها از دستوراتی مانند `usermod`, `useradd`, `groupdel`, `groupadd` و `groupmod` استفاده شود.

نکات امنیتی در مورد پارتیشن `/usr`

این پارتیشن (یا دایرکتوری) به صورت پیش فرض برای نصب برنامه‌ها روی سیستم مورد استفاده قرار می‌گیرد و از اهمیت بسیار زیادی برخوردار است. توصیه‌های امنیتی که در مورد این پارتیشن وجود دارد عبارت‌اند از:

- ۱- اگر سیستم از طریق اینترنت قابل دسترسی است اکیداً توصیه می‌شود مجوز دسترسی به این پارتیشن به صورت `read-only` تنظیم شود.
- ۲- ابتدا باید تمام برنامه‌های مورد نیاز را روی سیستم نصب و پیکربندی نمود و پس از تست و آزمایش صحت عملکرد آن‌ها، مجوز دسترسی `read-only` (فقط خواندنی) را روی پارتیشن `/usr` تنظیم کرد.
- ۳- برای تعیین این مجوز باید فایل `/etc/fstab` را ویرایش نمود.

تنظیم مجوزهای پیش فرض برای کل سیستم با استفاده از `umask`

وقتی کاربری فایل یا دایرکتوری جدید ایجاد می‌کند، لینوکس از مقداری پیش فرض برای تعیین مجوز آن‌ها استفاده می‌نماید. این مقدار پیش فرض را با دستور `umask` می‌توان تعیین کرد.

(مجوز پیش فرض 775 خواهد بود)
umask 002

برای تعیین مجوز، مقدار تعیین شده در دستور `umask` از عدد 777 کم می‌شود.

برای اعمال مجوز پیش فرض به تمام کاربران، این دستور به فایل `/etc/profile` اضافه می‌شود.

استفاده از ویژگی‌های امنیتی سیستم فایل ext2

سیستم فایل ext2 دارای ویژگی‌های امنیتی است که در حفظ امنیت فایل‌ها موثر است. توضیحات مربوط در جدول بعدی آمده است.

ویژگی‌های امنیتی سیستم فایل ext2

ویژگی	توضیح
A	با تنظیم این ویژگی زمان دسترسی به فایل به هنگام نمی‌شود. این امر می‌تواند برای کامپیوترهایی که مشکل مصرف زیاد انرژی دارند مفید باشد. زیرا از یک سری عملیات ورود و خروج غیرضروری جلوگیری می‌کند.
S	با تنظیم این ویژگی فایل با حافظه فیزیکی همزمان می‌شود. این مسئله در درازمدت سطح بالایی از جامعیت داده‌ها را فراهم می‌نماید.
a	با این تنظیم، فایل‌ها می‌توانند درون یک دایرکتوری خاص ایجاد شده و یا تغییر کنند. اما نمی‌توان آن‌ها را حذف نمود.
i	با این تنظیم فایل‌ها نمی‌توانند تغییر کنند. در یک دایرکتوری خاص فایل‌ها می‌توانند تغییر کنند ولی فایل‌های جدید نمی‌توانند ایجاد و یا حذف شوند.
d	برنامه‌های نامناسب فایل را نادیده می‌گیرند.
c	تنظیم این ویژگی باعث می‌شود که هر درخواست برای نوشتن روی فایل فشرده شود و درخواست خواندن فایل به صورت اتوماتیک از حالت فشرده خارج شود (این ویژگی در Kernel 2.4 و 2.2 در دسترس نیست).
s	وقتی فایل با این ویژگی حذف می‌شود داده‌های فایل با مقادیر صفر بازنویسی می‌شوند. (این ویژگی در Kernel 2.4 و 2.2 در دسترس نیست)
U	وقتی فایل با این ویژگی حذف شود امکان بازیابی آن وجود دارد. (این ویژگی در Kernel 2.4 و 2.2 در دسترس نیست)

برای تنظیم این ویژگی‌ها روی فایل‌ها از دستور **chattr** استفاده می‌شود:

#chattr + I filename برای اضافه کردن ویژگی

#chattr - I filename برای حذف ویژگی

استفاده از کنترل کننده جامعیت فایل‌ها

ابزار کنترل کننده جامعیت فایل‌ها برنامه‌هایی هستند که اجازه می‌دهند مقادیری شبیه **checksum** برای عملیات **hashing** استفاده شوند این مقادیر در محلی امن و حفاظت شده مانند **CD** نگهداری می‌شوند. با استفاده از این ابزار می‌توان جامعیت و صحت فایل‌ها را در مقایسه با بانک اطلاعاتی **checksum** بررسی کرد تا مشخص شود که آیا فایل تغییر کرده است یا خیر. اگر **checksum** فعلی با **checksum** قبلی یکسان باشد، مشخص می‌شود که فایل تغییر نکرده است. در غیر این صورت ممکن است فایل ویروسی شده باشد یا به وسیله برنامه‌های اسب تروا در آن‌ها تغییر ایجاد شده باشد.

Tripwire از جمله این ابزار است که بانک اطلاعاتی **checksum**‌ها را برای فایل‌ها و دایرکتوری‌ها ایجاد می‌کند و آن‌ها را درون یک فایل قرار می‌دهد و یا **checksum**‌های جدید را برای فایل‌ها و دایرکتوری‌ها محاسبه کرده و با اطلاعات درون بانک اطلاعاتی مقایسه می‌کند. در صورت مشاهده هرگونه ناسازگاری و ناهماهنگی مشخص می‌شود که کدامیک از فایل‌ها یا دایرکتوری‌ها تغییر کرده‌اند.

نکته مهم در این زمینه حفظ امنیت بانک اطلاعاتی است. در مواردی که مدیران سیستم تعداد کمی از فایل‌ها را به وسیله این ابزار مورد کنترل و بررسی قرار می‌دهند، اغلب این بانک اطلاعاتی درون یک دیسک فلاپی ذخیره می‌شود. در صورتی که **BIOS** اجازه دهد درایو فلاپی به عنوان یک درایو فقط خواندنی (**read-only**) تنظیم می‌شود تا از نوشتن یا تغییر روی فلاپی ممانعت شود. راه حل دیگر استفاده از **CD** است که امکان تغییر بانک اطلاعاتی روی آن وجود ندارد.

ابزار **Tripwire** در مواردی که تعداد زیادی از کاربردهای سیستم لینوکس بخواهد تحت کنترل جامعیت داده‌ها قرار گیرند مفید و موثر نیست و به جای آن از ابزار دیگری به نام **AIDE** استفاده می‌شود. این ابزار در محیط شبکه قابل استفاده است و کارایی و ویژگی‌های بیشتری نسبت به ابزار **Tripwire** دارد.

برای استفاده از **AIDE** و کنترل اتوماتیک جامعیت داده در شبکه لینوکس نیاز به ابزاری بر پایه زبان برنامه نویسی **Perl** به نام **ICU** است. نرم‌افزار سرویس گیرنده و سرویس دهنده **ICU** باید نصب و تنظیم شود. ضمناً نصب **Openssh** نیز لازم و ضروری است. بعد از نصب **AIDE** روی سرور **ICU** می‌توان عملیات بررسی و کنترل جامعیت داده‌ها را روی تمام سرویس گیرنده‌های **ICU** در سطح شبکه اجرا کرد.

مفهوم حفاظت امنیتی از سیستم‌ها چیزی فراتر از جلوگیری از نفوذ افراد خرابه‌کار به سیستم‌ها است. راه حل امنیتی مناسب دیگر تهیه نسخه‌های پشتیبان به صورت دوره‌ای و زمان بندی شده است. این عملیات می‌تواند به صورت روزانه برای تهیه نسخه‌های پشتیبان افزایشی صورت گیرد و در انتهای هفته نیز یک پشتیبان کامل از سیستم و اطلاعات آن تهیه شود. بهتر است نسخه‌های پشتیبان روی رسانه‌های ذخیره‌سازی قابل حمل مانند درایوهای DAT یا Tape‌های ۸ میلی متری ذخیره شوند تا بتوان آن‌ها را در محلی خارج از محل سیستم‌ها و اطلاعات نگهداری نمود. نوع دیگر پشتیبان‌گیری ثبت فعالیت‌های مدیریتی صورت گرفته است. این فعالیت‌ها باید به صورت مستند درآیند تا در مواقع لزوم بتوان مشکلات به وجودآمده را پی گیری کرد و جهت رفع آن‌ها اقدام نمود. سیستم فایل ext2 در لینوکس دارای ابزار و امکانات سودمندی جهت ایجاد، نگهداری، پیکربندی و اشکال زدایی از فایل‌های سیستمی است.

تعریف سیاست‌های مجوز دهی به کاربران

اغلب مشکلات کاربران سیستم‌های لینوکس و یونیکس مربوط به مجوزهای دسترسی فایل‌ها است و اغلب این مشکلات مربوط به مجوزهای کاربر root هستند.

۱- تنظیم مجوزهای دسترسی به فایل‌های پیکربندی برای کاربران

هر کاربر یک دایرکتوری با نام خود دارد که حاوی فایل‌های نیمه مخفی است. این فایل‌ها با نقطه آغاز می‌شوند و اغلب دستوراتی را برای کاربر جاری سیستم اجرا می‌کنند. به عنوان مثال shellها (bash, tcsh, csh و...) تنظیمات خود را از فایل‌های مانند cshrc یا bashrc می‌خوانند. اگر کاربری از مجوزهای دسترسی مناسب برای این فایل‌ها استفاده نکند سایر کاربران می‌توانند مشکلاتی را برای وی به وجود آورند. به عنوان مثال اگر مجوزهای فایل cshrc اجازه نوشتن روی این فایل را به سایر کاربران بدهد امکان اجرای دستور خروج از سیستم (logout) در هنگام شروع cshrc وجود دارد. در این صورت کاربر مربوطه به محض ورود به سیستم از آن خارج می‌شود.

۲- تنظیم مجوزهای دسترسی به فایل‌های اجرایی

تنها مالک فایل‌های اجرایی و برنامه‌ها باید مجوز نوشتن روی آن‌ها را داشته باشد. به عنوان مثال فایل‌های اجرایی که در مسیر /usr/bin قرار دارند باید مجوز خواندن، نوشتن و اجرا را تنها به کاربر root بدهند و به سایر کاربران فقط مجوز خواندن و اجرا بدهند.

ماژول‌های قابل اتصال برای تعیین اعتبار^{۳۸}

این ماژول‌ها در اصل برای سیستم عامل سولاریس طراحی شده است ولی نسخه‌ای از آن برای سیستم عامل لینوکس نیز در دسترس است. برنامه‌های PAM با استفاده از الگوهای مختلف مانند الگوی Shadow Password می‌توانند امنیت سیستم‌ها را بالا ببرند. الگوهای تعیین اعتبار موجود در این برنامه‌ها حقوق و امتیازاتی را به کاربران اعطا می‌کنند. به طور معمول برنامه‌هایی مانند Login یا Passwd کدهای لازم جهت تعیین اعتبار را دارند.

اما با گذشت زمان و با توجه به نیاز به الگوهای تعیین اعتبار جدید لازم است برنامه‌هایی که عمل تعیین اعتبار و اعطای مجوزها را انجام می‌دهند به هنگام سازی شوند برای سادگی کار برنامه نویسان، کد ماژول‌های PAM ارائه شده است که می‌توان با استفاده از این کدها برنامه‌های تعیین اعتبار را به هنگام سازی نمود. عملکرد این ماژول‌ها به صورت زیر است:

۱. کاربر، برنامه تعیین اعتبار را جهت دسترسی به سرویسی که ارائه می‌دهد درخواست می‌کند.
۲. این برنامه کتابخانه PAM را جهت اجرای عملیات تعیین اعتبار فراخوانی می‌کند.
۳. کتابخانه PAM فایل پیکربندی مخصوص برنامه را در دایرکتوری `/etc/pam.d` جست‌وجو می‌کند. این فایل برای PAM مشخص می‌کند که چه نوع تعیین اعتباری برای این برنامه لازم است.
۴. کتابخانه PAM ماژول‌های مورد نیاز را بارگذاری می‌کند.
۵. این ماژول‌ها ارتباط بین PAM با توابع محاوره‌ای قابل دسترسی در برنامه را ایجاد می‌کنند.
۶. توابع محاوره‌ای اطلاعاتی از کاربر درخواست می‌کنند. (مانند درخواست کلمه عبور).
۷. کاربر به درخواست پاسخ می‌دهد.
۸. ماژول‌های تعیین اعتبار PAM به وسیله کتابخانه PAM پیام وضعیت تعیین اعتبار را به برنامه ارائه می‌دهند.
۹. اگر فرآیند تعیین اعتبار موفقیت آمیز باشد برنامه یکی از کارهای زیر را انجام می‌دهد:
 - اعطای حقوق درخواستی به کاربر
 - آگاه کردن کاربر از شکست فرآیند

PAM در واقع وسیله‌ای است که بار فرآیند تعیین اعتبار را از برنامه دور می‌کند و تعدادی الگوی تعیین اعتبار را برای یک برنامه نگه می‌دارد. از جمله برنامه‌های تعیین اعتبار که می‌توان از **PAM** در آن‌ها استفاده نمود می‌توان به **Login** یا **rlogin** اشاره کرد.

جدول انواع ماژول‌های PAM

نوع ماژول	توضیح
auth	تعیین اعتبار واقعی را انجام می‌دهد و نیاز به کلمه عبور و یا سایر مدارک شناسایی کاربر دارد.
account	تمام جنبه‌های accounting مربوط به درخواست‌های تعیین اعتبار را مورد استفاده قرار می‌دهد. برای مثال این ماژول کنترل می‌کند که آیا کاربر امکان دسترسی به یک سرویس از یک میزبان امن را در زمان مشخص دارد یا خیر.
Password	این ماژول تنظیم کلمات عبور را انجام می‌دهد.
Session	این ماژول مدیریت نشست‌ها را برعهده دارد.

استفاده از ماژول‌های مختلف PAM برای افزایش امنیت

لینوکس ماژول‌های **PAM** زیادی جهت بالابردن امنیت سیستم ارائه کرده است که تعدادی از ماژول‌های مهم در جدول زیر معرفی شده اند:

جدول ماژول‌های PAM

نام ماژول	توضیح
Pam_access.so	این ماژول از فایل /etc/security/access.conf استفاده می‌کند و برای اعطا یا عدم اعطای مجوزها به کاربران مورد استفاده قرار می‌گیرد.
Pam_cracklib.so	این ماژول دوام و استحکام کلمات عبور را با استفاده از کتابخانه crack کنترل می‌کند.
Pam_ftp.so	این ماژول جهت تعیین اعتبار سرویس ftp مورد استفاده قرار می‌گیرد.
Pam_group.so	این ماژول دسترسی گروه‌ها به سرویس‌ها را کنترل می‌کند.
Pam_lastlog.so	این ماژول اطلاعاتی درباره کاربر قبلی که به سیستم وارد شده است، ارائه می‌دهد.
Pam_limits.so	این ماژول محدودیت استفاده از منابع را برای نشست کاربر عادی تنظیم و کنترل می‌کند.

نام ماژول	توضیح
Pam_mkhomedir.so	این ماژول یک home دایرکتوری برای کاربری که برای اولین بار به سیستم وارد شده است ایجاد می‌کند.
Pam_console.so	این ماژول دسترسی کاربرانی که از طریق کنسول فیزیکی به سیستم وارد شده‌اند را کنترل می‌کند و شامل کنترل دسترسی به دستورات و تجهیزات سیستم مانند فلاپی و CD ROM و... است.
Pam_nologin.so	این ماژول می‌تواند تمام کاربران به جز کاربر root را از ورود به سیستم منع کند.
Pam_permit.so	این ماژول برای اعطای مجوزهای دسترسی به کاربران مورد استفاده قرار می‌گیرد و باید تنها برای تعیین اعتبار با خطر امنیتی کم مورد استفاده قرار گیرد.
Pam_radius.so	این ماژول سرویس‌های نشست را برای کاربران تعیین اعتبار شده از طریق سرویس دهنده‌های RADIUS مهیا می‌کند.
Pam_shells.so	این ماژول کاربری را که Login Shell وی در فایل /etc/shells قرار دارد تعیین اعتبار می‌کند.
Pam_stress.so	این ماژول امکان تست تنش روی برنامه‌ها را فراهم می‌کند.
Pam_tally.so	این ماژول تمام تلاش‌های دسترسی به سیستم مربوط به کاربر را پی‌گیری و ثبت می‌کند.
Pam_time.so	این ماژول دسترسی کاربران را براساس زمان کنترل و مدیریت می‌کند.
Pam_warn.so	این ماژول از پیام‌های اخطار دهنده در مورد درخواست‌های تعیین اعتبار و فرآیند مجوزدهی گزارش تهیه می‌کند.

مدیریت منابع سیستم

با محدود کردن دسترسی کاربران به منابع سیستمی می‌توان سیستم را در برابر سوء استفاده کاربران امن نگه داشت. با استفاده از ماژول **Pam_limit.so** می‌توان منابع مورد استفاده کاربران یا گروه‌های خاص را مدیریت و کنترل کرد. منابع اصلی قابل مدیریت مطابق لیست زیر است:

۱. حداکثر تعداد فرآیندهای قابل اجرا
۲. حداکثر تعداد دفعات ورود به سیستم
۳. اولویت فرآیند برای کاربری که دستورات را اجرا می‌کند
۴. حداکثر زمان استفاده از CPU
۵. حداکثر سایز **stack** در برنامه‌های کاربر
۶. حداکثر تعداد فایل‌های باز
۷. حداکثر سایز داده
۸. حداکثر سایز فایل
۹. حداکثر سایز حافظه اختصاص داده شده به فرآیندهای کاربر
۱۰. حداکثر سایز فایل هسته (Kernel)
۱۱. حداکثر فضای آدرس دهی حافظه

کنترل دسترسی کاربران به سیستم از طریق کنسول فیزیکی

با استفاده از ماژول **Pam_console** می‌توان دسترسی افرادی را که از طریق کنسول فیزیکی به سیستم وارد شده‌اند، کنترل کرد. این کنترل و محدودیت شامل دسترسی به دستورات مهمی مانند **shutdown**، **reboot**، **halt** و ... و قسمت‌های مختلف سیستم مانند **CD ROM** یا **Floppy** می‌شود.

نکات مهمی که در زمینه دسترسی افراد به سیستم وجود دارد عبارت‌اند از:

۱. باید از **reboot** شدن یا **halt** شدن سیستم به وسیله کاربران معمولی کنسول جلوگیری کرد، این کار از طریق حذف فایل‌های **shutdown**، **reboot**، **halt** در مسیر **/etc/security/console.app** امکان پذیر است.
۲. اگر سیستم در محل ناامنی قرار گرفته باشد باید حتماً دسترسی کاربران به دستورات مهمی مانند **shutdown**، **reboot** و ... محدود شود این امر با تغییر در فایل‌های مربوطه در مسیر **/etc/pam.d** انجام خواهد شد. با اعمال تغییرات مناسب

در این فایل‌ها می‌توان مطمئن شد که حتی اگر فردی بتواند به **account** یک کاربر و محیط **shell** دسترسی پیدا کند بدون داشتن کلمه عبور کاربر نمی‌تواند سیستم را خاموش یا مجدداً راه اندازی نماید.

به طور کلی می‌توان گفت **PAM** مکانیزمی جهت تعیین اعتبار کاربران با قابلیت پیکربندی سطح بالا است و در بالا بردن امنیت سیستم نقش بسزایی دارد.

OpenSSL

SSL پروتکلی جهت برقراری ارتباطات امن در محیط اینترنت است و به عنوان پایه و اساس ساختار امنیتی در شبکه اینترنت شناخته می‌شود. این پروتکل، رمزگذاری اطلاعات ردوبدل شده بین دو نقطه در شبکه را بر عهده دارد. دو روش رمزگذاری وجود دارد که عبارت‌اند از:

۱. رمزگذاری متقارن: در این روش کلیدی جهت رمزگذاری اطلاعات مورد استفاده

قرار می‌گیرد و برای رمزگشایی اطلاعات نیز از همین کلید استفاده می‌شود.

۲. رمزگذاری نامتقارن: در این روش دو کلید جهت رمزگذاری و رمزگشایی

اطلاعات مورد استفاده قرار می‌گیرد. یک کلید عمومی و یک کلید خصوصی.

اگر اطلاعات به وسیله کلیدی عمومی رمزگذاری شود تنها به وسیله کلید خصوصی متناظر با آن کلید عمومی که تنها در اختیار یک نفر قرار دارد قابل رمزگشایی است. کلید عمومی در اختیار همه افرادی که قصد برقراری ارتباطی امن در شبکه با فرد دیگری را داشته باشند قرار می‌گیرد ولی کلید خصوصی تنها در اختیار فرد مورد نظر است. چنانچه اطلاعاتی از سوی فردی و به وسیله کلید خصوصی وی رمزگذاری شود همه افرادی که کلید عمومی متناظر با کلید خصوصی فرد را در اختیار داشته باشند می‌توانند اطلاعات را رمزگشایی کنند. این شکل رمزگذاری داده‌ها از امنیت بسیار بالایی برخوردار است. پروتکل **SSL** روی پروتکل **TCP/IP** و پروتکل‌های لایه **application** مانند **FTP**، **HTTP** و **IMAP** قابل استفاده است. این پروتکل امکان تعیین اعتبار سرور و سرویس گیرنده را به صورت دو طرفه فراهم می‌کند.

نحوه عملکرد **SSL** به صورت زیر است:

۱. در ارتباطاتی که برپایه پروتکل **SSL** هستند سرور گواهینامه‌ای الکترونیکی که به

وسیله مرجع معتبر صدور گواهی صادر شده است برای سرویس گیرنده ارسال

می‌کند. مرجع صادر کننده گواهی آن را به وسیله کلیدی خصوصی رمزگذاری

می‌کند. سرویس گیرنده نیز با استفاده از کلید عمومی متناظر با کلید خصوصی که توسط مرجع صادر کننده گواهی ارائه شده گواهی را رمزگشایی می‌کند. چون کلید عمومی به همراه گواهی برای سرویس گیرنده ارسال می‌شود بنابراین سرویس گیرنده می‌تواند هر داده رمزگذاری شده ارسالی از جانب سرور را رمزگشایی کند.

۲. سرور قسمتی از اطلاعات مربوط به هویت خود را که در گواهی ثبت می‌شود ارسال می‌کند سپس پیامی کوتاه شبیه اطلاعاتی که برای تشخیص هویت خود ارسال می‌کند ایجاد می‌نماید. این پیام به وسیله کلید خصوصی سرور رمزگذاری می‌شود. گواهی صادرشده از سوی مرجع معتبر صدور گواهی تعیین می‌کند که سرویس گیرنده باید از کدام کلید عمومی مربوط به سرور جهت رمزگشایی استفاده کند. ضمناً سرویس گیرنده پیام تشخیص هویت را از سوی سرور دریافت می‌کند که این پیام رمزگذاری شده است.

۳. با استفاده از کلید عمومی سرور، سرویس گیرنده می‌تواند این پیام را رمزگشایی کند. سپس سرویس گیرنده نیز پیام تشخیص هویت ایجاد نموده و با نمونه ارسال شده از جانب سرور مقایسه می‌کند. اگر این دو پیام یکسان باشند هویت سرور تأیید می‌شود و سرویس گیرنده از اعتبار سرور مطمئن می‌شود.

چون رمزگذاری به وسیله کلید متقارن سریع‌تر از کلیدهای نامتقارن (خصوصی و عمومی) است بنابراین برای حفظ امنیت و سرعت بیشتر در انتقال و رمزگذاری و رمزگشایی اطلاعات، سرویس گیرنده می‌تواند کلیدی متقارن که به وسیله کلید عمومی سرور رمزگذاری شده است را برای سرور ارسال کند، سرور از این کلید جدید جهت رمزگذاری داده‌ها و انتقال آن‌ها به سرویس گیرنده استفاده می‌کند.

در صورتی که در ارتباط بین سرور و سرویس گیرنده عاملی بخواهد خود را جای یکی از آن‌ها جا بزند و به اطلاعات ردوبدل شده دسترسی پیدا کند، بدلیل اینکه کلید متقارن را در اختیار ندارد نمی‌تواند اطلاعات را رمزگشایی کند، تنها کاری که می‌تواند انجام دهد اضافه کردن داده‌های اضافی به اطلاعات مورد نظر است. برای جلوگیری از این امر پروتکل SSL کدی جهت تعیین اعتبار پیام‌ها در نظر گرفته است که این کد با استفاده از کلید متقارن و داده‌های ارسال شده محاسبه و ایجاد می‌شود.

OpenSSL برنامه‌ای است که در امن‌سازی انواع ارتباطات کاربرد دارد. با توجه به ویژگی‌های پروتکل **SSL**، در بسیاری از برنامه‌ها برای بالابردن امنیت داده‌های ارسالی مورد استفاده قرار می‌گیرد. از جمله موارد استفاده **OpenSSL** می‌توان به موارد زیر اشاره نمود:

۱. امن کردن انتقال اطلاعات روی وب سرور **Apache**.
 ۲. امن کردن ارتباط کاربران راه دور با سیستم.
 ۳. امن کردن ارتباطات شبکه خصوصی مجازی (**VPN**) از طریق **PPP** با استفاده از نرم‌افزار ایجاد کانال امن بر پایه **OpenSSL**.
 ۴. امن کردن سرویس‌های پست الکترونیکی (**IMAP,POP3**) از طریق نرم‌افزار ایجاد کانال امن با استفاده از **OpenSSL**.
- OpenSSL** را از طریق بسته های **RPM** یا کد منبع آن (**source code**) می‌توان روی سیستم عامل لینوکس نصب و اجرا کرد. لازمه استفاده از **OpenSSL** دریافت گواهی الکترونیکی از یک مرجع معتبر صادر کننده گواهی است. دو منبع جهت صدور گواهی قابل استفاده هستند:
۱. مراجع تجاری صادر کننده گواهی: این مراجع جهت صدور گواهی برای سایر شرکت‌ها و سازمان‌ها در اینترنت مورد استفاده قرار می‌گیرند.
 ۲. مرجع خصوصی صدور گواهی: این مراجع اغلب در محیط‌های **LAN** و **WAN** مورد استفاده قرار می‌گیرند.

پنهان سازی کلمات عبور و استفاده از OpenSSH

ریسک‌های امنیتی ایجاد شده از طریق اینترنت شامل یکی از موارد زیر است:

۱. نفوذگر برنامه‌ای را جهت آشکار کردن اشکالات شناخته شده در سرویس اینترنت به سمت سیستم هدف ارسال می‌کند.
۲. برنامه افشاء کننده از اشکالات موجود استفاده کرده و شرایط را برای تغییر در فایل‌های سیستم یا دسترسی به سیستم آماده می‌کند.
۳. نفوذگر با **account** کاربر معمولی به سیستم وارد می‌شود که آن را به وسیله برنامه نفوذگر به دست آورده است.
۴. نفوذگر فایل‌های هدف سیستم را حذف کرده و یا برنامه‌های **Trojan** را روی سیستم نصب می‌کند تا در آینده از طریق آن‌ها بتواند به سیستم نفوذ پیدا کند.

اگر دسترسی کاربران راه دور به سرورهای شبکه چه از طریق اینترنت و چه در محیط LAN محدود شود و تنها یک راه برای دسترسی به محیط shell در سیستم عامل لینوکس برای کاربر وجود داشته باشد (دسترسی از طریق کنسول فیزیکی) در این صورت خطرات امنیتی نفوذ به سیستم به طور قابل توجهی کاهش می‌یابد. البته محدود کردن دسترسی کاربر در مجموع راه حل کاربردی و مناسبی در بیشتر موارد نیست بلکه باید ابتدا ریسک‌های ناشی از account کاربران و راه حل‌های کاهش این ریسک‌ها را مورد بررسی و شناسایی قرار داد.

شناسایی ریسک‌های مربوط به account کاربران

به طور کلی کاربر از طریق نام کاربر و کلمه عبور می‌تواند به سیستم لینوکس دسترسی پیدا کند. در بیشتر موارد نیز سیستم‌های سرویس گیرنده شبکه، نام کاربری و کلمه عبور خود را بدون رمزگذاری برای سرورها ارسال می‌کنند. این موضوع خطر امنیتی بزرگی محسوب می‌شود زیرا نفوذگر می‌تواند با شنود ترافیک شبکه به این اطلاعات مهم و حساس کاربر دسترسی پیدا کند. نکته مهم: اگر کاربران زیادی به shell دسترسی داشته باشند، باید مانع از دسترسی کاربران معمولی به گزارش‌های ثبت شده در مسیر /var/log شد.

در بسیاری موارد کاربر بعد از چند بار تلاش برای ورود به سیستم و عدم موفقیت، کلمه عبور را به اشتباه به جای نام کاربر وارد می‌کند و چون این اطلاعات در مسیر var/log/message ثبت می‌شوند بنابراین دسترسی کاربران معمولی یا غیرمجاز به این گزارش‌ها خطر آشکار شدن کلمه عبور سایر کاربران را به همراه دارد. بنابراین تنها کاربر root (مدیر سیستم) باید به این فایل دسترسی داشته باشد. نکته مهم دیگر، صدور مجوز تغییر کلمه عبور برای کاربران است. در بسیاری موارد بیشتر کاربران تمایل به استفاده از کلمات عبور با طول کوتاه و ساختاری ساده دارند تا همیشه در خاطر آن‌ها باقی بماند. بنابراین برای جلوگیری از این مسأله باید مدیر سیستم همواره روی انتخاب کلمات عبور کاربران کنترل و نظارت داشته باشد. اطلاعات مربوط به account کاربران در فایلی به نام Passwd در مسیر دایرکتوری /etc قرار دارد که فایلی متنی و قابل خواندن و تغییر است و نام کاربر، رمز عبور، شماره شناسایی و سایر اطلاعات در آن درج شده است. البته کلمه عبور کاربر به صورت رمزگذاری شده است ولی این فایل اولین هدف نفوذگران برای دسترسی به اطلاعات کاربران است. بنابراین حفظ امنیت این فایل بسیار مهم و حیاتی می‌باشد. برای افزایش امنیت فرآیند تعیین اعتبار کاربر به صورت امن، چند نکته امنیتی را باید مورد توجه قرار داد:

۱- استفاده از کلمات عبور مخفی و مدت دار ((shadow password

برای اطمینان از عدم افشای کلمه عبور کاربران در فایل `/etc/Passwd` نیاز به کلمات عبور مخفی است. سیستم عامل لینوکس از الگوی کلمات عبور مخفی استفاده می‌کند و کلمات عبور کاربر را در مسیر `/etc/shadow` ذخیره می‌کند و تنها کاربر `root` قادر به دسترسی به این فایل است. مکانیزم `shadow-password` می‌تواند کاربران را مجبور به استفاده از کلمات عبور مدت دار کند و این مسأله امنیت کلمات عبور را افزایش می‌دهد.

۲- کنترل و بررسی سازگاری و ثبات کلمات عبور

- دو نکته مهم در هنگام استفاده از فایل‌های `/etc/passwd` و `/etc/shadow` وجود دارد که عبارت‌اند از:
- الف - تهیه نسخه پشتیبان از این فایل‌ها قبل از هر گونه تغییر
 - ب - کنترل و تأیید اعتبار این فایل‌ها به وسیله اجرای دستورات کنترل‌کننده سازگاری و جامعیت داده‌ها (مانند دستور `pwck`).

حذف سرویس‌های پر خطر Shell

یکی از سرویس‌های پر خطر `Telnet` است که کلمات عبور کاربران را به صورت رمزگذاری نشده در شبکه ارسال می‌کند. بنابراین باید این سرویس را در مسیر `/etc/services` با قراردادن علامت `#` در ابتدای خط مربوط به این سرویس غیرفعال کرد و علاوه بر این در فایل `/etc/xinetd.conf` خط زیر را اضافه کرد:

`Disabled=telnet`

برای سایر سرویس‌ها مانند `rlogin`, `rsh` یا `rexec` که وضعیتی مشابه `Telnet` دارند باید همین تنظیمات را انجام داد.

استفاده از OpenSSH برای دسترسی امن از راه دور

`OpenSSH` ابزاری جهت اجرای پروتکل‌های `SSH1` و `SSH2` برای بالابردن امنیت ارتباطات راه دور با سیستم است. با استفاده از پروتکل‌های `SSH1` و `SSH2` می‌توان داده‌های ارسالی شبکه را رمزگذاری کرد.

مدیریت account کاربر root

در اکثر موارد افراد خرابه‌کار و نفوذگر سعی می‌کنند به کلمه عبور **root** برای دسترسی کامل به سیستم دست پیدا کنند. بنابراین مدیریت **account** کاربر **root** بسیار مهم و حیاتی است. هر کاربر با حقوق **root** باید برای حفظ امنیت سیستم و جلوگیری از نفوذ و خرابه‌کاری سایر کاربران به نکات زیر توجه خاص داشته باشد:

۱. تنها در صورت لزوم با نام و کلمه عبور **root** وارد سیستم شود. به عنوان مثال برای ویرایش و تغییر فایل‌های پیکربندی سیستم و فعال یا غیرفعال کردن سرویس‌ها

۲. انتخاب کلمه عبور سخت و پیچیده با طول مناسب

۳. تغییر کلمه عبور در دوره‌های زمانی مناسب

۴. از آنجایی که در یک محیط کاری واقعی کلمه عبور **root** در اختیار چند نفر قرار دارد باید مطمئن بود که در صورت تغییر کلمه عبور توسط یکی از آن افراد، سایرین از این امر آگاه خواهند شد. ضمناً نباید هرگز کلمه عبور **root** را برای دیگران از طریق پست الکترونیکی ارسال کرد.

محدود کردن دسترسی کاربری root

به صورت پیش فرض لینوکس اجازه ورود به سیستم را از طریق **Telnet** یا سایر سرویس‌های دسترسی راه دور با حساب کاربری **root** نمی‌دهد. این تنظیم در فایل **/etc/security** قرار دارد و هیچ کس جز کاربر **root** نباید اجازه دسترسی به این فایل را داشته باشد.

استفاده از دستور su برای ورود به سیستم با account کاربری دیگر

دستور **su** می‌تواند یک **shell** با شناسه کاربری متفاوت با شناسه کاربر فعلی سیستم اجرا کند.

استفاده از دستور sudo جهت اعطای حقوق دسترسی کاربر root به سایر کاربران

دو روش برای محول کردن وظایف **root** به سایر کاربران وجود دارد. اولین روش، تغییر مجوزها برای برنامه‌هایی است که به طور معمول تنها به وسیله **root** قابل اجرا هستند. برای این منظور می‌توان از **set-UID** که در بخش امنیت فایل سیستم توضیح داده شده است، استفاده کرد. این روش مناسب نیست. روش دیگر استفاده از برنامه **sudo** است. این دستور به کاربران معمولی اجازه می‌دهد که دستورات مشخص شده را به عنوان کاربر **root** اجرا کنند. فایل مربوط به تنظیم و پیکربندی **sudo** در مسیر **/etc/sudoers** قرار دارد. از دستور **visudo** می‌توان برای ویرایش و اعمال

تنظیمات در این فایل استفاده کرد. این دستور امکان تغییر همزمان به وسیله چند نشست **root** را غیر ممکن می‌کند.

توجه: این برنامه به صورت پیش فرض نصب نیست و باید کد منبع یا بسته نرم‌افزاری **rpm** آن را نصب و پیکربندی کرد.

تعریف سیاست امنیتی برای دسترسی کاربران

توجه به موارد زیر برای تعریف سیاست‌های امنیتی درمورد حقوق دسترسی کاربران ضروری است:

۱. دسترسی به سیستم یک امتیاز است و این حق با مسئولیت همراه است. بنابراین در اعطای حقوق دسترسی به کاربران باید دقت کرد.
۲. کلمات عبور نباید با سلیقه شخصی کاربران تعیین شوند.
۳. کاربران باید بپذیرند که کلمات عبور آن‌ها دائمی نیست.
۴. کلمات عبور به عنوان اسرار سازمانی به شمار می‌روند و کاربر نباید آن را در اختیار دیگران بگذارد.
۵. کلمات عبور نباید یکسان باشند. تنها داشتن کلمه عبور کافی نیست بلکه کلمه عبور مناسب که حدس زدن و حفظ کردن آن دشوار باشد نیز لازم است.

ایجاد رویه‌های امنیتی خاتمه همکاری برای کارمندان

با ایجاد این دسته از سیاست‌های امنیتی می‌توان از امنیت سیستم بعد از خاتمه قرارداد کارمندان و خروج ایشان از سازمان (به ویژه کاربران ناراضی) مطمئن شد. از جمله این رویه‌ها عبارت‌اند از:

۱. حذف **account** کاربران.
۲. غیرفعال کردن **account** کاربران برای جلوگیری از ورود آن‌ها به سیستم.
۳. اعلام مراتب به واحدهای مرتبط.

امنیت کلمات عبور راه دور^{۳۹}

SRP پروتکل تعیین اعتبار بر پایه کلمات عبور است. این پروتکل کلمات عبور را روی شبکه انتقال نمی‌دهد و بدین ترتیب مانع از دسترسی نفوذگران به کلمات عبور از طریق کنترل ترافیک شبکه می‌شود. ضمناً از رمزگذاری جهت تعیین اعتبار استفاده نمی‌کند که این امر باعث سرعت بیشتر این فرآیند می‌شود. برای استفاده از این پروتکل باید بسته **RPM** یا کد منبع آن را نصب و پیکربندی کرد. از این پروتکل می‌توان به همراه سرویس‌هایی مانند **Telnet** یا **ftp** استفاده کرد و امنیت ارتباطات را افزایش داد.

سرویس Xinetd

این سرویس نسبت به سرویس **inetd** از امنیت بالاتری برخوردار است و انعطاف پذیری بیشتری نسبت به آن سرویس دارد. البته عملکرد هر دو یکسان است، با این تفاوت که **xinetd** کنترل دسترسی، اختصاص پورت‌ها به سرویس‌ها و محافظت از سیستم در برابر حملات **DoS** (رد سرویس) را نیز انجام می‌دهد. سرویس اینترنت تحت سیستم عامل لینوکس در دو حالت **stand-alone** و **xinetd** قابل اجرا است. در مواردی که ترافیک و درخواست‌ها از وب سرور زیاد باشد سرویس **xinetd** می‌تواند به چندین درخواست به طور همزمان با اجرای چند فرآیند سرویس دهنده پاسخ دهد. بنابراین وقتی ترافیک وب سرور بالا باشد با اجرای سرویس وب در حالت **xinetd** می‌توان با کارایی بالا و بدون بروز اشکال در سرویس دهی و با ایجاد پردازش‌های جدید برای هر درخواست به آن‌ها پاسخ داد. سرویس‌های دیگری مانند **ftp** یا **POP3** نیز برای کارایی بهتر می‌توانند از **xinetd** استفاده کنند. هر سرویس فایل پیکربندی مربوط به خود را دارد که در مسیر **/etc/xinetd** قرار گرفته است و می‌توان آن را برای استفاده از **xinetd** پیکربندی و تنظیم نمود.

از دیگر ویژگی‌های سرویس **xinetd** امکان کنترل و مدیریت دسترسی به سرویس‌ها از طریق نام یا **IP** آدرس سیستم هاست که با استفاده از این ویژگی می‌توان از دسترسی یک یا چند سیستم مشخص به یک سرویس خاص مانند **Telnet** یا **ftp** ممانعت به عمل آورد. این تنظیم در فایل‌های پیکربندی **xinetd** مربوط به هر سرویس امکان پذیر است.

کنترل دسترسی به سرویس‌ها حتی براساس زمان نیز امکان پذیر است و می‌توان دسترسی به سرویس‌هایی را که به وسیله **xinetd** مدیریت می‌شوند به زمان‌های خاصی از روز محدود کرد. ویژگی دیگر سرویس **xinetd** کاهش خطرات ناشی از حملات **DoS** به سرویس‌هایی است که مدیریت می‌کند. این کار با محدود کردن تعداد نمونه پردازش‌های سرویس دهنده که **xinetd** می‌تواند در هنگام دریافت چندین درخواست اجرا کند امکان پذیر است. ضمناً می‌توان با محدود کردن ساین فایل گزارش‌های مربوط به سرویس‌ها مانع از پرشدن فضای دیسک به وسیله گزارش‌های ایجاد شده توسط نفوذگران شد. همچنین می‌توان حداکثر میزان بارگذاری سیستم را که براساس میانگین بار **CPU** در یک دقیقه است تعیین کرد تا در صورتی که میانگین بارگذاری سیستم از این مقدار بیشتر شد، سرویس مورد نظر به طور موقتی غیرفعال شود تا میانگین بارگذاری کاهش یابد.

سایر ویژگی‌های مهم **xinetd** عبارت‌اند از:

- تعیین اولویت پردازش‌ها برای سرویس‌هایی که به وسیله **xinetd** مدیریت می‌شوند.
- محدود کردن تعداد فرآیندهای سرویس دهنده در هر ثانیه.

ایجاد دسترسی‌های متمایز برای سرویس‌ها

گاهی اوقات دسترسی به سرویس‌هایی مانند **Http** یا **ftp** را می‌توان مطابق با نوع درخواست‌ها و جایی که ارسال می‌شوند تنظیم کرد. به عنوان مثال چنانچه سرویس دهنده **ftp** دارای دو کارت شبکه باشد که یکی از آن‌ها به شبکه داخلی و دیگری به شبکه اینترنت متصل باشد، می‌توان دسترسی به سرویس **ftp** را از طریق هر کدام از این دو شبکه به طور جداگانه تنظیم و کنترل نمود. این کار توسط سرویس **xinetd** و پیکربندی فایل مربوط به سرویس مورد نظر امکان پذیر است. ضمناً امکان ارسال درخواست‌ها به یک سرویس دهنده یا پورت دیگر امکان پذیر است.

استفاده از TCP wrapper با xinetd

اگر سرویس **xinetd** طوری تنظیم شود که از قابلیت **TCP wrapper** پشتیبانی کند، در این صورت می‌توان دسترسی به سرویس‌های تحت کنترل **xinetd** را محدود کرد. به این منظور به دو فایل **/etc/hosts.deny** و **/etc/hosts.allow** نیاز است که می‌توان **IP** آدرس سیستم‌هایی که مجاز به استفاده از یک سرویس خاص هستند و یا اجازه دسترسی به آن سرویس را ندارند، تعیین کرد.

ضمیمه سه :

(پیکربندی سرویس‌های پایه LINUX و ملاحظات امنیتی)

معرفی سرویس Firewall

سرویس فایروال لینوکس جهت بالا بردن امنیت شبکه، جلوگیری از حملات خارجی به شبکه و کنترل دسترسی کاربران در اینترنت مورد استفاده قرار می‌گیرد. به طور کلی عملکرد هر نوع فایروال اعم از نرم‌افزاری یا سخت‌افزاری به این صورت است که تمام بسته‌های پروتکل TCP و IP قبل از ورود به شبکه یا خروج از آن ابتدا وارد فایروال می‌شوند تا طبق قوانین حفاظتی و امنیتی تعیین شده در شبکه پردازش شوند. پس از پردازش ممکن است سه حالت رخ دهد:

۱- اجازه عبور به بسته داده می‌شود .

۲- بسته حذف می‌شود.

۳- بسته حذف شده و پاسخ متناظر به مبداء آن بسته ارسال می‌شود.

پیکربندی امنیتی شبکه، مجموعه‌ای از قواعد امنیتی است که بنابر ماهیتشان در یکی از لایه‌های

فایروال اجرا می‌شوند:

۱- قواعد تعیین بسته‌های غیرمجاز در اولین لایه فایروال

۲- قواعد بستن پورت‌های متعلق به سرویس‌های خاص

۳- قواعد تحلیل سرآیند (Header)، متن پیام الکترونیک یا صفحه وب در لایه سوم

به طور کلی فایروال‌ها دارای سه نوع NAT، Packet Filtering و Proxy هستند:

۱ - NAT (Network Address Translating)

این نوع فایروال‌ها امکان ترجمه IP آدرس‌ها را فراهم می‌کنند. در این حالت فایروال، IP آدرس‌های خصوصی مربوط به شبکه داخلی را به یک یا چند IP آدرس خارجی (معتبر در اینترنت) تبدیل می‌کند و به این طریق امکان برقراری ارتباط شبکه داخلی با اینترنت را در سطح امنیتی مناسب فراهم می‌کند.

همچنین می‌توان دسترسی کاربران داخلی شبکه، به سرویس‌های شبکه اینترنت را از طریق بستن پورت‌های مربوط کنترل کرد. این عمل برای کنترل دسترسی کاربران خارجی به سرویس‌های ارائه شده در شبکه داخلی نیز امکان پذیر است. اشکال این

نوع فایروال این است که وقتی کاربر داخلی با سرویس آن سوی فایروال ارتباط برقرار می‌کند نمی‌تواند مانع از فعالیت‌های خرابه‌کارانه در شبکه شود.

۲- Packet Filtering

نوع دیگری از فایروال، عملیات کنترل ترافیک بسته‌ها را انجام داده و ورود و خروج بسته‌ها را کنترل می‌کند. این نوع فایروال مطابق با تنظیمات امنیتی در نظر گرفته شده یا اجازه ورود و خروج بسته‌ها را صادر می‌کند و یا مانع عبور آن‌ها در شبکه می‌شود. هسته لینوکس دارای این قابلیت از طریق زیر سیستم‌های مرتبط با فیلترینگ شبکه می‌باشد. در این نوع فایروال نیاز به هیچ تنظیمی روی سیستم‌های سرویس گیرنده فایروال نیست و چون ارتباط مستقیم و بدون واسطه بین سیستم‌های ارسال کننده و دریافت کننده اطلاعات وجود دارد، سرعت و کارایی شبکه بیشتر و بهتر است. اشکال این نوع فایروال این است که نمی‌تواند عملیات فیلترینگ بسته را بر مبنای محتوای آن انجام دهد. ضمناً قادر به فیلتر کردن بسته‌ها در لایه کاربرد شبکه (Application) نیست.

۳- Proxy

دسته دیگر فایروال‌ها، پراکسی سرورها هستند که می‌توانند تمام درخواست‌های مربوط به یک پروتکل خاص از سیستم داخلی شبکه را کنترل و فیلتر کنند. این نوع فایروال به عنوان واسطه‌ای بین دو سیستم عمل می‌کند و به نیابت از سیستم مبدا با سیستم مقصد ارتباط برقرار می‌نماید و پس از دریافت داده‌ها همین ارتباط را با سیستم مبدا برقرار می‌کند. در این حالت امنیت بیشتر ولی کارایی و سرعت شبکه پایین است. برخی از پراکسی سرورها می‌توانند داده‌های دریافتی را ذخیره (Cache) کنند تا سرویس گیرنده‌ها در نوبت‌های بعدی از این داده‌ها استفاده کنند. زیر سیستم فیلترینگ شبکه در هسته لینوکس بسیار قدرتمند است و دارای قابلیت فیلتر کردن بسته‌ها و تبدیل آدرس شبکه (NAT) می‌باشد. این سیستم با ابزار iptables و از طریق خط فرمان کنترل و اجرا می‌شود.

نصب و راه اندازی iptables

برای نصب iptables و استفاده از امکانات فایروال لینوکس بسته نرم‌افزاری RPM مربوط به iptables با دستور زیر نصب می‌شود:

```
rpm -Uvh iptables-version-number.i386.rpm
```

با استفاده از دستورات زیر می‌توان سرویس را فعال و غیرفعال کرد:

```
/etc/rc.d/init.d/iptables Start
```

```
/etc/rc.d/init.d/iptables Stop
```

به منظور فعال شدن iptables در هنگام راه اندازی (Boot)، از دستور زیر استفاده می‌شود:

```
chkconfig --level 345 iptables on
```

کلیه قواعد و دستورات iptables در حافظه سیستم ذخیره می‌شوند و با راه اندازی مجدد سیستم از بین می‌روند. برای جلوگیری از این امر از دستور زیر استفاده می‌شود:

```
/sbin/iptables-save
```

برای اعمال قواعد ذخیره شده در مسیر /etc/sysconfig/iptables پس از راه اندازی مجدد

سیستم از دستور زیر استفاده می‌شود:

```
/sbin/iptables-restore
```

تنظیم و پیکربندی iptables

نکته: دستوراتی که برای تنظیم سرویس فایروال لینوکس استفاده می‌شوند، با توجه به نسخه هسته لینوکس و نسخه سیستم عامل متفاوتند. جدول زیر این دستورات را نشان می‌دهد:

Firewall Command	Linux Kernel Version	Red Hat Version
iptables	2.4X	7.1-9.0
ipchains	2.2X	6.X-7.0
ipfwadm	2.0X	5.X

در صورتی که از دستور ipchains روی سیستم استفاده شود، از آنجایی که سیستم در ابتدا فعال بودن آن را مورد بررسی قرار می‌دهد، هسته سیستم عامل قادر به فعال کردن دستورات iptables نخواهد بود. برای استفاده از دستورات iptables باید ipchains را غیرفعال کرد.

```
chkconfig --del ipchains
```

```
chkconfig --add iptables
```

```
ipchains -F
```

```
service ipchains stop
```

```
rmmod ipchains
```

```
service iptables start
```

تنظیمات پایه‌ای فایروال

بعضی از تنظیمات اصلی که از ابتدا فعال می‌شوند به عنوان پایه و اساس تنظیمات فایروال مفید و موثر هستند. **iptables** از سیاست‌ها جهت ایجاد قواعد پیش فرض استفاده می‌کند. به عنوان مثال دستورات زیر تمام داده‌های ورودی و خروجی شبکه را رد می‌کنند.

```
iptables -P INPUT DENY
iptables -P OUTPUT REJECT
```

بعد از ایجاد زنجیره تنظیمات پیش فرض می‌توان قواعد جدیدی برای فایروال ایجاد کرد.

دستورات و پارامترهای اصلی iptables

الف- دستورات

دستوراتی که در **iptables** تعریف می‌شوند، تعیین کننده نوع برخورد با بسته‌ها (Packet) است. تنها وجود یک دستور در هر رشته دستور **iptables** مجاز است. ضمناً این دستورها حتماً باید با حروف بزرگ نوشته شوند.

لیست دستورات iptables

دستور	توضیح
-A	اضافه کردن یک قاعده امنیتی به زنجیره iptables
-D	حذف یک قاعده امنیتی از زنجیره iptables
-E	تغییر نام یک زنجیره تعریف شده توسط کاربر
-F	حذف یک زنجیره
-H	ارائه لیست دستورات و پارامترهای آن
-I	اضافه کردن یک قاعده در زنجیره در نقطه تعیین شده توسط کاربر. اگر هیچ عددی تعیین نشود iptables قاعده را در بالای زنجیره قرار می‌دهد.
-L	لیست تمام قواعد درون زنجیره را مشخص می‌کند. مثال: IP iptables -L <chain_name> -t <table_name>

ب- پارامترها

بعد از تعیین دستورهای مناسب باید از پارامترها برای ایجاد قواعد استفاده کرد.

لیست پارامترهای iptables

پارامتر	توضیح
-d	تعیین IP آدرس یا نام کامپیوتر مقصد
-f	اعمال قاعده مورد نظر به بسته‌های قطعه قطعه شده
-i	تعیین کارت شبکه ورودی- این پارامتر تنها به همراه زنجیره INPUT, FORWARD در جدول فیلترینگ و زنجیره PREROUTING در NAT مورد استفاده قرار می‌گیرد.
-o	کارت شبکه خروجی را مشخص می‌کند و در زنجیره OUTPUT و FORWARD در جدول فیلترینگ و زنجیره POSTROUTING در NAT مورد استفاده قرار می‌گیرد.
-j	برای iptables مشخص می‌کند که وقتی یک بسته اطلاعاتی با یکی از قواعد تعیین شده مطابقت داشت چه برخوردی با آن بسته انجام دهد.
-p	نوع پروتکل را مشخص می‌کند (IP,TCP,UDP)
-s	تعیین IP آدرس یا نام کامپیوتر مبدأ

پس از تعیین نوع پروتکل، می‌توان از گزینه‌های زیر در تعریف قواعد استفاده کرد.

-- dport	تعیین شماره پورت یا نام سرویس مقصد.
-- sport	تعیین شماره پورت مبدأ.
-- syn	قاعده مربوطه، به تمام بسته‌های TCP که جهت آغاز ارتباط ارسال می‌گردند، اعمال می‌شود. (تنها در پروتکل TCP قابل استفاده است)
-- icmp-type	تعیین نوع بسته ICMP .

زمانی که یک بسته با یک قاعده خاص مطابقت داشته باشد، آن قاعده می‌تواند بسته را به سمت هدف‌های مختلف ارسال کند. این هدف‌ها در واقع سرنوشت بسته را از نظر رد یا قبول آن مشخص می‌کنند. هدف‌های استاندارد عبارت‌اند از:

ACCEPT	قبول بسته
DROP	رد بسته بدون آگاه کردن درخواست کننده.
QUEUE	بسته‌ها برای استفاده توسط برنامه‌های سطح کاربر در یک صف قرار می‌گیرند.
REJECT	ارسال یک بسته به سیستم راه دور جهت اطلاع از عدم پذیرش بسته.

نکته: قواعدی که توسط دستور **iptables** تعریف می‌شوند با توجه به دستورات و پارامترهای مورد استفاده، متعلق به یک جدول خاص هستند. سه نوع جدول در سرویس فایروال لینوکس تعریف شده است که هر جدول شامل تعدادی زنجیره پیش فرض است. بسته‌ها وارد زنجیره مربوطه شده تا مطابق با قواعد تعریف شده در آن زنجیره با آن‌ها برخورد شود:

1-Filter

- INPUT
- OUTPUT
- FORWARD

2-NAT

- PREROUTING تغییر بسته‌ها بعد از ورود به شبکه
- OUTPUT
- POSTROUTING تغییر بسته‌ها قبل از خروج از شبکه

3-Mangle

- INPUT
- OUTPUT
- FORWARD
- PREROUTING
- POSTROUTING

به طور کلی ساختار دستور **iptables** به شکل زیر است:

```
iptables [-t <table-name>] <command> <chain-name> <parameter-l> <option-l>
<parameter-n> <option-n>
```

فیلتر کردن بسته‌های ورودی شبکه

حفظ امنیت شبکه داخلی در برابر حملات کاربران خارجی از اهمیت بالایی برخوردار است. به همین منظور باید از دستورات فیلتر کردن بسته‌های ورودی به شبکه برای جلوگیری از ورود بسته‌های نامطمئن به شبکه استفاده کرد. به عنوان مثال دستورات زیر تمام ارتباطات سرویس **Telnet** از خارج به داخل شبکه را رد می‌کنند:

```
iptables -A INPUT -p tcp --dport telnet -j REJECT
iptables -A INPUT -p udp --dport telnet -j REJECT
```

در این دستورات به جای پارامتر **dport** می‌توان هم از شماره پورت مقصد و هم از نام سرویس استفاده کرد.

فیلتر کردن بسته‌های خروجی از شبکه

با استفاده از این نوع فیلتر می‌توان دسترسی کاربران داخلی شبکه به اینترنت را کنترل و محدود کرد. به عنوان مثال دستور زیر مانع از دسترسی کاربران به سرویس وب می‌شود:

```
iptables -A OUTPUT -p tcp --dport 80 -j DROP
```

دستور زیر نیز، تمام پرس و جوهای خروجی DNS را در کارت شبکه خارجی فایروال (متصل به اینترنت) می‌پذیرد.

```
iptables -A OUTPUT -p udp -o eth0 --dport 53 --sport 1024: 65535 -j ACCEPT
```

قواعد مربوط به تبدیل آدرس شبکه (NAT)

بسیاری از سازمان‌ها فقط دارای تعداد محدودی IP آدرس معتبر (قابل مسیریابی در اینترنت) هستند. بنابراین برای این‌که امکان استفاده از سرویس اینترنت توسط کاربران بیشتری فراهم شود، باید از روش خاصی استفاده کرد. این روش، تبدیل آدرس شبکه (NAT) نام دارد که آدرس‌های خصوصی شبکه را به آدرس معتبر در اینترنت تبدیل می‌کند و عکس این عمل را نیز انجام می‌دهد. یکی از ویژگی‌های iptables در فایروال لینوکس قابلیت NAT است.

تنظیمات و قواعد Forward این امکان را برای مدیران شبکه فراهم می‌کند که مسیریابی و ارسال بسته‌های داخل شبکه به خارج شبکه را کنترل و مدیریت کنند. به عنوان مثال دستور زیر امکان Forwarding را برای تمام آدرس‌های IP داخلی شبکه فراهم می‌کند (کارت شبکه داخلی eth1 به عنوان Gateway در نظر گرفته شده است):

```
iptables -A FORWARD -i eth1 -j ACCEPT
```

با استفاده از قواعد Forward می‌توان انواع مشخصی از ترافیک شبکه را محدود کرد. به عنوان مثال با استفاده از دستورات زیر می‌توان مانع از برقراری ارتباط کامپیوترهای داخل شبکه با سرور Samba شد:

```
iptables -A FORWARD -p tcp --dport 137:139 -j DROP
```

```
iptables -A FORWARD -p udp --dport 137:139 -j DROP
```

برای ایجاد محدودیت‌های بیشتر می‌توان تمام ارتباطات از خارج شبکه که قصد دارند خود را با یک IP اختصاصی معتبر در محدوده شبکه داخلی معرفی کنند، رد کرد. به عنوان مثال اگر فرض شود که آدرس شبکه 192.168.1.0/24 است و eth0 کارت شبکه متصل به اینترنت می‌باشد، با دستورات زیر می‌توان این محدودیت را ایجاد و امنیت شبکه داخلی را افزایش داد:

```
iptables -A FORWARD -p tcp -s 192.168.1.0/24 -i eth0 -j DROP
```

```
iptables -A FORWARD -p udp -s 192.168.1.0/24 -i eth0 -j DROP
```

همچنین می‌توان قواعد را طوری تنظیم کرد که ترافیک داده‌ها به سمت یک کامپیوتر مشخص هدایت شود، مانند وب سرور یا FTP سروری که در یک DMZ (یک شبکه مجزا از شبکه خصوصی) قرار گرفته است.

مثال: برای ایجاد قاعده‌ای که تمام درخواست‌های **Http** ورودی به شبکه را به یک وب سرور خصوصی با آدرس **10.0.4.2** و پورت ۸۰ ارسال می‌کند. از دستور زیر استفاده می‌شود:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 10.0.4.2:80
```

این نوع ارتباط، ارتباطی غیر امن برای اتصال به وب سرور داخلی شبکه است. در صورتی که وب سرور ارتباطات امن (SSL) را بپذیرد شماره پورت ۴۴۳ خواهد بود. بنابراین دستور فوق به شکل زیر تغییر می‌یابد:

```
Iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to 10.0.4.2:443
```

سرویس DHCP

پروتکل **DHCP**، اطلاعات لازم را برای راه اندازی ارتباط **TCP/IP**، به طور اتوماتیک به سیستم‌ها ارسال می‌کند. سیستمی که به سرور **DHCP** متصل می‌گردد، آدرس‌های **IP**، **Gateway** و **DNS** را از سرور **DHCP** دریافت می‌کند. **DHCP** به منظور پیکربندی سریع سیستم‌های متصل به شبکه (Client ها) به کار گرفته می‌شود. با انتخاب گزینه پیکربندی از طریق **DHCP**، از تنظیم دستی **IP**، **DNS** و **Gateway** به وسیله کاربر جلوگیری می‌شود و تغییر تنظیمات کل شبکه از جمله **IP** و **DNS** و... از طریق **DHCP**، به راحتی صورت می‌گیرد. به علاوه به جای تنظیم و پیکربندی تمام سیستم‌ها فقط کافی است تغییرات لازم را در سرور **DHCP** اعمال نمود. پس از اعمال تغییرات روی **DHCP** و با راه اندازی مجدد سرویس و سرویس گیرنده، این تغییرات در سیستم‌های موجود شبکه اعمال می‌گردد.

همچنین کامپیوترهای قابل حملی که از یک بخش به بخش دیگر انتقال پیدا می‌کند، نیازی به پیکربندی مجدد ندارند و در هر شبکه اطلاعات مورد نیاز برای اتصال به شبکه را از سرور **DHCP** دریافت می‌کنند.

پیکربندی DHCP

برای پیکربندی **DHCP** از فایل **/etc/dhcpd.conf** استفاده می‌شود. **DHCP** از فایل **/var/lib/dhcp/dhcpd.leases** برای نگهداری اطلاعات تخصیص داده شده به سیستم‌ها استفاده می‌کند.

پیکربندی فایل DHCP

اولین قدم برای پیاده‌سازی سرویس دهنده **DHCP**، ایجاد فایلی برای نگهداری اطلاعات شبکه می‌باشد. پارامترها و گزینه‌های عمومی روی تمام سیستم‌ها اعمال می‌گردند و همچنین می‌توان برخی پارامترها را روی یک سیستم خاص اعمال نمود.

باید توجه داشت که عبارت‌ها و پارامترهای به کار رفته نسبت به بزرگی و کوچکی حروف غیر حساس بوده و گزینه‌هایی که با علامت # آغاز می‌شوند فقط برای توضیح مورد استفاده قرار می‌گیرند.

همچنین امکان به روز رسانی DNS از طریق DHCP وجود دارد. این کار به دو روش امکان پذیر است:

۱- به هنگام سازی DNS از طریق DHCP

۲- به هنگام سازی DNS از طریق Client

به هنگام سازی DNS از طریق سرویس گیرنده DNS (روش قدیمی) با اضافه کردن دستور زیر به فایل **dhcpcd.conf** انجام می‌شود:

```
ddns-update-style ad-hoc;
```

اما پیشنهاد می‌گردد که از روش دوم برای به هنگام سازی DNS استفاده گردد. برای استفاده از روش دوم از دستور زیر استفاده خواهد شد:

```
ddns-update-style interim;
```

جهت اعمال پیکربندی جدید در DHCP لازم است سرویس مجدداً اجرا شود.

```
service dhcp restart
```

در مثال زیر پارامترهای **Domain-Name-Server**، **Domain-Name**، **Subnet-Mask**، **Routers**

Time Offset روی تمام سیستم‌هایی که در محدوده تعیین شده قرار دارند، اعمال گردیده است.

```
subnet 192.168.1.0 netmask 255.255.255.0{
    option routers 192.168.1.254;
    option subnet-mask 255.255.255.0;
    option domain-name "Example.com";
    option domain-name-servers 192.168.1.1;
    option time-offset -18000; #Eastern Standard Time
range 192.168.1.10 192.168.1.100;}
```

در مثال فوق، دسته‌ای از پارامترهای عمومی برای تمام سیستم‌های شبکه در نظر گرفته شده است و هر سیستم یک IP در بازه تعیین شده دریافت می‌کند. تمام زیرشبکه‌هایی (Subnet) که از یک شبکه فیزیکی مشترک استفاده می‌کنند در قسمت **Shared-Network** قرار دارند. پارامترهایی که جزء **Shared-Network** هستند و خارج از قسمت تعریف پارامترهای Subnet بررسی می‌شوند، به عنوان پارامترهای عمومی در نظر گرفته می‌شوند. در ضمن نام در نظر گرفته شده برای **Shared-**

Network باید طوری انتخاب شود که بتواند شبکه را توصیف کند. در مثال زیر گزینه‌های عمومی برای دو قسمت (Subnet) شبکه مشخص شده است :

```
Shared-Network name{
    option domain-name          "Test.redhat.com";
    option domain-name-servers  ns1.redhat.com, ns2.redhat.com;
    option routers              192.168.1.254;
    # more Parameters for Example Shared-network
    subnet 192.168.1.0 netmask 255.255.255.0{
        # Parameters for Subnet
        range 192.166.1.1 192.168.1.31;
    }
    subnet 192.168.1.32 netmask 255.255.255.0{
        # Parameters for Subnet
        range 192.168.1.33 192.168.1.63;
    }
}
```

همان‌طور که در مثال زیر اشاره شده است، پارامترهای عمومی را می‌توان به گروهی خاص اختصاص داد. گروه‌های مختلفی از جمله Subnet, Hosts و... را می‌توان ایجاد کرد.

```
group {
    option routers          192.168.1.254;
    option subnet mask      255.255.255.0;
    option domain-name      "Example.com";
    option domain-name-server 192.168.1.1;
    option time-offset       18000;

    Host Apex {
        option host-name      "Apex.example.com";
        hardware ethernet     00:A0:78:8E:9E:AA;
        fixed-address          192.168.1.4;
    }

    Host Raleigh {
        option host-name      "Raleigh.example.com";
        hardware ethernet     00:A1:DD:74:C3:F2;
        fixed-address          192.168.1.6;
    }
}
```

جهت اختصاص IP به هر یک از سیستم‌های شبکه می‌توان تغییرات بعدی را با توجه به مقادیر دلخواه، روی فایل مربوطه اعمال نمود.

در پیکربندی زیر مدت زمان پیش فرض اختصاص IP، حداکثر زمانی که IP می‌تواند به سیستم اختصاص داده شود و تنظیمات و مقادیر آن، نشان داده شده است. در مثال زیر آدرس‌های IP در محدوده 192.168.1.10 تا 192.168.1.100 به سیستم‌های شبکه اختصاص داده می‌شود.

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
```

```
option broadcast-address 192.168.1.255;
option routers            192.168.1.254;
option domain-name-servers 192.168.1.1,192.168.1.2;
option domain-name        "example.com";
subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.10 192.168.1.100;
}
```

برای اختصاص IP براساس MAC آدرس کارت شبکه از پارامتر **Hardware Ethernet** استفاده می‌گردد. در مثال زیر سیستمی با نام **Apex** با MAC آدرس **00:A0:78:8E:9E:AA** همیشه آدرس **192.168.1.4** را دریافت می‌کند.

```
host apex {
    option host-name "apex.example.com";
    hardware ethernet 00:a0:78:8E:9E:AA;
    fixed-address 192.168.1.4; }
```

توجه: می‌توان جهت سهولت در تنظیم سرور از فایل پیکربندی **dhcpd.conf** موجود در **Red Linux 9 Hat** استفاده کرد و تغییرات مورد نظر را به آن اضافه نمود.

سرویس دهنده **DHCP** اطلاعات مربوط به سیستم‌ها را در مسیر **/var/lib/dhcp/dhcpd.leases** ذخیره می‌کند. این فایل نباید به صورت دستی تغییر کند.

اطلاعات **DHCP** مربوط به هر IP آدرس اختصاص داده شده در یک بانک اطلاعاتی ذخیره می‌گردد. این اطلاعات شامل مدت زمانی که آدرس IP به یک سیستم اختصاص داده می‌شود، زمان شروع و پایان اختصاص IP و آدرس MAC کارت شبکه جهت اختصاص مجدد IP می‌باشد. (تمام زمان‌های ذکر شده براساس زمان استاندارد بین المللی (گرینویچ) می‌باشد). بانک اطلاعاتی مربوط به هر IP اختصاص داده شده، هر چند وقت یکبار دوباره ایجاد می‌شود. در ابتدا اطلاعات در مکان موقت ذخیره می‌شود، سپس فایل **dhcp.leases** به فایل **~dhcpd.leases** تغییر نام پیدا می‌کند و اطلاعات درون فایل موقتی در فایل **dhcpd.leases** نوشته می‌شود.

سرویس دهنده **DHCP** ممکن است در هنگام تغییر نام بانک اطلاعاتی و تهیه نسخه پشتیبان (قبل از تهیه فایل جدید) دچار مشکل شده و به درستی عمل نکند. هنگامی که این اتفاق رخ می‌دهد فایل **dhcpd.conf** دیگر وجود ندارد و با راه اندازی مجدد سرویس نیز مشکل حل نخواهد شد. باید توجه داشت که هیچ فایل جدیدی به این نام به طور دستی نباید ایجاد شود. زیرا باعث از بین رفتن

اطلاعات قبلی خواهد شد. در صورت مواجهه با چنین مشکلی باید فایل `dhcpd.leases` را به `dhcpd.leases` تغییر نام داده و سرویس مجدداً راه اندازی شود.

فعال یا غیرفعال کردن سرویس DHCP

<code>/sbin/service dhcpd start</code>	برای فعال نمودن سرویس از این دستور استفاده می‌شود
<code>/sbin/service dhcpd stop</code>	برای غیرفعال نمودن سرویس از این دستور استفاده می‌شود

اگر سرور دارای دو یا تعداد بیشتری کارت شبکه بوده و ارائه سرویس DHCP فقط از طریق یکی از کارت‌های شبکه امکان پذیر باشد، در فایل `/etc/sysconfig/dhcpd` نام کارت شبکه‌ای که سرویس از طریق آن ارائه می‌گردد، قید می‌گردد:

DHCPDARGS = eth0

پیکربندی فوق در استفاده از سیستم فایروال مفید است. در این حالت سیستم فایروال دارای دوکارت شبکه می‌باشد. یکی از کارت‌های شبکه باید طوری پیکربندی شود که IP را از طریق Internet دریافت کند و کارت شبکه دیگر به سیستم‌های شبکه داخلی IP اختصاص می‌دهد. اختصاص یک کارت شبکه به شبکه داخلی باعث بالا رفتن امنیت شبکه می‌شود، زیرا مانع از برقراری ارتباط کاربران اینترنت با سرویس می‌شود.

تنظیماتی که می‌توان در فایل `/etc/sysconfig/dhcpd` اعمال نمود عبارت است از:

<Port Number> -P: شماره پورتی که DHCP درخواست‌ها را از آن دریافت می‌کند. پورت پیش فرض تعیین شده 67 می‌باشد. DHCP پاسخ درخواست‌ها را از طریق اولین پورت آزاد بعد از پورت دریافت کننده، ارسال می‌کند. به عنوان مثال اگر درخواست‌ها را از پورت 67 دریافت کند، جواب آن را روی پورت 68 ارسال می‌کند.

-f: سرویس را در پس زمینه اجرا می‌کند و معمولاً برای اشکال یابی استفاده می‌شود.

-d: برای گزارش گیری از مشکلات DHCP استفاده می‌شود. فایل گزارش (Log) در مسیر `/var/log/messages` قرار می‌گیرد.

-cf filename: مسیر فایل پیکربندی را مشخص می‌کند. مسیر `/etc/dhcpd.conf` به عنوان پیش فرض انتخاب شده است.

If FileName: مسیر فایل بانک اطلاعاتی را مشخص می‌کند. این فایل به طور پیش فرض در مسیر `/var/lib/dhcp/dhcpd.leases` قرار دارد.

-q: از نمایش پیام‌های مربوط به Copy Right در زمان اجرای سرویس، جلوگیری می‌نماید.

سرویس DHCP Relay Agent

DHCP Relay Agent ارسال درخواست‌های **DHCP** و **BOOTP** را از بخشی از شبکه ((subnet که سرویس دهنده **DHCP** ندارد به یک یا چند سرویس دهنده **DHCP** که در بخش‌های ((subnet دیگر مستقر هستند امکان پذیر می‌سازد. زمانی که **DHCP Client** اطلاعاتی را درخواست می‌کند، **DHCP Relay Agent** این درخواست‌ها را به یک دسته سرویس دهنده **DHCP** از قبل تعیین شده، ارسال می‌نماید. زمانی که **DHCP** سرور به این درخواست‌ها پاسخ می‌دهد، این پاسخ‌ها به کل شبکه یا دستگاه درخواست کننده ارسال می‌گردد. **DHCP Relay Agent** به تمام درخواست‌های **DHCP** ارسال شده به تمام کارت‌های شبکه به جز کارت‌های شبکه‌ای که در فایل `/etc/sysconfig/dhcrelay` ذکر شده اند، گوش می‌دهد. برای فعال کردن سرویس فوق از دستور زیر استفاده می‌شود:

```
service dhcrelay start
```

پیکربندی سرویس گیرنده DHCP در سیستم‌های درون شبکه

اولین قدم برای پیکربندی **DHCP Client**، اطمینان از نصب کارت‌های شبکه می‌باشد. اگر کارت شبکه بعد از راه اندازی سرور لینوکس نصب شود، برنامه **Kudzu** معمولاً آن را شناسایی می‌نماید ولی در برخی موارد باید مازول مربوط به آن را به صورت دستی تنظیم و پیکربندی کرد. در **URL** زیر به سخت‌افزارهایی که با **Linux Red hat** مطابقت و سازگاری دارند اشاره شده است:

<http://hardware.redhat.com/hcl/>

برای پیکربندی **DHCP Client** به صورت دستی، باید فایل `/etc/sysconfig/network` را برای فعال کردن شبکه و همچنین فایل مربوط به پیکربندی هر کارت شبکه را در مسیر `/etc/sysconfig/network-script` ویرایش کرد. اطلاعات زیادی در فایل `/etc/sysconfig/network` وجود دارد ولی برای فعال شدن شبکه دستور زیر را باید به این فایل اضافه نمود:

NETWORKING= Yes

برای هر کارت شبکه باید یک فایل پیکربندی به نام `ifctg-eth0` در مسیر زیر وجود داشته باشد:

`/etc/sysconfig/network-scripts`

در فایل `/etc/sysconfig/Network-script/ifctg-eth0` باید دستورات زیر را اضافه کرد:

(`eth0` نام کارت شبکه می‌باشد)

DEVICE = eth0

BOOTPROTO = dhcp

ONBOOT= Yes

برای پیکربندی کارت شبکه از طریق محیط گرافیکی از ابزار **Network Administer Tool**

استفاده می‌گردد.

وب سرور Apache

نرم‌افزار Apache سرویس وب را در محیط سیستم عامل لینوکس ارائه می‌دهد. این نرم‌افزار **Open Source** است و دارای تعدادی ماژول برای افزایش کارایی وب سرور می‌باشد. نرم‌افزار Apache از طریق بسته‌های نرم‌افزاری **RPM** و هم از طریق کد منبع آن (**Source Code**) نصب می‌شود. تمام تنظیمات سرور در فایل به نام **httpd.conf** صورت می‌گیرد که در مسیر زیر قرار دارد:

/etc/httpd/conf/httpd.conf

توجه: این مسیر با توجه به نسخه سیستم عامل لینوکس و نرم‌افزار Apache ممکن است متفاوت باشد.

تعدادی از ماژول‌های مهم و کاربردی Apache

ماژول	کاربرد
1-Mod-auth	جهت تعیین اعتبار کاربران.
2- Mod-front page	امکان استفاده از ویژگی Front Page Extension مایکروسافت را فراهم می‌کند.
3- Mod-include	جهت فیلتر کردن
4- Mod-perl	امکان استفاده از برنامه‌های Perl روی وب سرور را فراهم می‌کند.
5- Mod-php	امکان استفاده از برنامه‌های PHP را فراهم می‌کند.
6- Mod-ssl	امکان استفاده از ویژگی SSL را روی وب سرور فراهم می‌کند.
7- Mod-proxy	جهت کنترل دسترسی از طریق Proxy
8- Mod-cache	جهت استفاده از امکانات Caching
9- Mod-disk-cache	جهت استفاده از امکانات Caching
10- Mod-file-cache	جهت استفاده از امکانات Caching

نصب و راه اندازی Apache

۱- نصب از طریق کد منبع (Source Code)

دستور	عملیات
<code>gzip -d httpd-version.tar.gz</code>	خارج کردن از حالت فشرده.
<code>tar-xvf httpd-version.tar ./configure --prefix = PREFIX</code>	خارج کردن فایل‌ها از حالت آرشیو.
<code>make</code>	جهت کامپایل کردن.
<code>make install</code>	جهت نصب
<code>vi PREFIX/conf/httpd.conf</code>	جهت ویرایش فایل پیکربندی.
<code>PREFIX/bin/apachectl start</code>	جهت تست سرویس.

توجه: منظور از PREFIX مسیر نصب سرویس است که به صورت پیش فرض `/usr/local/apache` می‌باشد.

۲- نصب از طریق بسته نرم‌افزاری RPM

برای نصب از دستور زیر استفاده می‌شود:

```
rpm -Uvh apache-[^d]*.rpm
```

برای این‌که بتوان ماژول‌های مرتبط با Apache را نصب کرد باید ابتدا بسته RPM مربوط به آن

را نصب نمود.

```
rpm -Uvh apache-devel*.rpm
```

<code>start /etc/rc.d/init.d/httpd</code>	دستور فعال کردن سرویس apache
<code>stop /etc/rc.d/init.d/httpd</code>	دستور غیرفعال کردن سرویس apache
<code>restart /etc/rc.d/init.d/httpd</code>	دستور Restart کردن سرویس apache

تنظیمات پایه‌ای Apache

فایل‌های پیکربندی Apache در مسیر `/etc/httpd/conf` قرار دارند و شامل موارد زیر هستند:

- `access.conf`
- `httpd.conf`
- `srm.conf`

فایل اصلی پیکربندی سرور Apache فایل `httpd.conf` است که شامل سه بخش اصلی است:

- محیط عمومی Global Environment

این بخش شامل گزینه‌هایی برای پیکربندی سرور است و بر عملکرد کلی سرور تاثیر می‌گذارد که شامل موارد زیر می‌باشد:

- نوع پیکربندی سرور که می‌تواند `stand-alone` یا `intend` انتخاب شود.
- اسم و محل ماژول‌های Apache.

- پیکربندی سرور اصلی Main Server Configuration

این قسمت شامل دستورات و گزینه‌هایی است که بر عملکرد سرور و تنظیمات اصلی آن تاثیر می‌گذارد. پیکربندی اولیه شامل موارد زیر می‌باشد:

- نام میزبان، سرور.
- شماره پورتی که سرور درخواست‌ها را دریافت می‌کند.
- کاربر و گروهی که سرور را راه اندازی می‌کند
- نوع گزارش گیری که براساس IP یا اسم میزبان می‌باشد
- محل دایرکتوری اصلی Apache.
- محل اسکرپت‌های CGI.

- پیکربندی مجازی میزبان Virtual Host Configuration

یکی از ویژگی‌های مهم سرور Apache استفاده از میزبان مجازی (Virtual Hosting) است. این ویژگی به وب سرور اجازه می‌دهد تا چند آدرس IP یا `Hostname` داشته باشد. به عنوان مثال سرور Apache می‌تواند طوری تنظیم شود که به پرس و جوهای که به آدرس‌های www.example1.com و www.example2.com ارسال می‌شوند پاسخ دهد. در واقع این ویژگی این امکان را فراهم می‌کند که دو یا چند وب سایت از یک وب سرور مشترک استفاده کنند. برای تنظیم این ویژگی روی Apache باید گزینه‌های زیر را تنظیم کرد:

- آدرس IP میزبان‌های مجازی (Virtual Host).
- آدرس پست الکترونیکی (E-Mail) مدیر هر میزبان مجازی.
- نام و مسیر فایل‌های گزارش مربوط به هر میزبان مجازی.
- محل قرارگرفتن دایرکتوری اصلی و دایرکتوری برنامه‌های CGI مربوط به هر میزبان مجازی.

پیکربندی اصلی Apache

پارامترهای پیکربندی اصلی در جدول زیر درج شده است.

عملکرد	پارامتر
شماره پورتهای که سرور از طریق آن به درخواست‌ها پاسخ می‌دهد.	Port
نام سرور Apache (به عنوان مثال www.test.com)	Server Name
تعیین محل قرارگیری دایرکتوری اصلی وب سایت	Document Root
Index وب سایت	Directory Index

جهت اعمال برخی از تنظیمات به قسمتی از سرور می‌توان محدودده آن تنظیمات را با استفاده از

گزینه‌ها و دستورات جدول زیر مشخص کرد:

عملکرد	قالب
اعمال دستورات به یک دایرکتوری خاص	<code><Directory>...</Directory></code>
اعمال دستورات به یک فایل مشخص	<code><Files>...</Files></code>
اعمال دستورات به محتویات وب	<code><Location>...</Location></code>
اعمال دستورات به یک میزبان مجازی مشخص	<code><Virtual Host>...</Virtual Host></code>

برای تنظیم مجوزهای دسترسی دایرکتوری‌ها و فایل‌ها می‌توان از دستورات زیر استفاده کرد:

`<Directory Directory-Name>`

`Options Indexes FollowSymLinks ExecCGI Includes`

`Allow Override All`

`Order allow, deny`

`Allow from all`

`</Directory>`

جهت تنظیم مجوزهای دسترسی به فایل‌های خاص از دستورات زیر استفاده می‌شود:

`<Files "*.inc">`

`Order allow, deny`

`deny from all`

`</Files>`

`<Files "*.conf">`

`Order allow, deny`

`Deny from all`

`</Files>`

دستورات زیر جهت تنظیم Virtual Host ها مورد استفاده قرار می‌گیرند:

```
<Virtual Host    Server_IP>
Document Root  /www/docs/ root directory
Server Name     www.example.com
Error Log       /logs/root directory
</Virtual Host >
```

افزودن ماژول‌ها به Apache

برای این که Apache بتواند از امکانات و ویژگی‌های بیشتری بهره‌برد، باید ماژول‌های مورد نیاز را نصب کرد. اگر سرور Apache طوری کامپایل شده باشد که اجازه بارگذاری ماژول‌ها به صورت اتوماتیک را بدهد، در آن صورت می‌توان ماژول‌ها را به صورت جداگانه کامپایل کرد و با استفاده از دستور زیر آن را برای استفاده Apache بارگذاری (Load) کرد:

```
Load Module <Mod_name> <Mod_pass>
```

در غیر این صورت باید برای حذف یا اضافه کردن ماژول‌ها، Apache را مجدداً کامپایل کرد. هنگام حذف یا اضافه کردن ماژول‌ها باید سرویس httpd راه اندازی مجدد شود.

تنظیمات شرطی در Apache

به طور کلی در Apache دو دسته تنظیم وجود دارد. یکی دستوراتی که به تمام درخواست‌ها اعمال می‌شوند و دسته دوم دستوراتی که شرطی هستند و در صورت مطابقت درخواست‌ها با شرط تعیین شده اعمال می‌شوند.

```
< If Define condition >
```

دستورات

```
< /IfDefine >
```

در دستور بالا اگر شرط مورد آزمایش در خط فرمان httpd برقرار باشد، تنظیمات و دستورات درون تگ‌های < If Define >, < /If Define > به درخواست‌ها اعمال می‌شوند.

```
<If Module Module_name>
```

دستورات

```
< /If Module >
```

با استفاده از فرمان‌های فوق در صورتی که ماژول مشخص شده روی سرور نصب و فعال باشد، تنظیمات مشخص شده بین تگ‌های <If Module>, < /If Module> اعمال می‌شوند.

```
<FilesMatch condition>
```

دستورات

```
< /FilesMatch >
```

با استفاده از تنظیم بالا می‌توان دسترسی به انواع فایل‌ها مانند انواع فایل‌های گرافیکی و .. را کنترل کرد.

<DirectoryMatch condition>

دستورات

</DirectoryMatch >

دستور فوق عملکردی شبیه دستور قبلی برای دایرکتوری‌ها دارد.

تنظیمات مربوط به محدودیت استفاده از منابع سیستم

این مجموعه دستورات برای کنترل منابعی که سرور در پذیرش درخواست‌ها مورد استفاده قرار می‌دهد به کار می‌روند:

Limit Request Body
Limit Request Fields
Limit Request Fields Size
Limit Request Line

دستورهای مربوط به کنترل دسترسی

با استفاده از این دستورها می‌توان دسترسی به یک قسمت خاص از سرور مانند یک فایل یا دایرکتوری را کنترل و دسترسی را براساس آدرس IP، نام یا سایر مشخصات سیستم درخواست کننده، بررسی و کنترل کرد.

- **Allow from Host | IPAddress**
- **Deny from Host | IPAddress**
- **Order**

دستورهای مربوط به اجرای اسکریپت‌ها

- **Action** : دستور **Action** امکان اجرای اسکریپت‌های CGI را در زمان درخواست یک نوع فایل خاص فراهم می‌کند.
- **Script** - : دستور **Script** نیز امکان اجرای اسکریپت‌های CGI، هنگامی که از یک متد خاص در درخواستی استفاده شود را فراهم می‌کند.

دستورهای مربوط به دسترسی به فایل‌های خارج از دایرکتوری ریشه وب

از این دستورها برای نگاشت (Map) بین URLها و مسیرهای فیزیکی استفاده می‌شود و به کمک آنها می‌توان به فایل‌هایی که در خارج از دایرکتوری اصلی وب سایت هستند دسترسی پیدا کرد.

- **Alias**
- **Alias Match**
- **Redirect**
- **Redirect Match**
- **Redirect Permanent**
- **Redirect Temp**
- **Script Alias**
- **Script Alias Match**

دستورهای مربوط به تعیین اعتبار کاربران

با استفاده از این دستورها می‌توان دسترسی به سرور را به دسته‌ای از کاربران تعیین شده محدود کرد. لیست کاربران و گروه‌های مجاز، درون فایل‌های متنی که مسیر آن‌ها در دستورات مربوط مشخص شده است، تعیین می‌گردد.

- **Authoritative On/Off**
- **Auth Group File file-path**
- **Auth User File file-path**

فایل مربوط به لیست کاربران شامل نام کاربر و کلمه عبور آن‌ها است.

با استفاده از دستور زیر می‌توان این فایل را ایجاد کرد:

```
#htpasswd -c file-name user-name
```

نکته: این فایل نباید درون دایرکتوری اصلی وب قرار گیرد.

دستورهای مربوط به Cache کردن محتویات وب

با استفاده از این دستورها می‌توان محتویات محلی وب یا پراکسی شده را Cache کرد. دو ماثول مرتبط با این دستورات عبارت‌اند از:

- **Mod-disk-cache**
- **Mod-mem-cache**

توجه: محتویات حفاظت شده قابل Cache نیستند.

دستورهای مهم این قسمت عبارت است از:

- **Cache Size**
- **Cache Root**
- **Cache Default Expire**
- **Cache Disable**
- **Cache Enable**
- **Cache Max Expire**
- **Cache Max File Size**
- **Cache Min File Size**

تنظیم و پیکربندی وب سرور امن (SSL)

سرور Apache به صورت پیش فرض، در حالت غیرامن پیکربندی می‌شود. اگر وب سرور در حالت امن تنظیم و پیکربندی شود، روی پورت 443 به درخواست‌ها گوش می‌دهد. در حالت پیش فرض دایرکتوری ریشه یک وب سایت چه در حالت امن و چه در حالت غیرامن یکسان است ولی توصیه می‌شود، که برای هر حالت، دایرکتوری جداگانه در نظر گرفته شود. برای غیرفعال کردن وب سرور در حالت غیرامن، باید گزینه مربوط به پورت 80 با استفاده از کاراکتر # (قبل از دستور مربوطه) غیرفعال شود.

سرویس BIND

در این متن نحوه راه اندازی و پیکربندی سرویس BIND شرح داده می‌شود. سرویس BIND وظیفه تبدیل IP به نام و نام به IP را بر عهده دارد. راه اندازی BIND به دو طریق امکان پذیر است:

۱- از طریق گرافیکی

۲- از طریق Command

در محیط گرافیکی ابزار BIND Configuration، پیکربندی BIND را به عهده دارد.

پیکربندی BIND از طریق محیط Command، با اعمال تنظیمات در فایل named.conf واقع

در مسیر /etc/named.conf و فایل‌های موجود در مسیر /var/named انجام می‌پذیرد. فایل

/etc/named.conf شامل تنظیمات مربوط به Zone ها و دایرکتوری /var/named شامل

فایل‌های مربوط به Zone ها می‌باشد.

دو نوع پیکربندی برای BIND موجود است:

- ایجاد سرور DNS ای که فقط عمل Caching را انجام می‌دهد.

- ایجاد سرور معمولی DNS.

سرور DNS ای که فقط عمل Caching را انجام می‌دهد، بازدهی کاربرانی که با سرعت پایین به

اینترنت متصل می‌شوند را بالا می‌برد. این نوع سرویس دهنده DNS برای تبدیل نام به IP یا بالعکس

از DNS سرورهای معمولی استفاده می‌کند ولی نتیجه این تبدیل را نگهداری می‌کند تا در مراجعات

بعدی از آن استفاده شود و نیازی به اتصال مجدد به سرور DNS معمولی نباشد.

انواع سرویس دهنده‌های نام

چهار نوع مختلف پیکر بندی برای سرویس دهنده‌های نام وجود دارد که عبارت‌اند از :

۱- master : رکوردهای اصلی برای یک یا چند دامنه مشخص را شامل می‌شود.

۲- slave : شامل رکوردهای دریافتی از سرور اصلی ((master است و به عنوان سرور پشتیبان

مورد استفاده قرار می‌گیرد.

۳- caching-only : در این پیکر بندی سرور شامل هیچ zone نیست و تنها پاسخ پرس و

جوها را برای استفاده‌های بعدی و بالا بردن سرعت پاسخ گویی به درخواست‌ها ذخیره می‌کند.

۴- forwarding : در این پیکر بندی درخواست‌ها برای لیستی از سرویس دهنده‌های نام ارسال

می‌شود.

نصب BIND از طریق بسته RPM

برای نصب سرویس BIND پس از قرار گرفتن در مسیر **rpm BIND** دستور زیر اجرا می‌شود:

```
rpm -Uvh bind-*.rpm
```

برای نصب سرویس BIND که فقط عمل **Caching** را انجام می‌دهد، دستور زیر اجرا می‌شود:

```
rpm -Uvh caching -name -server-*.rpm
```

نصب BIND از طریق کد منبع (Source Code)

```
tar -zxvf .bind-version.tar.gz
./Configure --Prefix = PREFIX
make
make Install
```

بسته‌های BIND

bind: بسته اولیه که شامل فایل‌های پیکربندی و مجموعه‌ای از اطلاعات، در ارتباط با **BIND**

می‌باشد

bind-util: ابزاری برای پرس و جو **DNS** سرورها

bind-conf: شامل ابزارهایی برای پیکربندی **DNS**

Caching-name Server: **BIND** را فقط به صورت یک **Caching Server** نصب می‌کند. فایل‌های

مهمی که توسط این بسته ایجاد می‌شوند به شرح زیر است:

نام فایل	عملکرد
/var/named/local host.zone	یک Forward Zone برای دستگاه محلی.
/var/named/named.ca	یک فایل Hint که شامل نام سرورهای اصلی DNS کره زمین می‌باشد.
/var/named/named.Local	یک Reverse Zone برای دستگاه‌های محلی

Open SSL: برای اعمال امنیت در **BIND** مورد استفاده قرار می‌گیرد. پورت‌هایی که **BIND** از

آنها استفاده می‌کند به شرح زیر است:

UDP 53: برای پرس و جوهای **DNS**.

TCP 53: برای عملیات **Zone Transfer** و پرس و جوهای **DNS** که اندازه آنها بیش از **512**

بایت باشد.

پیکربندی فایل /etc/named.conf

فایل `/etc/named.conf` zone ها، کنترل دسترسی‌ها و تنظیمات مربوط به سرور را مشخص می‌کند. نمونه این پیکربندی به شرح زیر می‌باشد:

عملکرد	پارامتر
مسیری که فایل‌های مربوط به تنظیم سرور در آن قرار دارد.	<code>option{directory "var / named";</code>
مشخص کننده سیستم‌هایی است که می‌توانند از این DNS سرور پرس و جو کنند.	<code>allow-query {any};</code>
تعیین کننده سیستم‌هایی است که می‌توانند در عملیات Zone Transfer شرکت کنند	<code>allow- transfer {192.168.1.0/24};</code>
امکان پرس و جو را از طریق بازگشتی (Recursion) میسر می‌کند.	<code>recursion yes; allow – recursion {192.168.1.0/24}</code>

نکته : Hint یک نوع zone است که شامل سرورهای اصلی DNS کره زمین می‌باشد.

```
zone "." IN{
    type hint ;
    File "named.ca";
};
zone " local host " IN {
    type master;
    file " localhost.zone " ;
    allow – update {none;} ;
}
zone "XYZ.com" IN{
    type master           مشخص کننده یک Master Zone می‌باشد
    file "db.XYZ.com";    اطلاعات مربوط به Zone در این فایل قرار دارد.
    allow – update {none;} ;
};
zone "somedomain.Gm" IN {
    type slave,           مشخص کننده یک Slave Zone می‌باشد
    File "ab. some domain.com";
};
```

دستور اخیر گزینه دلخواه برای Slave Zone می‌باشد که در صورت انتخاب این گزینه یک نسخه

کپی از اطلاعات Master Zone در مسیر `/var/named` ایجاد می‌گردد.

دستور: `include "/etc/rndc : key"` یک کلید خصوصی برای مدیریت امن از راه دور ایجاد

می‌کند.

Name سرورهایی که فقط عمل **Caching** را انجام می‌دهند برای هیچ کدام از **Zone**ها شناخته شده نیستند. این **Name** سرورها از سرورهای **DNS** اصلی یا یک سرور **DNS** شناخته شده به عنوان **Forward** کننده پرس و جویهای **DNS** استفاده می‌کنند. با اضافه کردن دستور زیر سرور **DNS** عمل **Forwarding** را نیز انجام می‌دهد.

```
forward {192.168.1.20;};
```

معرفی Zone ها

Master Zone - ۱

هر **Domain** دارای یک **Master Zone** می‌باشد، که شامل رکوردهای اطلاعاتی در مورد آن دامنه خواهد بود. نمونه پیکربندی یک **Master Zone** به شرح زیر است:

```
zone "somedomain.com" {
    type master;
    file "db.somedomain.com";
    allow-transfer {192.168.3.4;};
};
```

Slave Zone - ۲

این **Zone** به عنوان یک سرویس پشتیبانی (**Backup**) برای **Master Zone** به شمار می‌رود و در صورت بروز اشکال در **Master Zone** به صورت پشتیبان وارد عمل می‌شود. به عنوان مثال:

```
zone "somedomain.com" {
    type slave,
    masters {192.168.1.50};
    file "db.somedomain.com";
};
```

تعیین کننده سرور اصلی **DNS**

گزینه آخر ضروری نمی‌باشد و به نام فایل محلی که اطلاعات **Zone** در آن قرار دارد، اشاره می‌کند. زمانی که سرور **Slave** شروع به فعالیت می‌کند، شماره سریال خود را با سرور اصلی **DNS** چک می‌کند. اگر اطلاعات آن به هنگام شده باشد، آخرین اطلاعات را از آن دریافت می‌نماید. اگر سرور اصلی **DNS**، به هنگام نشده باشد، **Zone** پشتیبان از اطلاعات دیسک محلی خود استفاده کرده و باعث کاهش ترافیک شبکه می‌گردد. سرور پشتیبان **DNS** باید برای انتقال **Zone**ها از سرور اصلی **DNS** مجوز داشته باشد.

```
option {
    .....
    allow-transfer {192.168.1.5;};
    .....
};
```

Reverse Zone-۳

برای تبدیل IP به اسم به کار می‌رود. در **Reverse Zone** ها از دامنه **In-addr.arpa**. استفاده می‌شود. اسم **Zone** با عکس کردن آدرس شبکه و اضافه کردن عبارت **In-addr.arpa**. به انتهای آن به دست می‌آید. به عنوان مثال:

```
zone "1.168.192.In-addr.arpa"{
    type master;
    file "db.1.168.192-In-add.arpa" ;
};
```

Root Zone -۴

یک **Zone** از نوع **Hint** است که شامل سرورهای اصلی **DNS** در سطح دنیا می‌باشد.

```
zone "." {
    type hint;
    file "named.ca";      شامل سرورهای اصلی DNS
}
```

زمانی **Root Zone** به کار می‌رود که پرس و جوها توسط هیچ **Zone** دیگری جواب داده نشود.

اعطای مجوز برای مدیریت Zone

با اعطای این مجوز، می‌توان دامنه‌های بزرگ را به دامنه‌های کوچک‌تر تقسیم کرد و با این روش، مدیریت آن‌ها آسان‌تر می‌شود. به عنوان مثال کنترل سایت‌های:

support.somedomain.com و *development.somedomain.com*

را می‌توان به شخص دیگری واگذار کرد تا مدیریت *somedomain.com* آسان‌تر شود. به این منظور تنظیمات زیر اعمال می‌شود:

```
support.somedomain.com IN NS ns.support.somedomain.com
ns.support IN A 192.168.44.10
development.somedomain.com IN NS ns.development.somedomain.com.
ns.development IN A 192.168.45.10
```

استفاده از رکوردهای **NS** و **A** برای اعطای مجوز به افراد لازم است. این رکوردها به

رکوردهای چسبان (**glue** معروف می‌باشند که پرس و جوها را از یک **Name Server** به **Name Server** دیگر ارجاع می‌دهند).

رکوردهای اصلی (Resource Record)

قالب کلی رکوردها به صورت زیر است:

[domain/@] [ttl] [class] <type> <rdata> [comment]

پارامتر	عملکرد
domain	یک گزینه دلخواه که اگر مقداری برای آن در نظر گرفته نشود به صورت پیش فرض، مقدار آخرین رکورد اصلی را به خود اختصاص می‌دهد.
ttl	مشخص کننده مدت زمانی است که یک رکورد Cache می‌شود.
class	مقدار پیش فرض این گزینه دلخواه، IN می‌باشد.
type	تعیین کننده نوع رکورد است.
rdata	تعیین کننده اطلاعات وابسته به رکورد می‌باشد.
comment	توضیحات در مورد رکورد.

محدودیت کاراکترها: نام میزبان باید شامل حروف A-Z و اعداد 0-9 باشد.

۱- (SOA) Start of Authority

هر Zone باید فقط و فقط یک SOA داشته باشد. به عنوان مثال:

```
@ 1 D      IN      SOA      ns      root (
2002011201      ;Serial
3H          ;Refresh
15M        ;Retry
1W         ; expire
1D)        ;Minimum
```

Serial: برای کنترل شماره نسخه به کار می‌رود و با هر تغییر در zone، این مقدار تغییر می‌کند.

Refresh: تعیین می‌کند که سرور پشتیبان DNS باید بعد از چه مدت زمانی، Serial را چک کند.

Retry: مدت زمانی که سرور پشتیبان DNS باید منتظر بماند تا مجدداً با سرور اصلی DNS ارتباط برقرار کند. باید توجه داشت که این ارتباط مجدد، بعد از یک ارتباط ناموفق صورت می‌گیرد.

Expire: مدت زمانی که DNS Server می‌تواند بدون بازخوانی (Refresh)، از اطلاعات سرور اصلی DNS استفاده کند.

Minimum: مدت زمانی که سرور می‌بایست گزینه‌های بی مصرف را نگهداری کند.

۲- NS (Name Server)

هر Zone باید حداقل یک Name Server اصلی داشته باشد.

@ IN	NS	ns1.Somewhere.com.
somewhere.com	IN	NS ns2.Somewhere.com.
	IN	NS ns3.Somewhere.com.

هر سه خط بالا مربوط به Name Server های یک دامنه می‌باشد.

۳- (A) Address

تبدیل نام به IP را به عهده دارد و برای فرآیند پرس و جو از آن استفاده می‌شود.

ns1.somewhere.com	IN	A	192.168.20.10
www		IN	A 192.168.20.11

۴- CNAME

برای استفاده از چند نام به وسیله یک IP استفاده می‌گردد.

pop IN	CNAME mail
imap	IN CNAME mail

در مثال بالا pop و imap هر دو به رکورد A، "mail" اشاره می‌کنند.

۵- (MX (Mail Exchange

این پارامتر آدرس Mail سرور مربوط به دامنه را مشخص می‌کند. این رکورد به عنوان Revers

Zone عمل نمی‌کند. برای این نوع رکورد می‌توان اولویت تعیین کرد.

E-Mail سرورها با توجه به اولویت تعیین شده به درخواست‌ها پاسخ می‌دهند. عدد کوچکتر

نشان دهنده اولویت بالاتر است.

@	IN	MX	5	mail1.somewhere.com	بالاترین اولویت
	IN	MX	10	mail2.somewhere.com	
	IN	MX	15	mail3.somewhere.com	پایین ترین اولویت

سرویس NFS

سرویس NFS برای به اشتراک گذاشتن فایل‌ها بین کاربران شبکه طراحی شده است. به عنوان مثال گروهی از کاربران که روی پروژه مشابه کار می‌کنند، برای دسترسی به فایل‌های پروژه از پوشه مشترک که توسط NFS به اشتراک گذاشته شده است، استفاده می‌کنند. همچنین برای به اشتراک گذاشتن فایل بین Linux و ویندوز از Samba استفاده می‌شود که در ادامه شرح داده خواهد شد.

نصب NFS

همراه با سرویس NFS، سه سرویس دیگر نیز اجرا می‌گردد:

Portmap: برای ارجاع درخواست‌های سیستم‌ها به یک پروسه صحیح NFS.

rpc.nfsd: برای تبدیل درخواست‌های دسترسی از راه دور به درخواست‌های دسترسی محلی.

Rpc.mountd: Mount و UMount فایل سیستم‌ها را انجام می‌دهد.

در صورت نصب سرویس‌های NFS Server و NFS Client هر سه سرویس بالا اجرا می‌گردد.

برای نصب NFS، باید در مسیر فایل RPM NFS قرار گرفته و دستور زیر را اجرا کرد:

```
rpm -Uvh nfs-utils-*.rpm
rpm -Uvh portmap-*.rpm
```

برای اطمینان از نصب بسته‌های NFS از دستور زیر استفاده می‌شود:

```
rpm -qa | grep nfs
redhat-config-nfs-1.1.3-1
rpm -qa | grep portmap
portmap-4.0-57
```

برای اجرای سرویس NFS در زمان Boot از دستور chkconfig استفاده می‌شود. در ضمن برای

کاهش میزان خطر خرابی اطلاعات، می‌توان سرویس NFS File Locking را نیز فعال نمود.

```
chkconfig -- level 35 nfs on
chkconfig -- level 35 nfslock on
chkconfig -- level 35 portmap on
```

فعال و غیرفعال کردن سرویس‌ها

برای فعال یا غیرفعال کردن سرویس‌های NFS از دستورات زیر استفاده می‌شود:

```
/etc/init.d/portmap start
/etc/init.d/portmap stop
/etc/init.d/portmap restart

/etc/init.d/nfs start
```

```
/etc/init.d/nfs stop
```

```
/etc/init.d/nfs restart
```

```
/etc/init.d/nfslock start
```

```
/etc/init.d/nfslock stop
```

```
/etc/init.d/nfslock restart
```

برای اطمینان از نصب کامل و درست NFS از دستور **rpcinfo** استفاده می‌شود. این دستور لیست برنامه‌های **RPC** که در حال اجرا هستند را نشان می‌دهد. این برنامه‌ها شامل **mountd**، **Portmapper** و **nfs** و **nlockmgr** می‌باشد.

```
rpcinfo -p local host
```

```
100000      2      tcp  111  portmapper
100000      2      udp  111  portmapper
100003      2      udp 2649  nfs
100021      1      udp 2049  nfs
```

پیکربندی سرور

فایل پیکربندی سرور در مسیر **/etc/exports** قرار دارد. هر خط از این پیکربندی دایرکتوری‌های مشترک و مجوزهای دسترسی اختصاص داده شده را معین می‌کند. فرم کلی این فایل عبارت است از:

Path host-list (option)

Path مسیر پوشه و فایل‌های مشترک و **host list** میزبانی که می‌توانند به فایل‌های مشترک دسترسی پیدا کنند را مشخص می‌کند.

در فایل **Exports**، کلید **Option** می‌تواند یکی از مقادیر **Sync** یا **ASync** را انتخاب کند. با انتخاب گزینه **Sync**، سرور به هیچ درخواستی تا زمانی که تغییرات درخواست شده قبلی، روی دیسک اعمال نشود، پاسخ نمی‌دهد. به عنوان مثال :

```
/data/files company.example.com (sync)
```

کاربران **company.example.com** اجازه نصب (**Mount**) با مجوز فقط خواندن را دارند و درمثال

```
/data/files company.example.com (rw,sync)
```

کاربران مجوز خواندن و نوشتن را دارند. همچنین

باید هر میزبان با یک فاصله از میزبان دیگر جدا شود.

میزبان‌هایی که اجازه دسترسی به فایل‌های مشترک را دارند، به روش‌های مختلفی مشخص

می‌شوند که عبارت است از:

- ۱- استفاده از اسم میزبان، اگر میزبان عضو یک دامنه باشد.
 - ۲- استفاده از اسم کامل دامنه .
 - ۳- استفاده از میزبان همراه با (* Wild Card).
 - ۴- استفاده از IP آدرس .
 - ۵- استفاده از IP آدرس شبکه مانند 192.168.1.0/255.255.255.0
- منظور از Wild Card انطباق پیشوندهای مختلف یک میزبان می‌باشد.
- به عنوان مثال میزبان *.company.net :
- با www.company.net منطبق می‌باشد
- و با www.company.com منطبق نیست.
- از Wild Card برای انطباق قسمتی از پیشوند نیز استفاده می‌شود. به عنوان مثال
- ma*.company.com با mail.company.com مطابقت دارد.
- به طور پیش فرض سیستم‌ها فقط مجوز خواندن فایل‌های مشترک را دارند و برای اعطای مجوز خواندن و نوشتن، در ادامه اسم میزبان از عبارت rw استفاده می‌گردد.
- | | |
|----------------|------------------------|
| /data/database | company1.mail.com (rw) |
| /data/database | company2.mail.com (ro) |
- درمثال فوق میزبان company1 مجوز خواندن و نوشتن و میزبان company2 مجوز فقط خواندن را دارد. توجه شود که بین مجوزها و اسم میزبان فاصله‌ای نباشد.
- هر سیستمی که به عنوان root به سرور متصل (Login) گردد، مجوزهای دسترسی به فایل‌های Share را ندارد. برای اعطای مجوز دسترسی root باید گزینه No-Root-Squash را مطابق شکل زیر اعمال نمود:
- /data/database company.mail.com (rw,no-root-squash)
- فایل /etc/exports را به سادگی می‌توان به صورت دستی ویرایش نمود.
- توجه: گزینه root-squash حقوق کاربر root را به حقوق کاربر معمولی روی سیستم محلی کاهش می‌دهد.

پیگر بندی ایستگاه‌های سرویس گیرنده

ایستگاه‌های سرویس گیرنده با فایل‌های به اشتراک گذاشته شده (Share) مانند فایل‌های محلی برخورد می‌کنند. برای دسترسی (Mount) به مسیرهای به اشتراک گذاشته شده از دستور زیر استفاده می‌شود:

```
mount -t nfs Server:/data/database/mnt/database
```

با اجرای دستور فوق، مسیر `/data/database` از طریق میزبان `Server` در مسیر `/mnt/database` ذخیره می‌گردد. منظور از `Server` ها، سرور `NFS` می‌باشد که پوشه‌های به اشتراک گذاشته شده در آن تعریف شده‌اند.

با اعمال تغییرات زیر در فایل `/etc/fstab` دسترسی به مسیرهای مشترک (`Share`) به طور اتوماتیک و بدون استفاده از دستور `mount` انجام می‌شود.

```
Server: /data/database /mnt/database nfs default 0 0
```

گزینه‌های مختلف `Mount`، اجازه کنترل عملکرد فایل‌های به اشتراک گذاشته شده `NFS` را می‌دهد. برخی از این گزینه‌ها عبارت است از:

intr: اجازه قطع درخواست‌های `NFS` را در صورت در دسترس نبودن سرور فراهم می‌کند.
noexec: این گزینه اجازه اجرای دستورات و برنامه‌های اجرایی را نمی‌دهد و در مواردی مفید است که سیستم فایل سیستمی غیر از لینوکس را که حاوی فایل‌های اجرایی ناسازگار با لینوکس است، `mount` می‌کند.

hard or soft: تعیین می‌کند که آیا برنامه‌ای که از یک سیستم فایل `NFS` برای دسترسی به یک فایل استفاده می‌کند، در صورت قطع ارتباط با سرور `NFS` باید منتظر برقراری مجدد ارتباط باشد (`hard`) یا باید یک خطا را گزارش کند (`soft`).

نکته ۱: سرویس `nfsLock` سرویس `File Locking` را فعال می‌کند. در صورت نیاز به قفل کردن فایل‌ها باید سرویس `nfsLock` را فعال نمود.

نکته ۲: اسکریپت `autofs` امکان پیکربندی فرآیند `mount` کردن فایل‌های به اشتراک گذاشته شده به صورت اتوماتیک را فراهم می‌کند. این اسکریپت در مسیر `/etc/rc.d/init.d` قرار دارد. با استفاده از دستور زیر می‌توان این سرویس را اجرا کرد:

```
/sbin/service autofs start
```

مدیریت NFS

اسکریپت‌های اصلی مدیریت `NFS` عبارت‌اند از:

```
/etc/rc.d/init.d/portmap
```

```
/etc/rc.d/init.d/nfs
```

با اعمال این اسکریپت‌ها و استفاده از پارامترهای مناسب می‌توان عملکرد سرور `NFS` را کنترل نمود.

کنترل عملکرد سرور NFS

دستور **Exportfs** کنترل عملکرد سرور **NFS** را ممکن می‌سازد. در جدول زیر عملکردهای این

دستور شرح داده شده‌اند.

عملکرد	دستور
لیست پوشه‌های به اشتراک گذاشته شده (share) و گزینه‌های اختصاص داده شده را مشخص می‌کند.	Exportfs -v
به اشتراک گذاشتن فایل‌های مشخص را امکان پذیر می‌سازد. این گزینه برای ایجاد فایل exports جدید کاربرد دارد.	Exportfs -a share
به کاربران اجازه می‌دهد تا دایرکتوری‌های لیست نشده در فایل /etc/exports را، به اشتراک گذارند.	exportfs
عدم ارسال فایل‌های به اشتراک گذاشته شده معین	exportfs -u share
عدم ارسال تمام فایل‌های مشترک در مسیر /etc/exports	exportfs -ua
بازآرایی (Refresh) لیست فایل‌های به اشتراک گذاشته شده، این گزینه برای اعمال تغییرات در فایل exports به کار می‌رود.	exports -r

توجه: بعد از هر تغییر در فایل **/etc/exports** باید یکبار دستور **exports -r** را اجرا کرد.

برای کنترل وضعیت سرویس **NFS** از روی سرور میزبان از دستورهای زیر استفاده می‌شود:

```
/etc/rc.d/init.d/nfs status
/etc/rc.d/init.d/portmapstatus
```

برای کنترل سرور **NFS** از راه دور، از دستور زیر استفاده می‌شود:

```
rpcinfo -p Server-name
```

که در آن گزینه **Server**، نام سرور **NFS** را مشخص می‌کند. برای مشاهده لیست فایل‌های به

اشتراک گذاشته شده (**Share Exports**) از دستور زیر استفاده می‌شود:

```
show mount -e Server-name
```

گزارش گیری

NFS پیام‌ها را در مسیر **/var/log/messages** نگهداری می‌کند. در صورت عملکرد اشتباه **NFS**،

می‌توان با کنترل این پیام‌ها، دلیل آن را مشخص کرد.

نکات امنیتی:

سرویس‌های **NFS** و **Portmap** دارای مشکلات امنیتی هستند. پیشنهاد می‌شود از این سرویس‌ها

در شبکه‌های ناامن استفاده نگردد. در ضمن اطلاعات انتقال داده شده رمزنگاری نمی‌گردد.

مشکل NFS Hanging :

اکثر انتقالات در NFS از طریق پروتکل UDP انجام می‌شود که توانایی نگهداری مستندات اتصال (Connection) را ندارد اگر سرور NFS از بین برود، دستگاه سرویس گیرنده تا مدتی از به وجود آمدن مشکل، مطلع نمی‌شود.

در صورت به وجود آمدن چنین مشکلی، سرویس گیرنده مدت زیادی، برای دریافت مجدد سرویس از سرور قبلی، منتظر می‌ماند. به همین دلیل، پیشنهاد می‌گردد از گزینه Soft در `/etc/fstab` جهت اعلام I/O Error، بعد از گذشت زمان طولانی از قطع ارتباط استفاده شود. برای کاهش NFS Hanging باید موارد زیر رعایت شود:

- ۱- اجرای NFS در یک شبکه مطمئن.
- ۲- استفاده از گزینه Sync.
- ۳- منابع بحرانی سرور نباید با NFS در ارتباط باشند. (مانند فایل‌های مهم سیستمی).

سرویس مدیریت از راه دور با استفاده از SSH

هر مدیر سیستم که عهده دار دو یا چند سرویس دهنده شبکه است نیاز به اداره کردن آن‌ها از راه دور دارد. وجود چنین ویژگی امکان مدیریت متمرکز را فراهم می‌کند. سیستم عامل لینوکس ابزارهای مدیریتی بسیار کارآمدی را ارائه کرده است که از آن جمله می‌توان به ابزار SSH اشاره نمود. این ابزار نسبت به سایر ابزار مدیریت راه دور مثل Telnet, rsh, ftp, Rlogin از امنیت بیشتری برخوردار است و ارسال اطلاعات از طریق آن به صورت رمزگذاری شده صورت می‌گیرد. این ابزار از پروتکل SSH استفاده می‌کند. این پروتکل عملکردی شبیه پروتکل‌های Telnet, ftp دارد و اجازه دسترسی کاربران راه دور را، از طریق یک نشست رمزگذاری شده فراهم می‌کند. ویژگی‌های این ابزار عبارت است از:

- ۱- پس از برقراری اولین ارتباط، سرویس گیرنده می‌تواند در دفعات بعدی سرور را شناسایی کند.
- ۲- سرویس گیرنده اطلاعات مربوط به تعیین اعتبار خود را به صورت رمزگذاری ۱۲۸ بیتی ارسال می‌کند.
- ۳- تمام داده‌هایی که در طول برقراری یک نشست انتقال می‌یابند، به صورت ۱۲۸ بیتی رمزگذاری می‌شوند.

۴- سرویس دهنده و سرویس گیرنده SSH از امضای دیجیتال برای شناسایی یکدیگر استفاده می‌کنند.

۵- سرویس گیرنده‌ها می‌توانند از طریق این پروتکل، برنامه‌های گرافیکی را به صورت امن روی شبکه اجرا کنند. (X11 Forwarding)

پروتکل SSH برای محیط‌های سرویس دهنده و سرویس گیرنده (Client/Server) طراحی شده است و برنامه سرویس گیرنده SSH نیز تقریباً برای تمام سیستم عامل‌های مهم، موجود است و می‌توان از آن استفاده کرد. زمانی که یک سرویس گیرنده SSH با یک سرور SSH ارتباط برقرار می‌کند اطلاعات کلیدی بین دو سیستم رد و بدل می‌شود. این رد و بدل شدن اطلاعات در لایه Transport شبکه صورت می‌گیرد و باعث ایجاد ارتباطی امن بین سرویس گیرنده و سرور می‌شود. مراحل زیر در طول رد و بدل شدن این اطلاعات صورت می‌گیرد:

- ۱- کلیدها منتقل می‌شوند.
 - ۲- الگوریتم رمزگذاری کلید عمومی مشخص می‌شود.
 - ۳- الگوریتم رمزگذاری متقارن مشخص می‌شود.
 - ۴- الگوریتم تعیین اعتبار پیام‌ها مشخص می‌شود.
 - ۵- الگوریتم Hash مورد استفاده تعیین می‌شود.
- در مدت انتقال کلید، سرور خود را با یک کلید یکتا به سرویس گیرنده معرفی می‌کند. اگر سرویس گیرنده با آن سرور ارتباط برقرار نکرده باشد این کلید برای او ناشناخته است و ارتباط برقرار نمی‌شود. البته SSH این مشکل را رفع می‌کند و کلید سرور را بعد از این‌که کاربر جدید از وجود آن آگاه شد قبول می‌کند. کلید و الگوریتمی که برای رمزگذاری و انتقال امن داده‌ها مورد استفاده قرار می‌گیرد برای مدت مشخصی کاربرد دارد و بعد از این مدت مقدار Hash و کلید تغییر یافته و امنیت انتقال داده‌ها تضمین می‌شود. بعد از تعیین اعتبار بین سرور و سرویس گیرنده SSH، می‌توان چندین کانال ارتباطی بین آن‌ها ایجاد کرد که هر کانال دارای یک شماره منحصر به فرد خواهد بود. وقتی کاربر یک کانال ارتباطی ایجاد می‌کند، شماره آن برای سرور ارسال می‌شود. این شماره توسط سرور حفظ شده و جهت برقراری ارتباط از طریق این کانال مورد استفاده طرفین قرار می‌گیرد. این امر مانع از تاثیرگذاری هر نشست بر سایر نشست‌ها می‌شود. سرور و سرویس گیرنده به طور خودکار مشخصات هر کانال را شناسایی می‌کنند که این بستگی به نوع سرویس درخواستی از جانب سرویس گیرنده و روش ارتباطی کاربر با شبکه دارد.

نصب و راه اندازی سرویس SSH

برای راه اندازی سرویس باید ابتدا RPM مربوط به آن نصب شود:

```
rpm -Uvh ssh-version- number.rpm
```

بعد از نصب باید سرویس را فعال کرد:

```
/etc/rc.d/init.d/sshd start
```

با دستور زیر می‌توان سرویس را غیرفعال کرد:

```
/etc/rc.d/init.d/sshd stop
```

برای بررسی وضعیت سرویس از کلمه **status** به جای **stop** در دستور بالا استفاده می‌شود.

ضمناً لازم است روی سرویس گیرنده SSH نیز بسته نرم‌افزاری **ssh-client** نصب شود.

تنظیم و پیکربندی سرویس SSH

سرویس SSH دو نوع فایل پیکربندی دارد:

- فایل‌های مربوط به برنامه سرویس گیرنده (مانند **ssh scp sftp**).
- فایل‌های مربوط به برنامه سرویس دهنده (مانند **sshd**).

تمام فایل‌های پیکربندی SSH در مسیر **/etc/ssh** قرار دارند و در جدول زیر نمایش داده شده‌اند:

فایل	عملکرد
moduli	این فایل جهت انتقال کلید هنگام آغاز نشست ssh مورد استفاده قرار می‌گیرد.
ssh_config	این فایل شامل اطلاعات پیکربندی مربوط به سرویس گیرنده است.
sshd_config	این فایل شامل اطلاعات پیکربندی مربوط به سرور است.
ssh_host_dsa_key	شامل کلیدهای خصوصی DSA که توسط سرور استفاده می‌شوند.
ssh_host_dsa_key.pub	شامل کلیدهای عمومی DSA که توسط سرور استفاده می‌شوند.
ssh_host_rsa_key	شامل کلیدهای خصوصی RSA که توسط سرور استفاده می‌شوند.
ssh_host_rsa_key.Pub	شامل کلیدهای عمومی مورد استفاده سرور است و برای نسخه شماره دو پروتکل SSH است.
authorized_keys	این فایل لیستی از کلیدهای عمومی مجاز برای سرور را نگهداری می‌کند که هنگام تعیین اعتبار سرویس گیرنده مورد استفاده قرار می‌گیرند.
id_dsa	شامل کلید خصوصی DSA مربوط به کاربر است.
id_dsa.pub	شامل کلید عمومی DSA مربوط به کاربر است.
Id_rsa	شامل کلید خصوصی RSA مورد استفاده نسخه شماره دو پروتکل SSH است.
id_rsa.pub	شامل کلید عمومی RSA مورد استفاده نسخه شماره دو پروتکل SSH است.
Identity	شامل کلید خصوصی RSA مورد استفاده نسخه شماره یک پروتکل SSH است.

فایل	عملکرد
identity. Pub	شامل کلید عمومی RSA مورد استفاده نسخه شماره یک پروتکل SSH است.
known_hosts	این فایل شامل کلیدهای DSA مربوط به سرور SSH است که در دسترسی کاربر قرار دارد. وجود این فایل برای اطمینان از صحت ارتباط بین سرویس گیرنده و سرور SSH ضروری است.

نکته: اگر کلید مربوط به سرور تغییر کند، سرویس گیرنده مطلع می‌شود و تا موقعی که این کلید از فایل **known_hosts** پاک نشود، کاربر قادر به برقراری ارتباط با سرور نیست.

ویژگی Port Forwarding

SSH می‌تواند پروتکل ناامن **TCP/IP** را از طریق این ویژگی امن کند. وقتی از این تکنیک استفاده می‌شود، سرور **SSH** یک کانال رمزگذاری شده با سرویس گیرنده برقرار می‌کند. در این تکنیک یک عملیات نگاشت بین پورت محلی سرویس گیرنده و پورت سرور انجام می‌گیرد. برای ایجاد این نوع کانال و استفاده از ویژگی **Port Forwarding** از دستور زیر استفاده می‌شود:

```
ssh -L local-port: remote-hostname: remote-port username@hostname
```

برای چک کردن **E-Mail** از طریق ارتباط امن روی یک سرور که **mail.example.com** نام دارد از دستور زیر می‌توان استفاده کرد:

```
ssh -L 1100:mail.example.com:110 mail.example.com
```

سرور **Mail** باید سرویس دهنده **SSH** نیز باشد.

نکته: به منظور عملکرد صحیح سرویس **SSH** باید پروتکل‌های ارتباطی ناامن مانند **ftp**، **telnet**، **rsh**، **rlogin**، **vsftpd** را غیرفعال کرد.

دستور ssh

شکل کلی استفاده از دستور **ssh** به صورت زیر است:

```
ssh [-L login-name] hostname | user@hostname [command]
```

توجه: گزینه‌های داخل **[]** اختیاری هستند.

با استفاده از پارامتر **Command** می‌توان یک دستور را روی سیستم راه دور اجرا کرد.

مثال:

```
ssh PC ls /usr/share/doc
```

دستور scp

صفحه از

شماره مرجع: □-□ / ۱-۵-۷ / □ / □ تاریخ صدور:

این دستور جهت انتقال فایل‌ها بین دو کامپیوتر از طریق یک کانال امن مورد استفاده قرار می‌گیرد.

شکل این دستور برای انتقال فایل‌ها از سیستم محلی به یک سیستم راه دور به صورت زیر است:

```
scp localfile_name username@hostname: /newfile_name
```

شکل دستور برای انتقال فایل‌ها از یک سیستم راه دور به یک سیستم محلی به صورت زیر است:

```
scp user_name@hostname:/remote_file /new_local_file
```

دستور sftp

این دستور برای باز کردن یک نشست FTP به صورت امن مورد استفاده قرار می‌گیرد، شکل عمومی این دستور به صورت زیر است:

```
sftp user_name@hostname
```

بعد از تعیین اعتبار می‌توان از دستوراتی شبیه دستورات FTP استفاده کرد. (مانند put, get, و...) (این دستور در نسخه 2.5 open_ssh و بالاتر قابل استفاده است.)

تنظیمات عمومی فایل sshd_config

فایل sshd_config حاوی تنظیمات اصلی سرور SSH است. گزینه‌های اصلی جهت تنظیم این سرویس در جدول زیر مشخص شده اند:

گزینه‌های اصلی فایل sshd_config

نام گزینه	توضیح
Port	شماره پورت مربوط به سرویس sshd را تعیین می‌کند. پورت شماره ۲۲ مقدار پیش فرض است.
Protocol	شماره نسخه پروتکل SSH مورد استفاده را نشان می‌دهد.
Permit Root Login	تعیین می‌کند که آیا اجازه ورود به کاربر ریشه داده شود یا خیر.
Password Authentication	فعال سازی احراز هویت با استفاده از کلمات عبور. مقدار پیش فرض Yes است.
Permit Empty Passwords	تعیین می‌کند که آیا کاربران بدون کلمه عبور قادر به ورود هستند یا خیر. مقدار پیش فرض No است.
Allow Users & Deny Users	با استفاده از این گزینه می‌توان دسترسی کاربران به سرور را محدود کرد.
Listen Address	IP آدرس سرور SSH را مشخص می‌کند.

ایجاد زوج کلید عمومی و خصوصی

برای جلوگیری از وارد کردن کلمه عبور در هر بار استفاده از دستورات `ssh`، `scp` و `sftp` می‌توان یک زوج کلید ایجاد کرد. کلیدها باید برای هر کاربر ایجاد شوند.

۱- ایجاد زوج کلید RSA برای SSH Version 2

برای ایجاد این زوج کلید باید مراحل زیر را انجام داد:

- اجرای دستور زیر برای ایجاد کلید : `ssh-keygen -t rsa`
- تعیین مسیر فایل `id_rsa` (مسیر پیش فرض `~/.ssh/id_rsa`) :
- توجه: منظور از علامت ~ دایرکتوری `Root` است.
- وارد کردن عبارت عبور و تأیید مجدد آن.
- تغییر مجوز دایرکتوری `ssh` با استفاده از دستور زیر: `chmod 755 ~/.ssh`
- کپی محتویات `~/.ssh/id_rsa.pub` درون `~/.ssh/authorized_keys` در سیستمی که قرار است ارتباط با آن برقرار شود.

۲- ایجاد یک زوج کلید DSA برای SSH Version 2

- اجرای دستور زیر برای ایجاد کلید : `ssh-keygen -t dsa`
- تعیین مسیر فایل `id_dsa` (مسیر پیش فرض `~/.ssh/id_dsa`) .
- وارد کردن کلمه عبور و تأیید مجدد آن.
- تغییر مجوز دایرکتوری `ssh` با استفاده از دستور زیر: `chmod 755 ~/.ssh`
- کپی محتویات `~/.ssh/id-dsa.pub` درون `~/.ssh/authorized-key` روی سیستمی که قرار است ارتباط با آن برقرار شود.

تنظیم و پیکربندی ssh-agent

از `ssh-agent` برای ذخیره کردن کلمه عبور تعیین شده در مرحله ایجاد کلیدها و جلوگیری از وارد کردن مجدد آن‌ها در هر بار اتصال، استفاده می‌شود. برای تنظیم `ssh-agent` از دستورات زیر استفاده می‌شود:

```
exec /usr/bin/ssh-agent $SHELL
ssh-add
```

پس از دستور دوم باید کلمه عبور مورد نظر را وارد کرد. اگر بیش از یک زوج کلید تعیین شده باشد، برای هر کدام از آن‌ها باید این عمل را انجام داد.

تنظیم و پیکربندی فایل SSH-Config

این فایل تنظیمات مربوط به کاربران و سرویس گیرنده‌ها را تعیین می‌کند. برخی از گزینه‌های آن در جدول زیر درج شده است:

گزینه	عملکرد
Host <code>hostname*</code>	با این گزینه می‌توان لیستی از نام کامپیوترهایی که سرویس گیرنده SSH هستند و قرار است تنظیمات خاصی به هنگام ارتباط آن‌ها با سرور اعمال شود، تهیه کرد.
Port <code>Port_number</code> Protocol <code>number</code>	تنظیم این دو گزینه در دو سمت سرور و سرویس گیرنده یکسان است.
Compression <code>yes/no</code>	از این گزینه برای فشرده سازی داده‌ها هنگام انتقال استفاده می‌شود و تنظیم آن در دو سمت سرور سرویس گیرنده یکسان است.
Forwardx11 <code>yes/no</code>	امکان استفاده از Forward X11 مربوط به پروتکل SSH را فراهم می‌کند.
IdentityFile <code>~/ssh/key</code>	فایل حاوی نیمه دیگر کلید را برای تعیین اعتبار مشخص می‌کند.

سرویس Samba

سرویس Samba در سیستم عامل Linux از پروتکل SMB برای به اشتراک گذاشتن فایل و پرینتر در شبکه استفاده می‌کند. سیستم عامل‌های ویندوز، لینوکس و OSR از این پروتکل استفاده می‌کنند. در مواردی که سیستم عامل‌های ویندوز و لینوکس همزمان در شبکه وجود داشته باشند، استفاده از Samba برای به اشتراک گذاشتن فایل‌ها و پرینترها در سیستم عامل لینوکس ضروری است. تنظیمات این سرویس در فایلی به نام `smb.conf` صورت می‌گیرد. این فایل در مسیر `/etc/samba` واقع است. سرویس Samba را می‌توان هم از طریق محیط گرافیکی و هم از طریق محیط Command پیکربندی کرد. برای تنظیم آن نیاز به حقوق کاربری Root است. نصب این سرویس به دو طریق صورت می‌گیرد:

۱- نصب از طریق کد منبع (Source Code)

در این روش کد منبع Samba ابتدا باید از حالت فشرده و آرشیو خارج شده و سپس کامپایل شود، دستورات مربوط به این روش به صورت زیر است:

<code>tar -zxf samba-latest.tar.gz</code>
<code>cd samba-latest</code>
<code>./configure</code>
<code>make all</code>
<code>make install</code>

۲- نصب از طریق بسته‌های RPM

سرویس Samba دارای سه بسته نرم‌افزاری است که باید نصب شوند:

- **Samba-Common**: شامل فایل‌های مورد نیاز برای سرور Samba و سرویس گیرنده Samba است.

- **Samba**: شامل سرور Samba است.

- **Samba-Client**: شامل **smb client**، **smb mount** و **smb print** و فایل‌های مربوط به آن‌ها می‌باشد.

در روش نصب از طریق محیط **Command** ابتدا باید وارد مسیر دایرکتوری حاوی بسته‌های RPM مربوط به Samba شده و سپس دستور زیر را اجرا کرد:

```
rpm -Uvh samba-*.RPM
```

با اجرای این دستور هم **Samba Server** و هم **Samba Client** نصب می‌شود.

توجه: به هنگام نصب لینوکس در قسمت نصب **Package**‌ها می‌توان گزینه مربوط به نصب سرویس Samba را انتخاب کرد. در غیر این صورت باید از دو روش بالا جهت نصب آن استفاده شود.

بعد از نصب Samba باید سرویس را فعال کرد. برای این منظور باید از دستور زیر استفاده شود:

```
/etc/rc.d/init.d/smb start
```

توجه: بعد از انجام هر تغییر در فایل **smb.conf** باید سرویس را **Restart** نمود:

```
/etc/rc.d/init.d/smb restart
```

با استفاده از دستور زیر نیز می‌توان سرویس را غیرفعال کرد:

```
/etc/rc.d/init.d/smb stop
```

برای فعال کردن سرویس در هنگام **Boot** شدن سیستم باید از دستور زیر استفاده شود:

```
/sbin/chkconfig --level 345 smb on
```

برای بررسی وضعیت سرویس از دستور زیر استفاده می‌شود:

```
/etc/rc.d/init.d/smb status
```

تنظیم و پیکربندی سرویس Samba

تنظیم سرویس Samba به دو روش امکان پذیر است:

۱- از طریق محیط گرافیکی و ابزار تنظیم سرویس Samba در مسیر

(System Setting > Server Setting > Samba Server)

۲- از طریق محیط **Commnad** و ویرایش فایل **smb.conf**

در روش پیکربندی سرویس از طریق محیط **Command**، ابتدا فایل **smb.conf** در یک محیط ویرایشگر باز می‌شود.

vi /etc/samba/smb.conf

تنظیمات اصلی مربوط به این سرویس را می‌توان به چند بخش اصلی تقسیم کرد:

۱- روش تعیین اعتبار کاربران (**Authentication Mode**)

- روش **Domain** : در این روش **Samba** برای تعیین اعتبار کاربران خود از کنترل کننده **Domain** استفاده می‌کند و نام و کلمه عبور کاربران را برای تعیین اعتبار به این سرور ارسال می‌کند. در این حالت باید نام سرور را در قسمت مربوط به آن مشخص کرد.

توجه: باید حتماً از کلمات عبور رمزنگاری شده استفاده شود.

- روش **Server** : در این روش سرور **Samba** نام و کلمه عبور کاربران را برای تعیین اعتبار به یک سرور دیگر **Samba** (در شبکه) ارسال می‌کند.

- روش **Share** : در این روش کاربران **Samba** مجبور به وارد کردن نام و کلمه عبور نیستند، مگر بخواهند به یک **Share** خاص دسترسی پیدا کنند.

- روش **User** : در این روش کاربران باید نام و کلمه عبور معتبر در سرور **Samba** را وارد کنند. این گزینه برای مواردی که از نام کاربری ویندوز استفاده می‌شود مفید است. استفاده از کلمات عبور رمزگذاری شده در مواردی که سرویس گیرنده‌های **Smaba**، سیستم عامل‌های ویندوز 98، NT با **Service Pack 3** و یا سایر نسخه‌های ویندوز هستند، ضروری است.

در مورد **Guest Account** باید به این نکته اشاره شود که هنگام ورود کاربر **Guest** به سرور، باید به یک کاربر معتبر نزد سرور نگاشت (**map**) شود. بنابراین باید یکی از نام‌های کاربری موجود روی سیستم، برای این منظور استفاده شود. در این صورت کاربر **Guest** با حقوق این کاربر به سرور دسترسی پیدا می‌کند.

۲- مدیریت کاربران

برای اضافه کردن کاربران **Samba** می‌توان از کاربران محلی سرور استفاده کرد و نام کاربری این دسته از کاربران **Linux** را به گروه کاربران **Samba** اضافه کرد. در صورتی که کاربر از نام کاربری

متفاوتی روی سیستم های ویندوز و لینوکس استفاده کند، باید نام کاربر روی ویندوز را مشخص و سپس کلمه عبور کاربران را تعیین نمود. توصیه می شود کلمه عبور کاربران Samba با کلمه عبور آنها در لینوکس متفاوت باشد.

برای تعیین کلمه عبور یک کاربر جهت استفاده از سرویس Samba میتوان از دستور زیر استفاده کرد:

smbpasswd -a username

۳- تعیین دایرکتوری ها و پریترها برای به اشتراک گذاری
در این مرحله باید دایرکتوری هایی که قرار است به اشتراک گذاشته شوند را تعیین نمود. ضمناً مجوزهای مربوط به دسترسی کاربران به این دایرکتوری ها نیز باید تعیین شوند. این تنظیمات در فایل smb.conf صورت می گیرد. فایل smb.conf شامل دو قسمت است:

- تنظیمات عمومی سرور.
- تنظیمات مربوط به Share ها.

تنظیمات عمومی سرور [global]

نام گروه کاری که سرور عضو آن است = **Work Group**
تعیین IP آدرس سیستم هایی که اجازه دسترسی به سرور را دارند = **Host Allow**
انتخاب روش تعیین اعتبار = **Security**

تعیین مسیر فایل گزارش

Log File= /var/log/samba/samba - log %m
تعیین حداکثر سایز فایل = **Max Log Size= 50**
فعال یا غیرفعال کردن گزینه رمزگذاری کلمه عبور کاربران = **Encrypt Password = Yes / No**
تعیین اجازه دسترسی از طریق **Guest Account** = **Guest Ok= Yes/ No**
نام سرور = **Net Bios Name= Samba**
اعطا یا عدم اعطای مجوز چاپ = **Printable= Yes/ No**

تنظیمات Share ها

Share نام دایرکتوری [Share name] شده

Comment= توضیح

Path=/Share Share تعیین مسیر

Valid users= Share تعیین نام کاربران و گروه‌های مجاز به دسترسی به

Public= Yes/ No اعطا یا عدم اعطای مجوز دسترسی به تمام کاربران یک گروه

Writable= Yes/ No اعطا یا عدم اعطای مجوز نوشتن

Read-only= Yes/ No اعطا یا عدم اعطای مجوز خواندن

Browse able= Yes/ No نمایش یا عدم نمایش

Share جست‌وجو در لیست اشتراکی مورد نظر

create mask= 0700 تعیین مجوزهای دسترسی کاربران

برای Share کردن پرینترها داریم: [Printers]

Comment= All Printer
 Path= /.../ spool/samba
 Public= Yes
 Guest Ok= Yes
 Admin Users= Root
 Create Mask= 0700
 Print Ok= Yes
 Browse able = Yes
 Printable= Yes

تنظیمات سرویس گیرنده

برای دسترسی به Share های سرور Samba یا ویندوز 98 یا NT از طریق سیستم Linux از

دستور زیر می‌توان استفاده کرد:

smbmount /server-name/share_name/mount_point

علاوه بر این با نصب **smbclient** می‌توان از دستور زیر برای دسترسی امن‌تر به Share ها استفاده

نمود.

smbclient /server_name/share -u use_name

ضمناً برای دسترسی به Share ها از طریق سیستم ویندوز در قسمت Run، IP آدرس یا نام

سرور Samba را وارد کرده و سپس نام و کلمه عبور کاربر مجاز وارد می‌شود.

رفع اشکال سرویس

سرویس Samba دارای ابزاری برای تشخیص و رفع اشکالات موجود در سرور می‌باشد. مثلاً دستور زیر فایل `smb.conf` را جهت بررسی و شناسایی خطاهای احتمالی مورد بررسی و ارزیابی قرار می‌دهد.

```
testparm
```

دستور زیر لیست Shareهای قابل دسترسی روی سرور را نشان می‌دهد:

```
smbclient -L server-name-N
```

دستور زیر IP آدرس سرور را نشان می‌دهد:

```
nmblookup -B server -- SAMBA --
```

اگر هیچ Shareای با استفاده از دستور `smbclient -L` قابل مشاهده نباشد، ممکن است سرور Wins قادر به پاسخگویی نباشد. بنابراین باید بررسی کرد که سرویس گیرنده‌های SMB برای استفاده از سرور Wins به طور صحیح تنظیم شده باشند. برای این منظور از دستور زیر می‌توان استفاده کرد:

```
nmblookup -d 2`*`
```

نکته اول- با استفاده از ابزار گرافیکی Nautilus می‌توان Shareهای Samba را مشاهده کرد.

ضمناً در قسمت Location می‌توان با تایپ دستور زیر به Share مورد نظر دسترسی پیدا کرد:

```
Smb user:/password @server_name/share_name
```

نکته دوم- سرور Samba از NFS امن‌تر است.

سرویس Squid

کنترل دسترسی کاربران در وب برای اعمال امنیت کامل کار آسانی نیست. فایروال‌ها و سیستم‌های کنترل دسترسی که از طریق روترها اعمال می‌گردند، نمی‌توانند سطح قابل قبولی از امنیت را مهیا کنند. با وجود قوانین اولیه برای کاهش ترافیک و بالا بردن بازدهی، `Http Proxy` به عنوان یک لایه امنیتی اضافی و سیستم دیده بانی وب، نصب و راه اندازی می‌شود.

سرویس دهنده‌های `Proxy` که به عنوان محصولات تجاری ارائه می‌شوند، معمولاً گران هستند، بنابراین استفاده از نرم‌افزارهای `Open Source` مانند `Squid` پیشنهاد می‌گردد. `Squid`، نرم‌افزاری `Open Source` است و تحت سیستم عامل `Linux` کار می‌کند و دارای امکانات `Proxy` و `Cache` می‌باشد. این سرویس امکانات زیر را ارائه می‌دهد:

- `Caching` و `Proxy`
- `Proxy` نامرئی (`Transparent`)
- کنترل دسترسی کاربران
- ...

برای بالا بودن امنیت، سرویس **Squid** را در سروری جداگانه و در محلی امن نصب می‌کنند. علت این امر جلوگیری از اجرای سرویس‌های اضافی روی سرور **Proxy** می‌باشد.

مراحل نصب

برای نصب سرویس **Squid** ابتدا باید **rpm** آن را **Download** کرد و سپس آن را با استفاده از دستور زیر نصب کرد:

```
rpm -Uvh squid-*.rpm
```

بعد از نصب سرویس باید آن را فعال کرد. برای فعال کردن این سرویس از دستور زیر استفاده

می‌شود:

```
/etc/rc.d/init.d/squid start
```

برای متوقف کردن یا راه اندازی مجدد سرویس دستورات زیر به کار گرفته می‌شود:

```
/etc/rc.d/init.d/squid stop
```

```
/etc/rc.d/init.d/squid restart
```

پیکربندی Squid

Squid شامل گزینه‌ها و پارامترهای زیادی برای پیکربندی می‌باشد. فایل پیکربندی **Squid** در

مسیر زیر قرار دارد:

→ **/etc/squid/squid.conf**

این فایل شامل پارامترهایی است که برای راه اندازی سرور باید تنظیم شوند. در متن زیر به

تعدادی از پارامترهای مهم اشاره می‌گردد:

→ **http_port** *IP Add: Port No.*

این گزینه پورتهای را که **Squid** درخواست‌ها را از آن دریافت می‌کند، مشخص می‌نماید. مقدار

پیش فرض ۳۱۲۸ می‌باشد که توصیه می‌شود این مقدار تغییر پیدا کند.

maximum_object_size *Value*

minimum_object_size *Value*

اطلاعات ذخیره شده در سرور **Proxy**، معمولاً به صورت یک **Object** ارجاع داده می‌شوند.

پارامترهای بالا محدودیت سائز **Object**های **Cache** را اعمال می‌کند. هدف اصلی این گزینه بهینه

کردن کارایی **Cache** می‌باشد.

→ **dns_nameservers** *Value*

Squid از لیست‌های **name-server** خود برای ترجمه آدرس‌ها استفاده می‌کند. برای اعمال

name serverهای دیگر می‌توان از دستور بالا استفاده کرد.

→ **authenticate_ttl** *Value*

authenticate_ip_ttl *Value*

هنگامی که تعیین اعتبار (Authenticate) کاربران حائز اهمیت باشد از گزینه **Authenticate_ttl** برای نگهداری اطلاعات مربوط به شناسایی کاربران در یک زمان مشخص، استفاده می شود. تنظیم این گزینه باعث می شود کاربران بعد از گذشت مدت زمانی مشخص مجدداً تعیین اعتبار شوند. گزینه **authenticate_ip_ttl** مدت اعتبار شناسه کاربران روی یک **IP-address** مشخص را معین می کند:

→ **request_header_max_size Value**

این گزینه حداکثر سائز سرآیندهای **Http** پذیرفته شده را تعیین می کند:

→ **client_lifetime Value**

حداکثر زمان اجازه دسترسی به سرور **Squid** را معین می کند.

→ **pconn_timeout Value**

این گزینه محدودیت زمانی برای ارتباطات بی مصرف (**Idle**) با سرور **Squid** را تعیین می کند:

→ **acl_name element**

http_access [permit/deny] acl-name

یکی از موارد بسیار مهم برای پیکربندی **squid** از دید امنیتی، لیست های کنترل دسترسی (**acl**)

می باشند. لیست های کنترلی اجازه دسترسی یا عدم دسترسی به پروتکل **http** را تعیین می کنند. برای اعمال لیست های کنترلی باید پارامترهای بالا، تنظیم شوند. **acl**، عاملی که باید کنترل شود را مشخص می کند و با دستور **http_access** می توان اجازه دسترسی را محدود کرد. عوامل کنترلی

Squid عبارت است از:

توضیح	Element
IP Address منبع	src
IP Address مقصد	dst
آدرس IP که دستگاه به خود اختصاص داده است.	my IP
دامنه منبع	srcdomain
دامنه مقصد	dstdomain
شماره پورت مقصد	Port
شماره پورت دستگاه	my port
زمان برحسب ساعت، روز یا هفته	time
شناسایی کاربر از طریق یک روند خارجی	proxy_auth
مطابقت با آدرس کارت شبکه (MAC)	arp

اجازه دسترسی برای هر IP آدرس : **acl all src 0.0.0.0/0.0.0.0**

اجازه دسترسی آدرس‌های IP شبکه **10.50.0.0** : **acl main src 10.50.0.0/255.255.0.0**

http_access allow main

در مثال بالا امکان دسترسی به Proxy فقط از طریق شبکه **10.50.0.0** میسر می‌باشد.

Trusted_port یکی از مهمترین سیستم‌های کنترلی برای محدود کردن دسترسی به پورت‌ها

می‌باشد. مثال‌های زیر نمونه‌ای از این محدودیت‌ها را نشان می‌دهد.

لیست پورت‌های مجاز : **acl trusted_port port 21 80 443**

نادیده گرفتن پورت‌های غیرمجاز : **http_access deny ! Trusted-Port**

Squid دارای قابلیت تعیین اعتبار (**Authentication**) کاربران است. این ویژگی کنترل کاربران را

امکان پذیر می‌کند. ماژول‌های (**Module**) مختلفی برای تعیین اعتبار وجود دارد. این ماژول‌ها عبارت

است از **LDAP**، **NILM**، **NCSA** و...

Squid دو روش تعیین اعتبار را پشتیبانی می‌کند. این مدل‌ها عبارت است از مدل **Basic** و

مدل **Digest**.

در روش **Basic** کلمه عبور بدون رمزنگاری و در **Digest** کلمه عبور با رمزنگاری، ارسال

می‌گردد.

→ **acl acl_name proxy_auth REQUIRED**

در تعیین اعتبار کاربران برای دسترسی به سرویس **Squid** از عبارت فوق استفاده می‌شود. با

اعمال این گزینه، کاربر باید کلمه عبور خود را قبل از هر درخواستی، اعلام کند. بعد از تعیین اعتبار

کاربر، **Browser** این اطلاعات را برای درخواست‌های بعدی نگهداری می‌کند.

auth_param basic program {path}/libexec/ncsa_auth {path}/etc/passwd

Auth_param basic children 5

Auth_param basic credentialsttl 2 hour

Auth_param basic realm External network access

عبارات بالا مشخص می‌کند که برای تعیین اعتبار کاربران از چه نوع ماژولی و در چه مسیری

باید استفاده کرد. برای نمایش اعلان دلخواه در زمان نمایان شدن صفحه شناسایی از دستور زیر

استفاده می‌شود:

→ **reply_body_max_size value**

از این گزینه برای جلوگیری از **Download** فایل‌های حجیم مانند **mpeg** استفاده می‌شود. در

انتخاب مقدار این گزینه باید دقت گردد، زیرا اگر مقدار تعیین شده از حجم صفحه‌های اعلان خطای

squid کوچک‌تر باشد باعث از کارافتادن **Proxy** می‌شود.

→ **forward_for Value**

سرورهای وب نمی‌توانند با سیستم درخواست کننده سرویس به طور مستقیم ارتباط برقرار کنند، بلکه به وسیله Proxy سرور با سیستم مربوطه مرتبط می‌شوند. برای هماهنگ سازی لیست‌های کنترلی وب سرورها با IP سیستم درخواست کننده سرویس، سرور Squid از سرآیند Http به نام HTTP-FORWARD-FOR استفاده می‌کند. با انتخاب گزینه Off مشکلاتی برای دسترسی به وب سایت‌ها به وجود می‌آید.

→ delay_pools
delay_access

این گزینه برای محدود کردن نرخ انتقال به کار می‌رود. Squid باید بتواند برای کمک به مدیریت بهره وری پهنای باند، delay-pools را پشتیبانی کند.

→ cache_dir
cache_dir type maxobjsize directory-name mbyte level 1 level 2

عبارت type نوع سیستم ذخیره‌سازی را مشخص می‌کند. معمولاً نوع سیستم ذخیره‌سازی از نوع ufs انتخاب می‌گردد. اگر از Async I/O در Linux یا Solaris استفاده گردد باید گزینه auts انتخاب شود.

Max object : حداکثر اندازه یک Object که در یک منبع ذخیره (Storage) نگهداری می‌شود. در صورت انتخاب 1- ساینز Objectها می‌تواند به هر مقدار دلخواه انتخاب شود.
Directory : مسیری که Objectهای Cache شده در آن قرار می‌گیرد را مشخص می‌کند.
Mbytes : مقداری از ظرفیت دیسک که برای این منظور در نظر گرفته شده است.
Level 1 : تعداد زیر شاخه‌های اولین سطح که در شاخه اصلی ساخته می‌شوند را مشخص می‌کند.
Level 2 : تعداد زیر شاخه‌های دومین سطح که در شاخه اولین سطح ساخته می‌شوند را مشخص می‌کند.

مثال: Cache_dir ufs /usr/local/squid 100 15 256

→ cache_access_log Directory-path/file name

این گزینه برای مشخص کردن مسیر فایل access.log که گزارش درخواست‌های کاربران در آن ثبت می‌شود، به کار می‌رود.

→ cache_store_log directory-path/filename

cache_access_log /usr/local/squid/logs/store.log مسیر پیش فرض

این گزینه مسیر قرارگیری فایل store.log را که شامل گزارش‌های مدیریت منبع ذخیره (Storage) می‌باشد، مشخص می‌کند. این فایل اطلاعات راجع به Objectهایی که از Cache

دور انداخته می‌شوند یا درون آن ذخیره شده‌اند و مدت زمانی که در **Cache** قرار دارند را نگهداری می‌کند.

→ **quick_abort_min**
quick_abort_max
quick_abort_pct

با انتخاب این گزینه، **Cache** به **Download** کردن فایلی که از آن صرف نظر شده است ادامه می‌دهد. انتخاب این گزینه برای شبکه‌های کم ظرفیت مناسب نمی‌باشد. وقتی که کاربر از درخواست خود صرف نظر می‌کند، **Quick**، مقدار **Quick_abort** را با مقدار اطلاعات انتقال داده شده چک می‌کند.

اگر از اطلاعات انتقال داده شده کمتر از **quick_abort_min** باقیمانده باشد، باقیمانده را **Download** می‌کند. با انتخاب **1**- این گزینه غیرفعال می‌شود. اگر مقدار اطلاعات منتقل شده بیشتر از **Quick_abort_max** باشد، از ادامه **Download**، چشم پوشی می‌شود و اگر بیش از **Quick_abort_pct** (درصد) انتقال کامل شده باشد، عملیات را کامل می‌کند.

مثال :

quick_abort_min 16KB
quick_abort_max 16KB
quick_abort_pct 95 (برحسب درصد)

url_regex
acl ABC url_regex cooking
http_access allow/deny ABC

مثال:

در گزینه فوق یک **acl** با نام **ABC** به **URL**هایی که حاوی کلمه **Cooking** می‌باشند اشاره می‌کند. باید توجه داشت که این تنظیم **Case Sensitive** می‌باشد یعنی **cooking** با **Cooking** متفاوت است.

→ **urlpath_regex**
acl ABC urlpath_regex cooking
http-access allow/deny ABC

در این گزینه، **ABC** به **URL**هایی اشاره می‌کند که به جز در قسمت پروتکل و **Hostname** آن‌ها لغت **Cooking** استفاده شده باشد.

→ **acl acl-name time W 9:00- 15:05**

این دستور باعث تعیین محدودیت زمانی برای کاربران می‌گردد.

(((وزارت/ سازمان/ اداره کل/ شرکت/)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی سیستم عامل
شناسایی و احراز صلاحیت (تأیید اعتبار کاربر) شماره دستورالعمل: ۲-۵-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع:

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات

خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	دبیر*
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل بیان ضرورت و الزام شناسایی و احراز صلاحیت کلیه کاربرانی است که متقاضی دسترسی به دارایی‌های اطلاعاتی در اختیار (((وزارت/ اداره کل/ سازمان/ شرکت/....))) می‌باشند

مسئولیت‌ها

- - مسئولیت شناسایی و احراز صلاحیت کلیه کاربران متقاضی دسترسی به هر دارایی اطلاعاتی به عهده تحویل گیرنده یا مالک و یا متصدی همان دارایی اطلاعاتی می‌باشد. به علاوه این مسئولیت بر اساس سلسله مراتب سازمانی به مسئولین رده بالاتر انتقال می‌یابد. (انتخاب و پیشنهاد نوع مکانیزم یا مکانیزم‌های کنترل دسترسی در هر سطح به عهده واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و یا نهاد جایگزین وی و تصویب آن به عهده (((بالاترین مقام اجرایی سازمان))) خواهد بود).
- - مسئولیت نظارت بر اجرای این سیاست‌گذاری به عهده واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و یا نهاد جایگزین آن می‌باشد.

الزامات

- لازم است هر یک از کاربران استفاده کننده از دارایی‌های اطلاعاتی دارای یک شناسه منحصر به فرد (*User ID*) بوده و به هنگام کار با سیستم از آن استفاده نمایند، به نحوی که بتوان با استفاده از آن کلیه عملیات انجام شده در سیستم را ردیابی کرده و مسئولیت هر یک از افراد در انجام آن عملیات را تعیین نمود.
- شناسه کاربری باید به نحوی باشد که هیچ گونه اطلاعاتی در مورد مسئولیت سازمانی و یا امتیازهای ویژه استفاده کننده را نمایش ندهد.
- لازم است با استفاده از امکانات امنیتی در سطح شبکه، سیستم عامل، تجهیزات پردازشی، تجهیزات مسیریابی، تجهیزات امنیتی و ایستگاه‌های کاری و در صورت لزوم با استفاده از مکانیزم‌های مبتنی بر هویت دیجیتال^{۴۰} از دسترسی غیر مجاز به دارایی‌های اطلاعاتی

به‌خصوص سیستم‌های عامل جلوگیری کرد. این امکانات باید توانایی انجام فعالیت‌های زیر را ایجاد نمایند :

الف) شناسایی و بررسی هویت و در صورت ضرورت پایانه یا مکان هر یک از

کاربران

ب) ثبت اقدامات موفق یا غیر موفق ورود به سیستم

پ) فراهم آوری امکانات مناسب برای تصدیق هویت

ت) محدود ساختن زمان‌های ارتباط کاربران

- - در موقعیت‌های استثنائی، جایی که یک دلیل واضح سازمانی و یا یک سود تجاری ملموس در میان است، می‌توان از شناسه‌های کاربری مشترک برای گروه خاصی از کاربران یا انجام کاری خاص استفاده کرد. در این حالت باید تأییدیه مدیریت ارشد سازمان کسب و به‌طور مستند ثبت شود .
- - لازم است با توجه به نوع، ماهیت، و عملکرد هر دارایی اطلاعاتی از روش‌های مختلف موجود برای تصدیق هویت و اثبات ادعای هویت کاربر استفاده نمود.
- - تمامی دسترسی‌ها در سطح شبکه باید توسط راه‌کارهای اعلام شده از سوی نهاد متصدی امنیت اطلاعات و بر اساس سیاست‌گذاری کنترل دسترسی (دستورالعمل ۷-۱-۱)، احراز هویت شده و ضمن ثبت دسترسی، امکان ادامه فعالیت برای شخص (یا برنامه) فراهم شود. راه‌کار پایه و اولیه احراز هویت کاربران، استفاده از کلمه عبور (پیچیده) می‌باشد و راه‌کارهای تکمیلی مطابق با دستورالعمل‌های نهاد متصدی امنیت اطلاعات خواهد بود.

فرآیند

تأمین امنیت دارایی‌های اطلاعاتی به معنی حفظ مولفه‌های سه گانه امنیتی زیر است:

- محرمانگی
- جامعیت (صحت)
- دسترسی پذیری

هر گونه دسترسی به دارایی‌های اطلاعاتی یا بهره‌برداری از آن‌ها باید به نحوی باشد که منجر به نقض امنیت آن دارایی نشود. همچنین لازم است هرگونه فعالیت پردازشی به نحوی ثبت گردد که انکار انجام آن امکان ناپذیر باشد. بنابراین لازم است:

الف- اجازه دسترسی به دارایی‌های اطلاعاتی تحت حفاظت فقط به افراد یا نهاده‌هایی داده شود که شناخته شده باشند.

ب- افراد یا نهاده‌های احراز هویت شده فقط قادر به انجام فعالیت‌هایی باشند که صلاحیت آن را داشته باشند.

ج- هر عملی ثبت شده و افراد یا نهاده‌های مجری آن در مقابل انجام فعالیت خود پاسخگو باشند.

شناسایی و احراز صلاحیت کاربران به منظور تامین امنیت اطلاعات انجام می‌شود. مدل‌ها و فناوری‌های لازم برای این کار در پیوست‌های دستورالعمل کنترل دسترسی (دستورالعمل ۷-۱-۱) آمده است.

باید توجه داشت که مدیریت امنیت اطلاعات به این معنی نیست که با استفاده از روش‌های سخت گیرانه و آخرین فناوری‌های روز دسترسی به دارایی‌های اطلاعاتی را کاملاً محدود یا مسدود نمود بلکه لازم است با توجه به کاربرد، نوع کاربران، محیط عملیاتی و اهمیت دارایی اطلاعاتی بهینه ترین روش حفاظت از دارایی اطلاعاتی انتخاب و به کار گرفته شود.

رویه‌های اجرایی

برای مدیریت بهتر شناسایی و احراز صلاحیت کاربر اجرای رویه‌های زیر قابل به کارگیری است:

- یک سیاست کلی برای سیستم‌ها تهیه شود که فرآیندهای دسترسی، مدیریت، بروزرسانی، خصوصیات لازم معرف حسابهای کاربری، کلمه عبور، پشتیبان‌گیری و... را با جزئیات لازم شرح دهد.
- اطمینان حاصل شود که فرایندی مناسب جهت بررسی مرتب کسانی که مجوزهای دسترسی ممتاز دارند وجود دارد.
- مستندات مربوط به برنامه زمانبندی پشتیبان‌گیری، بروزرسانی و نصب وصله‌های امنیتی که به طور مقرر انجام می‌شود، نگهداری گردد.

- اطمینان حاصل شود که فروشندگان سیستم‌های عامل براساس اطلاعات گذشته و فعلی و برنامه‌های آینده، تعهدات خود را در مورد امن سازی سیستم عامل به‌طور منظم به اجرا می‌گذارند.
- سیاست کلی تدوین شده برای سیستم‌ها جهت تصدیق فرآیندهای دسترسی، مدیریت، بروزرسانی خصوصیات لازم برای حسابهای کاربری، هویت دیجیتال و... مورد بازبینی قرار گیرد.
- واحدهای سازمانی و سیاست‌های ممیزی آن‌ها مورد بررسی قرار گیرد.
- فهرست دسترسی که حقوق کاربری را برای کاربران، گروه‌ها و واحدهای سازمانی نشان می‌دهد تهیه و بروز رسانی شود.
- اطمینان حاصل شود که مدیر ارشد شبکه صلاحیت مورد نیاز برای مدیریت را از نظر میزان فهم سیستم عامل داراست.
- مستنداتی برای شرح سیستم عامل‌های متفاوت و نسخه‌های متفاوت سیستم عامل‌ها تهیه شود.
- اطمینان حاصل شود که شناسه کاربری مدیریتی متفاوت به‌منظور جداسازی دسترسی به سیستم عامل از سایر دسترسی‌هایی که نیاز به حقوق دسترسی ممتاز دارند وجود دارد.
- رسانه‌های مورد استفاده برای نصب در یک محیط امن ذخیره شود.
- رسانه‌های مورد استفاده برای پشتیبان‌گیری از سیستم عامل در یک محیط امن ذخیره شود.
- یک لیست از فرآیندهای صحیح و بروز شده برای نصب یا نصب مجدد سیستم عامل شامل تمامی وصله‌های بروزرسانی شده و داندل‌های مورد نیاز تهیه شود.
- یک طرح برگشت به قبل برای وقتی که برنامه بروزرسانی سیستم عامل با خطا مواجه شد تدوین شود.
- اطمینان حاصل شود که وقایع نگاری مناسبی به‌منظور ضبط رخداد‌های مربوط به دسترسی سیستم عامل وجود دارد.
- وقایع نگاریهای ثبت شده مربوط به رخداد‌های دسترسی سیستم عامل به‌طور مرتب مورد بررسی قرار گیرد.
- اطمینان حاصل شود که فایل‌های سیستم عاملی روی یک پارتیشن، دیسک و یا سرور مجزا از اطلاعات یا نرم‌افزارهای دیگر قرار گرفته است.

- کلمه‌های عبور پیش فرض مربوط به کاربران **superuser** و **administrator** برای جلوگیری از هر نوع دسترسی داخلی و خارجی به کلمه‌های عبور پیچیده، تغییر داده شود.
- اطمینان حاصل شود که دسترسی به فایل‌های سیستم عامل، بدرستی محدود شده است.
- فایل‌های سیستم عاملی به طور مرتب و زمانبندی شده پشتیبان‌گیری شود.
- همه وصله‌ها و داندادهای سیستم عاملی مورد نیاز بر روی سیستم نصب و به هنگام سازی شود.
- کلمه‌های عبور دسترسی‌های ممتاز مرتباً مورد بررسی و بازبینی قرار گیرد.
- کلمه‌های عبور دسترسی‌های ممتاز به‌طور منظم تغییر داده شود.
- اطمینان حاصل شود که کاربرانی که مجوزهای دسترسی ممتاز دارند، برخوردار از زمینه مناسب و آموزش‌های لازم براساس نیازمندیهای شغلی هستند.
- نرم‌افزارهایی که روی سیستم عامل بار می‌شود بررسی کامل و تاثیرات آن بر محیط سیستم عامل شناسایی شود.
- روال‌هایی برای رسیدگی به دسترسی‌های غیرمجاز به محیط و فایل‌های سیستم عامل تهیه شود.
- پروفایل‌های مربوط به گروه‌ها و کاربران به منظور اطمینان از اینکه هیچ دسترسی غیرمجازی، مجاز نشده باشد بررسی شوند.
- مدیر سیستم باید دو نوع شناسه کاربری متفاوت داشته باشد. یکی برای دسترسی‌های امن و محدود و دیگری برای استفاده عادی از کامپیوتر.
- اطمینان حاصل شود که در صورت ایجاد تغییرات در مجوزهای پیش فرض فایل‌ها و شاخه‌ها در نتیجه اعمال تنظیمات موقتی، در پایان کار مجوزها به حالت قبل برمی‌گردند.

مرجع:

این دستورالعمل به شماره □-□/۲-۵-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۷

روندنامه:

این دستورالعمل فاقد روندنامه می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی سیستم عامل
سیستم مدیریت کلمه عبور شماره دستورالعمل : ۳-۵-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات:

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل الزام کلیه استفاده کنندگان از سیستم عامل‌های در اختیار (((وزارت/ اداره کل/ سازمان/ شرکت/...))) به استفاده از کلمه عبور هنگام بهره‌برداری از سیستم عامل می‌باشد.

مسئولیت

مسئولیت اجرای این دستورالعمل به عهده مدیر ارشد شبکه (((وزارت/ اداره کل/ سازمان/ شرکت/...))) می‌باشد.

مسئولیت نظارت بر اجرای این دستورالعمل به عهده مدیر نهاد متصدی امنیت اطلاعات می‌باشد.

الزامات

- جهت دسترسی به کلیه سیستم‌های عامل استفاده از کلمه عبور الزامی است.
- در انتخاب و استفاده از سیستم مدیریت کلمه عبور رعایت دستورالعمل‌های سیاست‌گذاری کنترل دسترسی (دستورالعمل ۷-۱-۱) و استفاده از کلمه عبور (دستورالعمل ۷-۳-۱) الزامی باشد.
- در صورت استفاده از سیستم‌های خودکار جهت مدیریت استفاده از کلمه عبور لازم است:
- کاربر مجبور به استفاده از کلمه عبور باشد تا در بررسی‌ها و ممیزی‌های بعدی مسئولیت هر یک از افراد در انجام فعالیت‌های مختلف غیر قابل انکار باشد.
- در صورت امکان به کاربر اجازه انتخاب یا تغییر کلمه عبور اختصاصی خود را بدهد و در صورت اشتباه در ورود اطلاعات ضمن ثبت وضعیت، پاسخ مناسب را صادر نماید.
- فقط استفاده از کلمه‌های عبوری را تجویز نماید که طی دستورالعمل‌های مربوط در خصوص آن‌ها سیاست‌گذاری شده باشد.
- در صورتی که انتخاب و تغییر کلمه عبور در اختیار کاربر گذاشته شده باشد وی را مجبور به رعایت قواعد تشریح شده در مورد انتخاب کلمه عبور نماید.
- در صورتی که کاربر خود کلمه عبور را انتخاب می‌نماید وی را مجبور به تغییر کلمه عبور موقت هنگام اولین دسترسی و قبل از استفاده از سیستم نماید.

- کلمه‌های عبور قبلی مورد استفاده کاربر را به صورت رمزنگاری شده ثبت کرده و اجازه استفاده مجدد از آن‌ها را به کاربر ندهد.
- هنگام ورود کلمه عبور آن را روی نمایشگر نمایش ندهد.
- فایل کلمه‌های عبور را در محلی جدا از داده‌های کاربری نگهداری کند.
- در طی مراحل نصب نرم‌افزار کلمه عبور پیش فرض برنامه نویس را تغییر دهد.

فرآیند

کلمه عبور به عنوان کاراترین و معمولاً تنها روش کنترل دسترسی در بسیاری از مواقع به کار گرفته می‌شود. استفاده از این ابزار جهت دسترسی به سیستم عامل اهمیت بسیار زیادی دارد، زیرا در صورت دسترسی به سیستم عامل دسترسی به سایر داده‌ها و اطلاعات آسانتر خواهد بود. بنابراین حفاظت از سیستم عامل و به دنبال آن روش‌های دسترسی به آن در درجه اول اهمیت قرار داد.

حق دسترسی به سیستم عامل شبکه جزو حقوق دسترسی ممتاز محسوب می‌شود، بنابراین لازم است ابزار دسترسی به سیستم عامل شبکه تحت حفاظت کامل قرار گرفته و دارای استحکام کافی باشند. کلمه عبور نیز یکی از ابزار دسترسی مهم می‌باشد که باید از طریق اعمال سیاست‌های حفاظتی تحت کنترل و حفاظت قرار بگیرد.

در صورت نیاز به انتقال کلمه عبور در شبکه لازم است از ارسال آن به صورت کشف خودداری شده و از الگوریتم‌های مناسب و مستحکم رمزنگاری برای حفاظت استفاده شود. در صورت نیاز به نگهداری و ذخیره‌سازی کلمه عبور (به هر دلیل ممکن) نیز رمزگذاری آن ضروری است.

مرجع:

این دستورالعمل به شماره □-□/۳-۵-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۱-۷
- دستورالعمل ۱-۳-۷

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی سیستم عامل
استفاده از ابزارهای نرم‌افزاری سیستم شماره دستورالعمل : ۷-۵-۴	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد

بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل محدودسازی استفاده از ابزارهای سیستم در شبکه (های) ارتباط تحت مالکیت و یا در اختیار (((وزارت/ اداره کل/ سازمان/ شرکت/ ...))) است که می‌توانند به عنوان منبع ریسک و تهدیدات شدید امنیتی بر علیه دارایی‌های اطلاعاتی به شمار آیند.

مسئولیت

- - مسئولیت شناسایی، محدود سازی و کنترل استفاده از ابزارهای سیستم به عهده مدیر ارشد شبکه (((وزارت/ اداره کل/ سازمان/ شرکت/ ...))) می‌باشد.
- - مسئولیت نظارت بر اجرای این دستورالعمل به عهده مدیر نهاد متصدی امنیت اطلاعات یا نهاد جایگزین آن می‌باشد.

الزامات

- - استفاده و به‌کارگیری ابزارهای سیستم اعم از ابزارهای جانبی سیستم عامل مثل دستورهای مدیریت فایل یا دیسک (Format, Fdisk, Attrib, Regedit, ...)، ابزارهای مسیر یابی، ابزارهای انتقال فایل، ابزارهای دسترسی و رفع اشکال از راه دور، ابزارهای برنامه نویسی، ابزارهای تولید و مدیریت مالی مدیا، ابزارهای فشرده سازی یا رمزنگاری غیر رسمی، ابزارهای ترسیم و استخراج اطلاعات و همبندی شبکه، ابزارهای نفوذ و آزمایش شبکه و هرگونه ابزار نرم‌افزاری دیگر به‌جز برنامه‌های کاربردی رسمی سازمان ممنوع است، مگر آنکه قبلاً مجوز کتبی آن کسب شده و محل استفاده آن تعیین شده باشد.
- لازم است برای استفاده از ابزارهای سیستم مجاز نیاز به تصدیق هویت وجود داشته باشد.
- لازم است محل نگهداری ابزارهای سیستم مجاز از برنامه‌های کاربردی تفکیک شود.
- لازم است استفاده از ابزارهای سیستم مجاز فقط برای تعداد محدودی از افراد قابل اطمینان و مجرب سازمان، مجاز شمرده شود.
- لازم است فقط ابزارهای تک کاربره قابل استفاده باشند.
- لازم است بازه ی زمانی استفاده از این ابزارها محدود شود.
- لازم است هر نوع استفاده از این ابزارها ثبت شود.
- لازم است سطوح مجاز مختلف استفاده از این ابزارها تعریف شده و مستند شود.

- لازم است کلیه ابزارهای نرم‌افزاری و نرم‌افزارهای سیستمی غیرضروری از روی سیستم حذف شوند.
- رسانه‌های مورد استفاده برای نصب ابزارهای مجاز به نحوی مناسب در یک محیط امن ذخیره شود.

فرآیند

بسیاری از نرم‌افزارهایی که به همراه سیستم‌های رایان‌های ارائه می‌شوند حاوی یک یا چند ابزار نرم‌افزاری هستند که می‌توان با استفاده از آن‌ها اطلاعات را بازنویسی و یا رویه‌های کنترلی را اعمال نمود. استفاده از این ابزارها را باید محدود کرد و به شدت تحت کنترل قرارداد. بهترین روش برای اعمال این سیاست در درجه اول فرهنگ سازی و توجیه افراد در خصوص ضرورت عدم نصب ابزارهای نرم‌افزاری غیر مجاز و در درجه بعدی استفاده از **Thin Client** به جای **PC** و محدودسازی دسترسی به ابزارهای سیستم می‌باشد. در صورت عدم امکان استفاده از این نوع سخت‌افزار لازم است پس از نصب سیستم عامل، نرم‌افزارهای غیرضروری حذف شده و از طریق بستن ابزارهای ورود اطلاعات، از انتقال این گونه ابزار به کامپیوترها جلوگیری نمود. این روش‌های حفاظتی باید با استفاده از اقدامات انضباطی پشتیبانی شوند.

مرجع:

این دستورالعمل به شماره □-□/□-۵-۷/□-□ به ثبت رسیده است.

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی سیستم عامل
محدودیت مدت نشست شماره دستورالعمل : ۵-۵-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

جلوگیری از ایجاد فرصت حمله‌ی سوءاستفاده از آسیب پذیری‌های مرتبط با سرقت نشست^{۴۱} یا جعل آدرس^{۴۲}.

مسئولیت

- مسئولیت تعیین محدودیت‌های زمانی برای نشست‌های اجرای فرامین شبکه‌ای بین دو کاربر به عهده مدیر ارشد شبکه می‌باشد.
- مسئولیت نظارت بر اجرای این دستورالعمل به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن می‌باشد.

الزامات

- لازم است حداکثر زمان نشست ارتباطی بین دو کاربر به نحوی تعیین شود تا از امکان سوءاستفاده از سیستم و نقض امنیت آن حتی در صورت سرقت نشست یا جعل IP (از طریق محدودسازی فرصت حمله) جلوگیری شود.
- لازم است با استفاده از پروتکل‌های حفاظتی مانند IPSec یا Kerberos و یا الگوریتم‌های تأیید شده دیگر امکان سرقت نشست تحت کنترل قرار گیرد.
- لازم است تدابیر لازم برای جلوگیری از ایجاد کانال‌های پنهان^{۴۳} (مثلاً با استفاده از پروتکل ICMP برای عبور از فایروال) جهت برقراری نشست‌های غیرمجاز به کار گرفته شود.
- لازم است پس از پایان مدت زمان منظور شده برای یک نشست، به صورت خودکار به نشست پایان داده شود.
- پس از پایان یک نشست به صورت خودکار، لازم است از دسترسی به ترمینال ارتباطی جلوگیری شود (به عنوان مثال با استفاده از Screen Server و کلمه عبور)
- در صورت تجاوز زمان یک نشست از زمان تعیین شده برای آن لازم است علاوه بر قطع خودکار نشست وضعیت به وجود آمده به عنوان یک حادثه امنیتی ثبت و پیگیری گردد.

⁴¹- Session Hijacking

⁴²- Address Spoofing

⁴³- Covert Channel

- لازم است مکانیزم‌های مناسب برای پایان دادن خودکار به نشست جاری در صورت قطع ارتباط هر یک از طرفین نشست پیاده‌سازی شود.
- پس از تکمیل عملیات روی کامپیوترهای **Main frame** علاوه بر خاموش کردن **PC** یا ترمینال طرف ارتباط، لازم است به نشست جاری نیز پایان داده شود.

فرآیند

سرقت نشست یکی از روش‌های پیچیده اجرای حمله‌های کامپیوتری است. در این نوع از حمله نفوذگر با جعل آدرس **IP** یکی از طرفین ارتباط وارد کانال ارتباطی شده و خود را به جای طرف مقابل معرفی می‌نماید. به عنوان مثال اگر طرف **A** و طرف **B** در حال تبادل داده باشند، نفوذگر **C** با جعل آدرس طرف **A** وارد شده و خود را به جای طرف **A** به طرف **B** معرفی می‌نماید. در این حالت طرف **B** با تصور این که طرف **A** در حال دریافت اطلاعات است اطلاعات خود را در واقع به طرف **C** ارسال کرده و یا اطلاعات ارسال شده از طرف **C** را منشأ گرفته از طرف **A** محسوب کرده و به آن اعتماد می‌نماید.

معمولاً در طی این حمله طرف **C** با استفاده از اجرای حمله نوع **DoS**⁴⁴ (رد سرویس) علیه طرف **A** توانایی عکس‌العمل را از وی سلب می‌نماید. برای جلوگیری از دادن فرصت کافی به نفوذگر در اجرای این نوع حمله یا اقدامات متعاقب آن لازم است اولاً از روش‌های مناسب رمزنگاری و حفاظت از کانال و همچنین محدود سازی مدت زمان نشست (بر اساس خصوصیات نشست) استفاده کرده و ثانیاً در صورت تشخیص این نوع حمله نسبت به پیگیری فوری آن اقدام شود.

مرجع:

این دستورالعمل به شماره □-□/۵-۵-۷/□-□ به ثبت رسیده است.

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

⁴⁴ - Denial of Service

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
مدیریت دارایی‌های اطلاعاتی	کنترل دسترسی سیستم عامل
محدودیت زمان اتصال شماره دستورالعمل : ۶-۵-۷	

محرمانه

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **محرمانه** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات
خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	مسئول* دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف:

جلوگیری از احتمال دسترسی غیر مجاز به دارایی‌های اطلاعاتی در اختیار (((وزارت/ سازمان/ اداره کل/ شرکت...)))، از طریق محدود سازی زمان اتصال به ساعت‌های کاری رسمی یا ساعت‌های از قبل توافق شده.

مسئولیت:

- مسئولیت تعیین زمان‌های مجاز رسمی کار با دارایی‌های اطلاعاتی به عهده (((بالاترین مقام اجرایی سازمان))) می‌باشد.
- مسئولیت تعیین زمان‌های مجاز دسترسی خارج از ساعت‌های کار رسمی با دارایی‌های اطلاعاتی به عهده متصدی یا تحویل گیرنده یا مالک همان دارایی اطلاعاتی می‌باشد.
- مسئولیت نظارت بر اجرای مفاد این دستورالعمل به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن می‌باشد.

الزامات:

- لازم است ساعت پیش فرض مجاز کار با دارایی‌های اطلاعاتی در اختیار سازمان، معادل با ساعت کار رسمی سازمان باشد.
- دسترسی به کلیه دارایی‌های اطلاعاتی در ساعات خارج از زمان رسمی کار ممنوع است، مگر آنکه قبلاً مجوز آن به نحو مناسب کسب شده باشد.
- مسئولیت کار با دارایی‌های اطلاعاتی در ساعات کار غیر رسمی در هر صورت به عهده متصدی یا مالک یا تحویل گیرنده همان دارایی اطلاعاتی می‌باشد.
- لازم است ساعات مجاز دسترسی به دارایی‌های اطلاعاتی به اطلاع کلیه کاربران دارایی‌های اطلاعاتی برسد.
- لازم است در انتهای بازه زمانی مجاز، کاربران مجبور به خروج از سیستم شوند.
- مراجعه به دارایی‌های اطلاعاتی در ساعت‌های غیر مجاز باید به عنوان حادثه امنیتی تلقی و رسیدگی شود.

فرآیند:

بسیاری از حمله‌های موفق رایانه‌ای در ساعات کار غیر اداری یا روزهای پایان هفته اتفاق می‌افتند. در این ساعات معمولاً نظارت خاصی بر عملکرد دارایی‌های اطلاعاتی وجود ندارد و یا

حتی در صورت وجود سیستم‌های مانیتورینگ معمولاً یا کسی برای رسیدگی به اخطارهای صادر شده از سوی سیستم‌های تشخیص نفوذ وجود ندارد یا دسترسی به منابع پیشگیری از نفوذ و ترمیم خسارت‌های ناشی از نفوذ و دسترسی غیر مجاز تا ساعت کار رسمی روز یا هفته بعد امکانپذیر نمی‌باشد.

بنابراین لازم است دسترسی به دارایی‌های اطلاعاتی در ساعات‌های کار غیر رسمی یا در روزهای تعطیل به‌خصوص تعطیلات بلند مدت تحت کنترل کامل قرار گرفته و حتی الامکان ممنوع شود.

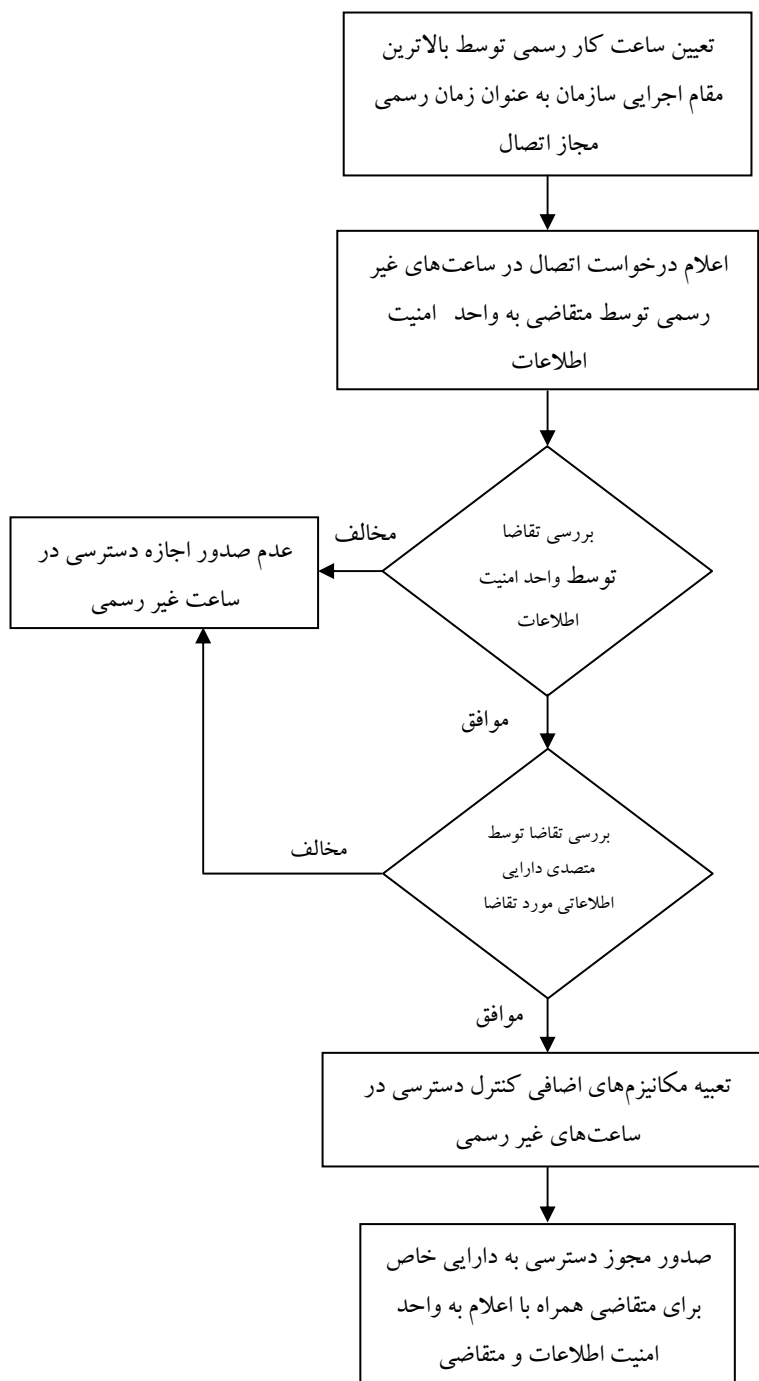
در صورت ضرورت نیاز به اعطای دسترسی در اینگونه زمان‌ها لازم است از مکانیزم‌های حفاظتی مناسب مثل استفاده از DMZ یا سرورهای واسطه‌ای استفاده شود تا از دسترسی مستقیم افراد به منابع جلوگیری شود. همچنین لازم است روال‌های مناسب تشخیص نفوذ تعبیه شده و گزارش‌های تولید شده در خصوص سعی در دسترسی غیر مجاز به دارایی‌های اطلاعاتی فوراً مورد رسیدگی قرار گیرد.

مرجع:

این دستورالعمل به شماره □-□/□-۵-۶/□-□ به ثبت رسیده است.

روندها:

روندنمای استفاده از کلمه عبور در نمودار زیر نمایش داده شده است:



(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی برنامه‌های کاربردی
محدود سازی دسترسی به اطلاعات شماره دستورالعمل : ۱-۶-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار ((بالاترین مقام اجرایی سازمان)))	رییس
	مسئول ((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات))	*دبیر
	معاون ((اداری، مالی و پشتیبانی))	عضو
	معاون ((برنامه‌ریزی))	عضو
	معاون ((فنی))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات ((معاون پشتیبانی)) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل بیان ضرورت جلوگیری از دسترسی غیرمجاز به اطلاعات نگهداری شده در سیستم‌های کاربردی و اطلاعاتی متعلق به (((وزارت/ اداره کل/ سازمان/ شرکت/...))) می‌باشد. همچنین باید دسترسی منطقی به اطلاعات و نرم‌افزارهای کاربردی فقط به کاربران مجاز محدود گردد.

مسئولیت

- مسئولیت تعیین محدوده‌های دسترسی به هر بخش اطلاعات و برنامه‌های کاربردی مختلف به عهده متصدی یا مالک یا تحویل گیرنده همان اطلاعات یا برنامه کاربردی می‌باشد. به علاوه این مسئولیت بر اساس سلسله مراتب سازمانی به مسئولین رده بالاتر انتقال می‌یابد. (انتخاب و پیشنهاد نوع مکانیزم یا مکانیزم‌های محدود سازی دسترسی در هر سطح به عهده واحد امنیت اطلاعات یا مرکز حراست فناوری اطلاعات و یا نهاد جایگزین وی و تصویب آن به عهده (((بالاترین مقام اجرایی سازمان))) خواهد بود.)

- مسئولیت تعیین داده‌ها، فایل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی موضوع این دستورالعمل به عهده (((مدیر ارشد شبکه سازمان))) می‌باشد.

- مسئولیت نظارت بر اجرای این دستورالعمل به عهده مدیر تهاد متصدی امنیت اطلاعات یا نهاد جایگزین آن می‌باشد.

الزامات

- دسترسی به داده‌ها، فایل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی باید بر اساس طبقه‌بندی حفاظتی (بر اساس دستورالعمل ۱-۲-۳) محدود شود. در خصوص دارایی‌های اطلاعاتی فاقد طبقه‌بندی نیز باید از در معرض افشا یا دید قرار گرفتن بی دلیل جلوگیری به عمل آید.

- دسترسی به داده‌ها، فایل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی موضوع این دستورالعمل به طور کلی ممنوع است مگر آنکه قبلاً صلاحیت و نیاز متقاضی به اثبات رسیده باشد.

- لازم است کلیه داده‌ها، فایل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی موضوع این دستورالعمل با استفاده از الگوریتم‌های معتبر رمزنگاری تحت حفاظت قرار گیرند به نحوی که در صورت

دسترسی افراد غیر مجاز به داده‌های خام یا کدهای منبع (Source Code) بهره‌برداری از آن‌ها غیرممکن باشد.

- روش اعطای حق دسترسی باید به نحوی باشد که احتمال نقض حدود دسترسی را به طور کامل منتفی نماید.

- دسترسی به کلیه داده‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی باید بر اساس مدل سه سطحی دسترسی عام، دسترسی خاص و دسترسی ممتاز تعریف گردد. حق دسترسی‌های عام، خاص و ممتاز به تفکیک داده‌ها، فایل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی اعطا خواهد شد و به صورت دوره‌ای بازنگری می‌گردد.

- افراد یا نهادهای فاقد حق دسترسی ممتاز، مجاز به تغییر در پیکربندی بانک‌های اطلاعاتی و برنامه‌های کاربردی و یا حذف کلی فایل نمی‌باشند. این نوع حق دسترسی فقط مختص به حوزه اختیار کاربر بوده و در سایر حوزه‌ها معتبر نمی‌باشد.

- افراد یا نهادهای فاقد حق دسترسی خاص مجاز به تغییر در داده‌ها، فایل‌ها و بانک‌های اطلاعاتی نمی‌باشند. این نوع حق دسترسی فقط مختص به حوزه اختیار کاربر بوده و در سایر حوزه‌ها معتبر نمی‌باشد.

- افراد یا نهادهای فاقد حق دسترسی عام مجاز به دسترسی به داده‌ها، فایل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی نمی‌باشند. این نوع حق دسترسی فقط مختص به حوزه اختیار کاربر بوده و در سایر حوزه‌ها معتبر نمی‌باشد.

- لازم است از تجهیزات و امکانات لازم برای جلوگیری از دسترسی‌های غیر مجاز به برنامه‌های کاربردی استفاده شود. لازم است:

الف) دسترسی به اطلاعات و سیستم‌های کاربردی بر اساس سیاست‌های کنترل دسترسی از قبل تعیین شده، تحت کنترل باشد.

ب) از کلیه ابزارهای نرم‌افزاری و سیستم‌های عامل که قابلیت دسترسی به اطلاعات خام را داشته و یا قادر به عبور از فرآیندهای کنترلی هستند، در مقابل دسترسی‌های غیر مجاز محافظت به عمل آید.

پ) به اشتراک گذاشتن منابع باعث نقض امنیت داده‌ها یا سیستم‌های اطلاعاتی نگردد.

- لازم است ابزار اعمال این دستورالعمل از جمله انطباق برنامه‌های کاربردی با الزامات فوق در اختیار مجریان گذارده شود.

فرآیند

کاربران سیستم‌های کاربردی، به علاوه نفرات بخش‌های پشتیبانی، باید با توجه به تدابیر کنترل دسترسی که بر اساس نیازهای سازمانی مختلف تعریف شده اند، امکان استفاده از سیستم‌های اطلاعاتی و برنامه‌های کاربردی را داشته باشند. این تدابیر بر اساس سیاست‌های کلی کنترل دسترسی سازمان اتخاذ می‌شوند.

فرآیند محدود سازی دسترسی به اطلاعات و برنامه‌های کاربردی بخشی از فرآیند کلی کنترل دسترسی دارایی‌های اطلاعاتی می‌باشد. در این فرآیند تاکید بر شناسایی داده‌ها، فایل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی و تعریف حدود هریک و شرایط دسترسی به آن‌ها می‌باشد.

بر اساس این فرآیند لازم است ابتدا دسترسی کلیه افراد و نهاده‌ها به داده‌ها، فایل‌ها، بانک‌های اطلاعاتی و برنامه‌های کاربردی موضوع این دستورالعمل ممنوع شده و سپس بر اساس اصل نیاز به دسترسی و بر اساس اصول دسترسی عام، دسترسی خاص و یا دسترسی ممتاز با توجه به حوزه اختیار مقتضای اجازه دسترسی به وی اعطا شود.

رویه اجرایی

- شناسایی همه سیستم‌های اطلاعاتی و کاربردی.
- شناسایی منابع غیر مجازی که ممکن است باعث نفوذ، تغییر، حذف و یا فاش کردن اطلاعات محرمانه شوند.
- شناسایی ابزارها و تکنیک‌هایی که برای پشتیبانی از قالب ارسال اطلاعات به کار می‌روند.
- ایجاد و جاری سازی منوهای لازم برای تعریف سطوح مختلف دسترسی در برنامه‌ها.
- ایجاد و جاری سازی حفاظت‌های مناسب و سیاست‌های پیشگیرانه به منظور جلوگیری از افشای اطلاعات.
- ایجاد و جاری سازی مجموعه ای کارا از ابزار لازم برای ارسال امن اطلاعات الکترونیکی.
- مانیتورینگ و بررسی همه جانبه نحوه استفاده از اطلاعات سازمانی.

- کنترل و بازنگری حقوق دسترسی کاربر مانند نوشتن، خواندن، پاک کردن و یا اجرا
- انتخاب کنترل‌های امنیتی لازم برای هر سیستم بر اساس طبقه‌بندی امنیتی، سطح تماس‌ها، الزام‌های عملیاتی و نیازهای محیطی
- انتخاب استاندارد مناسب برای شناسایی و طبقه‌بندی اطلاعات اختصاصی، حساس و محرمانه سازمان.
- تعیین اقدامات پیشگیرانه مناسب به منظور محافظت اطلاعات از خطاها و تغییرات غیرمجاز
- تعیین اقدامات انضباطی مناسب برای اعمالی غیرمجاز مانند تغییر داده‌ها، جست‌وجو در بانک‌های اطلاعاتی، افشاسازی اطلاعات، جست‌وجو به دنبال نقاط ضعف امنیتی سیستم‌های پردازشی و نقض حریم خصوصی افراد.
- استفاده از پرسنل کلیدی بخش IT برای یافتن راه حل‌های تکنیکی به منظور ارسال امن اطلاعات.
- حصول اطمینان از این‌که مالکان برای تعیین سطح حفاظتی که اطلاعاتشان لازم دارد همکاری می‌کنند.
- حصول اطمینان از این‌که ریسک فعالیت‌هایی مانند کار در خانه، دسترسی تلفنی (dial-in)، انجام کارهایی که برای انجام آن‌ها رعایت حقوق انحصاری لازم است و استفاده شخصی از تجهیزات پردازشی تحت کنترل کامل بوده و در حد قابل پذیرش است.
- اطلاعاتی که بر اثر گذشت زمان از اهمیت آن‌ها کاسته شده است به‌طور مناسب تغییر طبقه‌بندی داده شوند.
- شناسایی منابع غیر مجازی که ممکن است باعث نفوذ، تغییر، حذف و یا فاش کردن اطلاعات محرمانه می‌شود.

مرجع:

این دستورالعمل به شماره □-□/۱-۶-۷/□-□ به ثبت رسیده است و سایر دستورالعمل‌های مرتبط با آن عبارت‌اند از:

- دستورالعمل ۱-۲-۳

روندنا:

این دستورالعمل فاقد روندنا می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	کنترل دسترسی برنامه‌های کاربردی
جدا سازی سامانه (سیستم) های حساس شماره دستورالعمل : ۲-۶-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام‌الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامه‌ریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

* : در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل تامین امنیت بیشتر برای سیستم‌های حساس و حیاتی در اختیار (((وزارت/ اداره کل/ سازمان/ شرکت/ ...))) می‌باشد.

مسئولیت‌ها

- مسئولیت تعیین سیستم‌های حساس و حیاتی و تامین شرایط استفاده از آن‌ها به عهده (((بالاترین مقام اجرایی سازمان))) می‌باشد.
- مسئولیت انتخاب روش‌های حفاظت از سیستم‌های حساس به عهده مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن می‌باشد.
- مسئولیت حفاظت از دارایی‌های اطلاعاتی که به عنوان سیستم‌های حساس یا حیاتی شناسایی شده‌اند به عهده تحویل گیرنده یا مالک یا متصدی همان دارایی اطلاعاتی می‌باشد.
- کلیه افراد استفاده کننده از دارایی‌های اطلاعاتی، ملزم به رعایت حدود و شرایط استفاده از سیستم‌های حساس می‌باشند.

الزامات

- درجه حساسیت سیستم کاربردی باید صریحاً و به روشنی توسط دارنده آن سیستم تعریف شده جهت تصویب به (((بالاترین مقام اجرایی سازمان))) اعلام شود.
- در صورت نیاز لازم است سیستم‌های حساس را به نحو مناسب و به صورت فیزیکی یا منطقی از سایر سیستم‌ها جداسازی نمود.
- سیستم‌های دارای طبقه‌بندی حفاظتی بالاتر از خیلی محرمانه باید به صورت فیزیکی از سایر سیستم‌ها جداسازی شوند.
- هنگامی که از یک سیستم حساس در محیط اشتراکی استفاده می‌شود، لازم است سیستم‌های دیگری که به صورت اشتراکی با این سیستم مورد استفاده قرار می‌گیرند، شناسایی شده و توافق متصدی سیستم حساس در کار همزمان با بقیه سیستم‌ها کسب شود.
- مکانیزم‌های کنترل دسترسی در سیستم‌های پرخطر یا سیستم‌های حاوی اطلاعات بسیار حساس، با توجه به ارزش و طبقه‌بندی امنیتی دارایی‌های اطلاعاتی مربوط تنظیم شده و باید دارای پیچیدگی بیشتر و متناسب با اهمیت سیستم تحت حفاظت باشد.

- مدیریت سازمان باید اطمینان حاصل نماید که تفکیک کامل وظایف در قالب توسعه سیستم‌ها، عملیات سیستم‌ها و اداره سیستم‌ها صورت پذیرفته است.
- همه کارمندان برای دسترسی مجاز به سیستم‌های حساس باید احراز هویت شوند.

فرآیند

ممکن است سیستم‌های حساس نیاز به محیط پردازشی مشخصی (جدا شده) داشته باشند. برخی از سیستم‌های کاربردی به خودی خود حساس بوده و پتانسیل نشت اطلاعات از آن‌ها بسیار زیاد است، برای اجرا، نیاز به کامپیوتر خاصی دارند و یا لازم است آن‌ها را بدون محدودیت به بانک‌های اطلاعاتی متصل کرد. بنابراین نمی‌توان هیچ محدودیتی برای دسترسی به آن و یا دسترسی آن به سایر اطلاعات در نظر گرفت. در به کارگیری این سیستم‌ها باید الزاماتی نظر گرفته شود. همچنین ممکن است برخی دیگر از دارایی‌های اطلاعاتی به دلایل حفاظتی نیاز به حفاظت بیشتر یا سخت گیرانه‌تر داشته باشند.

جهت جدا سازی سیستم‌های حساس فرآیند زیر قابل اجرا می‌باشد:

- شناسایی و جداسازی سیستم‌های عملیاتی از سیستم‌های تحت توسعه
- شناسایی دارایی‌هایی مرتبط با سیستم‌های حساس اعم از رسانه‌ها، فایل‌ها و...
- ایجاد و جاری سازی سیستم پشتیبانی اضطراری مرتبط با سیستم‌های حساس
- ایجاد و جاری سازی یک طرح امنیتی برای محافظت از اطلاعات طبقه‌بندی شده و یا اسناد حیاتی سیستم‌های حساس در مواقع بحران
- ایجاد و جاری سازی سیستم ثبت وقایع (logging) برای ضبط روال‌های مربوط به داده‌های مرتبط با سیستم‌های حساس
- مانیتورینگ و بررسی همه جانبه نحوه استفاده از سیستم‌های حساس
- بازنگری منظم و دوره‌ای گزارش‌های سیستم ثبت وقایع مربوط به سیستم‌های حساس

رویه‌های اجرایی

رویه‌های اجرایی حفاظت از سیستم‌های حساس را می‌توان به شرح زیر فهرست کرد :

- نگهداری سیستم‌های حساس در اتاق‌های مجزای تحت کنترل درمناطق امن
- تهیه فهرست کامل از دارایی‌هایی مرتبط با سیستم‌های حساس اعم از رسانه‌ها، فایل‌ها و...

- محافظت ساختمان‌های محل استقرار سیستم‌های حساس با نرده‌های امنیتی، فنس‌ها، سیستم‌های هشداردهنده و یا سیستم‌های دیده بانی مدار بسته
- حصول اطمینان از اینکه سیم کشی همه کابل‌های ارتباطی و سیستم‌های هشدار دهنده و امنیتی ساختمان‌های دارای سیستم‌های حساس با لوله‌های حفاظ دار محافظت می‌شوند.
- آماده سازی طرح امنیتی برای محافظت از اطلاعات طبقه‌بندی شده و یا اسناد حیاتی سیستم‌های حساس درمواقع بحران و اضطراری.
- حفاظت از اسناد و اطلاعات مربوط به سیستم‌های حساس در مخزن نسوز و ضد آب (مثل گاوصندوق یا اتاق‌های نسوز و ضدآب)
- حصول اطمینان از حفاظت فیزیکی پنجره‌های رو به بیرون ساختمان‌های محل نگهداری سیستم‌های حساس، از شکستگی و امکان ورود غیرمجاز.
- تدارک برق و روشنایی اضطراری برای مواقع قطع برق برای سیستم‌های حساس
- رعایت الزامات پدافند غیرعامل در تامین نیازهای عملیاتی سیستم‌های حساس یا حیاتی

مرجع:

این دستورالعمل به شماره □-□/۶-۷/□-□ به ثبت رسیده است.

روندنما:

این دستورالعمل فاقد روندنما می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	پردازش همراه و کار از راه دور
پردازش همراه و مخابرات سیار شماره دستورالعمل : ۱-۷-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به‌عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

هدف

جلوگیری از نقض امنیت اطلاعات در حوزه محرمانگی به دلیل استفاده از تجهیزات پردازش همراه (سیار) یا هنگام استفاده از نوت بوک‌ها، منشی‌های الکترونیک شخصی یا تلفن‌های همراه

الزامات

هنگام استفاده از تجهیزات پردازش همراه و تجهیزات و کانال‌های ارتباطی مربوط مثل نوت بوک، منشی‌های الکترونیک شخصی، حافظه‌های جانبی قابل حمل مثل **Flash Memory**، تلفن‌های همراه عادی یا هوشمند و غیره یا هنگام استفاده از فناوری‌های ارتباط سلولی یا سیار اعم از **WLAN**، **WiFi**، **WiMAX**، **GSM**، **CDMA**، **GSM2**، **Tetra** ... باید به الزامات امنیتی مربوط به خصوص الزامات کار در مکان‌های حفاظت نشده توجه شود.

مسئولیت

- مسئولیت تدوین دستورالعمل‌های امنیتی کار با تجهیزات پردازش همراه به عهده مدیر نهاد متصدی امنیت اطلاعات یا نهاد جایگزین وی می‌باشد.
- مسئولیت نظارت بر اجرای این دستورالعمل و سایر دستورالعمل‌های مربوط به کار با تجهیزات پردازش همراه به عهده دبیرخانه امنیت اطلاعات می‌باشد.

الزامات

- استفاده از تجهیزات پردازش همراه برای پردازش، تبادل یا ذخیره‌سازی اطلاعات دارای طبقه‌بندی در مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حیاتی شناخته شده‌اند ممنوع است.
- استفاده از تجهیزات پردازش همراه برای پردازش، تبادل و یا ذخیره‌سازی اطلاعات دارای طبقه‌بندی در مراکزی که از سوی سازمان پدافند غیرعامل به عنوان مراکز حساس دسته‌بندی شده‌اند ممنوع می‌باشد مگر آنکه قبلاً مجوز کتبی استفاده از آن‌ها با ذکر نام استفاده کننده، نوع اطلاعات و مدت زمان مجاز استفاده کسب شده باشد.
- استفاده کننده از تجهیزات پردازش همراه باید قبلاً آموزش کافی در خصوص استفاده از تجهیزات مربوط و همچنین روش حفاظت از امنیت اطلاعات در مکان‌های خارج از محیط سازمان دیده باشد.

- کلیه اقدامات حفاظتی اعم از حفاظت فیزیکی، کنترل دسترسی، روش‌های رمزنگاری داده‌ها، تهیه نسخه پشتیبان و حفاظت در مقابل ویروس یا کدهای نفوذگر باید هنگام استفاده از تجهیزات پردازش همراه مورد توجه قرار گیرد.
- تجهیزات پردازش همراه حاوی اطلاعات طبقه‌بندی شده هنگام حمل و نقل و مسافرت باید دائماً در معرض دید و کنترل قرار داشته باشند.
- ورود و خروج تجهیزات پردازش همراه به مکان‌های حفاظت شده باید تحت کنترل کامل قرار داشته باشد.

فرآیند

استفاده از تجهیزات پردازش همراه به معنی امکان انتقال اطلاعات (به‌خصوص اطلاعات دارای طبقه‌بندی حفاظتی) به مکان‌های خارج از کنترل امنیتی سازمان می‌باشد. مثال‌های زیادی در خصوص سرقت تجهیزات پردازشی همراه از محیط‌های تحت کنترل و به‌خصوص خارج از کنترل وجود دارد که منجر به خسارت‌های مالی، امنیتی و سیاسی فراوان شده است.

همچنین هنگام استفاده از تجهیزات پردازش همراه معمولاً از کانال‌های ارتباطی برای برقراری ارتباط با شبکه‌های سازمانی یا شبکه‌های دیگر استفاده می‌شود که این موضوع نیز خود ریسک افشای اطلاعات را به شدت افزایش می‌دهد.

بنابراین استفاده از تجهیزات پردازش همراه و مخابرات سیار مستلزم کار در شرایط خارج از کنترل سازمان می‌باشد که باید ریسک‌های مربوط به آن را از طریق ارائه آموزش به استفاده کنندگان، به‌کارگیری مکانیزم‌ها و پروتکل‌های احراز و تصدیق هویت، رمزنگاری و امن‌سازی مناسب و تأکید بر رعایت دستورالعمل‌های سازمانی مدیریت امنیت اطلاعات کاهش داد.

مرجع:

این دستورالعمل به شماره □-□/۱-۷-۷/□-□ به ثبت رسیده است.

روندنا:

این دستورالعمل فاقد روندنا می‌باشد.

(((وزارت / سازمان / اداره کل / شرکت /)))

فصل	حوزه
کنترل دسترسی	پردازش همراه و کار از راه دور
کار از راه دور شماره دستورالعمل : ۲-۷-۷	

عادی

تأییدیه نهایی

نام و نام خانوادگی: (((نام و نام خانوادگی بالاترین مقام اجرایی سازمان)))

عنوان: (((بالاترین مقام اجرایی سازمان)))

امضاء:

تاریخ:

توزیع :

این سند به عنوان سند **عادی** طبقه‌بندی شده و در اختیار کمیته امنیت اطلاعات خواهد بود.

تصویب شده در کمیته توسط:

نام	عنوان سازمانی	سمت در کمیته امنیت اطلاعات
	نماینده تام الاختیار (((بالاترین مقام اجرایی سازمان)))	رئیس
	مسئول (((مرکز حراست IT یا نهاد متصدی حفظ امنیت اطلاعات)))	*دبیر
	معاون (((اداری، مالی و پشتیبانی)))	عضو
	معاون (((برنامهریزی)))	عضو
	معاون (((فنی)))	عضو
	مسئول حراست	عضو
		عضو
		عضو

*: در صورت عدم وجود واحد مستقل امنیت اطلاعات (((معاون پشتیبانی))) سازمان به عنوان دبیر منصوب خواهد شد.

سوابق تغییرات :

تاریخ	شرح

هدف

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی حفظ امنیت اطلاعات هنگام کار از راه دور توسط کارمندان و یا پیمانکاران و یا شرکای تجاری مرتبط با (((وزارت/ اداره کل/ سازمان/ شرکت/...))) می‌باشد.

مسئولیت

- مسئولیت تدوین دستورالعمل‌ها و رویه‌های مرتبط با حفظ امنیت کار از راه دور به عهده مدیر ارشد شبکه (((وزارت/ اداره کل/ سازمان/ شرکت/...))) می‌باشد.
- مسئولیت نظارت بر رعایت این دستورالعمل و سایر اسناد مرتبط با آن به عهده مدیر نهاد متصدی امنیت اطلاعات و یا نهاد جایگزین آن می‌باشد.

الزامات

- کار از راه دور فقط پس از صدور مجوز آن توسط (((بالاترین مقام اجرایی سازمان))) مجاز می‌باشد.
- در کار از راه دور از تجهیزات مخابراتی برای ایجاد توانایی انجام کار در خارج از محل ثابت سازمان استفاده می‌شود، بنابراین حفاظت از کانال ارتباطی از طریق رمزنگاری و احراز هویت و احراز صلاحیت در درجه اول اهمیت قرار دارد.
- لازم است هنگام استفاده از این روش، تدابیر حفاظتی لازم در مقابل حوادث احتمالی مانند سرقت تجهیزات یا اطلاعات، افشاء غیر مجاز، دسترسی غیر مجاز از راه دور یا سوءاستفاده از تجهیزات قرار داده شده در اختیار کارمند برای کار از راه دور به کار گرفته شود.
- کار از راه دور و روش‌های اجرای آن باید تحت نظارت مستقیم مدیر واحد امنیت اطلاعات یا نهاد جایگزین آن قرار داشته باشد.
- هنگام صدور مجوز کار از راه دور باید موارد زیر مورد توجه قرار گیرد:
 - امنیت فیزیکی محل کار از راه دور و مقایسه آن با الزامات امنیتی در نظر گرفته شده برای تجهیزات و داده‌های مرتبط با آن
 - نیازهای امنیتی شبکه مخابراتی با توجه به الزامات اتصال از راه دور به شبکه داخلی سازمان

- ریسک‌ها و تهدیدات ناشی از دسترسی غیر مجاز افراد حاضر در محل کار از راه دور مثل اعضای خانواده یا دوستان به اطلاعات
- ریسک‌ها و تهدیدات ناشی از دسترسی افراد فوق به تجهیزات یا کانال‌های مخابراتی
- روش‌های تهیه نسخه پشتیبان
- ممیزی و Log برداری از فعالیت‌های انجام شده توسط کاربر روی تجهیزات در اختیار و یا شبکه

فرآیند

کار از راه دور ((Teleworking یکی از روش‌های جدید انجام کار است که به دلیل استفاده از امکانات ناشی از گسترش خدمات ارتباطی امکانپذیر شده است. افراد زیر را می‌توان به عنوان کاربران راه دور (محل ثابت) در نظر گرفت:

- کارمندان و افرادی که دارای رابطه استخدام رسمی با سازمان می‌باشند.
- پیمانکاران یا افرادی که در یک دوره زمانی خاص و بر اساس قرارداد معین به انجام عملیات خاصی می‌پردازند.
- شرکای تجاری یا افرادی که بر اساس تفاهم نامه یا موافقت‌نامه یا بر اساس حق نمایندگی بخشی از عملیات سازمان (مثلاً فروش کالا یا خدمات پس از فروش) را به عهده دارند.
- تعامل این کاربران را به طور کلی می‌توان به دو قالب فعالیتی اتصال از طریق کانال ارتباطی و انجام کار مرتبط با حوزه فعالیت تقسیم بندی نمود.
- اتصال از طریق کانال ارتباطی و برقراری ارتباط از راه دور فعالیتی مشترک است، اما ممکن است روش انجام کار یا حوزه آن برای هر دسته از کاربران متفاوت باشد. بنابراین لازم است برای دسته از کاربران فوق روش‌های کنترلی متناسب با حوزه عملکرد طراحی و به کار گرفته شود.

مرجع

این دستورالعمل به شماره □-□/۷-۷/□-□ به ثبت رسیده است.

روندها:

این دستورالعمل فاقد روندها می‌باشد.

تعریف‌ها و اصطلاحات

مرتب شده بر اساس ستون اول

ISMS	Information Security Management System	نظام مدیریت امنیت اطلاعات
AAA	مدل مرجع کنترل دسترسی	مبتنی بر احراز هویت، احراز صلاحیت و پاسخگویی (Authentication, Authorization, Accountability))
ACL	Access Control List	فهرست کنترل دسترسی
Attack		حمله، هر گونه فعالیت که ناشی از فعالیت عمدی عامل انسانی باشد و باعث اختلال در عملکرد دارایی اطلاعاتی شود.
Audit		ممیزی، فرآیندی که طی آن عملکرد یا شرایط سیستم با عملکرد یا شرایط پیش بینی شده و مطلوب برای آن مقایسه می‌شود.
Availability	دسترسی پذیری	یکی از محورهای سه گانه امنیت اطلاعات که توسط استاندارد ISO/IEC-27001 معرفی شده است.
Back Door	در پشتی	برخی راههای پنهان برای دور زدن و عبور از سیستم کنترل دسترسی که معمولاً توسط برنامه نویسان و در مرحله برنامه نویسی تعبیه شده و ممکن است مورد استفاده واقع شوند.
Back up		تهیه نسخه پشتیبان (پشتیبان‌گیری)
Bad Ware	بدافزار	نرم‌افزارهایی که با اهداف بدخواهانه تولید و منتشر می‌شوند.
BCP	Business Continuity Plan	طرح پیوستگی (تداوم) عملیات- طرح احیای سیستم
Beneficiary	بهره‌بردار	فردی که از دارایی اطلاعاتی یا خدمات ارائه شده توسط آن بهره می‌برد اما ممکن است لزوماً کاربر یا مالک آن دارایی نباشد، مثل مشتریان بانک که از دستگاه ATM استفاده می‌نمایند.
Brute Force		سعی در فروپاشی یا نفوذ به مکانیزم کنترل دسترسی از طریق اقدام‌های مکرر
BS-7799		استاندارد ملی بریتانیا برای مدیریت امنیت اطلاعات که توسط مؤسسه استاندارد بریتانیا منتشر شده است.
BSI	British Standard Institute	مؤسسه استاندارد بریتانیا
Buffer Over Flow		سر ریز بافر، حالتی که منجر به فروپاشی سیستم به دلیل تجاوز حجم داده از فضای در نظر گرفته شده برای آن می‌باشد.

	Campus Area Network	CAN
گروه مقابله با شرایط اضطراری کامپیوتر	Computer Emergency Response Team	CERT
نهاد قانونی مجاز به صدور گواهی الکترونیک (مورد استفاده در زیرساخت کلید عمومی PKI)	مرکز صدور گواهی	Certificate Authority
	دفاع غیرنظامی، پدافند غیرعامل	Civil Defense
تعیین طبقه‌های مختلف جهت دسته‌بندی داده‌ها، اطلاعات و دارایی‌های اطلاعاتی و تعریف مکانیزم‌ها و حدود دسترسی خاص برای هر دسته	طبقه‌بندی	Classification
رخنه به مکانیزم‌های حفاظتی نرم‌افزارها یا سخت‌افزارها برای استفاده غیرمجاز	شکستن، تخریب	Crack
داده، مجموعه اطلاعات خام جمع‌آوری شده در خصوص پدیده‌های مختلف		Data
مرکز داده، مجموعه تجهیزات، ذخیره، بازیابی و پشتیبان‌گیری از اطلاعات که در محیطی امن از لحاظ فیزیکی مستقر شده و امکان دسترسی دائمی به اطلاعات نگهداری شده در خود را در اختیار مراجعه کنندگان قرار می‌دهد.		Data Center
	رمزگشایی (کشف رمز)	Decryption
فاجعه یا حادثه‌ای که منجر به تلفات جانی یا زیان‌های مالی شدید شود.		Disaster
طرح برنامه ریزی شده و زمانبندی راه‌اندازی یا نصب مجدد دارایی‌های اطلاعاتی و بازگشت به وضعیت قبل از وقوع فاجعه	طرح احیای پس از فاجعه	Disaster Recovery Plan
ناحیه‌ای که بین شبکه داخلی سازمان و اینترنت قرار گرفته و از دسترسی مستقیم از اینترنت به شبکه داخلی جلوگیری می‌نماید.	Demilitarized Zone	DMZ
وزارت دفاع ایالات متحده آمریکا	Department of Defense	DoD
رد سرویس، نوعی از حمله که علیرغم عدم فروپاشی سیستم، امکان پاسخ به سرویس دهنده میزبان به تقاضاهای رسیده از آن سلب می‌شود. حمله DoS معمولاً علیه کانال‌های ارتباطی (از طریق اشغال کامل پهنای باند) و یا ظرفیت پردازشی (از طریق اشباع ظرفیت به وسیله درخواست‌های نامفهوم یا غیرضروری) انجام می‌شود.	Denial of Service	DoS
خط دیجیتال مشترک	Digital Subscriber Line	DSL

تبادل الکترونیکی داده‌ها	Electronic Data Interchange	EDI
	تجارت الکترونیکی	Electronic Commerce
جمع آوری اطلاعات و داده‌های جاری در کانال‌های ارتباطی به منظور جاسوسی یا سوءاستفاده	شنود (استراق سمع) الکترونیکی	Electronic Eavesdropping
	رمزگذاری (رمزنگاری)	Encryption
هر گونه واقعه که منجر به تغییر حالت سیستم شود.	رویداد	Event
حمله از خارج شبکه خودی به اجزای داخل شبکه		External Attack
شبکه حاصل از اتصال چند Interanet به یکدیگر جهت اشتراک گذاری منابع بین اعضای Interanet ‌ها		Extranet
سامانه جلوگیری از حمله به شبکه تحت حفاظت بر اساس کنترل پورت‌های تبادل اطلاعات	دیواره آتش	Fire wall
فرد اقدام کننده به حمله دارایی‌های اطلاعاتی		Hacker
مرکز پاسخگویی (الکترونیک)		Help Desk (Electronic)
سیستم تشخیص نفوذ (با استفاده از مقایسه الگوهای ترافیکی شبکه با الگوهای شناسایی شده حمله قبلی یا تشخیص الگوهای غیر عادی)	Intrusion Detection System	IDS
کمیسیون بین المللی الکتروتکنیک		IEC
تنش ناشی از حمله به سیستم یا عدم عملکرد صحیح اخراجی آن	ضربه	Impact
اطلاعات، نتایج حاصل از پردازش داده‌ها		Information
دارایی اطلاعاتی		Information Asset
کمیته‌ای که باید بر اساس پیشنهاد استاندارد ISO/IEC-27001 تشکیل شده و راهبری فعالیت‌های مرتبط با مدیریت امنیت اطلاعات را به عهده می‌گیرد.	کمیته امنیت اطلاعات	Information Security Committee
Integrity یکی از محورهای سه گانه امنیت اطلاعات که توسط استاندارد ISO/IEC-27001 معرفی شده است.	جامعیت (صحت)	Integrity
حمله از داخل شبکه خودی به اجزای شبکه		Internal Attack

شبکه اطلاعاتی مشابه اینترنت که در حوزه یک یا چند سازمان مشترک المنافع بر پا شده و فقط به آن‌ها سرویس می‌دهد.		Intranet
فردی که به صورت غیر مجاز سعی در نفوذ به شبکه یا میزبان‌های موجود در آن را دارد.	نفوذگر	Intruder
	Intellectual Property Rights	IPR
سیستم پیشگیری از نفوذ	Intrusion Prevention System	IPS
محدوده تعیین شده جهت پیاده‌سازی سیستم مدیریت امنیت اطلاعات	قلمرو نظام مدیریت امنیت اطلاعات	ISMS SCOPE
سازمان بین المللی استاندارد	International Standard Organization	ISO
استاندارد بین المللی مدیریت امنیت اطلاعات که تحت شماره ۱۷۷۹۹ توسط سازمان بین المللی استاندارد منتشر شده است.		ISO/IEC-17799
استاندارد بین المللی بازنگری شده مدیریت امنیت اطلاعات که تحت شماره ۲۷۰۰۱ توسط ISO منتشر شده است.		ISO/IEC-27001
جداسازی منطقی بخش‌های مختلف شبکه		Isolation
دانش، نتایج حاصل از پردازش اطلاعات		Knowledge
پایگاه دانش		Knowledge base
فهرست برداری، ثبت عملکرد		Logging
نرم‌افزارهایی که با اهداف بدخواهانه تولید و منتشر می‌شوند.	بدافزار	Mal Ware
	Metropolitan Area Network	MAN
هر نوع وسیله ذخیره‌سازی اطلاعات اعم از فلاپی دیسک، دیسک سخت، نوار مغناطیسی، Blue Rey .DVD .CD ، حافظه‌های Flash ...	رسانه	Media
پردازش اطلاعات با استفاده از شبکه‌های ارتباطی سیار با تأکید بر اتصال دائم به شبکه هدف	پردازش همراه	Mobile Computing
آشکارسازی، دیده بانی، فعالیت نظارت بر ترافیک شبکه و داده‌های عبوری در آن برای تشخیص شرایط غیرعادی یا کنترل و مدیریت ترافیک		Monitoring

پروتکل مسیریابی بر اساس Labelها (به جای IP)	Multi Protocol Label Switching	MPLS
موافقت‌نامه عدم افشاء	Non Disclosure Agreement	NDA
ویژگی تعبیه شده در مدل‌های ارتباطی امن برای سلب امکان انکار ارسال یا دریافت پیام یا انجام عمل	انکارناپذیری (عدم انکار)	Non Repudiation
پروتکل تعیین زمان در شبکه	Network Time Protocol	NTP
سیستم عامل	Operating System	OS
فردی که دارایی اطلاعاتی در اختیار وی قرار گرفته است و مسئولیت حفاظت و بهره‌برداری صحیح از آن را به عهده دارد ممکن است این فرد همان کاربر باشد.	مالک، متصدی، تحویل گیرنده	Owner
بسته نرم‌افزاری (غیرقابل تغییر)	بسته نرم‌افزاری	Package
شرکت‌های عرضه کننده خدمات انتقال اطلاعات پر سرعت دارای پروانه از سازمان تنظیم مقررات رادیویی	Port Access Provider	PAP
مشخصه خاص احراز هویت جهت اثبات هویت ادعا شده	کلمه عبور، گذر واژه	Password
بررسی نرم‌افزار نقاط ضعف و نفوذپذیر دارایی‌های اطلاعاتی با استفاده از نرم‌افزار یا روش‌های ابتکاری	تست نفوذپذیری	Penetration Test
مکان فیزیکی قابل افراز حاوی تجهیزات یا دارایی‌های اطلاعاتی	بته اطلاعاتی	Perimeter
شماره شناسایی شخصی	Personal Identification Numbers	PIN
زیرساخت کلید عمومی که برابر تضمین محرمانگی و صحت پیام و عدم انکار ارسال یا دریافت آن به کار گرفته می‌شود.	Public Key Infrastructure	PKI
نرم‌افزارهای پویش شبکه جهت شناسایی پورت‌های فعال TCP (باز بودن پورت به معنی آن است که نرم‌افزاری وجود دارد که بسته‌های اطلاعاتی TCP ارسال شده به آدرس آن پورت را دریافت کرده و مورد پردازش قرار می‌دهد.	پویشگر پورت	Port Scanner
نقطه متمرکز ارائه خدمات سازمان در اینترنت که امکان ارائه کلیه خدمات الکترونیکی سازمان به مراجعان را ایجاد نموده و به علاوه امکان انتقال مراجعه کننده به سایر سازمان‌های دیگر مرتبط با فعالیت سازمان را فراهم می‌کند.		Portal
حق دسترسی ممتاز (در مدل‌های کنترل دسترسی)	ممتاز	Privilege

احیا		Recovery
ریسک غیر قابل اجتناب پس از امن سازی سیستم (به دلیل ماهیت دارایی اطلاعاتی یا محدودیت منابع مالی یا دانش امن سازی)	ریسک باقیمانده	Residual Risk
خطرپذیری، مقدار زیان احتمالی ناشی از بروز حادثه		Risk
بررسی دارایی‌های اطلاعاتی جهت شناسایی میزان زیان ناشی از عدم عملکرد صحیح هر یک و مقایسه آن‌ها با یکدیگر	ارزیابی ریسک	Risk Assessment
شرکت‌های عرضه کننده خدمات ارتباط ماهواره‌ای دارای پروانه از سازمان تنظیم مقررات و ارتباطات رادیویی	Satellite Access Provider	SAP
کیت توسعه نرم‌افزاری	Software Development Kit	SDK
هر واقعه‌ای که نشان دهنده احتمال تخطی از معیارهای تعیین شده امنیتی باشد.	واقعه امنیتی	Security Event
هر واقعه‌ای که منجر به تخطی از معیارهای امنیتی بشود.	حادثه امنیتی	Security Incident
برچسب (سخت‌افزاری یا نرم‌افزاری) الصاق شده به دارایی‌های اطلاعاتی که مبین نیازهای امنیتی کار با آن دارایی اطلاعاتی می‌باشد.	برچسب امنیتی	Security Label
جداسازی فیزیکی شبکه‌ها از یکدیگر		Segregation
موافقت‌نامه سطح خدمات	Service Level Agreement	SLA
بو کشیدن، استراق سمع جهت آگاهی از ترافیک و داده‌های در حال عبور از شبکه		Sniffing
بیانیه کاربردپذیری	Statement Of Applicability	SOA
استفاده از فریب، ناآگاهی یا خصوصیات اخلاقی افراد برای جمع آوری اطلاعاتی که از روش‌های مصاحبه مستقیم یا حضوری قابل نیست.	مهندسی اجتماعی	Social Engineering
وصله نرم‌افزاری، نسخه‌های تصحیحی که برای رفع نقص نرم‌افزارها و از سوی تولیدکنندگان نرم‌افزار منتشر می‌شود.		Software Patch
متن برنامه‌های کامپیوتری	کد منبع	Source Code
جعل، قرارداد خود به جای دیگری به خصوص با استفاده از آدرس‌های IP برای سرقت نشست یا معرفی خود به جای افراد مجاز به دسترسی به اطلاعات هدف		Spoofing

سر ریز پشته، حالتی که منجر به فروپاشی سیستم به دلیل تجاوز مقدار داده‌ها از حد مجاز قابل ذخیره‌سازی در حافظه سیستم می‌شود.		Stack Over Flow
فایل‌های موقتی که در حین پردازش ایجاد می‌شود. باقی ماندن این فایل‌ها روی سیستم و دسترسی افراد غیرمجاز به آن‌ها ممکن است باعث آسیب پذیری ناشی از دسترسی به اطلاعات محرمانه شود.		Temporary Files
تهدید، عبارت است شرایطی که ممکن است باعث سوءاستفاده از آسیب پذیری‌ها شده و یا ضربه پذیری از نقطه افزایش یابد.		Threat
نشانه نرم‌افزاری یا سخت‌افزاری مورد استفاده در اثبات هویت	نشانه	Token
کد مخربی که در قالب یک برنامه جذاب به کاربر عرضه می‌شود و پس از نصب امکان نفوذ نفوذگر به سیستم را ایجاد می‌نماید.	اسب تروا	Trojan Horse
	Uninterrupted Power Supply	UPS
فردی که به منظور خاصی اقدام به استفاده دائم از دارایی اطلاعاتی می‌نماید.	کاربر	USER
USER Identification مشخصه عام احراز هویت از طریق ادعای آن	شناسه کاربری	USER ID
نسخه		Version
کنترل نسخه (جهت اطمینان از سازگار بودن اجزای مختلف نرم‌افزارهای به کار گرفته شده از لحاظ سازگاری و توالی زمانی و صحت اطلاعات)		Version Control
شبکه اختصاصی مجازی	Virtual Private Network	VPN
آسیب پذیری، عبارت است از ضعف در برخی مشخصه‌های دارایی اطلاعاتی که می‌تواند باعث کاهش کارایی، توقف عملکرد و یا تحمیل زیان گردد.		Vulnerability
		War Dialer
موافقت‌نامه امنیتی محدود کننده صادرات تجهیزات دارای کاربرد دوگانه که از طرف دول عمدتاً غربی تبادل شده و صادرات این نوع کالاها یا خدمات به کشورهای خارج از حوزه کنترل ایشان را ممنوع می‌سازد.		Wassenaar
مرورگر وب (تارنما)		Web browser

Wild Line	خط وحشی	خط ارتباطی متصل به مودم
اصالت پیام		ویژگی اطمینان از انتساب پیام به فرستنده آن
افتا		امنیت فضای تبادل اطلاعات (شورای عالی افتا ۱۳۸۴)
چرخه PDCA	PLAN-DO-CHECK-ACT	چرخه بهبود مستمر فرآیند
رده اهمیت		رده بندی تعیین شده توسط سازمان پدافند غیرعامل برای نشان دادن میزان اهمیت مراکز و سازمان‌ها که به ترتیب دارای درجه‌های حیاتی، حساس و مهم می‌باشد.
سر پل امنیتی		نقطه انتخاب شده برای شروع امن سازی. ابتدا دارایی‌های اطلاعاتی موجود در این نقطه به طور همزمان امن سازی شده و سپس سایر دارایی‌های مرتبط با این نقطه و بعد از آن نیز دارایی‌های اطلاعاتی مرتبط با آن دارایی‌ها و به همین ترتیب سیستم به طور کامل امن سازی می‌شود.
سیستم نهفته		نرم‌افزارهای کنترلی نصب شده در تجهیزات سخت‌افزاری
منا		مطالعات تجارت الکترونیک (وزارت بازرگانی ۱۳۸۴)
محرمانگی		Confidentiality یکی از محورهای سه گانه امنیت اطلاعات که توسط استاندارد ISO/IEC-27001 معرفی شده است.
نظام جامع فناوری اطلاعات کشور		سند راهبردی مبین راهبردها و راهکارهای توسعه فناوری اطلاعات کشور که در تاریخ ۸۶/۱۰/۵ مورد تصویب هیأت وزیران قرار گرفته است.

مرتب شده بر اساس ستون دوم - فارسی

بررسی دارایی‌های اطلاعاتی جهت شناسایی میزان زیان ناشی از عدم عملکرد صحیح هر یک و مقایسه آن‌ها با یکدیگر	ارزیابی ریسک	Risk Assessment
کد مخربی که در قالب یک برنامه جذاب به کاربر عرضه می‌شود و پس از نصب امکان نفوذ نفوذگر به سیستم را ایجاد می‌نماید.	اسب تروا	Trojan Horse
ویژگی تعبیه شده در مدل‌های ارتباطی امن برای سلب امکان انکار ارسال یا دریافت پیام یا انجام عمل	انکارناپذیری (عدم انکار)	Non Repudiation
نرم‌افزارهایی که با اهداف بدخواهانه تولید و منتشر می‌شوند.	بدافزار	Bad Ware
نرم‌افزارهایی که با اهداف بدخواهانه تولید و منتشر می‌شوند.	بدافزار	Mal Ware
برچسب (سخت‌افزاری یا نرم‌افزاری) الصاق شده به دارایی‌های اطلاعاتی که مبین نیازهای امنیتی کار با آن دارایی اطلاعاتی می‌باشد.	برچسب امنیتی	Security Label
بسته نرم‌افزاری (غیرقابل تغییر)	بسته نرم‌افزاری	Package
مکان فیزیکی قابل افراز حاوی تجهیزات یا دارایی‌های اطلاعاتی	بنه اطلاعاتی	Perimeter
فردی که از دارایی اطلاعاتی یا خدمات ارائه شده توسط آن بهره می‌برد اما ممکن است لزوماً کاربر یا مالک آن دارایی نباشد، مثل مشتریان بانک که از دستگاه ATM استفاده می‌نمایند.	بهره‌بردار	Beneficiary
پردازش اطلاعات با استفاده از شبکه‌های ارتباطی سیار با	پردازش همراه	Mobile Computing

تأکید بر اتصال دائم به شبکه هدف		
نرم‌افزارهای پویش شبکه جهت شناسایی پورت‌های فعال TCP (باز بودن پورت به معنی آن است که نرم‌افزاری وجود دارد که بسته‌های اطلاعاتی TCP ارسال شده به آدرس آن پورت را دریافت کرده و مورد پردازش قرار می‌دهد.	پویشگر پورت	Port Scanner
	تجارت الکترونیکی	Electronic Commerce
بررسی نرم‌افزار نقاط ضعف و نفوذپذیر دارایی‌های اطلاعاتی با استفاده از نرم‌افزار یا روش‌های ابتکاری	تست نفوذپذیری	Penetration Test
Integrity یکی از محورهای سه گانه امنیت اطلاعات که توسط استاندارد ISO/IEC-27001 معرفی شده است.	جامعیت (صحت)	Integrity
هر واقعه‌ای که منجر به تخطی از معیارهای امنیتی بشود.	حادثه امنیتی	Security Incident
خط ارتباطی متصل به مودم	خط وحشی	Wild Line
برخی راههای پنهان برای دور زدن و عبور از سیستم کنترل دسترسی که معمولاً توسط برنامه نویسان و در مرحله برنامه نویسی تعبیه شده و ممکن است مورد استفاده واقع شوند.	در پشتی	Back Door
یکی از محورهای سه گانه امنیت اطلاعات که توسط استاندارد ISO/IEC-27001 معرفی شده است.	دسترسی پذیری	Availability
	دفاع غیرنظامی، پدافند غیرعامل	Civil Defense
سامانه جلوگیری از حمله به شبکه تحت حفاظت بر اساس کنترل پورت‌های تبادل اطلاعات	دیواره آتش	Fire wall
هر نوع وسیله ذخیره‌سازی اطلاعات اعم از فلاپی دیسک، دیسک سخت، نوار مغناطیسی، CD ، Blue Rey ، DVD	رسانه	Media

حافظه‌های Flash ...		
	رمزگذاری (رمزنگاری)	Encryption
	رمزگشایی (کشف رمز)	Decryption
هر گونه واقعه که منجر به تغییر حالت سیستم شود.	رویداد	Event
ریسک غیر قابل اجتناب پس از امن سازی سیستم (به دلیل ماهیت دارایی اطلاعاتی یا محدودیت منابع مالی یا دانش امن سازی)	ریسک باقیمانده	Residual Risk
USER Identification مشخصه عام احراز هویت از طریق ادعای آن	شناسه کاربری	USER ID
جمع آوری اطلاعات و داده‌های جاری در کانال‌های ارتباطی به منظور جاسوسی یا سوءاستفاده	شنود (استراق سمع) الکترونیکی	Electronic Eavesdropping
رخنه به مکانیزم‌های حفاظتی نرم‌افزارها یا سخت‌افزارها برای استفاده غیرمجاز	شکستن، تخریب	Crack
تنش ناشی از حمله به سیستم یا عدم عملکرد صحیح اخراجی آن	ضربه	Impact
تعیین طبقه‌های مختلف جهت دسته‌بندی داده‌ها، اطلاعات و دارایی‌های اطلاعاتی و تعریف مکانیزم‌ها و حدود دسترسی خاص برای هر دسته	طبقه‌بندی	Classification
طرح برنامه ریزی شده و زمانبندی راه اندازی یا نصب مجدد دارایی‌های اطلاعاتی و بازگشت به وضعیت قبل از وقوع فاجعه	طرح احیای پس از فاجعه	Disaster Recovery Plan
محدوده تعیین شده جهت پیاده‌سازی سیستم مدیریت امنیت اطلاعات	قلمرو نظام مدیریت امنیت اطلاعات	ISMS SCOPE

مالک، متصدی، تحویل گیرنده	فردی که دارایی اطلاعاتی در اختیار وی قرار گرفته است و مسئولیت حفاظت و بهره‌برداری صحیح از آن را به عهده دارد ممکن است این فرد همان کاربر باشد.	Owner
مدل مرجع کنترل دسترسی	مبثنی بر احراز هویت، احراز صلاحیت و پاسخگویی (Authentication, Authorization, Accountability)	AAA
مرکز صدور گواهی	نهاد قانونی مجاز به صدور گواهی الکترونیک (مورد استفاده در زیرساخت کلید عمومی (PKI)	Certificate Authority
ممتاز	حق دسترسی ممتاز (در مدل‌های کنترل دسترسی)	Privilege
مهندسی اجتماعی	استفاده از فریب، ناآگاهی یا خصوصیات اخلاقی افراد برای جمع‌آوری اطلاعاتی که از روش‌های مصاحبه مستقیم یا حضوری قابل نیست.	Social Engineering
نشانه	نشانه نرم‌افزاری یا سخت‌افزاری مورد استفاده در اثبات هویت	Token
نفوذگر	فردی که به صورت غیر مجاز سعی در نفوذ به شبکه یا میزبان‌های موجود در آن را دارد.	Intruder
واقعه امنیتی	هر واقعه‌ای که نشان دهنده احتمال تخطی از معیارهای تعیین شده امنیتی باشد.	Security Event
کاربر	فردی که به منظور خاصی اقدام به استفاده دائم از دارایی اطلاعاتی می‌نماید.	USER
کد منبع	متن برنامه‌های کامپیوتری	Source Code
کلمه عبور، گذر واژه	مشخصه خاص احراز هویت جهت اثبات هویت ادعا شده	Password

کمیته‌ای که باید بر اساس پیشنهاد استاندارد ISO/IEC-27001 تشکیل شده و راهبری فعالیت‌های مرتبط با مدیریت امنیت اطلاعات را به عهده می‌گیرد.	کمیته امنیت اطلاعات	Information Security Committee

مرتب شده بر اساس ستون دوم - لاتین

فهرست کنترل دسترسی	Access Control List	ACL
مؤسسه استاندارد بریتانیا	British Standard Institute	BSI
طرح پیوستگی (تداوم) عملیات - طرح احیای سیستم	Business Continuity Plan	BCP
	Campus Area Network	CAN
گروه مقابله با شرایط اضطراری کامپیوتر	Computer Emergency Response Team	CERT
ناحیه‌ای که بین شبکه داخلی سازمان و اینترنت قرار گرفته و از دسترسی مستقیم از اینترنت به شبکه داخلی جلوگیری می‌نماید.	Demilitarized Zone	DMZ
رد سرویس، نوعی از حمله که علیرغم عدم فروپاشی سیستم، امکان پاسخ به سرویس دهنده میزبان به تقاضاهای رسیده از آن سلب می‌شود. حمله DoS معمولاً علیه کانال‌های ارتباطی (از طریق اشغال کامل پهنای باند) و یا ظرفیت پردازشی (از طریق اشباع ظرفیت به وسیله درخواست‌های نامفهوم یا غیرضروری) انجام می‌شود.	Denial of Service	DoS
وزارت دفاع ایالات متحده آمریکا	Department of Defense	DoD
خط دیجیتالی مشترک	Digital Subscriber Line	DSL
تبادل الکترونیکی داده‌ها	Electronic Data Interchange	EDI
نظام مدیریت امنیت اطلاعات	Information Security Management System	ISMS
	Intellectual Property Rights	IPR
سازمان بین المللی استاندارد	International Standard Organization	ISO
سیستم تشخیص نفوذ (با استفاده از مقایسه الگوهای	Intrusion Detection System	IDS

ترافیکی شبکه با الگوهای شناسایی شده حمله قبلی یا تشخیص الگوهای غیر عادی)		
سیستم پیشگیری از نفوذ	Intrusion Prevention System	IPS
	Metropolitan Area Network	MAN
پروتکل مسیریابی بر اساس Label (به جای IP)	Multi Protocol Label Switching	MPLS
پروتکل تعیین زمان در شبکه	Network Time Protocol	NTP
موافقت‌نامه عدم افشاء	Non Disclosure Agreement	NDA
سیستم عامل	Operating System	OS
شماره شناسایی شخصی	Personal Identification Numbers	PIN
چرخه بهبود مستمر فرآیند	PLAN-DO-CHECK-ACT	چرخه PDCA
شرکت‌های عرضه کننده خدمات انتقال اطلاعات پر سرعت دارای پروانه از سازمان تنظیم مقررات رادیویی	Port Access Provider	PAP
زیرساخت کلید عمومی که برابر تضمین محرمانگی و صحت پیام و عدم انکار ارسال یا دریافت آن به کار گرفته می‌شود.	Public Key Infrastructure	PKI
شرکت‌های عرضه کننده خدمات ارتباط ماهواره‌ای دارای پروانه از سازمان تنظیم مقررات و ارتباطات رادیویی	Satellite Access Provider	SAP
موافقت‌نامه سطح خدمات	Service Level Agreement	SLA
کیت توسعه نرم‌افزاری	Software Development Kit	SDK
بیانیه کاربردپذیری	Statement Of Applicability	SOA
	Uninterrupted Power Supply	UPS
شبکه اختصاصی مجازی	Virtual Private Network	VPN

دستورالعمل‌های اجرایی مدیریت امنیت اطلاعات

به همان نسبت که استفاده از فناوری اطلاعات در فرایندهای کاری گسترش پیدا می‌کند، انگیزه برای دستیابی و دسترسی غیر مجاز به اطلاعات نیز اهمیت می‌یابد. بطوری که امروزه گروههای مختلفی به صورت سازمان یافته و یا غیر سازمان یافته شکل گرفته و اقدام به این کار می‌کنند.

جهت برقراری امنیت در سازمانها، موسسه بین‌المللی استاندارد اقدام به تدوین استاندارد تحت عنوان سیستم مدیریت امنیت اطلاعات (ISMS) نمود. این استاندارد در سال ۲۰۰۰ با نام ISO 17799 و سپس در سال ۲۰۰۵ با نام ISO 27001 (شامل ۱۱ حوزه) منتشر گردید. لازمه اجرایی شدن این استاندارد، تدوین دستورالعمل‌های لازم برای اجرای آن است. کتاب حاضر (جلد یک) بخشی از دستورالعمل‌های اجرایی با اهمیت این استاندارد می‌باشد. امید است با اجرای آنها در ارتقاء سطح امنیت سازمانها موثر واقع گردد.

طرح تدوین طرح جامع فناوری اطلاعات کشور

کد پروژه : ITMP : 40812001-04-3-4

www.nass.ir

شابک : ۹۷۸-۹۶۴-۴۱۰-۲۰۱-۱



دفتر انتشارات

تهران - م انقلاب - خ اردیبهشت - بن پست مبین - شماره ۶
تلفن : ۶۶۴۱۲۳۸۵ - ۶۶۹۵۳۸۸۳ - ۶۶۴۶۵۶۷۴ فکس : ۶۶۹۵۷۶۹۰