بنام خدا

معماری امنیت اطلاعات

(سیستم مدیریت امنیت اطلاعات)

Information Security Management System

ویژه دانشجویان

تدوین : علی ثاقب موفق

۱– مقدمه :

امروزه با افزایش حجم اطلاعات موجود و قابل تبادل و از طرفی گسترش روز افزون استفاده از شبکه ها، خصوصا شبکه های کامپیوتری وهمچنین ایجاد شبکه های جهانی ، چالش بزرگی برای صاحبان اطلاعات به لحاظ تهدیدات امنیتی این حوزه بوجود آمده که به مثابه زنگ خطری برای تمامی افراد و کاربران می باشد.

در حال حاضر سرقت دانش و اطلاعاتی که برای آن هزینه و وقت زیادی صرف شده ، یکی از خطرات بالقوه در شبکه های کامپیوتری می باشد . متاسفانه این خطرات توسط افرادی تحمیل میشود که باهوش تر از افراد معمولی هستند و قدرت نفوذ و ضربه به شبکه را دارند .

تهدیدهای بالقوه برای امنیت شبکه های کامپیوتری، به صورت عمده شامل افشای غیر مجاز اطلاعات، قطع ارتباط و اختلال در شبکه، جعل و دستکاری غیر مجاز اطلاعات و ... می باشد . یکی از مهم ترین مولفه های ایجاد یک سیستم امنیت شبکه ، ارائه سیاست گذاری در این خصوص میباشد.

در واقع خط مشی یا سیاست گذاری جهت حفظ امنیت شبکه ، انتظارات یک سازمان در جهت ایجاد امنیت در شبکه های مختلف آن سازمان را تعریف میکند و در عین حال روند پیشگیری از حوادث امنیتی شبکه را مشخص می نماید. تعیین خط مشی امنیت در شبکه بنیان و اساس امنیت شبکه است، زیرا دارایی ها و سرمایه های اصلی یک شبکه و سازمان که می باید در امان باشند، با این خط مشی مشخص می شود .

سیاست گذاری در قالب مولفه هایی چون : تحلیل تهدیدات امنیتی، تحلیل آسیب پذیری ها، سیاست گذاری امنیتی در خصوص محافظت از دارایی های اطلاعاتی، تجهیزات و ... صورت میگیرد . به هر حال امروزه امنیت ملی و اقتدار سیاسی و اقتصادی به طرز پیچیده ای به امنیت اطلاعات گره خورده است و نه تنها دولتها، بلکه تک تک افراد را نیز تهدید میکند .

از طرفی از آنجائیکه شبکه های نسل جدید تقریباً از تمامی امکانات مخابراتی به صورت یکپارچه و مجتمع استفاده نموده و با بکارگیری پروتکلهای مختلف انو اع سرویسهای مورد نظر مشترک را ارائه مینمایند، لذا ضروری است برای پیاده سازی این نوع فنآوریها نیز دقت و هوشیاری بسیار از دیدگاه امنیت مورد توجه قرار گیرد.

۲– معماری امنیت شبکه

مدیریت امنیت اطلاعات فرایندی است که بر اساس آن اطلاعات در مقابل تهدیدات مختلف حفاظت خواهد شد به نحوی که از ادامه فعالیت با حداکثر کارایی اطمینان حاصل شود.

امنیت یک فرایند است که بایستی دائم اصلاح و بهبود یابد و به عبارتی دیگر داخل حلقه PDCA دمینگ کامل شود که شامل Plan – Do – Check – Act می باشد که همان استقرار نرم افزار و سخت افزارهای امنیتی و سپس اجزاء آنها و در ادامه بازنگری و نهایتا بهبود وضعیت است که این مسیر دائم فعالی می باشد. امنیت صد در صد وجود ندارد بلکه ما همواره در حال افزایش امنیت سیستمها هستیم و آن را به ۱۰۰٪ نزدیک می کنیم. برای اعمال امنیت بایستی مراحل زیر طی شود:

۳– سیاست گذاری امنیت اطلاعات

سازمان پدافند غیر عامل بعنوان مرجع طبقه بندی سازمانها را به لحاظ امنیت و درجه حساسیت ، انجام می دهد و این مبنای آن سازمان به لحاظ میزان امنیت و اعمال موارد امنیتی میشود. سندافتا (امنیت فضای تبادل اطلاعات) نیز بدین منظور تهیه شده است. بعنوان مثال سازمانهای نظامی و دفاعی دارای درجه محرمانگی بیشتری نسبت به سازمانهای آموزشی می باشند و به همین ترتیب زیرساخت های حیاتی کشور تبیین می شود. پس از این مرحله سازمان بایستی متناسب به زیرساخت و درجه محرمانگی خود نسبت به اعمال ملاحظات امنیتی و حفاظتی اقدام نماید.

۴– سازماندهی امنیت اطلاعات

تفکیک اطلاعات به لحاظ عادی و محرمانگی و استقرار مناسب آنها در سیستم و سپس تعریف پارامترهای متنوع امنیتی و اعمال آنها بر روی منابع اطلاعاتی سازمان به نحوی که پرسنل متناسب با شغل ، سمت و درجه

حفاظتی بتوانند به منابع اطلاعاتی دستیابی پیدا نمایند. به عبارت دیگر بایستی مشخص شود که منابع اطلاعاتی سازمان در چه زمان هایی و به چه صورت و توسط چه کسانی می تواند مورد دستیابی واقع شود و پرسنل آن سازمان در چه زمانی و از چه ایستگاه های کاری و از چه روشی و با چه نوع مجوزهایی می توانند به اطلاعات دسترسی یابند.

۵– مدیریت دارایی ها

اطلاعات بعنوان دارایی سازمان قلمداد می شود که شامل نرم افزارهای سیستمی و کاربردی ، سخت افزارها ی پردازشی و ارتباطی و ذخیره سازی ، بانک های اطلاعاتی حاوی اطلاعات باارزش سازمان و خدمات پردازشی است که همه سخت افزارهای رایانه ای و شبکه ای به نحوی وظیفه ثبت ، نگهداری ، مبادله و حفاظت از اطلاعات را بعهده دارند و داده های تحلیل شده ارزش بیشتری پیدا خواهند کرد که عموما به شکل اطلاعات با معنی و در حالت پیشرفته تر بصورت دانش در سیستمهای مدیریت دانش ذخیره می شوند.

۶– کنترل دسترسی:

تعریف مجوزهای دسترسی و سطوح دسترسی کاربران به سیستم یکی از مهمترین بخش های برقرای امنیت اطلاعات می باشد به طوریکه مجوزهای خواندن ، نوشتن، حذف، ایجاد، اصلاح و کلیه مجوزهای دسترسی قابل تعریف برای کاربران سیستم می باشد و ناظر شبکه یا همان Administrator نسبت به تعریف کاربران و مجوزهای دسترسی ایشان اقدام می نماید.

مراحل پیاده سازی و اجرای نظام مدیریت امنیت اطلاعات به طرح ذیل است:

۱- سیاست گذاری کلان و تدوین برنامه راهبردی
۲- سازماندهی و ایجاد زیرساخت های سازمانی
۳- ایجاد زیرساخت های امنیتی و امن سازی اولیه
۴- حفاظت از امنیت و تداوم آن

۷–زیر ساخت های امنیتی:

۱- زیرساخت امنیت فیزیکی و محیطی
۲- زیرساخت کلید عمومی

۳- زیرساخت امنیت ارتباطات شبکه

۴- زیرساخت امنیت انرژی و نیازهای حیاطی

۵- زیرساخت پشتیبان گیری و مقابله با شرایط اضطراری

حال برای اجرایی نمودن سیاست های امنیتی متخده و ساماندهی امنیتی اطلاعات و ایجاد زیرساخت های امنیت شبکه و نهایتا استقرار استاندارد مدیریت امنیت اطلاعات (ISMS) ، ضروری است گام های ذیل طی شده و با دقت فرایند اجرایی آن تا حصول نتیجه مطلوب دنبال و پیگیری شود :

۸ –امنیت تجهیزات خارج از ابنیه:

هدف از تدوین این دستورالعمل محافظت از دارایی های اطلاعاتی مستقر در خارج از ابنیه و یا محوطه ها و سایت‌های تحت کنترل و اطمینان از حفظ امنیت تجهیزات و دارایی‌هایی است که خارج از مکان‌های تحت پوشش نصب شده یا قرار گرفته‌اند

الزامات

-فهرست موجودی دارایی های اطلاعاتی باید به صورت دوره ای از لحاظ شناسایی تجهیزات نصب شده در خارج از ابنیه و یا خارج از محوطه‌های تحت کنترل، مورد بازبینی قرار گیرد.

-لازم است تجهیزاتی که بنا به دلایل موجه یا به اجبار خارج از ابنیه تحت کنترل سازمان نصب می‌شوند، اعم از فعال و غیرفعال در برابر عوامل زیر محافظت شوند:

- سرقت و دسترسی غیر مجاز (دستکاری یا تخریب).

- شنود اطلاعات (الکترومغناطیسی).

- تخریب سهوی.

- تهدیدات محیطی (طوفان، سیل، زلزله، صاعقه، حیوانات).

- قطع یا نوسان جریان برق.

- باید در بازه‌های زمانی مرتب و یا تصادفی وضعیت تجهیزات خارج از ابنیه به صورت فیزیکی مورد بازبینی قرار گیرد.

- ضروری است جهت دسترسی به نرم‌افزارهای نصب شده بر روی اینگونه تجهیزات از کلمه عبور استفاده شود.

- لازم است برای هر یک از تجهیزاتی که جهت بهره‌برداری و بنا به ضرورت‌های فنی از ابنیه تحت کنترل خارج می‌شوند و در محل تحت مالکیت سازمانی دیگر نصب می‌گردند، دستورالعمل‌های حفاظتی خاص تدوین و به اجرا گذاشته شود.

- لازم است برای استفاده از تجهیزاتی که در داخل تونل و یا معابر زیرزمینی نصب شده یا قرار دارند نکات امن‌سازی آن محل رعایت شود. به عنوان مثال در صورتیکه کانال یا معبر زیرزمینی در محوطه‌ای قرار داشته باشد که امکان آب گرفتگی آن وجود دارد بایستی در خصوص جلوگیری از آب گرفتگی یا تخلیه آب تصمیم‌گیری به عمل آید.

- لازم است در مراکز حساس و حیاتی برای امنیت تجهیزات از سیستم‌های خودکار تشخیص صحت عملکرد و ثبت دسترسی استفاده گردد.

- تجهیزاتی که بنا به ضرورت در مکان‌های عمومی نصب می‌شوند باید به اندازه کافی در مقابل دسترسی غیرمجاز یا تخریب فیزیکی مستحکم‌سازی شوند.

فرآیند

مراحل اجرای دستورالعمل امنیت تجهیزات خارج از ابنیه به شرح زیر می باشد:

۱- ابتدا لازم است فهرستی از دارایی اطلاعاتی سازمان که خارج از ابنیه سازمان مستقر شده اند تهیه شود. همچنین بمنظور ارائه راهکارها و مکانیزم های امنیتی و حفاظتی مفید لازم است در این مرحله به شناسایی تهدیدات و ریسک های مرتبط با هر یک از دارایی های شناسایی شده اقدام گردد.

۲- پس از آن باید الزامات امنیتی برای حفاظت از هر یک از دارایی های اطلاعاتی تعیین شوند. همچنین لازم است در صورتیکه سازمان الزامات اختصاصی دیگری نیز در خصوص این موضوع دارد به الزامات بیان شده در این سند افزوده گردد.

۳- پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکانیزم های برآورده کننده الزامات تامین شود.

۴- پس از تامین تجهیزات و مکانیزم ها در این مرحله اقدام به پیاده سازی و اجرای مکانیزم ها و کلیه الزامات تدوین شده می گردد.

۵- در صورتی که پس از پیاده سازی مکانیزم ها، کلیه الزامات امنیت تجهیزات خارج از ابنیه تدوین شده ، برآورده شده باشد این دستورالعمل پایان می‌پذیرد. در غیر اینصورت لازم است مرحله ۴ مجددا اجرا گردد.

۹- خارج از رده سازی و استفاده مجدد:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی امحاء یا انهدام و خارج از رده‌سازی یا بازیابی دارایی‌های اطلاعاتی و اطمینان از رعایت الزامات امنیتی و اصول طبقه‌بندی اطلاعات در اجرای مراحل فوق می‌باشد.

الزامات

-لازم است قبل از ارسال دارایی‌های اطلاعاتی قدیمی برای امحاء یا انهدام یا استفاده مجدد، هرگونه اطلاعات موجود در تجهیزات فوق مورد بررسی قرار گرفته و در صورت مشاهده اطلاعات، اقدامات لازم در مورد حذف یا حفظ آنها انجام شود.

- ضروری است روش امحاء و انهدام به نحوی باشد که بازسازی مجدد و استخراج اطلاعات از آنها غیر ممکن باشد.

-می‌بایست سوابق عملیات انهدام رسانه‌های حاوی دارایی‌های اطلاعاتی ثبت گردد تا در رسیدگی‌های ممیزی قابل پیگیری باشد.

-در مراکز حساس و حیاتی (از دیدگاه سازمان پدافند غیرعامل) ضرورت دارد با توجه به موقعیت‌های زمانی و امکانات موجود، روش انهدام مورد پذیرش سازمان توسط نهاد متصدی امنیت تعیین و مصوب گردد.

- لازم است در موارد پیش‌بینی نشده و وضعیت‌های فوق‌العاده که امکان نگهداری و حفاظت از دارایی‌های اطلاعاتی یا رسانه‌های حاوی اطلاعات طبقه‌بندی شده وجود ندارد، بلافاصله اقدامات لازم در خصوص انهدام اطلاعات صورت گیرد. با توجه به این الزام ضروری است:

- فهرست دارایی های اطلاعاتی که باید در صورت وقوع شرایط اضطراری منهدم شوند قبلا تهیه شده و به صورت امن در اختیار امین سازمان قرار گیرد.

- روش و ابزار انهدام قبلا تهیه شده و در اختیار امین سازمان قرار داده شود.

-در مراکز حساس و حیاتی می‌بایست کمیته تشخیص، تفکیک و امحاء داده‌ها جهت کنترل و نظارت دقیق بر حسن اجرای امحاء اطلاعات تشکیل گردد.

- لازم است در مراکز حساس و حیاتی یک انبار یا بایگانی مرکزی جهت کنترل و نگهداری متمرکز اموال و دارایی‌های اطلاعاتی طبقه‌بندی شده ایجاد گردد و از پراکندگی اسناد و تجهیزات در قسمت‌های مختلف سازمان جلوگیری شود.

- در مراکز حساس و حیاتی می‌بایست میزان ارزش حفاظتی اسناد و تجهیزات حاوی دارایی‌های اطلاعاتی به منظور جلوگیری از افشاء یا دسترسی غیرمجاز و تعیین محدودیت‌های لازم قبل از امحاء یا انهدام و استفاده مجدد در طبقه‌بندی اطلاعات قرار گیرد.

- در مراکز حساس و حیاتی می‌بایست حتی‌الامکان از تکثیر و بازیابی تجهیزات حاوی دارایی‌های اطلاعاتی حساس و مهم خودداری شود، اما در صورت ضرورت، تکثیر دارایی‌های اطلاعاتی می‌بایست طبق قوانین و مقررات نظارتی و حفاظتی نهاد متصدی امنیت اطلاعات صورت گیرد.

فرآیند

مراحل اجرای دستورالعمل خارج از رده سازی و استفاده مجدد به شرح زیر می باشد:

۱- تحویل گیرنده، مالک یا متصدی دارایی اطلاعاتی پس از بررسی‌های لازم مراتب را در مورد عدم نیاز به وجود دارایی اطلاعاتی به نماینده نهاد متصدی امنیت اطلاعات اعلام می کند و پس از صدور دستور تشخیص، تفکیک و امحاء دارایی توسط نهاد متصدی امنیت اطلاعات، تحویل گیرنده، مالک یا متصدی دارایی اطلاعاتی تشکیل کمیته تشخیص، تفکیک و امحاء داده‌ها را درخواست می‌نماید.

۲- پس از بررسی در جلسه در صورتی که مشخص شود دارایی اطلاعاتی باید حتما منهدم شود ابتدا لازم است از پاک سازی و عقیم سازی دارایی اطلاعاتی از لحاظ وجود اطلاعات حساس یا دارای طبقه بندی اطمینان حاصل شود(بر اساس شیوه های بیان شده در بخش توضیحات) و سپس مطابق با برنامه‌های موجود اقدام به انهدام دارایی اطلاعاتی گردد. با انجام این کار این دستورالعمل پایان می

پذیرد. برنامه انهدام باید با توجه به دسته بندی سازمان از سوی پدافند غیرعامل و طبقه بندی سازمان تدوین شده باشد.

۳- در صورتی که نیاز نباشد دارایی اطلاعاتی حتما منهدم شود لازم است قابلیت استفاده مجدد دارایی اطلاعاتی یا نیاز بخشی از سازمان به آن بررسی شود. اگر جواب این بررسی منفی باشد مطابق با برنامه‌های موجود اقدام به انهدام دارایی اطلاعاتی می گردد. با انجام این کار این دستورالعمل پایان می پذیرد.

۴- در صورت قابلیت استفاده مجدد لازم است از پاک سازی و عقیم سازی دارایی اطلاعاتی از لحاظ وجود اطلاعات حساس یا دارای طبقه بندی اطمینان حاصل شود.

۵- پس از پاک سازی و عقیم سازی دارایی اطلاعاتی آماده استفاده مجدد و تحویل به واحد متقاضی می باشد. با تحویل دارایی اطلاعاتی این دستورالعمل پایان می پذیرد.

۱۰- استقرار و حفاظت تجهیزات:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی استقرار تجهیزات پردازش اطلاعات و دارایی‌های اطلاعاتی در مکان های اختصاصی فعالیت های پردازشی یا ارتباطی اعم از اتاق سرور، مرکز داده و یا مکان های نصب تجهیزات ارتباطی می باشد.

الزامات

- مکان یابی و استقرار تجهیزات پردازش اطلاعات یا زیرساخت های اطلاعاتی باید به نحوی باشد که:

الف- امنیت تجهیزات در مقابل دسترسی های فیزیکی غیرمجاز حفظ گردد.

ب- شرایط محیطی تعیین شده توسط سازنده تجهیزات از قبیل دما، رطوبت، فشار و عاری بودن از گرد و غبار قابل تامین باشد.

ج- امکان حفاظت از تجهیزات در مواقع بروز حادثه مثل آتش سوزی، آب گرفتگی، آوار و یا انفجار وجود داشته باشد.

د- تاسیسات مورد نیاز از قبیل جریان پیوسته و پایدار الکتریسیته، روشنایی، حفاظت در مقابل صاعقه و ارتینگ تامین شود.

هـ- دسترسی به تجهیزات هنگام عملیات نگهداری و تعمیرات به راحتی امکان پذیر باشد.

و- نیازهای اولیه (حیاتی) و ثانویه (تسهیلات) افراد مستقر در مکان استقرار تجهیزات تامین گردد.

- در مراکز حساس و حیاتی باید کلیه موارد مرتبط با مکان یابی و استقرار تجهیزات در قالب "طرح استقرار تجهیزات" مدون شده و به تایید کمیته امنیت اطلاعات برسد.

- طراحی جزئیات مکان استقرار تجهیزات باید بر اساس طرح استقرار تجهیزات انجام شود.

فرآیند

مراحل اجرای دستورالعمل استقرار و حفاظت تجهیزات به شرح زیر می باشد:

۶- در ابتدا باید اطلاعات لازم در خصوص نیازهای دارایی های اطلاعاتی جمع آوری شود، اطلاعاتی از قبیل:

- شرایط محیطی تعیین شده توسط سازنده
- تاسیسات مورد نیاز

و سپس اقدام به تدوین الزامات استقرار و حفاظت برای تجهیزات و دارایی های اطلاعاتی نمود. در تدوین الزامات توجه به جدول معیارهای حفاظتی مکان استقرار تجهیزات، مفید بوده و همچنین توجه به الزامات اختصاصی سازمان ضروری می باشد.

۷- پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکـانیزم هـا و روش هـای بـرآورده کننده الزامات تامین شود. همچنین در صورت نیاز به فرم، برچسـب و ... ، اقـدام بـه تهیـه ایـن مـوارد صورت پذیرد.

۸- تخصیص فضا و مکان مناسب ابتدایی ترین و همچنین از اصلی ترین راهکارهای استقرار و حفاظت از تجهیزات می باشد که باید کلیه الزامات تدوین شده در این خصوص را برآورده کند.

۹- پس از تامین تجهیزات و مکانیزم ها در این مرحله به پیاده سازی و اجرای مکانیزم ها و کلیه الزامـات تدوین شده پرداخته می شود.

۱۰-در صورتی که پس از پیاده سازی مکانیزم ها و روش ها، کلیه الزامات اسـتقرا و حفاظـت تجهیـزات تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شـده باشـد ایـن دستورالعمل پایان می‌پذیرد. در غیر اینصورت لازم است مرحله ۴ مجددا اجرا گردد.

۱۱- امکانات پشتیبانی:

هدف از تدوین این دستوالعمل بیان ضرورت وچگونگی بکارگیری و تامین تاسیسات مورد نیاز جهت تامین برق و برق اضطراری، اطفای حریق، تلفن، تهویه مطبوع و آب برای تداوم فعالیت و ارائه خدمات دارایی‌های اطلاعاتی در شرایط عادی و بحرانی می باشد.

الزامات

الزامات این دستورالعمل در قالب شش دسته الزامات توان الکتریکی، برق اضطراری، اطفاء حریق، تلفن، تهویه مطبوع و آب تقسیم بندی شده است.

الف- الزمات توان الکتریکی:

-لازم است توان مصرفی، مقدار جریان الکتریسیته و ظرفیت خطوط انتقال مورد نیاز برای راه‌اندازی و کار در شرایط امن دستگاه های الکترونیکی/ پردازشی یا مخابراتی بر اساس مقررات تولید کننده تجهیزات محاسبه و تامین گردد.

- لازم است اتصال زمین کلیه قطعات فلزی تجهیزاتی که در ارتباط مستقیم با مدار الکتریکی قرار ندارند و درحالت عادی باید بدون برق باشند به منظور حفاظت در مقابل برق گرفتگی و ایجاد ایمنی تجهیزات رعایت گردد.

-در مراکز حساس و حیاتی لازم است جریان و ولتاژ خطوط به طور دائم مانیتور شده و نوساناتی که ممکن است منجر به اشکال در کار سامانه ها گردد ثبت و به صورت مناسب به اطلاع افراد مسئول رسانیده شود.

- درمراکز حیاتی ضروری است یک کابل کشی اضطراری (پشتیبان)، علاوه بر کابل کشی اصلی سازمان برای مواقع بحرانی نصب گردد.

ب- الزامات برق اضطراری:

-جهت تنظیم جریان الکتریسیته مورد نیاز تجهیزات پردازشی و کاهش اثرات ناشی از نوسانات جریان الکتریکی لازم است از سیستم UPS متناسب با کاربرد تجهیزات استفاده شود تا اولاً از آسیب به تجهیزات جلوگیری شود و ثانیاً در مواقع قطع جریان اصلی برق ارائه خدمات پردازشی و ارتباطی با توقف مواجه نشود.

- در مراکز حساس و حیاتی می بایست علاوه بر اختصاص UPS از ژنراتور برق اضطراری برای برق دهی طولانی مدت استفاده شود. ظرفیت تولید ژنراتور برق اضطراری باید متناسب با توان مصرفی تجهیزاتی باشد که لازم است در شرایط قطع برق اصلی به کار خود ادامه دهند.

ج- الزامات اطفاء حریق:

- ضروری است وسایل اطفاء حریق سازگار با تجهیزات الکترونیکی- پردازشی در قسمت های مناسبی از محل نگهداری تجهیزات پردازشی تعبیه گردد.

- در مراکز حساس، می بایست سیستم های هوشمند اعلام خطر در محل های مناسب نصب شود تا در مواقع ضروری به وسیله آلارم های اخطار دهنده موجب آگاهی پرسنل از خطر آتش سوزی و جلوگیری از تشدید آتش شود.

- در مراکز حیاتی لازم است سیستم های اتوماتیک اطفاء حریق با مواد مناسب سازگار با دستگاه‌های الکترونیکی پردازشی تهیه و نصب گردد.

- در مراکز حیاتی، استفاده از لوازم و تجهیزات مناسب برای جلوگیری از گسترش آتش مثل دیوارهای مقاوم در برابر آتش و دریچه‌های خفه کننده ، ضروری است.

د- الزامات تلفن:

- از آنجا که تلفن معمولاً اولین و کاربردی ترین وسیله ارتباطی در شرایط اضطراری می باشد لازم است نحوه نصب و بهره برداری از آن به نحوی باشد که امکان قطع آن در شرایط اضطراری به حداقل برسد.

- در مراکز حساس لازم است برای جلوگیری از اختلال درکار تلفن هنگام قطع جریان برق از منبع تغذیه اختصاصی یا UPS برای تامین جریان الکتریکی مورد نیاز تلفن استفاده شود.

- در مراکز حساس و حیاتی ضروری است برای جلوگیری از قطع ارتباط در مواقع بحرانی (آتش سوزی، حوادث غیر مترقبه و حملات) خطوط ارتباطی جایگزین پیش بینی گردد.

- لازم است به صورت دوره ای نحوه عملکرد تجهیزات ارتباطی مرسوم در شرایط بحران از طریق مانور شبیه سازی شرایط بحران آزمایش شود.

هـ- الزامات تهویه مطبوع:

-لازم است دستگاههای تهویه مطبوع طبق استانداردهای موجود تهیه و در محل مناسب نصب گردد. هنگام انتخاب دستگاه های تهویه مطبوع باید به ظرفیت تولید حرارت تجهیزات یا نیاز به دمای خاص جهت عملکرد صحیح توجه شود.

- در مراکز حساس و حیاتی برای جلوگیری از ورود مواد آلوده سمی و آلرژی زا و همچنین گرد و خاک به محیط های بهره برداری از تجهیزات پردازشی و تامین هوای سالم جهت تنفس افراد لازم است از تجهیزات مناسب تصفیه هوا استفاده شود.

و- الزامات آب:

- ضروری است مکان قرارگیری وسایل الکتریکی به گونه ای طراحی شود که در صورت احتمال وقوع حوادث احتمالی ناشی از نم و رطوبت و یا آب گرفتگی از لطمه به تجهیزات جلوگیری شود.

-در مراکز حیاتی ضروری است برای ادامه فعالیت سازمان در شرایط بحرانی منابع تامین یا ذخیره آب پیش بینی گردد.

فرآیند

مراحل اجرای دستورالعمل امکانات پشتیبانی به شرح زیر می باشد:

۱- ابتدا به تدوین الزامات امکانات پشتیبانی پرداخته می شود. در این سند امکانات پشتیبانی در قالب ۶ گروه توان الکتریکی، برق اضطراری، ارتباطات صوتی(تلفن)، تاسیسات اطفاء حریق، تهویه مطبوع و تامین و حفاظت از آب دسته بندی شده اند. همچنین در صورت لزوم الزامات اختصاصی سازمان نیز باید افزوده شود.

۲- پیش از اجرا لازم است کلیه تجهیزات و مکانیزم هایی که جهت برآورده ساختن الزامات تدوین شده مورد نیاز می باشند تامین شوند.

۳- پس از تامین تجهیزات و مکانیزم ها در این مرحله به پیاده سازی و اجرای مکانیزم ها و الزامات پرداخته می شود.

۴- در صورتی که پس از پیاده سازی مکانیزم ها، کلیه الزامات تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شده باشد این دستورالعمل پایان می پذیرد. در غیر اینصورت لازم است مرحله ۳ مجددا اجرا گردد.

۱۲- امن سازی دفاتر، اتاق ها و امکانات:

هدف از تدوین این دستورالعمل ارائه راهکارها و روش های مناسب جهت امن سازی اتاق ها، دفاتر، امکانات و تجهیزات پردازشی و نگهداری دارایی های اطلاعاتی با توجه به ناحیه امنیتی محل استقرار آنها می باشد.

الزامات

- لازم است هر یک از اتاق ها، دفاتر، امکانات و تجهیزات جانبی مربوط به ساختمان ها با توجه به نواحی امنیتی تعریف شده و مطابق با الزامات آن امن سازی شود.

- بمنظور احتراز از شکست های امنیتی ناشی از نفوذ افراد غیرمجاز به دفاتر و اتاق ها لازم است دستورالعمل ها وشیو ه های تایید شده بطور صحیح اجرا شود و نظارت کامل بر اجرا به عمل آید.

- لازم است فهرست افرادی که مجاز به تردد در یک اتاق، دفتر یا محوطه هستند تهیه و در محل مناسب نصب شود و یا به سهولت در دسترس افراد مجاز قرار گیرد.

- در مراکز حساس و حیاتی لازم است اتاق ها، دفاتر و راهروها بطور دائم توسط دوربین های مدار بسته و سیستم مانیتورینگ تحت کنترل و نظارت قرار گیرد.

- دیوار اتاق ها، مراکز اصلی پردازش یا ذخیره اطلاعات و یا محل استقرار تجهیزات ارتباطی در مراکز حساس و حیاتی باید از نوع بتنی ضخیم بوده و نسبت به نفوذ رطوبت، صوت، ارتعاشات و امواج الکترومغناطیسی عایق‌بندی شده باشد. همچنین دیوارها باید مجهز به سیستم های امنیتی هشدار دهنده مانند سیستم کنترل دما، فشار و ضربه باشند.

- در صورت وجود پنجره در اتاق های محل نگهداری تجهیزات پردازشی و دارایی های اطلاعاتی طبقه‌بندی شده لازم است پنجره ها دارای حفاظ بوده و همچنین در صورت لزوم از شیشه های نشکن و عایق در مقابل نفوذ رطوبت، صدا و ارتعاشات استفاده شود.

- بمنظور نگهداری و محافظت از رسانه های ذخیره سازی و نگهداری اطلاعات اعم از اطلاعات چاپی مانند فرم‌ها، نامه ها، مستندات مختلف و تمام مواردی که به ثبت می رسد و نیز داده های اطلاعاتی ثبت شده بر روی میکروفیلم، رسانه های مغناطیسی، دیسک های نوری، دیسک های سخت، دیسک های فشرده نوری، فلاپی و

... باید از گاوصندوق های مخصوص نگهداری این دارایی ها با قفل‌های رمزی، کارت خوان یا بایومتری[1] استفاده شود.

- به عنوان یک قانون عمومی، سرورهای شبکه نباید در اتاق افراد خاص مثلا اتاق مدیر بخش قرار گیرد. برای سرورها باید اتاق های جداگانه و امنی در نظر گرفته شود. تردد به این اتاق ها باید تحت کنترل بوده و فقط افراد مجاز بتوانند به سهولت به این تجهیزات و امکانات پشتیبانی آنها دسترسی داشته باشند.

- در مراکز حساس و حیاتی لازم است اتاق ها، دفاتر و راهروها بطور دائم توسط دوربین های مدار بسته و سیستم مانیتورینگ تحت کنترل و نظارت قرار گیرند.

- محل قرار گرفتن کامپیوتر باید حتی الامکان در جایی باشد که افراد غیرمجاز قادر نباشند صفحه نمایش و صفحه کلید آن را مشاهده نمایند. رعایت این اصل در خصوص تجهیزات و دارایی‌هایی که برای دسترسی به اطلاعات دارای طبقه بندی به کار می روند الزامی است.

- تجهیزات مناسب ردیابی و کنترل نفوذ بر اساس استانداردهای حرفه ای باید نصب شده و مرتباً آزمایش گردند. این تجهیزات باید کلیه درها، پنجره ها و منافذ احتمالی که هنگام دسترسی غیرمجاز ممکن است مورد استفاده قرار گیرند را پوشش دهد. همه مکان های خلوت باید بوسیله سیستم تشخیص نفوذ فیزیکی تحت کنترل قرار گرفته و از پوشش حفاظتی مناسب برای اتاق کامپیوتر و تجهیزات مخابراتی استفاده شود.

- تجهیزات پشتیبانی مانند دستگاه فتوکپی یا فکس باید به نحوی درمنطقه امن پیش بینی شود که نیازی به خارج کردن اطلاعات نباشد. به منظور بالا بردن امنیت و حفظ اطلاعات باید از خارج شدن خارج از کنترل منابع

[1] - Biometry

ذخیره اطلاعا ت و ورود افراد غیرمجاز به اتاق ها و دفاتر محل نگهداری دارایی های اطلاعاتی دارای طبقه بندی جلوگیری بعمل آید.

فرآیند

مراحل اجرای دستورالعمل امن سازی دفاتر، اتاق ها و امکانات به شرح زیر می باشد:

۱۱-ابتدا لازم است بر اساس دسته بندی سازمان از دیدگاه پدافند غیرعامل(مهم، حساس و حیاتی) و همچنین طبقه بندی حفاظتی دارایی های اطلاعاتی سازمان(عادی، محرمانه، خیلی محرمانه و ...) مناطق و نواحی مختلف سازمان را حیطه بندی نمود. این حیطه بندی در امن سازی سازمان در مراحل مختلف تاثیرات مطلوب بسیاری بهمراه خواهد داشت.

۱۲-پس از تدوین طرح حیطه بندی لازم است بر اساس آن الزامات امنیتی نواحی مختلف ، تعیین شوند. از جمله این الزامات می توان به موارد زیر اشاره نمود:

- استفاده از دوربین مداربسته و سیستم مانیتورینگ
- تهیه فهرست افراد مجاز به تردد در یک اتاق
- استفاده از سیستم های امنیتی هشدار دهنده مانند سیستم کنترل دما، فشار و ضربه
- تجهیزات مناسب ردیابی و کنترل نفوذ

همچنین لازم است در صورتیکه سازمان الزامات اختصاصی دیگری نیز داشته باشد به الزامات بیان شده در این سند افزوده گردد.

۱۳-پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکانیزم های برآورده کننده الزامات تامین شود.

۱۴-پس از تامین تجهیزات و مکانیزم ها در این مرحله به پیاده سازی و اجرای کلیه الزامات امن سازی مبادرت می گردد.

۱۵-در صورتی که پس از پیاده سازی مکانیزم ها، کلیه الزامات امن سازی تدوین شده ، برآورده شده باشد این دستورالعمل پایان می‌پذیرد. در غیر اینصورت لازم است مرحله ۴ مجددا اجرا گردد.

۱۳- امنیت فیزیکی پیرامونی :

هدف از تدوین این دستورالعمل ایجاد محیطی امن برای نگهداری اطلاعات، دارایی های اطلاعاتی و تجهیزات مهم در اختیار از طریق ایجاد موانع، دیوارها یا حصارهای مناسب و مستحکم و ارائه راهکارهای عملی برای جلوگیری از ورود افراد غیرمجاز و ایجاد موانع امنیتی مناسب برای حفظ امنیت محیطی و پیرامونی است.

الزامات

- لازم است مکانیزم ها، امکانات و اقدامات مناسب برای حفاظت از پیرامون و محیط نگهداری اطلاعات و تجهیزات به کار گرفته شود.

- لازم است در مورد نواحی با طبقه بندی های مختلف عادی، محدود، محرمانه و خیلی محرمانه به ترتیب ازکنترل های اضافی و دقیق تری برای ایجاد امنیت استفاده شود.

- لازم است با توجه به سطح حساسیت **سازمان**، حفاظت فیزیکی از طریق ایجاد موانع چندگانه فیزیکی در اطراف منابع سازمانی و تجهیزات تامین شود.

- در انتخاب مکانیزم ها و روش های ایجاد امنیت محیطی و فیزیکی باید به سطح بندی و الزامات تعیین شده توسط سازمان پدافند غیرعامل توجه شود.

- در محیط های بسته، لازم است مرزهای فیزیکی بصورت کامل از کف تا سقف از مصالح مستحکم و متناسب با اهمیت سطح طبقه بندی محیط تحت حفاظت ایجاد شود.

- لازم است پیوستگی مرزهای فیزیکی و یا موانع ایجاد شده جهت محدود کردن محیط به طور کامل رعایت شود به طوری که امکان نفوذ به محیط تحت حفاظت، از هیچ یک از نقاط (بخصوص نقاطی که نوع مرز تغییر می کند، مثل نقاط اتصال فنس به دیوار یا تغییر روش حفاظت از مشاهده بصری به حفاظت الکترونیکی) وجود نداشته باشد.

- لازم است کانال های آب و راه های آب زیرزمینی مثل کاریز و مسیرهای رودخانه های فصلی که از داخل محوطه تحت نظارت می گذرد کنترل شود تا از ورود افراد غیرمجاز از این گونه مسیرها جلوگیری به عمل آید.

- نگهبانان متصدی حفاظت از مراکز داده حیاتی باید از بین افراد قوی با آمادگی جسمانی بالا انتخاب شوند تا آمادگی مقابله با حمله های احتمالی را داشته باشند.

- در مراکز داده (سازمان های) حساس و حیاتی لازم است سقف ها و کف ها از جنس بتنی و فولادی ساخته شود تا در برابر آتش، وزن زیاد و ریزش مقاوم باشد.

- بر روی دیوارهای پیرامونی مراکز داده حیاتی از تورهای سیمی با جریان الکتریسیته و یا سیم های خاردار استفاده شود و در صورت پاره شدن، اخطارهای لازم به صورت خودکار صادر شود.

- لازم است در پنجره های مراکز داده حساس یا حیاتی از نوارها و حفاظ هایی استفاده شود که در صورت شکستن پنجره اعلام خطر شود.

- باید توجه شود که اندازه، حجم و محل قرار گرفتن گیاهان، درختان و گلها به نحوی نباشد که بتوان با استفاده از آنها به محوطه تحت حفاظت نفوذ کرد.

فرآیند

مراحل اجرای دستورالعمل امنیت فیزیکی پیرامونی به شرح زیر می باشد:

۱۶-ابتدا لازم است بر اساس دسته بندی سازمان از دیدگاه پدافند غیرعامل(مهم، حساس و حیاتی) و همچنین طبقه بندی حفاظتی دارایی های اطلاعاتی سازمان(عادی، محرمانه، خیلی محرمانه و ...) مناطق و نواحی مختلف سازمان را حیطه بندی نمود. این حیطه بندی در امن سازی سازمان در مراحل مختلف تاثیرات مطلوب بسیاری بهمراه خواهد داشت.

۱۷-پس از تدوین طرح حیطه بندی لازم است بر اساس آن الزامات امنیتی نواحی مختلف ، تعیین شوند. از جمله این الزامات می توان به موارد زیر اشاره نمود:

- استفاده از مصالح مستحکم و متناسب با اهمیت سطح طبقه بندی محیط
- توجه به پیوستگی مرزهای فیزیکی و یا موانع ایجاد شده
- استفاده از نگهبانان قوی با آمادگی جسمانی بالا جهت تصدی حفاظت از مراکز داده حیاتی

همچنین لازم است در صورتیکه سازمان الزامات اختصاصی دیگری نیز داشته باشد به الزامات بیان شده در این سند افزوده گردد.

۱۸-پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکانیزم های برآورده کننده الزامات تامین شود. در این خصوص بعنوان مثال می توان به موارد زیر اشاره نمود:

- مصالح ساختمانی مناسب
- تورهای سیمی با جریان الکتریسیته و یا سیم های خاردار
- افراد قوی با آمادگی جسمانی بالا

۱۹-پس از تامین تجهیزات و مکانیزم ها در این مرحله به پیاده سازی و اجرای کلیه الزامات مبادرت می گردد.

۲۰-در صورتی که پس از پیاده سازی مکانیزم ها، کلیه الزامات امنیت فیزیکی پیرامونی تدوین شده، برآورده شده باشد این دستورالعمل پایان می پذیرد. در غیر اینصورت لازم است مرحله ۴ مجددا اجرا گردد.

۱۴- امنیت کابل کشی:

هدف جلوگیری از نقض امنیت اطلاعات در حوزه های محرمانگی، جامعیت و دسترسی پذیری به وسیله رعایت روش‌های استاندارد کابل‌کشی در شبکه‌های متعلق به سازمان و همچنین جلوگیری از کاهش پایداری و یا بروز ناپایداری زیاد در شبکه بر اثر مخاطرات و آسیب پذیری‌های مربوط به کابل‌کشی شبکه.

الزامات

- با توجه به اهمیت کابل کشی و همچنین دسترسی پیمانکاران آن به بخش های مختلف سازمان و در نتیجه اطلاع یافتن از نحوه استقرار تجهیزات و تاسیسات سازمان، ضروری است پیش از عقد قرارداد، الزامات امنیتی سازمان به وی ابلاغ شده و پیمانکار نیز متعهد به رعایت الزامات شود.
- در مراکز حساس و حیاتی معرفی شده از سوی سازمان پدافند غیرعامل ضروری است پیمانکار دارای گواهی صلاحیت فنی تایید شده از سوی مراجع ذیربط باشد. همچنین لازم است حین انجام عملیات اجرایی، نماینده سازمان بر کار پیمانکار نظارت دائمی و کامل داشته باشد.
- لازم است در عقد قرارداد با پیمانکار بر اساس اقدام گردد.
- لازم است هنگام تهیه نقشه مسیرهای عبور کابل، نقشه ساختمانی و مکان قرارگیری تاسیسات، لوله‌های آب و فاضلاب و سایر سیم ها مورد بررسی و توجه قرار گیرند.
- ضروری است توپولوژی شبکه ارتباطی بر اساس ساختار ستاره ای سلسله مراتبی طراحی و تدوین شود.

- انتخاب نوع کابل مورد استفاده در کابل کشی باید بر اساس پهنای باند مورد نیاز، موقعیت مکانی، مسافت و همچنین در نظر گرفتن کاربرد های احتمالی و قابلیت ارتقا در آینده باشد.
- لازم است بمنظور انتخاب کابل توصیه ها و رهنمودهای استاندارد مرجع در خصوص موارد استفاده هر کابل مورد نظر قرار گیرد.
- کابل کشی شبکه ارتباطی باید از سایر کابل ها مثل کابل های فشار قوی یا فشار ضعیف جداسازی شود. این امر موجب تسهیل حفاظت و نظارت و همچنین کاهش خطر تداخل الکترومغناطیسی تصادفی می شود.
- لازم است الزامات طراحی مطابق با استاندارد ISO/IEC 11801 رعایت گردد. مهمترین الزامات این استاندارد به شرح زیر است:
  - حداکثر طول کابل کشی افقی ۹۰ متر می باشد.
  - سیم[۲] های اتصال ایستگاه کاری به پریزهای شبکه به ۵ متر(ترجیحاً۳ متر)محدود شوند.
  - تنها در صورت استفاده از فیبر نوری، مسافتهای بیش از ۲۰۰۰متر مجاز می باشد.
- ضروری است سازگاری میان کابل‌ها و تجهیزات غیرفعال[۳] شبکه با پروتکل های ارتباطی مورد استفاده رعایت شود.
- در محیط های باز و مکان هایی که احتمال وجود حیوانات جونده و یا عوامل محیطی مخرب از قبیل نور خورشید، رطوبت و ... می باشد ضروری است از پوشش های محافظ برای کابل ها استفاده شود.
- در مراکز حساس و حیاتی ضروری است در کابل کشی خارج از ساختمان از فیبر نوری استفاده شود.

[2] - Patch cord

[3] - Passive

- در مراکز مهم، حساس و حیاتی لازم است کابل ها در پوشش ها و یا لوله های محافظ که به سرعت قابل بازرسی هستند قرار گیرند. همچنین لازم است از تجهیزات مقاوم در مقابل دستکاری[4] استفاده شود. این امر موجب تسهیل شناسایی دستکاری در مواقع بحرانی می شود.
- در مراکز مهم، حساس و حیاتی و همچنین بخش های حساس و حیاتی سایر سازمان ها ضروری است توزیع کننده های سطح طبقات(FDها) با استفاده از لینک های مستقیم به یکدیگر اتصال داشته باشند. این امر موجب تسهیل احیای سیستم[5] در شرایط بحرانی و مواقع نیاز می شود.
- توصیه می شود در بخش های حساس و حیاتی کلیه سازمان ها حتی الامکان کابل ها دارای حفاظ[6] مناسب بمنظور حفاظت در مقابل نشت سیگنال[7] و همچنین سازگاری الکترومغناطیسی(EMC) باشند.
- ضروری است توزیع کننده های موجود در بخش های حساس و حیاتی سازمان ها در محفظه های شیلد شده و یا اتاق های با شیلد مناسب قرار گیرد.
- در مراکز حساس و حیاتی کابل کشی خارج از سازمان باید به گونه ای باشد که خارج از دید افراد متفرقه بوده و موجبات جلب توجه افراد را ایجاد نکند.
- در مراکز حساس و حیاتی ضروری است کلیه کابل های مورد استفاده بخصوص کابل های موجود در محوطه خارج از ساختمان دارای حفاظ مناسب بمنظور محافظت در مقابل نشت سیگنال و همچنین ایجاد سازگاری الکترومغناطیسی باشد. همچنین لازم است کلیه توزیع کننده ها بصورت مناسب پوشش داده شده و یا در محفظه ها و اتاق های با پوشش مناسب قرار گیرند.

---

4 - Tamper proof

5 - Disaster recovery

6 - Shield

7 - Tempest

- مطابق با استاندارد ISO/IEC 11801 ضروری است از طریق ایجاد نقطه انفصال ساختمان[8] جهت جداسازی کابل های خارج و داخل ساختمان از یکدیگر استفاده نمود.
- در استفاده از نقاط تقویت سیگنال[9] بین توزیع کننده های سطح طبقه و پریزهای ارتباطی لازم است نکات زیر مورد نظر قرار گیرد:
  - نقطه تقویت سیگنال برای بیش از ۱۲ مکان کاری[10] توصیه نمی شود.
  - حداقل فاصله نقطه تقویت از توزیع کننده سطح طبقه ۱۵ متر باشد. این امر موجب کاهش اثر اختلالات دیگر عناصر بر روی توزیع کننده سطح می شود.
- لازم است سیستم ارتینگ مناسب مطابق با استاندارد IEC 60364 برای سیستم کابل کشی در نظر گرفته شود. سه دلیل زیر ضرورت این امر را بیان می کند:
  - ایمنی کاربران در مقابل برق گرفتگی
  - کمک به جلوگیری از تشعشع امواج الکترومغناطیسی از شبکه کابل مسی
  - کمک به جلوگیری از تخریب ناشی از نفوذ امواج الکترومغناطیسی به داخل شبکه کابل مسی
- ضروری است کابل های ارتباطی به اندازه کافی دور از کابل های تغذیه و همچنین لامپ های فلورسنت قرار گیرند.
- در هنگام کابل کشی لازم است درجه حرارت محل نصب و همچنین محدوده حرارتی مجاز کابل مورد توجه قرار گیرد.

---

[8] -Building Entrance Facilities: عبارت است از محلي مناسب كه ترمينال هاي ورودي و خروجي ارتباطي ساختمان در آن نصب شده و آرايش كابل بندي ساختمان از آنجا آغاز مي شود.

[9] -Consolidation Point

[10] -Work Place

- در سازمان های حساس و حیاتی و همچنین بخش های حساس و حیاتی سایر سازمان ها ضروری است پوشش های محافظ مورد استفاده، در برابر حرارت نیز مقاوم باشند.
- ضروری است کلیه کابل ها و همچنین کانکتور ها دارای برچسب مشخص باشند. بر چسب کابل ها باید در دو سر کابل قرار گیرد. همچنین لازم است از رنگ بندی های مختلف برای تمایز شبکه های آزمایشی و تحقیقاتی از شبکه های عملیاتی استفاده شود.
- در هنگام کابل کشی توجه به موارد زیر ضروری می باشد:
  - وارد نکردن فشار بیش از حد به کابل ها
  - مورد توجه قرار دادن محدودیت شعاع خمش
  - عدم نصب و کشیدن کابل ها در اطراف لبه های تیز
  - پر نکردن بیش از حد محفظه ها و لوله های گذر سیم ها
- ضروری است برای هر ۱۰ متر مربع و یا یک محیط کاری حداقل دو عدد پریز ارتباطی در نظر گرفته شود. یکی از پریزها باید برای سیم متوازن[11] و پریز دیگر می تواند برای سیم متوازن یا فیبر نوری تعبیه شود.
- مبدل‌های PABX، ISDN، مبدل سیگنال‌های الکتریکی متوازن به نامتوازن و ... باید خارج از پریزهای ارتباطی قرار داشته باشند.
- ضروری است کلیه پریزها دارای برچسب های پایدار و قابل رویت توسط کاربران باشند.
- لازم است کلیه پریزها و نودهای ارتباطی بوسیله شماره اختصاصی شماره گذاری و تعریف شوند تا به راحتی قابل تشخیص و شناسایی باشند. این امر موجب تسهیل شناسایی محل نفوذ به شبکه می شود.

فرآیند

[11] - Balanced Cable

مراحل اجرای دستورالعمل امنیت کابل کشی به شرح زیر می باشد:

۱- بررسی و بازبینی پلان ساختمان، تاسیسات و محیط از این جهت که می تواند اطلاعات بسیار مفیدی در خصوص نقشه کاربری بخش های مختلف و مکان استقرار تاسیسات، لوله های آب و فاضلاب، دیگر کابل‌ها و ... ارائه دهد دارای اهمیت زیادی است. مخاطرات و آسیب پذیری های ناشی از موارد مذکور در صورت عدم توجه خسارات فراوانی را به سازمان تحمیل خواهد نمود.

۲- پس از بررسی های فوق تدوین توپولوژی مناسب بر اساس استاندارد ISO 11801 در اولویت بعدی قرار دارد چرا که یک توپولوژی نامناسب باعث بوجود آمدن ناپایداری و در پی آن نقض امنیت شبکه خواهد شد.

۳- توپولوژی سیستم کابل توسط پیمانکار تدوین و به تایید مدیر ارشد شبکه و یا مشاور شبکه سازمان می رسد. در صورت عدم تایید لازم است مجددا توپولوژی طراحی و تدوین گردد.

۴- نوع کابل مورد استفاده در هر بخش از شبکه با در نظر گرفتن پهنای باند مورد انتظار، مسافت، موقعیت مکانی و نوع استفاده از آن انتخاب می شود. این مشخصات و همچنین مشخصات کلی مورد انتظار شبکه، توسط مدیر ارشد شبکه و بر اساس کلاس های مختلف ارائه شده در استاندارد ISO 11801 (شامل مشخصات کانال های مختلف) تبیین و در اختیار افراد ذیربط قرار می گیرد.

۵- نقشه سیستم کابل بر اساس توپولوژی تدوین شده و بررسی های صورت گرفته طراحی می گردد، بگونه ای که با یک طراحی مناسب و بهینه موجبات افزایش بهره وری، پایداری و امنیت و همچنین در صورت امکان صرفه جویی در فضا و هزینه را به دنبال داشته باشد. همچنین بر اساس مشخصات ارائه شده باید کابل هایی متناسب با انتظارات تهیه گردد.

۶- پس از تایید نقشه طراحی شده و کابل های منتخب برای هر بخش توسط مدیر ارشد شبکه و مدیر نهاد متصدی امنیت اطلاعات عملیات اجرایی آغاز خواهد شد. عملیات نصب و کابل کشی باید با دقت ویژه ای انجام شود و کلیه نکات مطرح شده در الزامات بایستی رعایت شود.

در صورتی که مطابق با الزامات، نیاز به استفاده از پوشش های محافظ، شیلدینگ و سایر تجهیزات و نکات امنیتی دیگر بود عملیات اجرایی پس از تامین موارد مذکور و انجام اقدامات لازم ادامه می یابد.

۷- پس از پایان عملیات اجرایی مطابق با استاندارد تست هایی بمنظور اطمینان از صحت عملکرد و همچنین رعایت پارامترهای تعیین شده مطابق با کلاس مورد نظر در طراحی انجام می شود. این تست ها با نظارت مستقیم مدیر ارشد شبکه و همچنین نماینده نهاد متصدی امنیت اطلاعات صورت خواهد پذیرفت.

۸- در صورتی که پس از تست، مشخص شود کلیه الزامات امنیت کابل کشی تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شده است این دستورالعمل پایان می‌پذیرد. در غیر اینصورت لازم است مرحله ۶ مجددا اجرا گردد.

۱۵- حفاظت در مقابل تهدیدهای محیطی و خارجی:

هدف از تدوین این دستورالعمل حفاظت از دارایی های اطلاعاتی در اختیار **سازمان** اعم از تجهیزات‌پردازشی، تجهیزات ذخیره اطلاعات و تاسیسات پشتیبانی در مقابل تهدیدهای خارجی و محیطی از قبیل آتش سوزی، سیل، طوفان، زلزله، قطع برق، قطع ارتباطات مخابراتی، شورش ها و اغتشاشات اجتماعی، سرقت، تخریب و سعی در به حداقل رساندن خسارات ناشی از این گونه تهدیدها می باشد.

الزامات

- درصورت پیش بینی احتمال وقوع تهدیدهای خارجی و محیطی از قبیل آتش سوزی، سیل، طوفان، زلزله، قطع برق، قطع ارتباطات مخابراتی، شورش، سرقت و تخریب لازم است از تجهیزات و اقدامات حفاظتی مناسب استفاده شود.

- به منظور پیشگیری از وقوع آتش‌سوزی لازم است تدابیر لازم در مراحل مکان‌یابی، طراحی و پیاده‌سازی ساختمانِ محل نگهداری تجهیزات پردازشی و تاسیسات پشتیبانی آن در نظر گرفته شود.

- لازم است هماهنگی های لازم با سازمان آتش نشانی یا واحدهای دفاع غیرنظامی به عمل آمده و تجهیزات مقابله با حوادث تحت نظر و تایید ایشان به کار گرفته شود.

- لازم است قبلاً آموزش های لازم و برنامه های تمرینی در مورد مقابله با حوادث به افراد داده شود و مسئولیت های افراد در هنگام وقوع حادثه تعیین شده باشد.

- لازم است ساختمان از لحاظ مقاومت در مقابل آتش سوزی و اطفاء حریق به وسیله ارگان های معتبر مثلاً سازمان آتش نشانی و خدمات ایمنی یا نهادهای معتبر دیگر ممیزی و بررسی شود.

- لازم است قبلاً اطلاعات تماس با آتش نشانی در اختیار افراد قرار گیرد.

- در مراکز حساس و حیاتی در هنگام وقوع آتش سوزی باید از مکانیزم های اطلاع رسانی خودکار به آتش نشانی استفاده شود.

- بمنظور کاهش خسارت های ناشی از سیل و یا نفوذ آب لازم است حتی الامکان محل قرار گرفتن تجهیزات پردازشی و الکترونیکی در ساختمان پایین تر از سطح عادی زمین در نظر گرفته نشود.

- لازم است ساختمان هایی که تجهیزات پردازشی و کامپیوترها در آن نگهداری می شوند در موقعیت جغرافیایی مناسب و دور از محل عبور رودخانه ها و سیلاب های فصلی و مسیرهای اصلی انتقال آب قرار داشته باشند.

- در مراکز حساس و حیاتی استفاده از حسگرهای رطوبتی و تشخیص نفوذ آب و سیستم آلارم و اعلام خطر در مراکز پردازش و نگهداری تجهیزات الکترونیکی ضروری است.

- در مراکز حساس و حیاتی استفاده از سیستم مناسب تخلیه آب در اتاق های پردازش اطلاعات، مکان‌های مجاور و طبقات فوقانی ضروری است.

- لازم است ساختمان هایی که دارایی های اطلاعاتی و تجهیزات پردازشی و الکترونیکی درآنها نگهداری می شود از طراحی تا پیاده سازی آن تابع اصول مهندسی ساختمان بوده و درتمامی مراحل، از نیروی متخصص استفاده گردد و بر نحوه انجام مراحل نیز، همواره نظارتی دقیق توسط مهندسان ناظر تایید صلاحیت شده صورت گیرد. استقرار دارایی‌های اطلاعاتی سازمان ها و مراکز حساس و حیاتی در ساختمان های فاقد محاسبات و تاییدیه مهندسی ممنوع است.

- در مراکز حیاتی پیش بینی سیستم حمل و نقل هوایی بمنظور استفاده در هنگام وقوع حوادث فاجعه آمیز از قبیل سیل، زلزله، طوفان و سایر مواقع اضطراری که منجر به انسداد راه های عبور زمینی می شود، ضروری است.

- بمنظور حفاظت خارجی، حفظ بدنه و ساختار ساختمان در مقابل آتش سوزی و یا تخریب در اثر اصابت صاعقه و محافظت از کلیه تجهیزات برقی و الکترونیکی و تاسیسات پردازشی مستقر در آن، نصب تجهیزات صاعقه گیر(برق گیر) خارجی و داخلی جهت جذب و هدایت صاعقه از پشت بام تا زمین طبق استاندارد-IEC 61024 ضروری می باشد.

- در مراکز حساس و حیاتی لازم است برنامه هایی برای برقراری ارتباط با نهادهای دولتی و غیردولتی یا عمومی یا مراجع قانونی مقابله با تهدیدهای امنیتی وجود داشته باشد.

- تمام اشخاصی که حفاظت و حراست از مکان های حساس را به عهده دارند علاوه بر آموزش های عملیاتی و پروتکل های امنیتی باید بیاموزند که چگونه در برابر تکنیک های خلاقانه مهندسی اجتماعی مقاومت کنند و در تله آن گرفتار نشوند. مهندسی اجتماعی[12] عبارت است از سوء استفاده از خصوصیات روانی افراد برای دستیابی به اطلاعاتی که فرد به صورت معمول آنها را افشاء نمی کند.

فرآیند

مراحل اجرای دستورالعمل حفاظت در مقابل تهدیدهای محیطی و خارجی به شرح زیر می باشد:

۱- بمنظور اجرای این دستورالعمل ابتدا لازم است کلیه تهدیدهای محیطی و خارجی از قبیل آتش‌سوزی، سیل، طوفان، زلزله، قطع برق، قطع ارتباطات مخابراتی، شورش‌ها و اغتشاشات اجتماعی، سرقت و تخریب شناسایی شده و سطح مخاطره هر یک برای سازمان ارزش گذاری گردد تا در مقابله با آنها بتوان بر اساس اولویت تعیین شده عمل نمود.

۲- در این مرحله متناسب با تهدیدهای شناسایی شده الزامات امنیتی با توجه به دسته بندی سازمان از دیدگاه پدافند غیرعامل تعیین می شود. همچنین در صورت وجود الزامات اختصاصی سازمان، آنها نیز به موارد قبلی افزوده خواهند شد.

۳- پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکانیزم های برآورده کننده الزامات تامین شود.

[12] - Social Engineering

۴- پس از تامین تجهیزات و مکانیزم های حفاظتی در این مرحله به پیاده سازی و اجرای کلیه الزامات بر اساس اولویت تعیین شده مبادرت می گردد.

۵- در صورتی که پس از پیاده سازی مکانیزم ها، کلیه الزامات حفاظتی تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شده باشد این دستورالعمل پایان می پذیرد. در غیر اینصورت لازم است مرحله ۴ مجددا اجرا گردد.

۱۶- خروج دارایی:

هدف از تدوین این دستورالعمل جلوگیری از خروج خارج از کنترل دارایی های اطلاعاتی تحت اختیار از مکان های استقرار می باشد.

الزامات

- خروج دارایی های اطلاعاتی منقول و رسانه های حاوی نرم افزارهای تحت مالکیت ، از محل استقرار باید تحت کنترل کامل قرار داشته باشد.(خروج داده ها و اطلاعات تحت مالکیت، تابع سیاست های کنترل دسترسی است .)

- در مراکز حساس و حیاتی لازم است خروج کلیه دارایی های اطلاعاتی منقول و رسانه های حاوی نرم‌افزارهای تحت مالکیت ثبت شود.

- در مراکز مهم لازم است خروج دارایی های اطلاعاتی دارای طبقه بندی ثبت شود.

- در مراکز حساس و حیاتی لازم است از روش های مکانیزه الصاق برچسب های مغناطیسی و یا RFID[۱۳] جهت حفاظت از دارایی ها و کنترل ورود و خروج آن ها استفاده شود.

[13] - Radio Frequency Identification

- در مراکز حساس و حیاتی لازم است جابجایی دارایی های اطلاعاتی در واحدهای مختلف سازمان نیز تحت کنترل کامل قرار داشته باشد .

- در صورت نیاز به خروج دارایی های اطلاعاتی از محوطه های تحت کنترل سازمان، لازم است کلیه دسترسی های مربوط به آن مسدود گردد و به هنگام بازگرداندن، مجدداً دسترسی های مجاز تعریف شده و تخصیص داده شود. بدیهی است در صورتیکه دارایی اطلاعاتی پس از خروج در اختیار افراد بیگانه (مثلاً تعمیرکاران یا ماموران نهادهای دولتی غیر وابسته به سازمان و یا سایر افرادی که در حالت عادی مجاز به دسترسی به دارایی نمی باشند) قرار گرفته باشد ، لازم است مجدداً مراحل صدور مجوز استفاده از تجهیزات پردازش اطلاعات را طی نماید.

- فهرست ورود و خروج دارایی های اطلاعاتی باید به صورت دوره ای مورد بازبینی قرار گرفته و دلایل خروج ارزیابی و پیگیری شود.

- هنگام خروج دارایی های اطلاعاتی حاوی اطلاعات طبقه بندی شده لازم است مفاد دستوالعمل امحاء امن داده ها به طور کامل رعایت شود.

- هنگام خروج دارایی های اطلاعاتی دارای طبقه بندی لازم است از عدم نقض امنیت اطلاعات به دلیل افشاء ساختار، نقشه ها، طراحی و روش کار دارایی اطلاعاتی (و یا حتی روش استفاده از آن نوع دارایی در سازمان) اطمینان حاصل شود.

- لازم است قبل از خروج دارایی‌های اطلاعاتی دارای طبقه‌بندی در کلیه مراکز و همچنین کلیه دارایی‌های اطلاعاتی در مراکز حساس و حیاتی، مجوز خروج که به تایید مرکز حراست فناوری اطلاعات یا نهاد جایگزین آن رسیده باشد، کسب گردد.

- برداشتن قطعات حساس از روی تجهیزات مربوط نیز تابع این دستوالعمل می باشد. به عنوان مثال لازم است برداشتن یا جابجایی تجهیزات ذخیره و پردازش اطلاعات بخصوص در ماشین های Hot plug[۱۴] و همچنین بردهای حساس مثل ماژول های رمز نگاری یا اینترفیس های ارتباط با سایر تجهیزات الکترونیکی تحت کنترل کامل قرار داشته باشد.

- در مراکز حساس و حیاتی لازم است از مکانیزم های کنترل موجودی برخط[۱۵] برای حفاظت از تجهیزات و دارایی های اطلاعاتی فیزیکی ضروری برای تداوم عملیات استفاده شود و در صورت برداشتن، جابجایی یا خارج از سرویس شدن تجهیزات اخطارهای لازم صادر شود.

فرآیند

مراحل اجرای دستورالعمل خروج دارایی اطلاعاتی به شرح زیر می باشد:

۱- ابتدا لازم است انواع دارایی های اطلاعاتی سازمان مشخص شده و بر اساس دسته بندی سازمان از دیدگاه پدافند غیرعامل(مهم، حساس و حیاتی) و همچنین طبقه بندی حفاظتی دارایی های اطلاعاتی سازمان(عادی، محرمانه، خیلی محرمانه و ...) مقررات و الزامات خروج هر یک از انواع دارایی های اطلاعاتی از سازمان تدوین شود.

۲- پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکانیزم های برآورده کننده الزامات تامین شود. همچنین در صورت نیاز به فرم، برچسب و ... ، اقدام به تهیه این موارد صورت پذیرد.

۳- پس از تامین تجهیزات و مکانیزم ها در این مرحله به پیاده سازی و اجرای مکانیزم ها و کلیه الزامات تدوین شده اقدام می گردد.

---

[۱۴] - ماشین هایی که امکان تعویض یا اضافه کردن یا برداشتن بعضی از قطعات آنها حین کار وجود دارد.

[15] -On Line

۴- در صورتی که پس از پیاده سازی مکانیزم ها، کلیه الزامات تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شده باشد این دستورالعمل پایان می‌پذیرد. در غیر اینصورت لازم است مرحله ۳ مجددا اجرا گردد.

۱۷- دسترسی عمومی ، نواحی ارسال و بارگیری:

هدف از تدوین این دستورالعمل امن سازی نواحی در دسترس عموم از طریق تبیین الزامات و بیان ضرورت ایجاد مرز بین نواحی امن و مکان های دسترسی عمومی و مکان های محدود شده، کنترل نقاط دسترسی عمومی، نواحی ارسال، تحویل، بارگیری و سایر نقاطی است که افراد غیر مجاز ممکن است به تجهیزات و دارایی های اطلاعاتی دسترسی پیدا کنند.

الزامات

- لازم است محدوده های جغرافیایی سازمان ها یا مراکز از نقطه نظر روش حفاظتی به دو (و یا سه) ناحیه شامل ناحیه امن و ناحیه دسترسی عمومی (و یا ناحیه امن، مکان های محدود شده و ناحیه دسترسی عمومی) تقسیم شده و برای این نواحی مرزهای مشخصی تعریف شود.

- لازم است مکانیزم های متناسب با حفاظت از مکان های امن، محدود شده و دسترسی عمومی ، ایجاد شود.

- لازم است مرزهای مکان های دسترسی عمومی به نحوی مشخص گردد که برای مراجعه کنندگان به مناطق دسترسی عمومی در هنگام مراجعه قابل تشخیص باشد.

- لازم است معیارها و مقررات امنیتی مربوط به عملکرد ارباب رجوع و یا اشخاص ثالث که به نحوی منجر به تاثیر در امنیت دارایی های اطلاعاتی و تجهیزات پردازشی می شود اعلام شود و مقدمات رعایت این مقررات از سوی ارباب رجوع تامین گردد.

- لازم است جهت جلب رضایت ارباب رجوع امکانات ضروری با توجه به اهمیت مکان تحت حفاظت به کار گرفته شود و اطلاع رسانی مناسب در مورد نحوه ارائه خدمات و لزوم رعایت امنیت در اختیار ایشان قرار داده شود.

- لازم است مناطق دریافت و ارسال و مکان های تخلیه و بارگیری تحت کنترل بوده و در صورت امکان برای جلوگیری از دسترسی های غیر مجاز از امکان استقرار تجهیزات پردازش اطلاعات جدا گردد.

- لازم است دسترسی به انبارها یا مکان های نگهداری تجهیزات، از خارج سازمان فقط برای افراد شناخته شده و مجاز امکان پذیر باشد.

- انبارها یا مکان های نگهداری را باید به صورتی طراحی کرد که متصدیان حمل و نقل بتوانند بدون نیاز به دسترسی به مناطق امن، مواد مورد نیاز منطقه را تخلیه نمایند.

- به هنگام باز بودن درهای داخلی انبار یا مکان امن باید درهای خارجی بسته و یا کاملا امن نگه داشته شود.

- مواد ورودی به مکان استفاده باید از نظر پتانسیل خطر مورد بازرسی قرار گیرد و در صورت امکان باید لیست مواد ورودی ثبت شود.

فرآیند

مراحل اجرای دستورالعمل دسترسی عمومی، نواحی ارسال و بارگیری به شرح زیر می باشد:

۱- ابتدا لازم است بر اساس دسته بندی سازمان از دیدگاه پدافند غیرعامل(مهم، حساس و حیاتی) و همچنین طبقه بندی حفاظتی دارایی های اطلاعاتی سازمان(عادی، محرمانه، خیلی محرمانه و ...) مناطق و نواحی مختلف سازمان را حیطه‌بندی کرده و مناطق دسترسی عمومی و نواحی ارسال و بارگیری را شناسایی نمود.

۲- پس از شناسایی مناطق دسترسی عمومی و نواحی ارسال و بارگیری لازم است الزامات امنیتی (بیان شده در این سند) تعیین شوند. همچنین لازم است در صورتیکه سازمان الزامات اختصاصی دیگری نیز در خصوص این موضوع دارد به الزامات بیان شده در این سند افزوده گردد.

۳- پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکانیزمهای برآورده کننده الزامات تامین شود. همچنین در صورت نیاز به فرم، کارت و ... ، اقدام به تهیه این موارد صورت پذیرد.

۴- پس از تامین تجهیزات و مکانیزم ها در این مرحله به اجرای کلیه الزامات مبادرت می گردد.

۵- در صورتی که پس از پیاده سازی مکانیزم ها، کلیه الزامات مناطق دسترسی عمومی تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شده باشد این دستورالعمل پایان می‌پذیرد. در غیر اینصورت لازم است مرحله ۵ مجددا اجرا گردد.

۱۸- کار در نواحی امن:

هدف از تدوین این دستور العمل افزایش امنیت مناطق امن و ارائه رویه های مناسب و معرفی مسئولیت هر یک از افراد در اجرای هر رویه و مکانیزم های کنترلی اضافی به منظور نظارت بر اجرای وظایف و عملکرد افراد سازمان هنگام کار در مناطق و بخش هایی از سازمان است که به عنوان محل امن تعریف شده اند.

الزامات

- لازم است در صورت نیاز به استفاده از دارایی های اطلاعاتی در شرایط تحت کنترل و حفاظتی خاص، مناطقی به عنوان مناطق امن تعریف و در خصوص افراد و شرایط کار در آن مناطق تصمیم گیری شود.

- لازم است بصورت دوره ای نواحی امن استقرار تجهیزات و دارایی های اطلاعاتی سازمان، تحت بازرسی و بازبینی قرار گیرند تا در صورت یافتن تجهیزات بدون صاحب یا بدون مراقب فوراً نسبت به تعیین متصدی یا مسئول آن اقدام گردد.

- فقط درمواقع ضرورت افراد وابسته به طرف های قرارداد و یا اشخاص ثالث و یا حتی افراد سازمان که به صورت عادی نیاز به کار در مناطق امن ندارند مجاز به دسترسی به منطقه امن می باشند. این دسترسی باید قبلا تایید شده و به ثبت برسد در صورت تفاوت درجه امنیتی واحدهای مستقر در منطقه امن لازم است از حفاظ و موانع مناسب برای جدا کردن این واحدها از یکدیگراستفاده شود.

- افرادی که بصورت مستقیم با سیستم های پردازش اطلاعات کار می کنند باید به قدر کافی آموزش دیده باشند و شرایط آموزش برای تعامل با سیستم های جدید برای ایشان فراهم گردد. همچنین لازم است برای سایر افراد برنامه های اطلاع رسانی و آگاهی بخشی از طریق اعلان در تابلو اخبار و یا ارسال نامه و بروشور در زمینه امنیت اطلاعات در نظر گرفته شود.

- لازم است رویه هایی برای تعامل با پرسنل ناراضی سازمان و یا محدود کردن یا انفصال فوری کارمندانی که امنیت فرآیندهای پردازشی سازمان را مورد تهدید قرار می دهند وجود داشته باشد.

- لازم است سابقه افرادی که در حال استخدام در سازمان هستند (بر اساس دستورالعمل های امنیت منابع انسانی) بررسی شود. این کار برای استخدام در پست های حساس اهمیت بیشتری دارد، همچنین لازم است سابقه افراد بطور دوره ای مورد بررسی مجدد قرار گیرد.

- عکاسی، فیلم برداری، ضبط صدا و استفاده از تجهیزات استراق سمع و سایر تجهیزات مشابه در منطقه امن بدون کسب مجوز ممنوع است.

- در مراکز حیاتی لازم است ساختمان ها چشمگیر نبوده و هیچ نشانی از مورد استفاده شان نداشته باشند. هیچ علامت بصری چه در داخل و چه درخارج، ساختمان را به عنوان مرکز پردازش اطلاعات معرفی ننماید و راهنما و دفاتر تلفن داخلی مورد استفاده که در آن، آدرس منزل و یا شماره تلفن افراد یا آدرس های شبکه ای

تجهیزات پردازش اطلاعات حساس درج شده است، نباید در دسترس عموم قرار داشته باشد و فقط در صورت ضرورت به یک کارمند گفته خواهد شد که منطقه امنی وجود دارد و یا فعالیت هایی در رابطه با این منطقه به انجام می رسد.

- کار در نواحی امن برای افراد غیرمجاز ممنوع است. رعایت این امر به دلایل امنیتی (حفظ ایمنی فیزیکی) و یا جلوگیری از نفوذ ویروس و یا برنامه های نفوذگر اهمیت دارد.

- مناطق امن خلوت یا متروک باید بصورت فیزیکی قفل شده و به صورت دوره ای مورد بازرسی قرار گیرد.

- بمنظور شناسایی افراد موظف به کار در محوطه پردازش اطلاعات استفاده از لباس های فرم و متحدالشکل و کارت شناسایی عکسدار و هر روش شناسایی لازم دیگر الزامی می باشد.

- لازم است رویه های تعاملی برخورد با افرادی که هویت آنها غیر قابل شناسایی و تشخیص است به درستی تنظیم شود.

- لازم است رویه های جلوگیری از دسترسی افراد در خارج از ساعات کاری خود به تجهیزات پردازش اطلاعات به درستی تنظیم و به کار گرفته شود.

- لازم است روشی مناسب برای تخلیه زباله و مواد مصرف شده اضافی از محوطه پردازش اطلاعات و نظافت تجهیزات و سطوح کاری وجود داشته باشد.

- افراد نظافتچی یا نیروهای خدماتی مجاز به تردد به مناطق امن نیز بایستی آشنا و ملزم به الزامات کار در مناطق امن باشند.

- هنگام ورود هر کاربر به سیستم در مناطق امن بایستی نوع سیستم، ساعت آغاز به کار، اخطارهای لازم در مورد سطح امنیتی آن، آخرین زمان استفاده کاربر حاضر از سیستم و سایر اطلاعاتی که به حفظ امنیت سیستم کمک می نماید نمایش داده شود.

فرآیند

مراحل اجرای دستورالعمل کار در نواحی امن به شرح زیر می باشد:

۱- ابتدا لازم است بر اساس دسته بندی سازمان از دیدگاه پدافند غیرعامل(مهم، حساس و حیاتی) و همچنین طبقه بندی حفاظتی دارایی های اطلاعاتی سازمان(عادی، محرمانه، خیلی محرمانه و ...) مناطق و نواحی مختلف سازمان را حیطه بندی کرده و نواحی امن را مشخص نمود.

۲- لازم است پیش از هر اقدامی ابتدا الزامات افرادی که مجاز به دسترسی به نواحی امن می باشند تدوین شود. در این الزامات باید به دسترسی اشخاص ثالث، افراد نظافتچی، نگهبانان و همچنین چگونگی برخورد با دسترسی های غیرمجاز نیز اشاره شود.

۳- پس از آن لازم است الزامات امنیتی کار در نواحی امن (بیان شده در این سند) تعیین شوند. همچنین لازم است در صورتیکه سازمان الزامات اختصاصی دیگری نیز در خصوص این موضوع دارد به الزامات بیان شده در این سند افزوده گردد.

۴- پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکانیزم ها و روش های برآورده کننده الزامات تامین شود. همچنین در صورت نیاز به فرم، کارت و ... ، اقدام به تهیه این موارد صورت پذیرد.

۵- پس از تامین تجهیزات و مکانیزم ها در این مرحله به پیاده سازی و اجرای کلیه الزامات مبادرت می گردد.

۶- در صورتی که پس از پیاده سازی مکانیزم ها و روش ها، کلیه الزامات کار در نواحی امن تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شده باشد این دستورالعمل پایان می‌پذیرد. در غیر اینصورت لازم است مرحله ۵ مجددا اجرا گردد.

۱۹- کنترل فیزیکی ورودی ها :

هدف از تدوین این دستورالعمل نظارت وکنترل بر نقاط ورود به محوطه های تحت کنترل یا مالکیت به منظور جلوگیری از ورود افراد غیرمجاز و ورود غیرمجاز افراد به نواحی نگهداری دارایی‌های اطلاعاتی سازمان، ایجاد کنترل و سهولت دسترسی به اطلاعات حساس و تجهیزات پردازش اطلاعات فقط برای افراد مجاز، با استفاده از تجهیزات مناسب کنترل مبادی ورود و خروج می باشد.

الزامات

- درانتخاب تجهیزات مناسب برای کنترل مبادی ورود و خروج لازم است به سطح بندی و الزامات تعیین شده از سوی سازمان پدافند غیر عامل توجه شود.

- لازم است درمورد ورود به نواحی دارای طبقه بندی محرمانه به ترتیب کنترل های اضافی از قبیل کنترل شناسه کاربری و کلمه عبور، کنترل نشانه[۱۶] های سخت افزاری و یا کنترل عوامل بیومتری بکار گرفته شود، به علاوه در نواحی خیلی محرمانه از روش تایید دسترسی توسط مقام بالاتر نیز استفاده شود.

- لازم است نقاط و درهای ورودی به نواحی امنیتی طبق دستورالعمل‌های تهیه شده توسط مدیریت حراست تحت مراقبت و حفاظت قرار گیرد.

[1]- Token

- لازم است افرادی که از مکان های امن بازدید می کنند همراهی یا تایید شوند و زمان ورود و خروجشان ثبت گردد. فقط افراد مجاز می توانند به مکان هایی که از نظر مدیریت سازمان مکان های خاص تلقی می شوند دسترسی داشته باشند.

- لازم است تجهیزات کنترل دسترسی مانند کارت های الکترونیکی عکسدار و یا کدهای دسترسی شخصی فقط در اختیار افراد مجاز بوده وکلیه دسترسی ها ثبت شود.

-لازم است رویه های تعاملی و برخورد مناسب با افرادی که هویت آن ها غیر قابل شناسایی و تشخیص است تنظیم و به اجرا گذاشته شود.

- لازم است رویه های کنترل بازدیدکنندگان و میهمانان مراجعه کننده به محوطه های پردازش اطلاعات یا محل نصب تجهیزات مسیریابی یا سوییچینگ یا ترمینال های مخابراتی به درستی انتخاب، تنظیم و اجراء شود.

- لازم است افراد مجاز از مقررات و الزامات امنیتی محیط آگاهی داشته و رویه های اضطراری را نیز به یاد داشته باشند.

- لازم است دسترسی به اطلاعات حساس و تجهیزات پردازش اطلاعات فقط برای افراد مجاز تعریف شود. افراد موظفند هنگام کار در محوطه پردازش اطلاعات از لباس فرم و کارت شناسایی الصاق شده به لباس استفاده نمایند.

-لازم است رویه های جلوگیری از دسترسی افراد به تجهیزات پردازش اطلاعات خارج از ساعات کاری مجاز به درستی تنظیم و به کار گرفته شود.

-افراد حراست باید متناسب با اهمیت مکانی که از آن حفاظت می نمایند، آمادگی لازم برای مقابله با افرادی که به تنهایی یا به صورت گروهی قصد ورود بدون مجوز را بنمایند داشته باشند.

- لازم است مجوزهای دسترسی به مناطق امن مرتباً بازنگری شوند.

- استفاده از مکانیزم هایی که مانع از ورود خودروهای غیر مجاز می شوند در مراکز حساس و حیاتی ضروری است.

فرآیند

مراحل اجرای دستورالعمل کنترل فیزیکی ورودی ها به شرح زیر می باشد:

۱- در ابتدا لازم است بر اساس جدول سطح بندی عملیات امن سازی(ارائه شده در بخش توضیحات) سطوح مختلف نواحی سازمان را تعیین نمود. این سطح بندی در تعیین الزامات نواحی مختلف و همچنین مکانیزم های مورد استفاده در هر یک بسیار موثر خواهد بود.

۲- در این مرحله لازم است الزامات امنیتی ورودی برای هر بخش بر اساس سطح تعیین شده در مرحله قبل تدوین گردد. همچنین لازم است در صورتیکه سازمان الزامات اختصاصی دیگری نیز داشته باشد به الزامات بیان شده در این سند افزوده گردد.

۳- بر اساس الزامات بیان شده در این سند و یا الزامات اختصاصی سازمان ممکن است نیاز به فرم های خاصی جهت کنترل بیشتر ورود افراد باشد. در اینصورت در این مرحله اقدام به تدوین این فرم ها صورت می پذیرد. از جمله این فرم ها می توان به موارد زیر اشاره نمود:

- فرم مرخصی ساعتی
- فرم ورود میهمان
- فرم خروج کارمندان

۴- پس از تعیین کلیه الزامات، باید تجهیزات مورد نیاز و همچنین مکانیزم های برآورده کننده الزامات تامین شود.

۵- پس از تامین تجهیزات و مکانیزم‌ها در این مرحله به پیاده‌سازی و اجرای کلیه الزامات مبادرت می‌گردد.

۶- در صورتی که پس از پیاده سازی مکانیزم ها، کلیه الزامات کنترل فیزیکی ورودی‌ها تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شده باشد این دستورالعمل پایان می پذیرد. در غیر اینصورت لازم است مرحله ۵ مجددا اجرا گردد.

۲۰- نگهداری تجهیزات:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی نگهداری و تعمیرات کلیه تجهیزات پردازش اطلاعات و ارتباطات در اختیارو ابزار پشتیبان آن به منظور ایجاد حداکثر پایایی و افزایش قابلیت اطمینان و در دسترس بودن تجهیزات پردازشی و مخابراتی می باشد.

الزامات

- لازم است برنامه های نگهداری و تعمیرات برای کلیه دارایی های موجود در فهرست دارایی های اطلاعاتی تدوین و به اجرا گذاشته شود.

- لازم است در سازمان ها و مراکزی که از طرف سازمان پدافند غیرعامل تحت عنوان مراکز مهم یا حساس دسته بندی شده اند، تعمیرات و نگهداری تجهیزات پردازشی بر اساس مدل پیشگیرانه انجام شود.

- لازم است در مراکز حیاتی، تعمیرات و نگهداری تجهیزات پردازشی بر اساس مدل برنامه های پیشگویانه انجام شود.

- لازم است برنامه ریزی با هدف حداکثر کردن پایایی تجهیزات و خدمات پردازشی انجام شود.

- لازم است امنیت فیزیکی و محیطی تجهیزات پردازش اطلاعات بر اساس دستوالعمل های مربوط برآورده شود.

- لازم است اطلاعات و تجهیزات پردازش اطلاعات هنگام اجرای برنامه های نگهداری و تعمیرات در مقابل افشاء، لو رفتن و تغییر یا سرقت محافظت شوند.

- لازم است تجهیزاتی که پس از تعمیر به سازمان بازگردانده می شوند مجدداً فرآیند صدور مجوز را طی نمایند.

- لازم است مسئولیت افراد در حفاظت از هر یک از دارایی های اطلاعاتی هنگام اجرای برنامه های نگهداری و تعمیرات یا در ارسال برای تعمیر بطور شفاف تعریف شود.

- هنگام عقد قراردادهای نگهداری و تعمیرات با طرف های خارج از سازمان که ممکن است منجر به دسترسی به تجهیزات پردازشی، ارتباطی، امنیتی یا پشتیبانی شود بایستی کلیه الزامات حفاظت از امنیت دارایی های اطلاعاتی به رویت و امضای طرف قرارداد رسیده و به نحو مناسب تضمین اجرای تعهد از ایشان اخذ شود.

- لازم است هنگام انجام عملیات نگهداری و تعمیرات، به مجوزهای دسترسی به اطلاعات و تجهیزات و سطح دسترسی افراد تعمیرکار توجه و الزامات آن رعایت شود.

- تجهیزات باید در مقابل افت جریان برق یا هر اختلالی که بر اثر عدم پشتیبانی تاسیسات بوجود می آید حفاظت شوند.

- کابل کشی های برق و مخابراتی که انتقال داده یا تغذیه برق سرویس‌های اطلاعاتی را به عهده دارند باید در مقابل قطع یا آسیب محافظت شوند.

-برنامه نگهداری و تعمیرات تجهیزات خارج از سازمان باید با در نظر گرفتن مخاطرات متفاوت کاری که در خارج از محدوده سازمان وجود دارد تنظیم و بکار گرفته شود.

-در مراکز حساس و حیاتی تجهیزات، اطلاعات یا نرم افزارها نباید بدون مجوز قبلی حتی با فرض نیاز به انجام تعمیرات خارج از سازمان از محل خارج شود.

-قبل از اجرای برنامه های نگهداری و تعمیرات باید از اطلاعات و نرم افزارها بطور مرتب و مطابق با خط‌مشی پشتیبان گیری، نسخه پشتیبان تهیه شود.

-لازم است در برنامه های نگهداری و تعمیرات پیش بینی های لازم طبق الزامات تعیین و تخمین ظرفیت آینده جهت حصول اطمینان از عملکرد سیستم رعایت گردد.

- سیستمهای حساس باید محیط کامپیوتری (محاسباتی) اختصاصی مجزا داشته باشند.

- در مراکز حساس و حیاتی لازم است هرگونه درخواست تهیه و خرید دارایی های اطلاعاتی یا تولید سیستمهای اطلاعاتی منضم به پیوست نگهداری و تعمیرات باشد.

-هنگام اعمال هرگونه تغییرات در سیستم های پردازش اطلاعات و مخابراتی سازمان، لازم است پیش بینی های لازم درخصوص به هنگام سازی برنامه های نگهداری و تعمیرات انجام شود.

- در مراکز حساس و حیاتی لازم است سوابق خرابی و تعمیرات تجهیزات ثبت و نگهداری شده و بصورت دوره ای مورد بازبینی قرار گیرد.

- لازم است برنامه های بازرسی و نگهداری و تعمیرات بر اساس رهنمودهای تولیدکننده یا تامین کننده و شرایط بهره برداری تجهیزات پردازشی تدوین شود.

فرآیند

مراحل اجرای دستورالعمل نگهداری تجهیزات به شرح زیر می باشد:

۲۱-در ابتدا لازم است سطح دارایی های اطلاعاتی سازمان با توجه به دسته بندی سازمان از سوی پدافند غیرعامل(مهم، حساس و حیاتی) و همچنین طبقه بندی حفاظتی دارایی های اطلاعاتی سازمان(عادی، محرمانه، خیلی محرمانه و ...)تعیین گردد. این تعیین سطح در برنامه ریزی عملیات مطلوب در این فرآیند بسیار موثر خواهد بود.

۲۲-در این مرحله باید اطلاعات لازم در خصوص نیازهای دارایی های اطلاعاتی جمع آوری شود، اطلاعاتی از قبیل:

- شرایط محیطی تعیین شده توسط سازنده
- تاسیسات مورد نیاز
- خرابی های احتمالی و چگونگی برطرف نمودن آنها

۲۳-پس از جمع آوری اطلاعات در این مرحله اقدام به برنامه ریزی برای عملیات اجرایی می گردد. این عملیات در قالب ۳ مدل بازدید، تعمیرات پیشگیرانه و تعمیرات پیشگویانه(که در بخش توضیحات شرح داده شده اند) و بر اساس سطح دارایی اطلاعاتی تدوین و به اجرا گذاشته می‌شود.

۲۴-بعد از اجرای عملیات برنامه ریزی شده در صورتی که نیاز به تعمیرات اصلاحی باشد لازم است که از دارایی اطلاعاتی و یا محتوای اطلاعات درون آن نسخه پشتیان تهیه گردد. در صورت عدم نیاز به تعمیرات اصلاحی این دستورالعمل پایان می پذیرد.

۲۵-پس از تهیه نسخه پشتیان و بمنظور تعمیرات اصلاحی اگر نیازی به خروج دارایی اطلاعاتی از سازمان نباشد پس از انجام تعمیر اصلاحی این دستورالعمل پایان می پذیرد. در صورتی که نیاز به خروج

دارایی اطلاعاتی از سازمان باشد ابتدا لازم است مجوز خروج توسط مراجع ذیربط صادر شده و تاییدیه نهاد متصدی امنیت اطلاعات اخذ گردد.

۲۶-در این مرحله تعمیر اصلاحی توسط شرکت پشتیبان و یا شرکت متخصص انجام خواهد شد.

۲۷-پس از تعمیر اصلاحی جهت بازگرداندن دارایی اطلاعاتی به سازمان بمنظور حفظ اصول و ضوابط امنیتی لازم است فرآیند صدور مجوز استفاده برای دارایی اطلاعاتی به اجرا گذاشته شود.

۲۱- جمع آوری شواهد و مدارک:

هدف از تدوین این دستورالعمل بیان ضرورت وجود شواهد و مدارک مستدل و محکمه پسند بعد از وقوع هرگونه حادثه امنیتی به منظور پیگیری های قانونی و بررسی مطابقت با قوانین و انجام اقدامات قانونی آتی در اختیار می باشد.

الزامات:

- لازم است اطلاعات و آگاهی لازم در خصوص نحوه جمع آوری شواهد و مدارک مستدل مبنی بر وقوع حادثه امنیتی به کاربران داده شود. این کار باید بصورت عام در هنگام استخدام و بصورت خاص در زمان مقتضی به کاربر انجام شود.
- بایستی در بازه های زمانی از پیش تعیین شده نسبت به بهنگام‌سازی روشهای جمع آوری شواهد و مدارک مستدل مبنی بر وقوع حادثه امنیتی اقدام شود.
- شواهد جمع آوری شده مبنی بر وقوع حادثه امنیتی و پیامدهای آن باید به عنوان اطلاعات دارای طبقه‌بندی بایگانی گردد.
- سطح طبقه بندی حفاظتی مدارک و شواهد جمع آوری شده درخصوص وقایع یا حوادث امنیت اطلاعات حداقل معادل رده حفاظتی دارایی اطلاعاتی موضوع حادثه می باشد.

- افشاء مدارک جمع آوری شده مبنی بر وقوع حادثه امنیتی و پیامدهای آن ممنوع است.
- مدارک باید از نقطه نظر قابلیت استفاده، کیفیت و کامل بودن جهت تصمیم گیری در برخورد با حادثه امنیتی توسط نهاد متصدی امنیت اطلاعات بررسی شده و تایید این نهاد را اخذ نمایند.
- برای دست یافتن به شواهد قابل قبول باید اطمینان حاصل گردد که مدارک جمع آوری شده با استانداردهای مورد پذیرش مراجع قانونی یا قضایی مطابقت دارد.
- مدارک جمع آوری شده مبنی بر وقوع حادثه امنیتی و پیامدهای آن باید مطابق با قوانین و روالهای کنترل مستندات تعریف شده توسط مدیر ذیربط کنترل و مستند گردد.
- ذخیره و پردازش مدارک جمع آوری شده مبنی بر وقوع حادثه امنیتی جهت هرگونه اقدام و پیگیری قانونی بر عهده مدیر ذیربط می باشد.
- اسناد کاغذی باید مطابق با قوانین مرتبط با حفاظت اسناد کاغذی به طور امن حفظ و نگهداری گردند.
- فرد یا گروه ارائه دهنده سند یا اسناد، باید ثبت و مشخص گردد. جهت بررسی ها و پیگیری های بعدی زمان مصدق ارائه نیز باید در این مستندات قید گردد.
- اسناد الکترونیکی باید مطابق با قوانین مرتبط با اسناد الکترونیکی به طور امن حفظ و نگهداری گردند بطوریکه انکارناپذیر، قابل اثبات و قابل استفاده باشند.(به پیوست یک مراجعه شود)
- فرآیند کپی برداری از مدارک و اسناد جمع آوری شده مبنی بر وقوع حادثه امنیتی که ممکن است مورد استفاده قانونی قرار گیرد، باید با نظارت نماینده معرفی شده از طرف مدیر ذیربط و تحت کنترل انجام گردد.
- زمان و مکان انجام فرآیند کپی برداری از مدارک و اسناد جمع آوری شده مبنی بر وقوع حادثه امنیتی باید با جزییات کامل ثبت گردد. این جزییات باید از طرف مدیر ذیربط به اطلاع متصدیان نگهداری اطلاعات برسد.

فرآیند:

مراحل انجام دستورالعمل جمع آوری شواهد و مدارک به شرح زیر می باشد:

۱- بهترین روش برای اطمینان از آگاهی کاربر نسبت به اهمیت نحوه جمع آوری مدارک مبنی بر وقوع حادثه امنیتی، امضای سند کتبی مبین الزامات جمع آوری شواهد و مدارک مبنی بر وقوع حادثه امنیتی پس از مطالعه آن می باشد.

۲- لازم است روشها و مقررات جمع‌آوری شواهد و مدارک تدوین شده و اطلاع رسانی و آموزش در خصوص نحوه جمع آوری شواهد و مدارک مستدل مبنی بر وقوع حادثه امنیتی به کاربرانی که ممکن است در معرض وقوع حوادث موثر بر سرنوشت سازمان باشند داده شود.

۳- جمع آوری مدارک و شواهد باید با استفاده از روش های قابل استناد قانونی مانند استفاده از امضای الکترونیک یا مهر زمانی[۱۷] انجام شود.

۴- پس از جمع آوری مدارک و شواهد لازم است آنها را مستند نموده و یک نسخه از آنها را بایگانی نمود.

۵- ذخیره و پردازش مدارک جمع آوری شده مبنی بر وقوع حادثه امنیتی جهت هرگونه اقدام و پیگیری باید بر اساس رهنمودهای قانونی انجام پذیرد.

۶- در صورت نیاز به رسیدگی فنی لازم است شواهد و مدارک بررسی شده به مراجع فنی ارسال شده و پیگیری کافی در خصوص دریافت پاسخ صورت گیرد.

۷- در مرحله پایانی این دستورالعمل نیز در صورت نیاز به رسیدگی قضایی لازم است مدارک لازم در اختیار مراجع قضایی قرار داده شده و پیگیری کافی در خصوص دریافت پاسخ صورت گیرد.

۲۲- سیاست گذاری مدیریت حوادث امنیت اطلاعات:

[17]- Time Stamping

هدف از تدوین این دستورالعمل بیان ضرورت شناسایی حوادث امنیتی و گزارش به موقع آنها به مراجع ذیصلاح و چگونگی مخابره گزارش حوادث به وقوع پیوسته مرتبط با سیستم‌های اطلاعاتی در اختیار جهت انجام اقدام اصلاحی مناسب در زمان مناسب می باشد.

الزامات

- گزارش هرگونه حادثه امنیت اطلاعات یا واقعه مهم امنیتی برای کارکنانی که با آن مواجه می‌شوند الزامی است. این گزارش باید در اسرع وقت و با کسب اطمینان از مورد توجه واقع شدن آن به مراجع ذیربط ارسال شود و حاوی اطلاعات لازم (بخصوص زمان وقوع حادثه) باشد.
- رویدادها یا وقایع امنیتی باید از طریق کانال های مناسب مدیریتی و با سرعت گزارش شوند.
- رویه گزارش‌دهی رسمی باید همراه با یک رویه پاسخ امنیتی بوده و ترتیب عملیاتی پس از دریافت یک گزارش رویداد امنیتی را دربرداشته باشد.
- روش‌های مقابله با حوادث امنیتی شناسایی شده باید توسط واحد امنیت اطلاعات و یا نهاد جایگزین آن معرفی گردد.
- طراحی روش بازخورد مناسب برای اطمینان از مورد توجه قرارگرفتن گزارش واقعه امنیتی و پیگیری آن تا حصول نتیجه قابل پذیرش الزامی است.
- ثبت فعالیت های انجام شده جهت مقابله با رویداد امنیتی، برای جلوگیری از اثرات سوء آن الزامی است.
- رویدادهای امنیتی باید به عنوان بخشی از مواد آموزشی در زمینهٔ چگونگی وقوع رویداد، چگونگی پاسخ به آن و یا شرایط بروز وقایع مشابه و چگونگی پیشگیری از بروز مجدد آن مورد استفاده قرار گیرند.

- روال‌های رسمی محدود سازی هرحادثه امنیتی بایستی در دسترس افراد باشد.
- تمام کارمندان و پیمانکاران و کاربران غیر وابسته به سازمان که به ضرورت از خدمات رایانه ای سازمان بهره می برند باید از نحوه گزارش انواع مختلف رخدادها و نقاط ضعف تاثیرگذار بر امنیت دارایی های اطلاعاتی سازمان آگاهی داشته و حتی الامکان قادر به اجرای روال های رسمی محدود سازی حوزه اثر حادثه باشند.
- روال رسمی گزارش رخداد امنیت اطلاعات همراه با پاسخ حوادث و روال محدود سازی بایستی تدوین و ابلاغ شود تا در هنگام دریافت یک گزارش رخداد امنیت اطلاعات اقدام مناسب صورت گیرد.
- یک نقطه تماس برای گزارش رخدادهای امنیت اطلاعات باید ایجاد و به کلیه کاربران معرفی گردد.
- بایستی اطمینان حاصل شود که نقطه تماس شناخته شده از طریق سازمان، همیشه در دسترس بوده و قادر است پاسخ کافی و مناسبی را فراهم کند. به عبارت دیگر لازم است فرآیند مدیریت حوادث امنیت اطلاعات از طریق ایجاد روش بازخورد مناسب پشتیبانی گردد.

فرآیند

مراحل اجرای دستورالعمل سیاست گذاری مدیریت حوادث امنیت اطلاعات به شرح زیر می باشد:

۱- بهترین روش برای اطمینان از آگاهی کاربر نسبت به اهمیت گزارش دهی هرگونه حادثه امنیتی و نحوه برخورد و یا هرگونه مکانیزم اطلاع حادثه به مراجع ذیصلاح، امضای سند کتبی مبین آگاهی از الزامات گزارش وقایع و حوادث امنیت اطلاعات می باشد.

۲- لازم است جهت نظم بخشی و ایجاد سهولت در روند کار فرم های لازم تدوین و تهیه شوند.

۳- گزارش دهنده باید فرم های مربوط را تکمیل نموده و جزییات حادثه را بصورت کامل گزارش نماید.

۴- پس از تکمیل فرم حادثه امنیتی باید به نقطه تماس تعیین شده در سازمان اطلاع داده و فرم های تکمیل شده در اختیار مراجع ذیربط(نهاد متصدی امنیت اطلاعات) قرار داده شود.

۵- پس از دریافت گزارش حادثه امنیتی، نهاد ذیربط نسبت به بررسی گزارش حادثه امنیتی اقدام کرده و و اطلاعات جمع آوری شده را پردازش می کند و بر اساس آنها نسبت به انتخاب روش مقابله با واقعه یا حادثه تصمیم گیری می نماید.

۶- بررسی ها و اقدامات انجام شده توسط نهاد ذیربط مستند سازی و یک نسخه از آن بایگانی خواهد شد.

۷- در صورت نیاز به پیگیری، گزارش های ارسالی، توسط نهاد ذیربط پیگیری شده و بازخوردهای آن دریافت و مورد بررسی قرار می گیرد.

۸- سوابق گزارش های حوادث امنیتی باید به صورت دوره ای(مثلاً هر سه ماه یکبار و یا هر بازه زمانی که توسط مدیریت تعیین می شود) به اطلاع مراجع ذیصلاح برسد تا در خصوص پیشگیری از وقوع مجدد آنها تصمیم گیری شود. همچنین فعالیتهای انجام شده جهت مقابله و پیشگیری از وقوع مجدد حادثه توسط این نهاد ثبت می‌گردد.

۹- حادثه وقوع یافته باید در دفترچه ثبت خلاصه وقایع و حوادث امنیت اطلاعات جهت پیگیری های آتی ثبت گردد.

۱۰-دفترچه ثبت وقایع امنیت اطلاعات باید به منظور اطمینان از مورد رسیدگی قرارگرفتن تمام وقایع بصورت مرتب بررسی شود.

۲۳- گزارش ضعف های امنیت اطلاعات:

هدف از تدوین این دستورالعمل بیان ضرورت شناسایی ضعفهای امنیتی و چگونگی ثبت و ارائه گزارش ضعفهای امنیتی مشاهده شده و یا مشکوک در سیستم های پردازشی و یا سرویس های رایانه ای در اختیار به منظور محدود کردن خسارات و اطمینان از ادامه خدمات سیستم هنگام مواجهه با تهدیدات می باشد.

الزامات

- هرگونه تلاش شخصی برای شناسایی یا اثبات نقاط ضعف امنیتی دارایی های اطلاعاتی ممنوع می‌باشد.
- لازم است استفاده کنندگان از خدمات اطلاعاتی در مورد نکات مربوط به نقاط ضعف مشاهده شده و یا احتمالی امنیتی، توجه داشته و رویداد و یا امکان بروز چنین وقایعی را گزارش دهند. بدیهی است این موضوع نمی تواند بهانه ای برای تلاش شخصی جهت شناسایی یا اثبات ضعف امنیتی باشد.
- لازم است اطلاعات و آگاهی لازم نسبت به ثبت وگزارش هر نوع مشاهده یا مشکوک بودن به ضعف امنیتی در سیستم ها یا سرویس ها به کاربران داده شود. این کار باید به صورت عام در هنگام استخدام و به صورت رسمی در دوره های آموزشی و به صورت خاص در زمان وقوع هر حادثه به کاربر انجام شود.
- بایستی در بازه های زمانی از پیش تعیین شده نقاط ضعف امنیتی از طریق انجام آزمون نفوذ[۱۸] شناسایی و نسبت به رفع آنها اقدام شود. انجام آزمون نفوذ باید بر اساس سیاستگذاری های امنیتی سازمان و در چارچوب رسمی به عمل آید و کلیه افراد مرتبط با آن در جریان امر قرار گیرند.
- تمام کارمندان، پیمانکاران و کاربران سوم شخص سیستم ها و سرویس های اطلاعاتی موظف به ثبت وگزارش هر نوع مشاهده یا مشکوک بودن به ضعف امنیتی در سیستم ها یا سرویس ها می‌باشند.
- مکانیزم گزارش بایستی هر چقدر که می تواند آسان، در دسترس و قابل استفاده باشد.
- در گزارش ارائه شده لازم است تاریخ دقیق ارائه گزارش، فرد یا گروه گزارش دهنده و جزئیات دیگر از قبیل نام دارایی های اطلاعاتی و پیامدهای احتمالی ناشی از ضعف موجود جهت پیگیری بعدی مشخص باشد.

[18]- Penetration Test

- بمنظور جلوگیری از رخدادهای امنیت اطلاعات، تمام کارمندان، پیمانکاران و سایر کاربران موظفند هر چه سریعتر این قبیل موضوعات را به مدیر مستقیم یا مستقیماً به تامین کننده سرویس[19] (مثل اپراتورهای مخابراتی یا شرکت های پشتیبانی کننده سیستم های رایانه ای)گزارش کنند.
- از آنجا که آزمایش آسیب پذیری ممکن است بعنوان یک سوء استفاده پنهانی از سیستم تفسیر شود و همچنین می تواند به سیستم یا سرویس اطلاعاتی خسارت وارد کند، لذا لازم است پیامدهای قانونی هرگونه تلاش شخصی جهت شناسایی یا اثبات نقاط ضعف امنیتی سیستم ها به کاربران مؤکداً یادآوری شود.

فرآیند

مراحل اجرای دستورالعمل گزارش ضعف های امنیت اطلاعات به شرح زیر می باشد:

۱- بهترین روش برای اطمینان از آگاهی کاربر نسبت به عدم آزمایش آسیب پذیری و عدم انجام اقدامات شخصی، امضای سند کتبی مبین آگاهی از الزامات می باشد.

۲- لازم است جهت نظم بخشی و ایجاد سهولت در روند کار فرم های لازم تدوین و تهیه شوند.

۳- گزارش دهنده باید فرم های مربوط را تکمیل نموده و جزییات ضعف امنیتی را بصورت کامل گزارش نماید.

۴- پس از تکمیل فرم ضعف امنیتی امنیتی باید فرم های تکمیل شده در اختیار مراجع ذیربط(نهاد متصدی امنیت اطلاعات) قرار داده شود.

۵- پس از دریافت گزارش ضعف امنیتی، نهاد ذیربط نسبت به بررسی گزارش ضعف امنیتی اقدام کرده و اطلاعات جمع آوری شده را پردازش می کند و بر اساس آنها نسبت به انتخاب روش مقابله با ضعف امنیتی تصمیم گیری می نماید.

[19] - service provider

۶- بررسی ها و اقدامات انجام شده توسط نهاد ذیربط مستند سازی و یک نسخه از آن بایگانی خواهد شد.

۷- در صورت نیاز به پیگیری، گزارش های ارسالی، توسط نهاد ذیربط پیگیری شده و بازخوردهای آن دریافت و مورد بررسی قرار می گیرد.

۸- گزارش ضعف امنیتی باید به صورت دوره ای(مثلاً هر سه ماه یکبار و یا هر بازه زمانی قابل تعیین توسط مدیریت) به اطلاع مراجع ذیصلاح برسد تا در خصوص پیشگیری از وقوع حوادث ناشی از ضعف امنیتی شناسایی شده تصمیم گیری شود. همچنین فعالیتهای انجام شده جهت مقابله و پیشگیری از وقوع حادثه ناشی از ضعف امنیتی گزارش شده، توسط نهاد متصدی امنیت اطلاعات و یا نهاد جایگزین آن ثبت می گردد.

۹- آزمون نفوذ یکی از راه های موثر برای شناخت ضعف های امنیتی کشف نشده می باشد. طی آزمون نفوذ می توان به بررسی رفتار یا پاسخ دارایی های اطلاعاتی به تلاش های منجر به دسترسی غیر مجاز و یا تغییر در شرایط عادی کار پرداخت و با آگاهی از آنها اقدام به امن سازی سیستم نمود.[۲۰]

۲۴- مسئولیت ها و روش های اجرایی مدیریت حوادث:

هدف از تدوین این دستورالعمل حصول اطمینان از پاسخ سریع، موثر و منظم به حوادث امنیت اطلاعات و تعیین مسئولیت های مدیریتی و تدوین روش های اجرایی پاسخ به حوادث در سیستم های رایانه ای یا شبکه‌های ارتباطیمی باشد.

الزامات

- لازم است روش های اجرایی پاسخ به حوادث امنیت اطلاعات توسط نهاد ذیربط تدوین شده و به اطلاع کلیه کاربران سیستم‌های رایانه‌ای سازمان برسد.

[۲۰] - برای آگاهی بیشتر در مورد روش های آزمون نفوذ می توان به پایگاه های متعدد اینترنتی از جمله www.verisign.co.uk و www.iss.net مراجعه کرد.

- لازم است روش های اجرایی پاسخ به حوادث خلاصه، واضح و روشن بوده و در آن رئوس فعالیت‌هایی که کاربران هنگام مواجهه با حوادث باید به آن مبادرت ورزند همراه اطلاعات تماس افراد یا مراجعی که باید با آنها تماس گرفته شود درج شده باشد.
- روش اجرایی حفاظت باید متناسب با وضعیت دارایی اطلاعاتی در معرض تهدید باشد. بنابراین لازم است به ازای هر دسته از دارایی های اطلاعاتی مندرج در فهرست موجودی دارایی های اطلاعاتی روش های اجرای پاسخ به حوادث در محل مناسب و در معرض دید کاربران قرار داشته باشد.
- از آنجا که ممکن است بروز حوادث سلسله وار کوچک موجب آسیب های بزرگ یا فاجعه امنیت اطلاعات شود، بنابراین لازم است شرایط (مکانیزم) آغاز طرح پیوستگی عملیات[۲۱](BCP) به نحوی تنظیم شده باشد که نسبت به حوادث سلسله وار حساس بوده و آمادگی اجرای آن بدون اعلام شرایط فاجعه از سوی مراجع رسمی وجود داشته باشد.
- در صورتی که حادثه اتفاق افتاده منجر به فعال شدن طرح پیوستگی عملیات شود لازم است بلافاصله مقدمات طرح احیای سیستم[۲۲] (DRP) آماده شود تا در صورت نیاز از طریق آن به حادثه پاسخ داده شود.
- تدوین روش اجرایی پاسخ به حادثه باید بر اساس اطلاعات قبلی و واقعی در مورد دارایی های اطلاعاتی و فرآیندهای اجرایی و همچنین ظرفیت های از پیش تعیین شده برای عملکرد دارایی های اطلاعاتی انجام شود. بنابراین لازم است مسئولیت جمع آوری اطلاعات لازم برای شناسایی نیازها و الزامات عملیاتی هر یک از دارایی های اطلاعاتی به تحویل گیرنده، متصدی و یا مالک دارایی اطلاعاتی سپرده شود. مسئولیت شناسایی ظرفیت های لازم برای فرآیندهایی که از لحاظ ماموریت سازمانی حیاتی تلقی می شوند بر عهده مدیر واحد یا بخشی است که اجرای آن فرآیند بر عهده وی می باشد.

---

[21] -Business Continuity Plan

[22] - Disaster Recovery Plan

- لازم است کارایی و اثربخشی روش های اجرایی پاسخ به حوادث به صورت دوره‌ای (حداقل هر یک سال یک بار) و یا هنگام تغییر در وضعیت دارایی های اطلاعاتی با فرآیندهای اجرایی مورد بازنگری قرار گیرد.
- در صورتی که حوادث امنیت اطلاعات منجر به خسارت عمده یا فاجعه امنیت اطلاعات شود لازم است بلافاصله روش های اجرایی پاسخ به حوادث مورد بازبینی و بهبود قرار گیرند.

فرآیند

مراحل اجرای دستورالعمل مسئولیت ها و روش های اجرایی مدیریت حوادث به شرح زیر می باشد:

۱- لازم است نهاد ذیربط اقدام به جمع آوری اطلاعات کافی در مورد ماموریت سازمان، فرآیندها و دارایی های اطلاعاتی نماید تا در موقع بروز حوادث بتواند با استفاده از آنها مناسب ترین پاسخ را صادر نموده و از وارد آمدن زیان جلوگیری نماید و یا در صورت بروز حادثه بتواند ابعاد آن را کنترل یا محدود نماید.

۲- کلید اصلی پاسخ موفق به حوادث امنیت اطلاعات آگاهی از وضعیت دارایی های اطلاعاتی یا فرآیندهای اجرایی و روند تغییرات در فضای فناوری اطلاعاتی یا تهدیدهای موجود یا جدید می باشد. نهاد ذیربط باید دائماً تغییرات در فناوری های اطلاعاتی یا تهدیدهای موجود را تحت نظر داشته و روش های اجرایی پاسخ به حادثه را بر اساس آن بهنگام نمایند.

۳- پس از آن لازم است مسئولیت ها، مکانیزم ها و روش های اجرایی متناسب با تهدیدات و تغییرات (بیان شده در این سند) تدوین شوند. همچنین لازم است در صورتیکه سازمان الزامات اختصاصی دیگری نیز در خصوص این موضوع دارد به الزامات بیان شده در این سند افزوده گردد.

۴- پس از تامین تجهیزات و مکانیزم ها در این مرحله به پیاده سازی و اجرای مکانیزم ها و برنامه های تدوین شده پاسخ به تهدیدات مبادرت می گردد.

۵- در صورتی که پس از پیاده سازی مکانیزم ها و روش ها، کلیه الزامات تدوین شده (شامل الزامات این سند و همچنین الزامات اختصاصی سازمان) برآورده شده باشد این دستورالعمل پایان می‌پذیرد. در غیر اینصورت لازم است مرحله ۴ مجددا اجرا گردد.

۲۵- یادگیری از حوادث امنیت اطلاعات:

هدف از تدوین این دستورالعمل بیان ضرورت تشخیص حوادث تکراری بوسیله ارزیابی حوادث امنیت اطلاعات و یادگیری از آنها جهت جلوگیری از تکرار حوادث می باشد.

الزامات

- حوادث تکراری باید با ارزیابی حوادث امنیت اطلاعات تشخیص داده شده و شناسایی گردند.
- وجود مکانیزم شناسایی حوادث امنیت اطلاعات الزامی است به نحوی که به کمک آن بتوان انواع حوادث امنیت اطلاعات، دفعات وقوع حوادث مشابه یا شرایط مشابهی که منجر به وقوع حادثه های مختلف می شود و حجم و شدت آنها را مورد سنجش قرارداده وآشکار نمود.
- شناسایی انواع مختلف حوادث امنیت اطلاعات و تشخیص حجم و شدت آنها باید توسط نهاد متصدی امنیت اطلاعات و یا نهاد جایگزین آن انجام گردد. بعلاوه سایر کاربران موظفند در صورت مواجه شدن با تکرار حوادث، مراتب را گزارش نمایند.
- ارزیابی حوادث امنیتی به منظور تشخیص امکان وقوع مجدد حوادث به کمک اطلاعات حاصل از ارزیابی الزامی است.
- نتایج حاصل از ارزیابی به منظور یادگیری از آنها و پیشگیری از وقوع مجدد آنها باید مستند و مکتوب گردد.

- لازم است هنگام تهیه برنامه های آموزشی امنیت اطلاعات گزارش وقایع و حوادث امنیتی قبلی مورد بازبینی قرار گرفته و نتیجه آن در تدوین برنامه های آموزشی مورد توجه قرار گیرد. بدیهی است حوادثی که بیش از یکبار اتفاق افتاده اند دارای اهمیت بیشتری بوده و ضروری است آموزش لازم در جهت جلوگیری از تکرار آنها به کاربران داده شود.

- از نتایج حاصل از ارزیابی حوادث امنیت اطلاعات باید نیاز به کنترلهای اضافی یا ارتقاء یافته تشخیص داده شود و فرکانس، خسارت و شدت رخدادهای آینده پیش بینی گردد.

- در فرآیند مرور سیاستهای امنیتی سازمان باید از نتایج حاصل از ارزیابی حوادث امنیت اطلاعات استفاده کرد تا فرکانس و خسارت ناشی از حوادث امنیت اطلاعات محدود شده و کاهش یابد.

- دفترچه ثبت خلاصه وقایع و حوادث امنیت اطلاعات باید به صورت دوره ای بازبینی گردد و نتایج حاصل از این بازبینی در یادگیری از حوادث و پیشگیری از وقوع مجدد آنها مورد استفاده قرار گیرد.

- در مراکز حیاتی و حساس پس از یک بار رخ دادن حادثه باید بررسی های لازم صورت پذیرد و اقدامات لازم جهت پیشگیری از وقوع مجدد آنها انجام شود.

- در سایر مراکز پس از دوبار رخ دادن حادثه باید بررسی های لازم صورت پذیرد و اقدامات لازم جهت پیشگیری از وقوع مجدد آنها انجام شود.

فرآیند

مراحل اجرای دستورالعمل یادگیری از حوادث امنیت اطلاعات به شرح زیر می باشد:

۱- انواع مختلف حوادث امنیت اطلاعات به منظور تشخیص حجم و شدت آنها باید شناسایی شده و در دسترس کاربران قرارگیرد. به منظور تشخیص امکان وقوع مجدد حوادث امنیتی باید اقدام مناسب صورت گیرد.

۲- حادثه امنیتی باید گزارش شود.

۳- حادثه امنیتی گزارش شده مورد بررسی و ارزیابی قرار گرفته و حجم و شدت آن تعیین می شود.

۴- به منظور بررسی امکان وقوع مجدد حوادث امنیتی و پیشگیری از وقوع مجدد حوادث امنیتی، شواهد حاصل از ارزیابی‌های انجام شده و نتایج حاصل از آنها باید جمع آوری گردد. لازم است اطلاعات جمع آوری شده و به منظور پیگیری های آتی به صورت اسناد دارای طبقه بندی، مکتوب و بایگانی گردد. همچنین وقایع امنیتی گزارش شده باید به صورت دوره‌ای کنترل و ممیزی گردد.

۵- در صورت وجود امکان وقوع مجدد حوادث، لازم است راهکارهایی بمنظور پیشگیری از بروز چنین امری ارائه شده و اجرا گردد.

۶- در مرحله پایانی این دستورالعمل نیز در صورت نیاز به تصحیح یا تغییر سرفصل های آموزشی لازم است این کار هر چه سریعتر انجام شود.

۲۶- اطلاعات در دسترس عموم:

هدف از تدوین این دستورالعمل بیان ضرورت حفظ امنیت اطلاعاتی است که لازم است در دسترس عموم قرار گیرد به نحوی که جامعیت آنها تضمین گشته و منجر به لطمه به محرمانگی اطلاعات متعلق به سازمان نشود.

الزامات:

- لازم است اطلاعاتی که انتشار آنها توسط قانون منع نشده است به نحو مقتضی در اختیار متقاضیان قرار داده شود.
- اطلاعاتی که متضمن حق و تکلیف برای کاربران، مشتریان یا ارباب رجوع است باید از طریق انتشار و اعلان عمومی و یا سایر روش های قابل دسترس توسط عموم، به اطلاع ایشان برسد.

- انتشار عمومی اطلاعات فاقد طبقه بندی باید به نحوی باشد که منجر به نقض حریم خصوصی اشخاص، زیان جانی و یا زیان مالی افراد نشود. علاوه بر آن انتشار عمومی اطلاعات نباید موجب نقض قوانین و مقررات جاری کشور شود.
- نهادها یا بخش های دولتی یا عمومی که اطلاعات آنها فاقد طبقه بندی حفاظتی تایید شده از سوی مراجع ذیصلاح دولتی باشد موظفند اطلاعات مربوط به چگونگی تعامل کاربران یا ارباب رجوع را به نحو مناسب و قابل دسترسی برای ایشان منتشر نمایند.
- انتشار عمومی اطلاعات مربوط به اسرار اختصاصی شبکه ها و تسهیلات رایانه ای سازمانی اعم از جزییات فنی سخت افزارها، نرم افزارها، شبکه ها، فرآیندهای داخلی غیرمرتبط با ارائه خدمات فرآیندها و روش های اعطاء و کنترل دسترسی، روش های تهیه نسخه پشتیبان و بازیابی اطلاعات، طرح های BCP[۲۳] و DRP[۲۴]، مدل های آدرس دهی و مسیریابی، روش های تبادل یا رمزنگاری اطلاعات، ظرفیت های پردازش یا انتقال اطلاعات، روش ها و فناوری های تامین امکانات پشتیبانی (الکتریسیته ، تهویه، آتش نشانی و ...) ، استقرار و حفاظت فیزیکی و مانند آن ممنوع است.
- هنگام انتشار اطلاعات عمومی باید ریسک های مرتبط با نقض جامعیت اطلاعات (تحلیل ریسک) ارزیابی شده و تدابیر لازم برای جلوگیری از آن اتخاذ شود.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

[23]- Business Continuty Plan

[24]- Disaster Recovery Plan

۱- در ابتدا کلیه اطلاعاتی که باید در دسترس عموم قرار گیرد (مانند اطلاعاتی که متضمن حق و تکلیف برای مشتریان است) شناسایی شده و لیستی از آنها تهیه می گردد.

۲- در این مرحله الزامات امنیتی و همچنین روش های امن انتشار اطلاعات برای کلیه اطلاعات شناسایی شده در مرحله قبل تدوین می شود.

۳- در صورتی که انتشار اطلاعاتی که در لیست ذکر شده موجب نقض محرمانگی و جامعیت اطلاعات سازمان می شود دستور جلوگیری از انتشار اطلاعات توسط بالاترین مقام سازمان صادر می شود و فرآیند خاتمه می یابد.

۴- در صورت عدم نقض محرمانگی و جامعیت اطلاعات سازمان، مکانیزم های لازم جهت برآورده ساختن الزامات و روش های انتشار تدوین شده تامین می شوند.

۵- در این مرحله مکانیزم ها پیاده سازی و روش های تدوین شده انتشار اطلاعات به اجرا در می آید.

٦- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد اطلاعات انتشار یافته و در دسترس عموم قرار می گیرد. در غیر اینصورت بایستی به مرحله ۵ بازگشت.

۲۷- امحاء رسانه های ذخیره سازی:

هدف از تهیه این دستورالعمل استفاده از مجموعه ای از راهکارها و ابزارهای سخت افزاری و نرم افزاری برای امحاء رسانه های ذخیره سازی خارج از رده یا معیوب در شرایط امن می باشد تا بدین وسیله از هرگونه سوءاستفاده و دسترسی غیرمجاز به اطلاعات دارای طبقه بندی جلوگیری شود.

الزامات:

- کلیه رسانه های ذخیره سازی اطلاعات، قبل از امحاء می بایست بطور دقیق شناسایی شده و سیاههای از کلیه محتویات رسانه ذخیره سازی آماده شده برای امحاء تهیه و نگهداری شود.

– لازم است تخریب یا انهدام رسانه های ذخیره سازی اطلاعات و روش‌های استفاده شده برای پاک‌کردن یا از بین‌بردن رسانه های حاوی اطلاعات دارای طبقه بندی به صورت مدون ثبت گردد.

– در مراکز حساس و حیاتی می‌بایست کمیته تشخیص، تفکیک و امحاء رسانه های ذخیره سازی اطلاعات جهت کنترل و نظارت دقیق بر حسن اجرای انهدام رسانه ها، تشکیل گردد.

– باید رسانه های ذخیره سازی اطلاعات و یا کلیه دارایی های اطلاعاتی که حاوی وسایل ذخیره سازی هستند بررسی شوند تا به این ترتیب اطمینان حاصل شود که تمام داده های دارای طبقه بندی قبل از امحاء به طور ایمن پاکسازی یا با استفاده از اطلاعات بی ارزش بازنویسی[۲۵] شده است، بطوریکه در صورت دستیابی افراد غیرمجاز به قراضه های حاصل از انهدام، افشاء اطلاعات غیرممکن باشد. (به مطالب پیوست رجوع شود.)

– می بایست انهدام رسانه های ذخیره سازی اطلاعات که حاوی اطلاعات دارای طبقه بندی بوده اند، تحت نظارت نهاد ذیربط باشد و این کار باید توسط کارکنان مجاز انجام شود.

– برای تصمیم گیری در مورد امحاء دارایی های اطلاعاتی و شیوه مورد استفاده در زمان از بین بردن رسانه های ذخیره سازی لازم است طبق مصوبه کمیته تشخیص، تفکیک و امحاء رسانه های ذخیره سازی اطلاعات انجام گیرد. در سازمانهای حساس و حیاتی ضرورت دارد با توجه به پیش بینی شرایط اضطرار، موقعیت زمانی، موقعیت‌های مکانی و امکانات موجود روش انهدام مورد پذیرش سازمان توسط نهاد ذیربط تعیین و مصوب گردد.

[25] - Overwrite

– رسانه های ذخیره سازی که در مرحله امحاء هستند و یا در نوبت انهدام قرار دارند ممکن است باعث دسترسی غیرمجاز به اطلاعات دارای طبقه بندی شوند. برای جلوگیری از سوءاستفاده های احتمالی، می‌بایست دارایی های اطلاعاتی مدنظر را در محل هایی که از حفاظت فیزیکی متناسب برخوردار است نگهداری شوند.

– انتخاب و تامین تجهیزات مورد نیاز برای امحاء دارایی های اطلاعاتی باید کنترل شده و با تایید نهاد ذیربط باشد.

فرآیند:

مراحل امحاء و انهدام رسانه های ذخیره سازی اطلاعات به شرح زیر می باشد:

۱- تحویل گیرنده، مالک یا متصدی دارایی اطلاعاتی پس از بررسی‌های لازم مراتب را در مورد عدم نیاز به وجود دارایی اطلاعاتی به نماینده نهاد متصدی امنیت اطلاعات اعلام می کند.

۲- در این مرحله رسانه مورد نظر بطور دقیق شناسایی شده و سیاهه‌ای از کلیه محتویات درون آن تهیه و نگهداری شود.

۳- پس از صدور دستور تشکیل کمیته تشخیص، تفکیک و امحاء رسانه های ذخیره سازی اطلاعات توسط نهاد متصدی امنیت اطلاعات، کمیته مذکور تشکیل شده و به موضوع رسیدگی می کند. اگر در بررسی کمیته فوق انهدام دارایی اطلاعاتی مورد نظر مورد تایید قرار نگیرد دارایی اطلاعاتی به محل بهره برداری خود بازگردانده شده و این فرآیند خاتمه می یابد.

۴- پس از تایید انهدام دارایی اطلاعاتی از سوی کمیته تشخیص، تفکیک و امحاء رسانه های ذخیره سازی اطلاعات، الزامات امنیتی و روش انهدام متناسب با نوع و سطح طبقه بندی حفاظتی دارایی اطلاعاتی توسط کمیته تشخیص تفکیک و امحاء رسانه های ذخیره سازی اطلاعات تدوین می‌شود.

۵- در این مرحله تامین مکانیزم و تجهیزات مورد نیاز از قبیل مکان مناسب، سخت افزارها و نرم افزارهای لازم و همچنین فرم های مربوط صورت می پذیرد.

۶- پس از تامین موارد فوق انهدام رسانه ذخیره سازی مطابق با روش و الزامات تدوین شده انجام می شود.

۷- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۶ بازگشت.

۲۸-امنیت سرویس های شبکه:

هدف از اجرای این دستورالعمل جلوگیری از اختلال در عملکرد سرویس های مجاز شبکه و نصب سرویس‌های غیرضروری به منظور حذف آسیب پذیری های ناشی از آنها و پیشگیری از دسترسی غیرمجاز به سرویس‌های شبکه یا شبکه‌های تحت اختیار یا مالکیت می‌باشد

الزامات:

-ضروری است با تحلیل نیازهای شبکه ارتباطی موجود، سرویس‌ها و پروتکل‌های غیرضروری شبکه شناسایی شده و از نصب آنان جلوگیری به عمل آید.

- لازم است قبل از نصب و پیکربندی سرویس‌ها و پروتکل‌های ضروری، نکات و مسائل امنیتی مربوط به هر سرویس و نحوه بهره‌برداری از آن در قالب مراحل تحلیل ریسک (که در مراکز حساس و حیاتی باید به صورت رسمی اجراء شود) مورد رسیدگی قرار گیرد.

-ضروری است نهاد متصدی امنیت اطلاعات درخصوص ممیزی و نظارت بر سرویس‌های فعال، پروتکل‌های مورد استفاده و پورت‌های باز شبکه، اقدام نماید.

- لازم است در مراکز حساس و حیاتی قبل از بهره برداری از سرویس‌های شبکه از قبیل احراز هویت، تعیین اعتبار، کنترل دسترسی، دسترسی از راه دور، پست الکترونیکی، WEB، DNS، DHCP، LDAP و یا هر نوع خدمات شبکه ای دیگر علاوه بر مجوز صادره توسط مدیر ارشد شبکه تاییدیه نهاد متصدی امنیت اطلاعاتسازمان نیز اخذ شود.

- ضروری است قبل از اجرای هر سرویس، پیکربندی خاص مربوط به آن تعیین و تدوین گردد و پس از اجرا و به صورت دوره‌ای پیکربندی‌های مربوط بازنگری و کنترل شود.

- ضروری است قبل از صدور مجوز استفاده از هر یک از سرویس‌های شبکه، ریسک‌های مرتبط با بهره‌برداری از آن سرویس شناسایی شده و ارزیابی گردند. صدور مجوز فقط پس از اثبات قابل پذیرش بودن ریسک مجاز خواهد بود. در مراکز حساس و حیاتی باید صدور مجوز به صورت کتبی انجام پذیرد.

- می‌بایست حوادث امنیتی در سرویس‌های شبکه در کمترین زمان ممکن تشخیص داده شده و توسط مدیر ارشد شبکه رسیدگی شود و واکنش مناسب در مقابل آنها اعمال شود. لازم است ابزار مناسب اجرای این الزام در اختیار وی قرار داده شود.

- هرگونه نقص یا نقض سیاست‌های امنیتی باید در کمترین زمان ممکن توسط نهاد ذیربط رسیدگی شود تا صدمات ناشی از آن مشخص شده و محدود سازی دامنه آسیب‌پذیری، بازیابی و تعمیرات لازم انجام گیرد. در مراکز حساس و حیاتی و یا شبکه‌های حساس مراکز مهم، مدارک مربوط به هر یک از این موارد باید به طور رسمی ثبت، جمع‌آوری و گزارش شود.

- ضروری است در مراکزی که از سوی سازمان پدافند غیرعامل به عنوان مراکز حساس و حیاتی دسته‌بندی می‌شوند کلیه سرویس‌ها و پروتکل‌های مورد نیاز از لحاظ امنیتی در برابر آسیب‌پذیری‌های احتمالی آزمایش شود و مورد تأیید افراد متخصص قرار گیرد.

- لازم است تنها در صورت شناسایی کامل و پس از اطمینان از داشتن حقوق دسترسی خاص، اجازه استفاده مستقیم از خدمات شبکه ای به کاربر داده شود.

- ضروری است در زمانبندی‌های از پیش تعیین شده سیاست‌های امنیتی سرویس‌های شبکه ارزیابی شده و در مواردی که امنیت شبکه را خدشه‌دار می کند، تجدید نظر شود.

- اطلاعات پیکربندی سرویس های شبکه باید به عنوان اطلاعات محرمانه (و در مراکز حساس و حیاتی و یا مراکز حیاتی سازمان های مهم به عنوان اطلاعات خیلی محرمانه) طبقه بندی شوند. بدیهی است در هیچ حالتی نباید رده طبقه بندی حفاظتی اطلاعات پیکربندی سرویس های شبکه یا تجهیزات ارائه دهنده آنها پایین تر از رده طبقه بندی حفاظتی سرویس یا تجهیزات مربوط باشد.

- ضروری است در مراکز حساس و حیاتی، نهاد متصدی امنیت اطلاعات سخت‌افزارهای مربوط به هر سرویس شبکه را قبل و بعد از نصب در مرکز از نظر شاخص‌های امنیتی آزمایش نمایند و در صورت تأیید این نهاد اجازه استفاده از آن تجهیزات در شبکه صادر گردد.

- در مراکز حیاتی می‌بایست اجازه ورود هیچ دستگاه الکترونیکی همانند کامپیوترهای کیفی یا دستی، تلفن همراه و یاسایر ابزار شخصی قابل اتصال به شبکه (اعم از بی سیم یا کابلی) به کارمندان یا اشخاص متفرقه ای که قبلاً مجوز مربوط را تهیه نکرده اند، داده نشود.

- در مراکز حساس و حیاتی ضروری است خطوط مستقیم مخابراتی(مانند خط تلفن مستقیم، خط ADSL، ارتباط بی‌سیم و مشابه آنها) در اختیار کارکنان قرار داده نشود و تنها کانال‌های ارتباطی تحت کنترل برای این منظور در نظر گرفته شود.

-در سازمان های حیاتی می‌بایست فهرست شماره‌هایی که در طول ماه با آن شماره‌ها تماس گرفته شده است اعم از تماس صوتی یا فاکس و یا مودمی به دقت بررسی شود و برای شماره‌های نامشخص و مشکوک از کاربر توضیح خواسته شود.

- باید برای تمامی تجهیزات مدیریت و کنترل شبکه از رمزهای عبور مستحکم و قوانین دسترسی محدود شده استفاده شود.

-در مراکز حساس و حیاتی و شبکه‌های حساس مراکز مهم ضروری است هر دو نوع IDS/IPS اعم از IDS/IPS مبتنی بر شبکه (NIDS) و IDS/IPS مبتنی بر لایه کاربرد(HIDS) به کار گرفته شود و در زمان‌های از پیش تعیین شده به روز رسانی شوند.

- لازم است از ورود کاربران میهمان (Guest) به سیستم جلوگیری شود و کاربرانی که مجاز به استفاده از سرویس دهنده وب هستند به همان کسانی که لازم است از آن استفاده کنند، محدود گردد.

-می‌بایست به طور منظم و از پیش تعیین شده، وقایع ثبت شده در رابطه با تلاش برای دسترسی‌های غیرمجاز به سرویس های شبکه ای و یا دایرکتوری‌ها و فایل‌های مربوط به آنها بررسی شوند.

-باید طرح‌های احتمالی حمله به شبکه و سرویس های آن بررسی شده و روش دفاعی متناسب با هر طرح حمله آماده و آزمایش گردد.

-لازم است دسترسی راه دور از طریق شناسه Admin یا هر شناسه دیگری که دارای حق دسترسی ممتاز[۲۶] است به ماشین‌ها یا نرم افزارهایی که سرویس‌های اصلی شبکه را ارائه می‌نمایند، مسدود شده باشد.

- می‌بایست کاربران مجاز در شبکه در مورد امنیت سرویس‌های شبکه، دسترسی به فایل‌ها و طرح‌های امنیتی دوره های آموزشی مناسب را گذرانده باشند.

- لازم است با استفاده از بخش‌بندی[۲۷] مناسب شبکه ترتیبی اتخاذ شود تا سرویس‌های ضروری در هر بخش فقط در اختیار افراد مستقر در آن قرار گیرد و سایر افراد به چنین سرویس‌هایی دسترسی نداشته باشند.

- آرایش هندسی شبکه و دیوار آتش باید به گونه‌ای تنظیم شود که دسترسی مستقیم به سرویس‌دهنده پایگاه داده برای افراد خارج از سازمان غیرممکن باشد.

-ضروری است تجهیزات سرویس‌های شبکه در مکان‌هایی استقرار یابند که از دسترسی‌های غیرمجاز فیزیکی محفوظ بمانند.

- ضروری است سرویس‌دهنده DNS به گونه‌ای پیکربندی شود که درخواست‌های ارسالی از محدوده آدرس‌های IP جعلی را رد کند.

-لازم است سرویس دهنده DNS بر روی کامپیوتری به اجرا درآید که فاقد شناسه‌های کاربری باشند.

-باید تخصیص IP به سرویس‌های مختلف شبکه بصورت محرمانه، طراحی و پیاده‌سازی شود.

-می‌بایست هرگونه اتصال غیرامن به سرویس‌های شبکه که می‌تواند موجب اثرات سوء بر عملکرد کلی شبکه باشد، حذف گردد.

---

[26] - Privilege Access

[27] - Segmentation

- باید از عدم وجود کامپایلرها[۲۸]، پوسته‌ها[۲۹]، موتورهای اجرای قطعه برنامه‌ها[۳۰] و سایر برنامه‌های قابل توسعه در یک شاخه متعلق به برنامه‌های CGI اطمینان حاصل شود.

- ضروری است در صورت عدم نیاز به سرویس‌دهنده SNMP در تجهیزات شبکه ای، سرویس مورد نظر غیرفعال گردد. در صورت نیاز به این سرویس لازم است از فهرست دسترسی برای محدود کردن دسترسی به آن استفاده شود.

- ضروری است شبکه‌ها و یا سرویس‌های شبکه‌ای که اتصال به آنها مجاز است، شناسایی شده و بر اساس آن توپولوژی سرویس‌های شبکه طراحی گردد.

- لازم است یک نقشه از وضعیت کاربران برای شرح کامل دسترسی به سرویس‌های شبکه تهیه و دسترسی‌های غیرمجاز شناسایی و حذف گردند.

- سرویس‌های شبکه که لازم است دسترسی‌های آنها از بقیه جدا شوند به سوییچ یا روتر جداگانه وصل شوند.

- ضروری است کلیه پورت‌هایی که برای دسترسی‌های خارجی استفاده می‌شود با محافظت از طریق کلمه عبور کنترل شوند.

- بایستی اطلاعات مخصوص هر سرویس شبکه مانند نام، مکان و کارکرد سرویس شبکه (همانند سرویس FTP و ...) در قسمتی ثبت و نگهداری شود و به صورت دوره‌ای کنترل گردد.

- لازم است تمامی سرویس‌های در حال اجرا بر روی سرورهای اختصاص داده شده به برنامه‌های کاربردی خاص بررسی شوند و از اجرای سرویس‌های غیرمجاز جلوگیری به عمل آید.

---

[28] - Compilers

[29] - shells

[30] - CGI components

-باید از فایل های Startup به صورت زمانبدی شده بازدید صورت گیرد و از عدم وجود نرم‌افزارهای هک در فایل های مذکور اطمینان حاصل شود.

- لازم است ابزارهای توسعه [۳۱] و برنامه‌های کاربردی بر روی سرویس دهنده‌های وب غیرفعال گردد.

-باید سیاست‌های مربوط به حق دسترسی کاربران به سرویس‌های شبکه‌ای که حاوی اطلاعات طبقه‌بندی شده می‌باشند، به صورت منظم مورد بررسی قرار گیرد.

- لازم است پیکربندی سرویس‌دهنده DNS به نحوی صورت گیرد تا از انتقال کامل رکوردها جلوگیری بشود. (بسته شدن پورت TCP-53)

- ضروری است برای جلوگیری از سرقت اطلاعات سرویس دهنده DNS از سرویس دهنده نام دو بخشی (Split DNS) استفاده شود.

فرآیند:

۱- در ابتدا لازم است دسته بندی سازمان از دیدگاه پدافند غیرعامل و همچنین طبقه بندی حفاظتی بخش های مختلف شبکه سازمان مورد بررسی قرار گیرد.

۲- تحلیل نیازهای شبکه بمنظور شناسایی کلیه سرویس‌های مورد نیاز و همچنین غیرضروری در شبکه سازمان در این مرحله انجام می شود.

۳- پس از تحلیل و شناسایی در این مرحله فهرستی از سرویس های مجاز قابل ارائه در شبکه سازمان از قبیل پروتکل های مجاز ارتباطی، خدمات مجاز اشتراک فایل و منابع، سرویس های مجاز تشخیص

1- Development tools.

هویت یا احراز صلاحیت و سرویس های مجاز کنترل دسترسی تهیه می شود. همچنین در کنار فهرست مذکور، لیستی از سرویس ها و پروتکل های غیرضروری شبکه تهیه می شود.

۴- پیش از هر گونه اقدامی، لازم است ریسک نصب و بهره برداری از هر یک از سرویس های شبکه ارزیابی شده و مخاطرات آن برآورد شود.

۵- در صورتی که ریسک ارزیابی شده قابل پذیرش نباشد ادامه این فرآیند متوقف شده و خاتمه می‌یابد.

۶- در صورت قابل پذیرش بودن ریسک ارزیابی شده الزامات امنیتی در خصوص چگونگی نصب و نحوه بهره برداری هر سرویس تدوین می شود. همچنین در این مرحله پیکربندی مناسب هر سرویس متناسب با الزامات امنیتی تدوین می شود.

۷- در این مرحله مکانیزم ها و منابع امن سازی مورد نیاز جهت اجرای الزامات تامین می شود.

۸- پس از تامین موارد فوق، به پیاده سازی مکانیزم ها، اجرای کلیه الزامات و نصب و پیکر بندی سرویس های مورد نیاز شبکه مطابق با پیکربندی تدوین شده اقدام می شود.

۹- در صورتی که پس از بررسی مشخص شود کلیه الزامات امنیت سرویس های شبکه تدوین شده (الزامات بیان شده در این سند و الزامات اختصاصی سازمان) برآورده نشده است جهت برآورده نمودن کلیه الزامات به مرحله ۸ بازگشت.

۱۰-در صورت بر آورده شدن کلیه الزامات مجوز بهره برداری از سرویس توسط (((**نهاد متصدی امنیت اطلاعات**))) صادر شده و سرویس مزبور مورد بهره برداری و استفاده قرار می گیرد.

۲۹- امنیت سیستم های اطلاعاتی کاربردی:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی امن سازی سیستم های اطلاعاتی می باشد.

الزامات

- لازم است سیستم های اطلاعاتی اختصاصی سازمان شامل فایل های داده، بانک های اطلاعاتی، پایگاه های دانش، نرم افزار های کاربردی مدیریت و بهره برداری از بانک های اطلاعاتی و پایگاه های دانش اختصاصی سازمان و فایل پیکربندی شناسایی شده و به عنوان بخش مستقلی از فهرست دارایی های اطلاعاتی فهرست بندی شوند.
- از آنجا که سیستم های اطلاعاتی ساختمان (بخصوص فایل های داده، بانک های اطلاعاتی و پایگاه های دانش) دارای ماهیتی یکتا بوده و در صورت لطمه دیدن، تنش زیادی را متوجه سازمان خواهد نمود، لازم است فرآیندهای انتخاب محیط های مدیریت بانک های اطلاعاتی، تهیه نسخه پشتیبان[۳۲] و احیای سیستم[۳۳] و طرح های تداوم و عملیات[۳۴] با توجه به نیازهای عملیاتی آنها تدوین شود.
- افرادی که با کار با سیستم های اطلاعاتی اختصاصی سازمان (فایل های داده، بانک های اطلاعاتی، پایگاه های دانش، نرم افزارهای کاربردی مدیریت و بهره برداری از آنها و فایل های پیکربندی مربوط) می پردازند باید در دو سطح کار با سیستم اطلاعاتی و حفظ امنیت آن آموزش داده شوند.
- در صورتی که فایل های داده، بانک های اطلاعاتی و پایگاه های دانش اختصاصی سازمان حاوی اطلاعات طبقه بندی شده باشد لازم است به نحو مناسب رمزگذاری شوند، به نحوی که در صورت دستیابی افراد غیرمجاز به آنها دستیابی به محتوای آنها غیرممکن شود.
- کنترل دسترسی به داده ها، بانک های اطلاعاتی، پایگاه دانش، نرم افزارهای کاربردی و نرم افزارهای بنیادی مدیریت اینگونه داده ها باید مطابق با سه سطح کنترل دسترسی عام، کنترل دسترسی خاص و کنترل دسترسی ممتاز (سیاست گذاری کنترل دسترسی) تعریف شود.

---

[32] - Back Up

[33] - Disaster Recovery

[34] - Business Continuity Plan

- حتی الامکان لازم است محل نگهداری داده های سیستم های اطلاعاتی اختصاصی سازمان، جدا از محل نگهداری نرم افزارهای مدیریت و بهره برداری مربوط باشد به نحوی که در صورت فروپاشی نظام کنترل دسترسی یکی از آنها نتوان به دیگری دست یافت. به عنوان مثال لازم است نرم‌افزار AutoCAD جدا از فایل های تولید شده توسط آن نگهداری شود.
- لازم است حتی الامکان (و در مراکز حساس و حیاتی الزاماً) هر سیستم اطلاعاتی روی یک سرویس دهنده جداگانه (با رعایت الزام قبلی) نصب شود. به عنوان مثال اگر در یک سازمان یک بانک اطلاعاتی از اطلاعات شخصی مشتریان و یک بانک از اطلاعات گردش حساب نگهداری می شود باید این اطلاعات روی دو ماشین جداگانه نصب شود تا در صورت فروپاشی نظام کنترل دسترسی یا تخریب یک ماشین امنیت اطلاعات دیگر مورد تهدید واقع نشود.
- نصب نرم افزارهای بنیادی مدیریت داده ها و بانک های اطلاعاتی روی ایستگاه کاربران عادی یا کاربرانی که نیازی به آن ندارند (مانند SQL، Oracle، DB2،...) ممنوع است.
- تمام مراحل کار با فایل های داده، بانک های اطلاعاتی، پایگاه دانش، نرم افزارهای کاربردی، ابزار بنیادی و فایل های پیکربندی مربوط به آنها باید ثبت(Log برداری) شده و به نحو مناسب نگهداری شوند.
- اطلاعات ثبت شده فوق باید در فواصل زمانی مناسب به منظور کشف موارد مشکوک بازبینی شوند.
- در مواقعی که نوع بهره برداری از اطلاعات مستلزم تجمیع آنها و یا بهره برداری از آنها از طریق یک سیستم نرم افزاری جامع (مانند ERP، نرم افزارهای Core Backing، نرم افزارهای نظام جامع اختصاصی مثل بیمه ای، ثبت احوال، قضایی، انتظامی،...)باشد لازم است:
  - الزامات امنیتی مورد نظر سازمان که حداقل باید شامل نظام کنترل دسترسی، رمزنگاری و تبادل کلید، تهیه نسخه پشتیبان، احیای سیستم، طرح تداوم عملیات و آموزش پرسنل باشد، تحت عنوان پیوست امنیتی به صورت جداگانه در قرارداد درج شده و چگونگی پاسخ گویی به آنها معلوم شود.

- هنگام تحویل قرارداد و قبل از عملیاتی سازی آن باید بازبینی کد منبع[۳۵] انجام و از عدم وجود راه‌های نفوذ مخفی[۳۶] در آن اطمینان حاصل شود.
- کنترل دسترسی ممتاز به فایل های پیکربندی سیستم های اطلاعاتی اختصاصی سازمان در مراکز حساس باید از طریق استفاده از نشانه های سخت افزاری[۳۷] و یا علائم بیومتری[۳۸] و در مراکز حیاتی باید از طریق استفاده از تایید مقام بالاتر و یا حضور شخص همراه تقویت شود.
- در صورتی که فایل داده، بانک اطاعاتی یا پایگاه دانش اختصاصی سازمان حاوی اطلاعات کنترل دسترسی به سایر سیستم ها باشد لازم است از نگهداری آنها بر روی ماشین هایی که فاقد استانداردهای لازم برای HSM[۳۹] هستند خودداری شود. این استانداردها به صورت مفصل در FIPS 140-2 و CC[۴۰] تشریح شده اند.

فرآیند

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا کلیه سیستم های اطلاعاتی سازمان از قبیل فایل های داده ، بانک های اطلاعاتی، نرم افزارهای کاربردی شناسایی شده و فهرست آنها تهیه می شود.

۲- در این مرحله الزامات امنیتی و رویه های امن سازی سیستم های اطلاعاتی و بهره برداری از آنها تدوین می شود. در تدوین موارد مزبور توجه به ارزش و طبقه بندی حفاظتی اطلاعات موجود در سیستم اطلاعاتی ضروری می باشد.

---

35 - Source Code Review

36 - Back Door

37 -Hardware Token

38 - Biometrics

39 - Hardware Security Module

40 - Common Criteria

۳- تامین مکانیزم و امکانات مورد نیاز از قبیل سیستم رمزنگاری و تبادل کلید، تجهیزات تهیه نسخه پشتیبان در این مرحله انجام می شود.

۴- پس از تامین مکانیزم و امکانات به پیاده سازی و اجرای الزامات و رویه های امن سازی اقدام می‌شود.

۵- پیش از بهره برداری از سیستم های اطلاعاتی سازمان باید به پرسنلی که با این سیستم ها در ارتباط می باشند در دو سطح کار با سیستم و حفظ امنیت آن آموزش های لازم ارائه شود.

۶- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد بهره برداری و استفاده از سیستم اطلاعاتی انجام شده و کلیه مراحل کار با سیستم های اطلاعاتی ثبت و به نحو مناسبی نگهداری می شود. در غیر اینصورت بایستی به مرحله ۴ بازگشت.

۳۰- امنیت سیستم های الکترونیک دفتری:

هدف از تهیه این دستورالعمل بیان ضرورت حفاظت از داده‌ها و اطلاعاتی است که به هنگام کار با سیستم‌های الکترونیک دفتری مثل سامانه های نشر رومیزی[۴۱]، ابزار تولید محتوا برای اطلاع رسانی اختصاصی یا عمومی در محیط وب و پست الکترونیک در قلمرو پیاده سازی نظام مدیریت امنیت سازمان ، تولید، نگهداری و ارسال می شوند.

الزامات

- لازم است در سازمان های حساس و حیاتی به منظور حفظ محرمانگی داده‌ها و اطلاعات طبقه بندی شده هنگام نگهداری و انتقال، از رمزنگاری متقارن یا نامتقارن بر مبنای اهمیت و طبقه‌بندی داده ها و اطلاعات استفاده شود.

- لازم است نسخه‌های الکترونیکی اطلاعات تولید شده در نرم‌افزارهای نشر رومیزی قبل از توزیع به نسخه‌های غیرقابل تغییر تبدیل شوند.

41 - Desktop Publishing

-لازم است کلیه افرادی که محتوای تولید شده توسط نرم‌افزارهای دفتری (مثل مجموعه Microsoft Office یا سایر نرم‌افزارهای رومیزی تولید محتوا) را در اختیار دارند طبق روش تهیه نسخه پشتیبان از اطلاعات در اختیار خود نسخه پشتیبان تهیه کرده و با توجه به طبقه‌بندی حفاظتی داده‌ها از آنها نگهداری نمایند.

-لازم است در نرم‌افزارهای تولید محتوا چند رسانه‌ای، وب و گرافیکی، فرمت اطلاعات الکترونیکی به نحوی ایجاد شوند تا در صورت لزوم پس از دریافت توسط گیرنده قابل تغییر نباشد.

- در مراکز حساس و حیاتی ضرورت دارد در راستای اصل انکار ناپذیری هنگام تبادل رسمی اطلاعات از سیستم امضاء دیجیتال استفاده شود.

- لازم است سطوح دسترسی افراد به محتوای تولید شده و دارای طبقه‌بندی حفاظتی (طبق دستورالعمل های کنترل دسترسی و سطوح دسترسی عام، خاص و ممتاز) تعیین و کنترل گردد.

-ضرورت دارد نهاد متصدی امنیت اطلاعات نرم‌افزارهای تولید محتوای خریداری شده را قبل از نصب بر روی سیستم‌ها در محیط آزمایش کنترل شده تست کند.

فرآیند

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا به شناسایی سیستم های الکترونیک دفتری مورد نیاز سازمان (مانند مجموعه Microsoft Office) پرداخته شده و فهرستی از آنها تهیه می شود.

۲- پس از تهیه فهرست کلیه الزامات امنیتی که جهت استفاده و بهره برداری امن از هر سیستم باید رعایت شود تدوین می شود.

۳- در این مرحله مکانیزم و امکانات مورد نیاز اعم از تجهیزات سخت افزاری یا نرم افزارهایی که جهت برآورده شدن الزامات مورد نیاز می باشد تامین می شود.

۴- پس از تامین موارد فوق به پیاده سازی مکانیزم ها و اجرای کلیه الزامات اقدام می شود.

۵- در صورتی که کلیه الزامات امنیتی تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد مجوز بهره برداری از سیستم مورد نظر توسط مدیر ارشد شبکه صادر شده و پس از صدور مجوز، بهره برداری از سیستم مورد نظر بوسیله فرد مجاز امکانپذیر می‌باشد. در غیر اینصورت بایستی به مرحله ۴ بازگشت.

۳۱- امنیت مستندات سیستم:

هدف از تهیه این دستورالعمل نگهداری امن اطلاعات و مستندات مربوط به تشریح و چگونگی عملکرد و اجرای فرآیندها و دارایی‌های اطلاعاتی در اعم از مستندات الکترونیکی یا کاغذی به گونه‌ای است که در هنگام نیاز به راحتی در دسترس افراد مجاز قرار گیرد.

الزامات:

- لازم است فهرستی از کلیه مستندات مرتبط با نظام مدیریت امنیت اطلاعات تحت عنوان «فهرست اسناد مرجع» تهیه، نگهداری و به هنگام سازی شود.

- لازم است به ازای کلیه برنامه‌های کاربردی تهیه شده یا خریداری شده در حال کار، شناسنامه‌ای بابت نرم‌افزار تهیه شود که در آن مواردی همچون اطلاعات دسترسی به تأمین کننده یا خدمات پس از فروش، روش تهیه نسخه پشتیبان از نرم افزار و فایل های پیکر بندی و بانکهای اطلاعاتی مربوط به آن، نوع زبان برنامه‌نویسی، و سایر اطلاعات مرتبط با کار با آن تهیه گردد. همچنین در خصوص نرم‌افزارهای عام مانند سیستم عامل‌ها،

ابزارهای سیستم و ابزارهای مهندسی نرم‌افزار به کمک کامپیوتر (CASE[۴۲])، تهیه و نگهداری راهنمای کاربران[۴۳] و مرجع فنی[۴۴] منتشر شده به وسیله تولید کننده الزامی است.

- لازم است جهت کلیه تجهیزات سخت‌افزاری مورد استفاده در ارائه خدمات رایانه‌ای حداقل دو مستند راهنمای کاربری و مرجع فنی تهیه و نگهداری شود.

-لازم است با رعایت طبقه‌بندی حفاظتی سازمان از مستندات سیستم، نسخه پشتیبان (طبق دستورالعمل ۶-۵-۱) تهیه گردد.

- حتی‌الامکان مستندات باید دارای فرمت یکسان و قابل شناسایی باشد.

- لازم است در صورت ارتقا یا تغییر سیستم‌ها، مستندات مربوط به آنها نیز به روز رسانده شود.

- در مراکز حساس و حیاتی، هرگونه جابجایی و حمل و نقل مستندات فرآیندها، نرم‌افزارهای اختصاصی یا سخت‌افزاری به بیرون از سازمان و یا جابجایی در بخش‌های داخلی باید با اجازه رسمی و در صورت طبقه‌بندی حفاظتی با پر کردن فرم مربوطه انجام پذیرد.

- در صورت وجود مسئول مستندات سیستم، این شخص موظف است بلافاصله پس از دریافت تجهیزات یا نرم‌افزارها، شناسنامه و راهنمای استفاده از آن را تهیه و نگهداری نماید.

- لازم است از مستندات سیستم در مقابل دسترسی غیرمجاز محافظت شود.

---

[42] - Computer Aided Software Engineering

[43] - User Manual

[44] - Technical Reference

- لازم است سطوح دسترسی افراد بخش‌های مختلف سازمان به مستندات سیستم دارای طبقه بندی حفاظتی تعیین و مشخص شده باشد.

- لازم است تمامی فعالیت‌های مرتبط با «ارائه خدمات مبتنی بر فناوری اطلاعات»، شناسایی و آنالیز شده و به صورت مکتوب در قالب روش اجرائی، دستورالعمل، فرم‌ها و ... مستند سازی شود.

- لازم است سطح طبقه‌بندی حفاظتی مستندات سیستم، حداقل معادل سطح طبقه‌بندی حفاظتی همان سیستم یا دارائی اطلاعاتی باشد. مستندات مربوط به کنترل دسترسی دارایی اطلاعاتی باید تحت طبقه‌بندی حفاظتی سخت‌گیرانه‌تر قرار داشته باشد.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا فهرستی از کلیه مستندات مرتبط با نظام مدیریت امنیت اطلاعات که باید تدوین شوند تحت عنوان فهرست اسناد مرجع تهیه می شود.

۲- الزامات امنیتی تهیه، تدوین و نگهداری مستنداتی که در فهرست فوق می باشند در این مرحله تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۳- پس از آن مستنداتی که در فهرست اسناد مرجع ذکر شده اند مطابق با الزامات، تهیه و تدوین می‌شوند.

۴- در این مرحله مطابق با دستورالعمل طبقه بندی حفاظتی دارایی های اطلاعاتی سازمان، طبقه بندی مستندات تدوین شده تعیین می گردد.

۵- پیش از نگهداری مستندات و با رعایت طبقه بندی حفاظتی سازمان از مستندات تدوین شده نسخه پشتیبان تهیه می گردد.

۶- در صورتی که کلیه الزامات امنیت مستندات سیستم تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد مستندات سیستم و نسخ پشتیبان تهیه شده مورد محافظت و نگهداری قرار می‌گیرند در غیر اینصورت بایستی مجدداً به مرحله تدوین مستندات بازگشت.

۳۲- پایش کاربرد سیستم ها:

هدف از تهیه این دستورالعمل الزام کلیه آحاد **سازمان** به ایجاد روش های منظم اجرایی پایش[۴۵] و نظارت اثربخش بر استفاده از دارایی های اطلاعاتی (شامل رهگیری فعالیت ها و حرکات مشکوک و پیگیری و برخورد با آسیب های ایجاد شده و یا پیش بینی مکانیزم های بهبود امنیت) می باشد.

الزامات:

- پایش دوره ای سوابق ثبت شده فعالیت های مرتبط با بهره برداری از دارایی های اطلاعاتی اعم از سوابق مکتوب یا سوابق الکترونیکی ضروری است. فاصله بین دو پایش نباید بیش از فاصله بین دو ممیزی برنامه ریزی شده نظام مدیریت امنیت اطلاعات باشد. همچنین لازم است در مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حساس و حیاتی دسته بندی می شوند، فاصله بین دو پایش با نظر کمیته امنیت اطلاعات به نحوی تعیین شود که حداقل دو پایش در فاصله بین دو ممیزی انجام شود. همچنین لازم است در اینگونه مراکز حداقل یک پایش به صورت برنامه ریزی نشده انجام شود.
- لازم است عملکرد و دسترسی به دارایی های اطلاعاتی و فرآیندهای بحرانی به صورت مداوم(On-Line) پایش شده و تحت کنترل قرار داشته باشد.

45 _ Monitoring

- در مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حساس و حیاتی دسته بندی می شوند لازم است کلیه فرآیندها و فعالیت دارایی های اطلاعاتی به صورت مداوم (On-Line) پایش شده و تحت کنترل قرار داشته باشد.
- لازم است به صورت دوره ای دسترسی به دارایی های اطلاعاتی از نقاط غیرمعمول و یا فعالیت های غیرمعمول از طریق پایش Log فایل های ایجاد شده بر روی سیستم‌ها شناسایی شوند.
- ضروری است در شناسایی نقاط آسیب پذیر نرم افزارها از فایل های گزارش دسترسی و عملکرد نرم‌افزار نیز استفاده شود.
- ساعت همه کامپیوترهایی که فایل های گزارش را نگهداری می کنند باید بر اساس (همزمان سازی ساعت‌ها) همزمان باشد. این موضوع نهاد متصدی امنیت اطلاعات را قادر می سازد تا رویدادهای مابین کامپیوترها و سرویس ها را جهت شناسایی تهدیدات با هم مقایسه کند.
- پایش سیستم می بایست به نحوی انجام شود تا منجر به شناسایی هرگونه حملات موفق یا غیرموفق علیه امنیت اطلاعات شود. بررسی رویدادهای ناموفق برای دنبال کردن رد یک حمله و نفوذ اهمیت دارد.
- در مراکز حساس و حیاتی لازم است ثبت رویدادها بر اساس نیازهای ممیزی دسته بندی شود تا در آینده بررسی، پایش و رسیدگی به اطلاعات ثبت شده راحت تر باشد.
- ضروری است برای جلوگیری از عضویت کاربران نامعتبر یا اعطای حقوق دسترسی غیرضروری همه گروه ها پایش شوند.
- هنگام پایش سیستم می بایست حقوق کاربران بررسی شود و امکان انجام فعالیت های غیرمنطقی از آنها گرفته شود.
- لازم است از عدم اجرای برنامه های غیرمجاز اطمینان حاصل شود. یک نفوذگر می تواند با استفاده از روش های متنوعی از یک برنامه درپشتی را اجرا کند.

- سیستم باید برای شناسایی سرویس های نامعتبر مورد بازرسی قرار گیرد. برخی از برنامه های درپشتی خود را به عنوان سرویس بر روی دستگاه نصب کرده و در زمان روشن شدن دستگاه فعال می شوند.
- باید پورت های باز روی سرور بصورت مداوم کنترل و پایش شود که این امر در شناسایی تهدیدات و حملات علیه سیستم موثر است. این حملات اغلب از طریق پورت های باز روی آن که نشان دهنده سرویس فعال روی آن سیستم است، صورت می گیرد.

فرآیند:

مراحل اجرای این دستورالعمل به شرح زیر می باشد:

۱- در مرحله اول این فرآیند لازم است کلیه دارایی های اطلاعاتی و فرآیندهای بحرانی شناسایی و تعیین شوند تا به صورت مداوم(On-Line) پایش شده و تحت کنترل قرار داشته باشند.

۲- الزامات امنیتی، روش ها و طول دوره پایش و نیز فرم های لازم در این مرحله تدوین می‌گردند. همچنین نهاد متصدی امنیت اطلاعات باید نحوه گزارش دهی پایش توسط کاربران را نیز تدوین کرده و در اختیار آنها قرار دهد. در صورتی که سازمان دارای الزامات اختصاصی خود باشد الزامات مورد نظر نیز به موارد بیان شده در این سند افزوده خواهند شد.

۳- در این مرحله بر اساس روش های تدوین شده و در راستای برآورده نمودن الزامات تدوین شده به انجام پایش و کنترل اقدام می شود.

۴- پس از اتمام پایش، فردی که اقدام به انجام پایش نموده (متصدی، تحویل گیرنده و یا مالک همان دارایی اطلاعاتی) مطابق با نحوه گزارشدهی که توسط نهاد ذیربط تدوین شده است گزارش پایش را تهیه و به مراجع ذیصلاح ارسال می نماید.

۵- در صورتی که پس از بررسی مشخص شود کلیه الزامات پایش کاربرد سیستم ها تدوین شده (الزامات بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده است فرآیند خاتمه می یابد در غیر اینصورت نیاز است جهت برآورده نمودن کلیه الزامات به مرحله ۳ بازگشت.

۳۳- پایش و بازنگری خدمات شخص ثالث:

هدف از تدوین این دستور العمل بیان ضرورت چگونگی پایش و بازنگری خدمات خریداری شده از اشخاص ثالث جهت ارائه یا پشتیبانی خدمات حوزه فناوری اطلاعات و ارتباطات به نحوی که از کیفیت و کمیت خدمات ارائه شده اطمینان حاصل شود.

الزامات:

- لازم است خدمات ارائه شده توسط اشخاص ثالث در جهت ارائه یا پشتیبانی خدمات حوزه فناوری اطلاعات و ارتباطات از طریق اندازه گیری منظم معیارهای ارزیابی کمی و کیفی (براساس دستورالعمل ۶-۲-۱: تحویل خدمت) تحت نظارت قرارداشته و کلیه رفتارهای طرف های قرارداد آشکارسازی و پایش شوند.
- خدمات ارائه شده توسط اشخاص ثالث باید مانند خدمات سازمانی به صورت دوره ای از لحاظ کارآیی و اثر بخشی بررسی شده و در صورت نیاز نسبت به تغییر فرآیند یا روش اجرای آنها اقدام لازم به عمل آید.
- لازم است در مرحله عقد قرارداد به ضرورت بازنگری توجه شده و با لحاظ کردن عامل بازرسی در متن قرارداد التزام طرف قرارداد (پیمانکار) به رعایت تصمیمات سازمان برای افزایش بهره وری یا اثربخشی کسب شود.
- اگر خدماتی که برون سپاری یا از اشخاص ثالث خریداری شده جزء خدمات اصلی سازمان باشد، لازم است کلیه مراحل جمع آوری داده و پردازش اطلاعات مربوط به پایش خدمات به صورت مستند (کتبی یا الکترونیکی)، استنادپذیر و غیرقابل انکار باشد.

- تغییر در کیفیت مقدار و روش ارائه خدماتی که بر اساس بازنگری ضروری تشخیص داده می شود باید به صورت مکتوب مستند شده و به امضای نمایندگان قانونی طرفین (که در قرارداد به آنها اشاره می شود) برسد و به صورت رسمی به طرف های ذیربط ابلاغ شود.
- هرگونه تغییر در کیفیت مقدار و روش ارائه خدمات باید قبل از اجرایی شدن مورد ارزیابی قرار گرفته و اثرات احتمالی آن مطالعه شود.
- لازم است فرم های پایش و بازنگری خدمات شخص ثالث به تفکیک خدمات و با استعلام نظر واحدهای بهره بردار طراحی و تدوین شود.
- استفاده از روش های آماری مدیریت کیفیت برای پایش فعالیت های برون سپاری شده سازمان های حیاتی و حساس و فعالیت های حیاتی مراکز مهم (براساس دسته بندی سازمان پدافند غیرعامل) الزامی است.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا کلیه الزامات امنیتی و معیارهای کنترل کیفی و کمی خدماتی که از اشخاص ثالث خریداری می شود تدوین می گردد. معمولاً این الزامات و معیارها در هنگام عقد قرارداد ذکر شده و شخص ثالث ملزم به پذیرش و رعایت آنها می باشد. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- در حین قرارداد ارائه خدمات و همچنین پس از پایان آن کلیه الزامات و معیارهای تدوین شده که شخص ثالث ملزم به پذیرش و برآورده ساختن آنها شده است مورد بررسی و کنترل قرار می‌گیرد.

۳- در صورتی که کلیه الزامات و معیارهای پایش و بازنگری خدمات شخص ثالث تدوین شده (در این سند و الزامات و معیارهای اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد در غیر

اینصورت بایستی اقدامات اصلاحی مورد نیاز انجام شده و یا در نحوه ارائه خدمت بـازنگری شـود و مجدداً مرحله ۲ فرآیند به اجرا در آید.

۳۴- پذیرش سیستم:

هدف از تدوین این دستورالعمل بیان ضرورت آزمایش و بررسی دارایی‌های اطلاعاتی بر اساس معیارهای از پیش تعیین شده قبل از شروع بهره‌برداری از آنها و معرفی روشی برای انجام آزمایش‌های پذیرش سیستم[۴۶] می‌باشد.

الزامات:

- لازم است تمامی تجهیزات پردازشی، نرم‌افزارها، سخت‌افزارها و سایر دارایی‌های اطلاعاتی یا تجهیزات پشتیبانی قبل از ورود به مرحله بهره‌برداری مورد آزمایش و بررسی قرار گیرند. بایستی انتقال به محیط عملیاتی تنها پس از صدور مجوز بهره‌برداری صورت پذیرد. در مراکزی که از دیدگاه سازمان پدافند غیرعامل به عنوان مراکز حساس و حیاتی دسته بندی می شوند لازم است مراحل صدور مجوز به شکل مستند و از طرف نهاد ذیربط انجام شود. در سایر مراکز لازم است مراحل صدور مجوز بهره برداری از دارایی های اطلاعاتی بحرانی (که توسط کمیته امنیت اطلاعات مشخص می شوند) به شکل مستند انجام شود.

- لازم است فرم های پذیرش سیستم به تفکیک نوع دارایی اطلاعاتی (سخت‌افزار یا نرم‌افزار) تهیه شده و نظر واحدهای بهره‌بردار در مرحله طراحی فرم استعلام شود.

- لازم است پیش از تهیه سیستم معیارهای لازم جهت پذیرش آن توسط واحد تحقیق، توسعه و آزمایش و با استفاده از نظر متقاضی یا واحد بهره بردار سیستم تدوین شود.

[46]- System Acceptance

- بایستی با توجه به دسته‌بندی مراکز از دیدگاه سازمان پدافند غیرعامل و همچنین طبقه‌بندی حفاظتی سازمان روشها و سیاست‌های مختلفی را برای آزمایش دارایی‌های اطلاعاتی در نظر گرفته و اجراء شود.

- پس از تأیید و پذیرش سیستم بایستی اطلاعات و آموزش‌های لازم در خصوص بهره‌برداری صحیح از دارایی‌های اطلاعاتی به تحویل گیرنده، متصدی یا مالک آن ارائه شود.

- لازم است از کاربران و بهره‌برداران تعهد لازم برای استفاده صحیح از دارایی‌های اطلاعاتی اعم از سخت‌افزار یا نرم‌افزار گرفته شود.

- لازم است آزمایشهای عمومی برای کلیه سیستم ها (سخت‌افزار یا نرم‌افزار) مطابق آزمایشهای پیوست یک انجام شود.

- لازم است تجهیزات، نرم‌افزارها و سخت‌افزارهای به روز شده پیش از ورود به محیط عملیاتی آزمایش شده و بررسی شود که چه اندازه با تجهیزات و نرم‌افزارهای محیط عملیاتی سازگاری دارد.

- امنیت اطلاعاتی که طی فرآیند آزمایش مورد استفاده قرار می‌گیرد یا تولید می شود باید حفظ شود. انهدام اطلاعات خروجی از عملیات آزمایشی باید طبق دستورالعمل های مربوط انجام شود.

- بایستی حافظه ماندگار در سخت‌افزار پس از فرآیند آزمایش به صورت کامل خالی از اطلاعات شود.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا با توجه به دسته بندی سازمان از دیدگاه پدافند غیرعامل و همچنین طبقه بندی حفاظتی سازمان، سطح دارایی اطلاعاتی مطابق با جدول یک- تعیین سطح دارایی اطلاعاتی (ارائه شده در بخش توضیحات) تعیین می شود.

۲- در این مرحله الزامات امنیتی متناسب با سطح دارایی اطلاعاتی تدوین شده و آزمایش های لازم متناسب با سطح و نوع دارایی اطلاعاتی برنامه ریزی می شود.

۳- در این مرحله به تامین مکانیزم ها و امکانات مورد نیاز اعم از تجهیزات سخت افزاری و نرم افزار ها جهت برآورده ساختن الزامات و اجرای آزمایش های برنامه ریزی شده اقدام می شود.

۴- پس از تامین مکانیزم ها و ابزار، پیاده سازی مکانیزم صورت گرفته و آزمایش های برنامه ریزی شده انجام می شود.

۵- در صورتی که نتیجه آزمایش ها مورد قبول نباشد اصلاحات لازم بر روی سیستم مورد نظر صورت گرفته و مجدداً تست انجام می شود.

۶- در صورت مقبول بودن نتیجه آزمایش ها مطابق با دستورالعمل خارج از رده سازی و استفاده مجدد باید داده ها و اطلاعات مورد استفاده در آزمایش از بین برده و امحا گردند.

۷- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) بر آورده نشده باشد بایستی به مرحله ۴ بازگشت.

۸- در صورت برآورده شدن کلیه الزامات تدوین شده، مطابق با دستورالعمل سیاست گذاری کنترل دسترسی یک سیستم کنترل دسترسی مناسب برای دارایی اطلاعاتی به اجرا گذاشته می شود.

۹- پس از تعریف مکانیزم کنترل دسترسی متناسب با سطح و نوع دارایی اطلاعاتی مجوز بهره برداری از سوی نهاد ذیربط صادر می شود.

۱۰-پیش از بهره برداری و استفاده از دارایی اطلاعاتی آموزش های لازم برای کاربرانی که با دارایی اطلاعاتی مورد نظر در ارتباط می باشند ارائه خواهد شد.

۳۵- تجارت الکترونیک:

هدف از تدوین این دستورالعمل بیان الزامات قانونی فعالیت های مبتنی بر تجارت الکترونیک و حصول اطمینان از امنیت خدمات تجارت الکترونیک و محافظت از آن در برابر فعالیت های کلاهبرداری، مناقشات در قرارداد، افشاء و دستکاری غیرمجاز می باشد.

الزامات:

- کلیه تراکنش های منجر به تجارت الکترونیک باید در قالب داده پیام انجام شود.
- داده های ارسالی باید دارای منشاء مشخص باشد به نحوی که بتوان با استفاده از آن ها به هویت اصل‌ساز پی برد.
- کلیه تراکنش های منجر به تجارت الکترونیک باید منضم به امضای الکترونیک قابل پذیرش در مراجع قضایی باشد.
- لازم است تدابیر امنیت شبکه بر اساس (کنترل های شبکه) و (امنیت سرویس های شبکه) برای حفاظت از اموال، اطلاعات شخصی و امضای الکترونیکی مطمئن اتخاذ شود.
- لازم است روش های ارسال، ذخیره سازی یا نمایش اطلاعات به نحوی باشد که منجر به خدشه به تمامیت پیام نشود.
- کلیه فرآیندهایی که منجر به تجارت الکترونیک می شود باید طبق رویه امن انجام گردد.
- اصل سازان، مخاطبین، بایگانان، مصرف کنندگان و کلیه کسانی که داده پیام را در اختیار دارند موظفند داده پیام هایی را که تحت مسئولیت خود دارند به طریقی نگهداری نموده و نسخه پشتیبان تهیه نمایند تا در صورت بروز هرگونه خطری برای یک نسخه، نسخه دیگر مصون بماند.

- سیستم های تولید (اصل سازی)، ارسال، دریافت، ذخیره یا پردازش باید از سیستم های اطلاعاتی مطمئن باشند.
- تامین کنندگان در تبلیغ کالا و خدمات خود، ملزم به رعایت مقررات و قواعد تبلیغ فضای واقعی می‌باشند.
- هرگونه تغییر در تولید، ارسال، دریافت، ذخیره یا پردازش داده پیام باید با توافق و قرارداد خاص طرفین صورت گیرد.
- انجام تبادل های زیر از طریق تجارت الکترونیک ممنوع است:

الف- انتقال اسناد مالکیت اموال غیرمنقول

ب- فروش مواد دارویی به مصرف کنندگان نهایی

ج- اعلام، اخطار ، هشدار و یا عبارات مشابهی که دستور خاصی برای استفاده کالا صادر می کند و یا از بکارگیری روش های خاصی به صورت فعل یا ترک فعل منع می کند.

- نگهداری و ارائه داده پیام باید به صورت زیرانجام شود تا بتوان از آن به عنوان سند قابل استناد در مراجع قانونی بهره برد:

الف: اطلاعات مورد نظر قابل دسترسی بوده و امکان استفاده در صورت رجوع بعدی فراهم باشد.

ب: داده پیام به همان قالبی (فرمتی) که تولید شده، ارسال و یا دریافت شود و یا به قالبی که دقیقاً نمایشگر اطلاعاتی می باشد که تولید، ارسال و یا دریافت شده، نگهداری شود.

ج: اطلاعاتی که مشخص کننده مبدأ، مقصد، زمان ارسال و زمان دریافت داده پیام می باشند نیز باید نگهداری شوند.

د: شرایط دیگری که هر نهاد، سازمان، دستگاه دولتی و یا وزارتخانه در خصوص نگهداری داده پیام مرتبط با حوزه مسئولیت خود مقرر نموده، فراهم باشد.

- در صورت ایجاد شرایطی که از مقطعی معین ارسال داده پیام خاتمه یافته و استفاده از اسناد کاغذی جایگزین آن شود، سند کاغذی که تحت این شرایط صادر می شود باید به طور صریح ختم تبادل داده پیام را اعلام کند. جایگزینی اسناد کاغذی به جای داده پیام اثری بر حقوق و تعهدات قبلی طرفین نخواهد داشت.

- فروشندگان کالا و ارائه دهندگان خدمات بایستی اطلاعات لازم جهت خرید مواد یا خدمات موضوع قرارداد را قبل از عقد و به روش مناسب در اختیار مصرف کننده قرار دهند.

- خریداران و فروشندگان کالا و خدمات ملزم به آگاهی و رعایت مقررات انصراف(حق انصراف) درفعالیت های منجر به تجارت الکترونیک می باشند.

- تحصیل غیرقانونی اسرار تجاری و دارایی های الکترونیکی که به طور مستقل دارای ارزش اقتصادی می باشد در بستر مبادلات الکترونیکی ممنوع است.

- استفاده از علائم تجاری به صورت نام دامنه (Domain Name) و یا نمایش بر خط (Online) که موجب ایجاد شک در اصالت کالا می شود ممنوع است.

فرآیند:

۱- در ابتدا بایستی تجارت الکترونیک مورد ارزیابی قرار گرفته و ریسک انجام آن و مخاطرات پیش رو برآورد شود.

۲- پس از تحلیل ریسک، الزامات امنیتی و رویه های امن تجارت الکترونیک در جهت حذف، کاهش و یا مدیریت ریسک ها و مخاطرات بدست آمده تدوین می شودند. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۳- در این مرحله مکانیزم ها و امکانات مورد نیاز جهت برآورده ساختن الزامات و دستیابی به رویه های امن تدوین شده تامین می شوند.

۴- پس از تامین موارد فوق مکانیزم ها پیاده سازی شده و کلیه الزامات و رویه های تدوین شده اجرا می شوند.

۵- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۴ بازگشت.

۳۶- تحویل خدمت:

هدف از تدوین این دستورالعمل حصول اطمینان از رعایت مکانیزم های کنترلی امنیت اطلاعات در خرید خدمت اشخاص ثالث، تبیین نوع و سطح کیفیت خدمات ارائه شده توسط ایشان (در قلمرو پیاده سازی نظام مدیریت امنیت اطلاعات) و نظارت بر چگونگی اجرای قرارداد توسط طرف های قرارداد می باشد.

الزامات :

- عقد قرارداد با اشخاص ثالث باید بارعایت معیارهای امنیتی در قراردادهای اشخاص ثالث انجام شود.
- کلیه قراردادهای برون سپاری یا خرید خدمات مرتبط با فناوری اطلاعات و ارتباطات باید منضم به پیوست فنی و یا توافقنامه سطح خدمات باشند که در آنها به صورت روشن، واضح و قابل اندازه گیری به روش، مقدار و کیفیت انجام کار موضوع قرارداد اشاره شده باشد.
- در متن کلیه قراردادها بایستی بندی گنجانده شود که در آن پیمانکار ملزم به رعایت الزامات امنیتی کارفرما شده باشد.
- در مراکز حساس و حیاتی از دیدگاه سازمان پدافند غیرعامل و یا در مواردی که انجام قرارداد مستلزم دسترسی طرف قرارداد به داده ها، شبکه یا تجهیزات در حال کار متصل به آن باشد لازم است علاوه بر رعایت

الزام فوق یک پیوست امنیتی به قرارداد ضمیمه شده باشد که در آن به طور کامل کلیه معیارهای امنیتی قابل رعایت توسط پیمانکار و کارفرما قید شده و الزام طرفین در خصوص رعایت آنها به روشنی اخذ شده باشد.

- افراد وابسته به اشخاص ثالث که به دلیل ماهیت خود ممکن است به دارایی های اطلاعاتی طبقه بندی شده دسترسی داشته باشند ملزم به امضای توافقنامه عدم افشاء می باشند.

- لازم است در برنامه های اطلاع رسانی و آگاهی بخشی به آموزش افراد وابسته به اشخاص ثالث نیز توجه شود.

- در صورتی که قرارداد اشخاص ثالث مستلزم کار افراد وابسته به ایشان در مناطق امن (موضوع دستورالعمل ۵-۱-۵: کار در نواحی امن) باشد، لازم است آموزش چگونگی کار در این نواحی و رعایت الزامات آن توسط کارفرما در اختیار این افراد قرار گیرد.

- تجهیزات مستقر در خارج از سایت که در معرض کار افراد وابسته به اشخاص ثالث قراردارند (مثل تجهیزات ارتباطی مستقر در سایت های مخابرات) باید در مقابل نفوذ یا سوءاستفاده محافظت شوند. به علاوه لازم است حتی الامکان از پیمانکار یا مالک محل استقرار تعهد لازم در خصوص جلوگیری از دسترسی افراد غیرمرتبط به این تجهیزات کسب شود.

- در صورتیکه خرید خدمات مستلزم استفاده از نرم افزارهای اختصاصی یا فایل های داده ای باشد که کد منبع (Code Source) آنها در اختیار کارفرما قرار داده نمی شود، باید در متن قرارداد ترتیباتی اتخاذ شود که در صورت استنکاف عمدی یا غیرعمدی پیمانکار از ارائه خدمات، امکان دسترسی کارفرما به این گونه اطلاعات وجود داشته باشد (به عنوان مثال با استفاده از خدمات امانت گذاری[۴۷] که توسط برخی بنگاه های خوشنام یا مراکز دولتی مورد اعتماد طرفین ارائه می شود)

[47] - Escrow Service

- برون سپاری فعالیت ها یا خرید خدمات فقط وقتی مجاز است که اولاً ریسک حاصل از آن کار ارزیابی شده باشد و ثانیاً امکان مدیریت ریسک حاصل از برون سپاری یا خرید خدمات وجود داشته باشد.

فرآیند:

مراحل اجرای فرآیند تحویل خدمت به شرح زیر می باشد:

۱- در صورت نیاز به عقد قرارداد با شخص ثالث بایستی ریسک برون سپاری و قرارداد با شخص ثالث مورد ارزیابی و تحلیل قرار گیرد.

۲- در صورتی که ریسک ارزیابی شده قابل مدیریت و پذیرش نباشد ادامه این فرآیند لغو شده و فرآیند خاتمه می یابد.

۳- در صورت قابلیت مدیریت و پذیرش ریسک، الزامات امنیتی و معیارهای کمی و کیفی تدوین می‌شود. در صورتی که سازمان دارای الزامات و معیارهای اختصاصی باشد به الزامات بیان شده در این سند افزوده خواهد شد.

۴- پس از تدوین الزامات و معیارها، مکانیزم ها و ابزار مناسب برای اندازه گیری و ارزیابی الزامات و معیارهای تدوین شده تامین خواهد شد.

۵- در این مرحله بایستی شخص ثالث ملزم به پذیرش الزامات و ابزارها و رعایت آنها گردد.

۶- در صورت عدم پذیرش الزامات ابزارهای اندازه گیری تدوین شده از سوی شخص ثالث بایستی از ادامه همکاری با وی صرفنظر نموده و شخص ثالث دیگری جهت عقد قرارداد جایگزین وی شود و مجدداً مرحله ۵ به منظور الزام شخص ثالث جدید به پذیرش الزامات و ابزار اجرا شود.

۷- در صورت پذیرش الزامات و معیارها از سوی شخص ثالث، ارائه خدمات به وی واگذار شده و عقد قرارداد صورت می گیرد.

۳۷ – تفکیک وظایف:

هدف از تدوین این دستورالعمل بیان ضرورت تفکیک وظایف و تعریف حوزه اختیارات هر یک از افراد یا بخش‌های سازمان در حفظ امنیت دارایی‌های اطلاعاتی می‌باشد تا هر کس به طور شفاف وظایف مشخصی داشته باشد و میزان مسئولیت هر پست نسبت به حفظ امنیت دارایی های اطلاعاتی مورد استفاده در فرآیندهای ارائه خدمات همان پست مشخص گردد.

الزامات:

- لازم است فهرست موجودی دارایی‌های اطلاعاتی به عنوان مرجع شناسایی دارایی‌های اطلاعاتی سازمان مبنای تعیین مسئولیت قرار گیرد.

- ضروری است مسئولیت حفاظت هر یک از دارایی‌های اطلاعاتی ثبت شده در فهرست دارایی‌های اطلاعاتی مشخص شود، بطوریکه هر فرد بطور مشخص بداند مسئولیت حفاظت از کدام دارایی اطلاعاتی را به عهده دارد.

- از تحویل یک دارایی به بیش از یک نفر خودداری شود اما تحویل چند دارایی اطلاعاتی به یک نفر بلامانع است.

- می‌بایست مسئولیت حفاظت از هر دارایی اطلاعاتی به بهره‌بردار اصلی سازمانی همان دارایی اطلاعاتی سپرده شود.

- ضروری است شرح وظایف افراد و شرایط احراز شغل مورد بازبینی قرار گیرد و مسئولیت هر فرد بر اساس مهارت‌ها و تجارب وی در خصوص دارایی‌های اطلاعاتی مشخص شود.

- لازم است هر فرد بنا به مسئولیت و شغل سازمانی خود فقط به اطلاعات و منابعی دسترسی داشته باشد که برای انجام وظایف خود به آنها نیاز دارد.

- در صورت لزوم بایستی شرح وظایف افراد و شرایط احراز شغل بصورت دوره‌ای مورد بازبینی قرار گیرد و مسئولیت هر فرد بر اساس مهارت‌ها و تجارب وی در خصوص دارایی‌های اطلاعاتی مشخص شود.

- از آنجایی که حضور کارکنان معمولاً همراه با اشتباهات اجتناب ناپذیر انسانی است، می‌بایست تفکیک وظایف مربوط به هر مسئولیت به نحوی صورت گیرد که حتی الامکان از تداخل محل استقرار یا تردد کارکنانی که دارای تفاوت فاحش در سطوح دسترسی به اطلاعات یا تجهیزات هستند جلوگیری شود.

- ضروری است کنترل و تأییدهای حفاظتی لازم قبل از واگذاری مسئولیت به کارکنان انجام شود و مسئولیت‌های ناشی از تحویل گرفتن دارایی‌های اطلاعاتی و مهارت‌های لازم جهت اجرای وظایف ناشی از آن لحاظ گردد.

- هنگامیکه ارائه یک سرویس به وسیله در اختیار گرفتن مجموعه‌ای از دارایی‌های اطلاعاتی صورت می‌گیرد لازم است فردی به عنوان متصدی سرویس انتخاب شده و مسئولیت حفاظت از امنیت آن سرویس به وی سپرده شود.

- ضروری است وظایف مختلف از یکدیگر تفکیک شده و قبل از واگذاری مسئولیت به هر یک از کارکنان سازمان در هر زمینه‌ای، اختیارات لازم برای اجرای آن وظایف به مسئول مربوطه به نحوی واگذار شود که از دخالت بی‌مورد کارکنان در کار یکدیگر به بهانه انجام مسئولیت جلوگیری شود.

- در صورت جابجایی فرد در سازمان باید حقوق دسترسی وی به اطلاعات یا تجهیزات مورد بازنگری کامل قرار گیرد و اطمینان حاصل شود آن فرد قادر نخواهد بود از حقوق دسترسی مربوط به مسئولیت قبلی خویش استفاده نماید.

- لازم است تعداد افرادی که در سازمان نقش‌های کلیدی بر عهده دارند، محدود شوند و از افراد معتمد و احراز صلاحیت شده استفاده شود.

- می‌بایست آموزش‌های لازم در خصوص شیوه استفاده صحیح و حفاظت از دارایی‌های اطلاعاتی در اختیار فرد تحویل گیرنده، متصدی یا مالک و سایر افراد دخیل در کار با دارایی‌های اطلاعاتی گذاشته شود.

- لازم است حفاظت از دارایی های اطلاعاتی سازمان به کلیه افراد و کارکنان گوشزد شده و کلیه افراد، خود را در حفظ و صیانت از کلیه دارایی‌های اطلاعاتی مسئول بدانند.

- در مراکز مهم، حساس و حیاتی (از دیدگاه سازمان پدافند غیرعامل) باید حوزه های زیر برای تامین امنیت در حوزه مدیریت ارتباطات و عملیات مورد توجه قرار گرفته و در خصوص تفکیک وظایف و تدوین شرح وظایف آنها تعیین تکلیف شده، کلیه موارد مستند شده و به مورد اجرا گذاشته شود:

- پایش و بازنگری تغییرات خدمات شخص ثالث[۴۸]
- مدیریت ظرفیت و پذیرش سیستم
- حفاظت در مقابل کدهای مخرب یا سیار[۴۹]
- تهیه نسخه پشتیبان[۵۰]
- امن سازی شبکه و سرویس های آن (دستورالعمل های ۶-۶-۱ و ۶-۶-۲)
- کنترل و مدیریت رسانه های[۵۱] ذخیره اطلاعات
- تبادل اطلاعات

[48] - Third party services

[49] - Malicious and mobile codes

[50] - Back-up

[51] - Media

- تجارت الکترونیکی
- ثبت وقایع و همزمان سازی[۵۲]

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا باید به شناسایی کلیه دارایی های اطلاعاتی، سرویس و فرآیندهای موجود در سازمان و همچنین الزامات بهره برداری و اجرای آنها پرداخت.

۲- در این مرحله به تهیه و تدوین فهرست کلیه پست ها و جایگاه های شغلی که باید در سازمان وجود داشته باشند اقدام می شود.

۳- پس از تهیه فهرست فوق لازم است الزامات و شرایط احراز پست ها و جایگاه های مختلف تدوین شده و شرح اختیارات، وظایف و مسئولیت های هر کدام تعریف شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۴- در این مرحله مکانیزم ها، امکانات و ابزار مورد نیاز برای بهره برداری امن از منابع و سرویس های سازمان و اجرای امن فرآیندها تامین می شود.

۵- پس از تامین موارد فوق در این مرحله به پیاده سازی مکانیزم ها اقدام می شود.

۶- پس از انتخاب فرد جهت تصدی پست مورد نظر لازم است آموزش های مورد نیاز برای او ارائه گردد.

۷- در صورتی که کلیه الزامات تفکیک وظایف تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد پس از آموزش و اطمینان از صلاحیت فرد تفویض اختیار به وی صورت می گیرد. در غیر اینصورت بایستی به مرحله ۵ بازگشت.

---

[52] - Synchronization

توافق نامه های تبادل:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی ایجاد زمانتوافقنامه برای تبادل اطلاعات و نرم افزار میان سازمان و سایر سازمان ها می باشد.

الزامات:

- لازم است در خصوص تبادل با سایر نهادها و سازمان ها، توافقنامه ای که مورد تایید سازمان و طرف مقابل می باشد تدوین و به امضای طرفین برسد.
- لازم است عملیات تبادل اطلاعات و نرم افزارها در کلیه سازمان ها و بخصوص سازمان های حساس و حیاتی تحت کنترل و حفاظت قرارداشته باشد.
- در توافقنامه های تبادل حداقل شروط زیر بایستی قید شوند:
  - مسئولیت مدیریت در خصوص کنترل و آگاه سازی تبادل (اعم از مخابره، ارسال و دریافت)
  - حداقل استانداردهای فنی برای بسته بندی و ارسال اطلاعات و نرم افزارها
  - رویه های اطمینان از قابلیت پیگیری و عدم انکار
  - روش های اطمینان از صلاحیت و هویت پیک (به عنوان مثال نامه رسان)
  - لزوم پاسخگویی و تعیین مسئولیت ها در هنگام رخداد حوادث امنیت اطلاعات از قبیل گم شدن اطلاعات
  - رعایت حق مالکیت و لزوم مسئولیت پذیری در خصوص حفاظت از اطلاعات، قانون کپی رایت، انطباق گواهینامه نرم افزار و ملاحظات مشابه
  - استانداردهای فنی برای ثبت، بایگانی و بازخوانی اطلاعات و نرم افزارها

- لازم است در موارد خاص (مانند پرداخت های الکترونیکی از طریق اینترنت) از توافقنامه های Escrow[53] استفاده شود.
- در صورت استفاده از مکانیزم های اختصاصی در تبادل اطلاعات و نرم افزارها، لازم است مکانیزم‌های مورد استفاده با مکانیزم های دیگر سازمان ها سازگار باشد.
- لازم است پیش از تدوین توافقنامه، خط مشی ها و روش های اجرایی تبادل اطلاعات مورد بررسی قرار گرفته و توافقنامه همسو با الزامات دستورالعمل مزبور تدوین گردد.
- در تدوین توافقنامه تبادل لازم است (توافقنامه حفظ محرمانگی) و(رسانه های ذخیره سازی فیزیکی حین حمل و نقل) و الزامات بیان شده در خصوص آنها مورد توجه قرار گیرد.

فرآیند:

مراحل اجرای این دستورالعمل به شرح زیر می باشد:

۱- در این مرحله و با توجه به دستورالعمل های مطالعه شده و الزامات بیان شده در آنها، الزامات امنیتی تدوین توافقنامه تبادل تدوین می شود.در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- پس از آن و مطابق با الزامات امنیتی تدوین شده در مرحله قبل، توافقنامه تبادل با سازمان مورد نظر تدوین می شود.

۳- در صورتی که کلیه الزامات و معیارهای تدوین شده (در این سند و الزامات و معیارهای اختصاصی سازمان) برآورده نشده باشد بایستی مرحله تدوین توافقنامه مجدداً به اجرا در آید.

[53] - توافقنامه ای که بین دو طرف تنظیم شده و به عنوان امانت نزد شخص ثالث سپرده می شود و تنها پس از وقوع شروطی خاص قابل اجرا می باشد.

۴- در صورت برآورده شدن کلیه الزامات توافقنامه های تبادل، لازم است توافقنامه تدوین شده به تایید و امضای طرفین تبادل برسد.

۵- پس از تایید توافقنامه در مرحله پایانی این دستورالعمل مکانیزم ها و امکانات مورد نیاز جهت اجرای شروط توافقنامه (مانند سیستم برچسب گذاری) باید تامین شود. تعیین مسئولیت تامین مکانیزم ها و امکانات مورد نیاز توسط هر یک از طرفین تبادل، خود به عنوان یکی از بندهای الزامی در توافقنامه می‌باشد.

۳۸- تهیه نسخه پشتیبان اطلاعات:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی تهیه نسخه پشتیبان از داده‌ها و اطلاعات تحت مالکیتو تعیین چگونگی حفظ و نگهداری اطلاعات می‌باشد.

الزامات:

- لازم است از کلیه داده‌های الکترونیک اعم از بانک‌های داده و اطلاعات، نرم‌افزارهای کاربردی، فایل‌های پیکربندی، سیستم عامل‌ها، فایل‌های داده، ابزارهای سیستم و غیره و اسناد فیزیکی نسخه پشتیبان مصدق تهیه شده و در محلی امن نگهداری شود.

- لازم است نسخه پشتیبان در بازه‌های زمانی مرتب یا به صورت خودکار به‌هنگام‌سازی شود.

- بلافاصله پس از هرگونه اعمال تغییرات در نرم‌افزارها یا فایل‌های داده ضروری است پشتیبان‌گیری انجام شده و یا نسخه پشتیبان به‌هنگام‌سازی شود.

- لازم است در مورد ایجاد نسخه پشتیبان داده‌ها و اطلاعات به حجم، طبقه‌بندی و نوع اطلاعات و نوع فایل توجه و از ابزار مناسب مورد نیاز هر کدام استفاده شود.

-لازم است کفایت، صحت و سلامت نسخه‌های پشتیبان تهیه شده از داده‌ها و اطلاعات مورد بررسی و کنترل مداوم قرار داشته باشد.

- لازم است فرم های لازم (مانند فرم درخواست تهیه نسخه پشتیبان، فرم خلاصه اطلاعات نسخه پشتیبان و ...) طراحی و تدوین شده و هنگام اجرای این دستورالعمل تکمیل گردند.

-لازم است هنگام تولید یا خرید نرم‌افزارهای جدید، روش تهیه نسخه پشتیبان از اطلاعات نیز مورد توجه قرار گرفته و از وجود و صحت آن اطمینان حاصل شود.

- سلسله مراتب بازیابی نسخه پشتیبان باید به نحوی باشد که از تخریب اطلاعات به دلیل عدم یکسان بودن اطلاعات بازیابی شده با اطلاعات اصلی ایمن باشد.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا طرح تهیه نسخه پشتیبان تهیه شده و بهمراه الزامات امنیتی آن تدوین می شود. در این طرح بایستی به دسته بندی سازمان از دیدگاه پدافند غیرعامل و طبقه بندی حفاظتی سازمان توجه شود. همچنین ارزش و اهمیت اطلاعات از دیگر مواردی است که در تدوین این طرح باید مدنظر قرار گیرد. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- در این مرحله کلیه مکانیزم ها، امکانات و تجهیزات مورد نیاز اعم از فضا، سخت افزارها و نرم افزارهای مورد نیاز و متناسب با طرح و الزامات تدوین شده تامین می شود. همچنین فرم های مربوط به این فرآیند نیز در این مرحله تهیه می شود.

۳- پس از تامین موارد فوق، طرح تدوین شده پیاده سازی گشته و الزامات امنیتی به اجرا گذاشته شده و نسخه پشتیبان تهیه می گردد.

۴- در صورت غیرقابل قبول بودن نسخه پشتیبان تهیه شده (مثلاً ناقص بودن نسخه تهیه شده) نسخه پشتیبان مجدداً تهیه می گردد.

۵- در صورت قابل قبول بودن نسخه تهیه شده اگر نسخ پشتیبانی وجود داشته باشند که مورد نیاز نباشند (مثلاً از نظر زمانی دارای ارزش نمی باشند) و یا نامعتبر باشند (بعنوان مثال دارای نقصان باشند) باید مطابق (خارج از رده سازی و استفاده مجدد) از بین برده شده و امحاء شوند.

۶- در صورتی که کلیه الزامات پشتیبان گیری تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد بایستی کلیه اقدامات لازم برای نگهداری و حفاظت از نسخ تهیه شده متناسب با الزامات امنیت فیزیکی پیرامونی انجام شود.

۳۹- ثبت فعالیت های مدیران و اپراتورهای سیستم:

هدف از تدوین این دستورالعمل بیان ضرورت ثبت و نگهداری فهرست فعالیت های مدیران و اپراتورها و هر فردی است که دارای دسترسی ممتاز به دارایی های اطلاعاتی و شبکه های رایانه ای و ارتباطی موجود در قلمرو پیاده‌سازی نظام مدیریت امنیت اطلاعات سازمان می‌باشد.

الزامات:

- لازم است کلیه فعالیت های افرادی که دارای حق دسترسی ویژه (ممتاز) به دارایی های اطلاعاتی هستند ثبت و نگهداری شود، به نحوی که در مواقع نیاز بتوان با بررسی اطلاعات ثبت شده نقش هر فرد در انجام هر عملی را تعیین نمود.

- از فایل ها و پرونده های حاوی اطلاعات ثبت شده در مورد فعالیت افراد دارای حق دسترسی ممتاز به نحوی حفاظت شود که تغییر محتوای آنها غیرممکن باشد. سطح طبقه بندی این نوع اطلاعات برای هر دارایی اطلاعاتی باید حداقل معادل سطح طبقه بندی اطلاعات ثبت وقایع دسترسی های عادی آن باشد.
- در مراکز حساس و حیاتی و در مواردی که ممکن است نیاز به ارائه شواهد فعالیت های افراد به مراجع قضایی یا قانونی است باید روش جمع آوری و ثبت اطلاعات منطبق بر قوانین ناظر بر تولید، نگهداری و ارسال "داده پیام" (در حال حاضر قانون تجارت الکترونیک) باشد.
- کاربران دارای حق دسترسی ممتاز هنگام انجام عملیات عادی که نیاز به استفاده از حق دسترسی ممتاز ندارند نباید از شناسه کاربری دارای دسترسی ممتاز استفاده نمایند. اگر در بررسی فهرست فعالیت های سیستم به چنین موردی برخورد شود باید به عنوان یک واقعه امنیتی تلقی شده و مورد پیگیری قرار گیرد.
- کاربران دارای حق دسترسی ممتاز از شناسه کاربری خود فقط باید برای انجام کاری که مجاز به انجام آن هستند استفاده نمایند. در صورت مشاهده استفاده غیرمجاز از شناسه کاربری دارای حق دسترسی ممتاز این وضعیت باید به عنوان یک حادثه امنیتی تلقی شده و مورد پیگرد قرار گیرد.
- روش های تخصیص شناسه کاربری و کلمه عبور، تشخیص هویت و احراز صلاحیت کاربران دارای حق دسترسی ممتاز باید متفاوت با کاربران عادی باشد. این موضوع باید هنگام ممیزی فهرست فعالیت های کاربران دارای حق دسترسی ممتاز مورد بررسی قرار گیرد.
- لازم است کاربران دارای حق دسترسی ممتاز از ثبت فعالیت های خویش آگاه باشند.
- نادیده گرفتن سوءاستفاده افراد از حق دسترسی ممتاز بسیار خطرناک است و نباید اتفاق بیافتد. در صورت مشاهده چنین وضعیتی (حین کار و یا حین ممیزی فهرست ثبت فعالیت ها) لازم است اولاً شناسه کاربری مربوط غیرفعال گردد، ثانیاً میزان ریسک و زیان احتمالی چنین فعالیتی (در حوزه های نقض محرمانگی،

لطمه به جامعیت و نقض در دسترسی پذیری) برآورد شده و در خصوص تصحیح فرآیندهایی که منجر به این وضعیت شده و یا ترمیم رخنه های احتمالی یا خسارت های ناشی از آن اقدام شود.

- بطور کلی در سازمان های حساس و حیاتی لازم است از اعطای حق دسترسی ممتاز به کاربرانی که از راه دور به سیستم متصل می شوند خودداری شود. در صورت ضرورت اعطای این نوع از حقوق دسترسی به برخی از کاربران، لازم است:

  الف: تعداد افرادی که از این حقوق استفاده می کنند به شدت محدود نگهداشته شود.

  ب: از مکانیزم های رمزنگاری و حفاظت کانال متناسب با نوع دسترسی استفاده شود.

  ج: ثبت اطلاعات به نحوی انجام شود که علاوه بر ثبت فعالیت های این دسته از کاربران، اطلاعات مربوط به برقراری ارتباط از جمله اطلاعات مبداء، زمان و مشخصات فنی ارتباط نیز ثبت گردد.

- ممیزی فهرست فعالیت افراد دارای حقوق دسترسی ممتاز باید به صورت مستقل و با رعایت الزامات ممیزی انجام شود.

- هنگام ممیزی فهرست فعالیت افراد دارای حقوق دسترسی ممتاز باید اطمینان حاصل شود که این افراد قادر به دسترسی به اطلاعات سایر کاربران و ایستگاه های کاری خارج از حوزه مسئولیت خود (و حدودی که برای دسترسی ممتازمشخص گشته است) نمی باشد.

- دوره زمانی نگهداری سوابق دسترسی ممتاز نباید کمتر از چهار برابر دوره زمانی نگهداری سوابق دسترسی عادی باشد.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا کلیه فعالیت های موجود در سازمان مورد بررسی قرار گرفته و فهرستی از فعالیت هایی که باید ثبت شوند تهیه می شوند.

۲- در این مرحله نیز کلیه پست ها بررسی شده و لیستی از افرادی که باید فعالیت ایشان ثبت شود (افرادی که دارای دسترسی ممتاز به دارای های اطلاعاتی و شبکه های رایانه ای و ارتباطی موجود در سازمان می باشند) تهیه می شود.

۳- الزامان امنیتی در خصوص چگونگی ثبت و نحوه نگهداری اطلاعات ثبت شده در این مرحله تدوین می شود. در تدوین این الزامات دسته بندی سازمان از دیدگاه پدافند غیرعامل و همچنین اهمیت جایگاه شغلی مورد توجه قرار می گیرد.

۴- پس از تدوین الزامات، مکانیزم‌ها و امکانات مورد نیاز از قبیل تجهیزات سخت‌افزاری و نرم‌افزارها تامین می شوند. همچنین در صورت نیاز فرم های مربوط نیز در این مرحله تدوین می شوند.

۵- در این مرحله به پیاده سازی مکانیزم ها جهت برآورده ساختن الزامات تدوین شده و همچنین ثبت فعالیت های مورد نظر اقدام می شود.

۶- پس از ثبت فعالیت ها لازم است طبقه بندی حفاظتی اطلاعات ثبت شده مطابق با دستورالعمل طبقه‌بندی دارایی اطلاعاتی سازمان تعیین شده و مطابق با دستورالعمل مدیریت دسترسی های ممتاز سطح دسترسی به اطلاعات ثبت شده مشخص می شود.

۷- در صورتی که کلیه الزامات ثبت فعالیت های تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۵ بازگشت.

۴۰- جداسازی تجهیزات آزمایشی از عملیاتی:

هدف از تدوین این دستورالعمل، جداسازی تجهیزات و دارایی‌های اطلاعاتی تحقیق، توسعه و آزمایش از تجهیزات و دارایی های اطلاعاتی عملیاتی به منظور جلوگیری از بروز مشکلاتی از قبیل نقض محرمانگی به دلیل

استفاده از داده‌ها یا دارایی‌های اطلاعاتی دارای طبقه‌بندی در سیستم‌های آزمایشی، استفاده اشتباه از داده‌های آزمایشی در سیستم‌های عملیاتی و یا از کار افتادن سیستم‌های عملیاتی به دلیل عدم اطمینان از صحت عملکرد تجهیزات آزمایشی تست نشده می باشد.

الزامات:

- لازم است مکان، تجهیزات، دارایی‌های اطلاعاتی و کارمندان محیط آزمایشی تا آنجا که امکان دارد از مکان، تجهیزات، دارایی‌های اطلاعاتی و کارمندان محیط عملیاتی جداسازی شود.

- در صورت نبود تجهیزات و مکان مجزا بایستی نرم‌افزارهای آزمایشی و عملیاتی، روی دستگاه‌های جدا از یکدیگر و پوشه های جداگانه و یا حداقل در دامنه‌ها و دایرکتوری‌های جدا از یکدیگر نگهداری شود به طوری که دارایی‌های اطلاعاتی آزمایشی کاملاً از دارایی‌های اطلاعاتی عملیاتی مجزا باشند.

- در مراکز حساس و حیاتی لازم است محیط های آزمایش کاملا شبیه محیط های عملیاتی بوده و شرایط عملیاتی واقعی در محیط آزمایشی شبیه سازی شود.

- نرم افزارهای تست، کامپایلرها و سایر ابزارهای نرم افزاری بخصوص محیط های تولید یا تصحیح کد منبع نباید در دسترس متولیان و سیستم‌های عملیاتی خودکار قرار گیرند و یا روی تجهیزات عملیاتی نصب شوند. در مواقع ضروری پس از کسب تائیدیه مقام مسئول می بایست از وجود نسخه های پشتیبان قابل اطمینان از داده های در معرض ریسک اطمینان حاصل شود.

- متولیان سیستم های عملیاتی نباید نسبت به کامپایل، اجرای آزمایشی، تست نرم افزارها و یا تغییر در کد منبع در محیط عملیاتی اقدام نمایند مگر در مواقع ضروری پس از کسب تائیدیه مقام مسئول و ارزیابی ریسک در صورتی که ریسک برآورد شده قابل پذیرش باشد.

- برای کاهش ریسک خطا بایستی از رویه‌های مجوزدهی متفاوت برای عملیات آزمایشی و عملیاتی استفاده شود.

- لازم است کاربران واحد آزمایش و توسعه برای دسترسی به سیستم های یکسان مستقر در محیط های آزمایشی و عملیاتی از کلمه‌های عبور متفاوت استفاده نمایند.

- شکل منوها و فرم‌های مورد استفاده در محیط های آزمایشی و عملیاتی باید متمایز از یکدیگر باشد. همچنین لازم است رویه‌های آغاز کار و پایان کار سیستم‌های در حال آزمایش یا توسعه در محیط آزمایشی، متمایز و متفاوت از سیستم های مشابه در محیط‌های عملیاتی باشند.

-افرادی که در قسمت توسعه و آزمایش به کار گرفته می‌شوند بایستی از شرایط احراز شغل برخوردار بوده و همچنین دارای سطح کیفیت بالایی از نظر فنی باشند.

-برنامه‌نویسان و اعضاء گروه توسعه و تحقیق فقط در صورت ضرورت و تحت کنترل، مجاز به استفاده از کلمه عبور قابل استفاده در سیستم‌های عملیاتی می‌باشند. بلافاصله پس از پایان کار بایستی کلمه عبور استفاده شده بر اساس دستورالعمل مدیریت کلمه عبور کاربر تغییر کند.

-لازم است قواعد و مقررات انتقال نرم‌افزار، داده‌های اطلاعاتی و تجهیزات از محیط تحقیق و توسعه به محیط عملیاتی، تعریف شده و مستند سازی آن انجام شود.

- باید از رنگ بندهای متفاوت به منظور جداسازی تجهیزات و دارایی‌های اطلاعاتی آزمایشی از تجهیزات و دارایی‌های عملیاتی استفاده کرد تا ریسک خطا کاهش یابد.

-لازم است که داده‌ها و اطلاعاتی که در بخش آزمایش و توسعه به کار گرفته می‌شود پس از پایان کار طبق دستورالعمل خارج از رده سازی و استفاده مجدد به دلایل زیر از بین برده شود:

- جلوگیری از افشاء اطلاعات
- جلوگیری از افشاء فرمت و نوع اطلاعات
- جلوگیری از استفاده اطلاعات آزمایشی در محیط عملیاتی
- جلوگیری از افشاء نتایج آزمایش ها

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا به بررسی سازمان در خصوص امکانات و توانایی های موجود در زمینه دارا بودن فضاهای مختلف، تجهیزات و دارایی های گوناگون پرداخته می شود و پس از آن الزامات امنیتی جداسازی تجهیزات آزمایشی از عملیاتی و نیازهای هر یک از محیط های آزمایشی و عملیاتی تدوین می‌شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- در صورتی که امکان جداسازی کامل محیط آزمایشی از عملیاتی به واسطه نبود فضای کافی و یا عدم توانایی سازمان در تامین تجهیزات مورد نیاز نباشد طرح جداسازی سیستم های آزمایشی از عملیاتی در یک مکان و یا بر روی سیستم های یکسان بهمراه الزامات امنیتی آن تدوین می شود.

۳- در این مرحله تامین مکانیزم ها و امکانات مورد نیاز اعم از فضا، تجهیزات سخت افزاری و نرم افزارهای لازم برای برآورده ساختن الزامات صورت می گیرد.

۴- پس از تامین مکانیزم ها و امکانات عملیات تست بر روی سیستم های آزمایشی انجام می شود.

۵- در صورتی که نتیجه تست ها غیرقابل قبول باشد اصلاحات لازم برروی سیستم تست شده انجام شده و مرحله ۴ مجدداً اجرا می شود.

۶- در صورت موفقیت تست ها، داده ها و اطلاعات مورد استفاده در تست باید مطابق با دستورالعمل خارج از رده سازی و استفاده مجدد از بین رفته و امحاء شوند.

۷- در صورتی که کلیه الزامات برآورده شده در این سند و الزامات اختصاصی سازمان برآورده شده باشد باید پیش از انتقال تجهیزات به محیط عملیاتی کلیه تست ها و اقدامات صورت گرفته مستند شده و به صورت مناسبی نگهداری شود. در غیر اینصورت بایستی به مرحله ۳ بازگشت.

۸- پس از مستند سازی و همچنین کسب مجوز لازم از (((**مدیر ارشد شبکه**))) تجهیزات به محیط عملیاتی منتقل می شوند.

۴۱- حفاظت از اطلاعات ثبت شده وقایع:

هدف از تدوین این دستورالعمل ارائه راهکارهای مناسب به منظور حفاظت از اطلاعات ثبت شده مربوط به رویدادهای مرتبط با دارایی های موجود در فهرست موجودی دارایی های اطلاعاتی از قبیل رویدادهای سیستم، عملکرد کاربران و وقایع امنیت اطلاعات از طریق دسته بندی اطلاعات ثبت شده وقایع، رمزنگاری و کنترل دسترسی به این دسته از اطلاعات می باشد.

الزامات:

- به دلیل اهمیت بسیار زیاد وجود و صحت اطلاعات ثبت شده در مورد وقایع امنیت اطلاعات در کشف دلایل بروز حوادث، لازم است روش ها و راهکارهای توصیه شده (توسط مراجع ذیصلاح) در مورد حفاظت از اطلاعات به منظور حفاظت از اطلاعات ثبت شده وقایع نیز با دقت کامل بکار برده شود.
- دلایل و شرایط بروز لطمه به امنیت اطلاعات ثبت شده در مورد وقایع امنیت اطلاعات باید بصورت دوره ای مورد بررسی قرار گرفته و تدابیر لازم برای جلوگیری از تکرار آنها در نظر گرفته شود.

- لازم است دسترسی به اطلاعات فقط با توجه به نوع طبقه بندی هر دسته از اطلاعات، نوع کاربرد آن، زمان استفاده، تأیید هویت و اصالت کاربر برای کاربران مجاز امکان پذیر باشد.
- طبقه بندی حفاظتی اطلاعات ثبت شده در مورد وقایع امنیت اطلاعات باید حداقل معادل طبقه بندی حفاظتی دارایی اطلاعاتی باشد که اطلاعات مورد نظر به آن مربوط می باشد. در مراکز حساس و حیاتی این طبقه بندی باید سخت گیرانه تر از طبقه بندی دارایی اطلاعاتی مربوط باشد.
- به منظور جلوگیری از فعالیت غیرمجاز مهاجمان لازم است لاگ های سیستم بر روی سرورها بطور مرتب بررسی گردد. تعیین دوره زمانی بازرسی با توجه به ماهیت و اهمیت شبکه تحت حفاظت انجام خواهد پذیرفت.
- لازم است به منظور کنترل دسترسی کاربران به اطلاعات ثبت شده وقایع از روش های مناسب کنترل دسترسی استفاده شود.
- به منظور حفاظت از اطلاعات ثبت شده وقایع و سهولت دسترسی های مجاز کاربران استفاده از روش های کارآمد رمزنگاری و بایگانی اطلاعات ضروری است.
- هرگونه دسترسی به اطلاعات ثبت شده در مورد وقایع امنیت اطلاعات و بطور کلی وقایع سیستم باید ثبت گردد. نحوه ثبت دسترسی باید به گونه ای باشد که بتوان از طریق آن به هویت متقاضی دسترسی و زمان مصدق دسترسی پی برد.
- هرگونه تغییر یا حذف در اطلاعات ثبت شده در مورد وقایع امنیت اطلاعات و بطور کلی وقایع سیستم باید تحت نظرنهاد ذیربط انجام شود.

- روش ثبت دسترسی به اطلاعات ثبت شده در مورد وقایع و نگهداری این اطلاعات باید به نحوی باشد که استفاده از آن در مراجع قانونی و قضایی امکان پذیر باشد. بنابراین لازم است این گونه فعالیت ها منطبق بر روش های قانونی بوده و مطابق با رهنمودهای مندرج (تجارت الکترونیک) درخصوص صحت و اصالت پیام، جمع آوری و نگهداری گردد.
- دسترسی به اطلاعات ثبت شده در خصوص وقایع باید بر اساس دستورالعمل های کنترل دسترسی تحت کنترل قرار گیرد.
- برای جلوگیری از دسترسی نفوذگران به اطلاعات ثبت شده در خصوص وقایع لازم است (کنترل های شبکه) و امنیت فیزیکی و پیرامونی رعایت شود.
- هرکاربر باید امکان دسترسی (بدون حق تغییر یا حذف) به اطلاعات ثبت شده در مورد وقایع امنیت اطلاعات و دارایی های اطلاعاتی تحت تصدی مالکیت یا تحویل شده به خود را داشته باشد.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا مطابق با دستورالعمل های مربوط اطلاعات در مورد وقایع سیستم ثبت می شود.

۲- پس از ثبت اطلاعات مطابق با دستورالعمل های طبقه بندی دارایی های اطلاعاتی سازمان، طبقه بندی حفاظتی اطلاعات ثبت شده تعیین شده و سطح دسترسی به آن مشخص می شود.

۳- در این مرحله الزامات امنیتی مربوط به حفاظت از اطلاعات ثبت شده وقایع متناسب با سطوح طبقه‌بندی حفاظتی اطلاعات ثبت شده تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۴- مکانیزم ها و تجهیزات مورد نیاز جهت حفاظت از اطلاعات ثبت شده و برآورده ساختن الزامات تدوین شده در این مرحله تامین می گردد.

۵- در این مرحله مکانیزم ها پیاده سازی شده و کلیه الزامات تدوین شده به اجرا در می آیند.

۶- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۵ بازگشت.

۴۲- خط مشی ها و روش های اجرایی تبادل اطلاعات:

هدف از تدوین این دستورالعمل تامین امنیت تبادل اطلاعات با استفاده از انواع امکانات ارتباطی در اختیار می‌باشد

الزامات:

- تدوین سیاست ها و روش‌های اجرایی و کنترل تبادل اطلاعات برای کلیه تعامل‌های منجر به تبادل اطلاعات در قلمرو پیاده‌سازی نظام مدیریت امنیت اطلاعات الزامی است.

- ضرورت دارد تمام امکانات ارتباطی موجود و قابل دسترس در سازمان مانند تلفن، فاکس، تلفکس و خطوط انتقال داده و سایر روش های تبادل اطلاعات از طریق دیگر مثل پیک، شبکه پست و مانند آن شناسایی شوند.

- لازم است عملیات انتقال اطلاعات که شامل ارسال و دریافت اطلاعات می‌باشد تحت کنترل باشد تا حفاظت از امنیت انتقال اطلاعات در کل سازمان ساری و جاری شود.

- ضروری است به منظور هر چه بهتر کنترل امور حفاظت تبادل اطلاعات، خط مشی‌هایی رسمی و در راستای امکانات سازمان به ازاء هر روشی که قبلاً شناسایی شده باشد تدوین و دسته بندی شوند.

- در حالت عادی استفاده از هر روش تبادل اطلاعات فقط پس از تحلیل ریسک و اثبات قابل پذیرش بودن آن مجاز می‌باشد. استفاده از روش های تبادلی که تحلیل ریسک نشده اند باید بر اساس طرح پیوستگی عملیات (BCP[۵۴]) و یا طرح احیای سیستم (DRP[۵۵]) انجام پذیرد.

- در تدوین خط مشی‌های فوق لحاظ نمودن دیدگاه اجرائی لازم و ضروری است. به عبارتی در تدوین آئین‌نامه‌هایی که برای کنترل تبادل اطلاعات در بسترهای مختلف اقدام می‌شود می‌بایست مقدورات سازمان در انجام کنترل‌ها و سطح ریسک قابل پذیرش در نظر گرفته شود.

-ویژگی‌هایی نظیر گستردگی، فناوری‌های انتقال (بی‌سیم و باسیم) و توپولوژی (هم بندی) شبکه‌ها برای تدوین دستورالعمل‌های کنترل تبادل اطلاعات باید در نظر گرفته شود.

- نوع طبقه‌بندی حفاظتی اطلاعات قابل تبادل می‌بایست در متن آئین‌نامه‌ها مورد توجه قرار گیرد.

- در تدوین خط مشی‌های اجرائی برای حفاظت تبادل اطلاعات ضرورت دارد کلیه انواع بسترهای ارتباطی عبور دهنده اطلاعات و نوع نظام های مسیریابی مورد نظر قرار گرفته و با توجه به نوع عملکرد آنها مکانیزم‌های کنترلی در نظر گرفته شوند.

- نرم‌افزارهای مورد استفاده در تبادل اطلاعات و مدل‌های رفتاری آنها بایستی در آئین‌نامه کنترلی تبادل اطلاعات مورد نظر قرار گرفته و به این لحاظ باید قابلیت‌های سیستم عامل نیز لحاظ شوند.

-ضروری است سخت‌افزارهای مسیریابی مثل سیستم‌های مسیریاب، سوییچ‌ها و ... در تدوین دستورالعمل‌های کنترل تبادل اطلاعات مورد توجه قرار گیرند.

---

[54] - Business Continuity Plan

[55] - Disaster Recovery Plan

-رعایت اصول حفاظت از رسانه‌های مختلف انتقال بخش مهمی از آئین‌نامه موصوف است که در نظر داشتن آن ضروری است.

-اعتبار بین بخشی طبقه‌بندی‌های حفاظتی به لحاظ طبقه‌بندی اطلاعات برای یک مرجع (توافق‌نامه‌ای) و یا برای بیش از یک مرجع می‌بایست از طریق رعایت توافق‌نامه های حفظ محرمانگی مورد توجه قرار گیرد.

- آموزش و توجیه خط مشی و آئین‌نامه حفاظت تبادل اطلاعات برای کارکنان الزامی می‌باشد.

- قلمرو عمل خط مشی تدوین شده باید کلیه ابعاد قلمرو پیاده سازی نظام مدیریت امنیت اطلاعات را تحت پوشش قرار دهد.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا کلیه امکانات و فناوری های ارتباطی موجود و قابل دسترس برای سازمان از قبیل تلفن، خطوط انتقال داده، پیک و شبکه پست شناسایی می شوند. همچنین در این مرحله معماری و توپولوژی شبکه سازمان نیز مورد بررسی و شناسایی قرار می گیرند.

۲- در این مرحله الزامات امنیتی که بایستی در تبادل اطلاعات مورد توجه قرار گیرد تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۳- پس از تدوین الزامات در این مرحله خط مشی ها و روش های اجرایی تبادل امن اطلاعات همراستا با الزامات امنیتی تدوین می گردد.

۴- پیش از بهره برداری از روش های تدوین شده ریسک استفاده از آن مورد ارزیابی قرار می گیرد.

۵- در صورت غیرقابل پذیرش بودن ریسک استفاده از روش تدوین شده بایستی مرحله ۳ مجدداً اجرا شود.

۶- در صورت قابل پذیرش بودن ریسک در این مرحله به تامین مکانیزم ها و امکانات مورد نیاز جهت اجرای روش ها و برآورده ساختن الزامات تدوین شده اقدام می شود. همچنین در این مرحله آموزش و توجیه خط مشی و آیین نامه حفاظت تبادل اطلاعات برای پرسنل صورت می پذیرد.

۷- پس از تامین مکانیزم ها پیاده سازی الزامات و اجرای روش های اجرایی تبادل امن اطلاعات که در مراحل پیش تدوین شده اند صورت می پذیرد.

۸- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۷ بازگشت.

۴۳- داد و ستدهای برخط (متصل و مستقیم):

هدف از تدوین این دستورالعمل محافظت از اطلاعات در داد و ستدهای برخط[۵۶] (متصل و مستقیم) به منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه، تغییر غیرمجاز پیغام، افشای غیرمجاز و بازیابی یا تکرار غیرمجاز پیام هایی است که در قلمرو پیاده سازی نظام مدیریت امنیت اطلاعات سازمان مبادله می شوند.

الزامات:

- به منظور پیشگیری از انتقال ناقص اطلاعات، کنترل دقیق SLA[۵۷] در کانال های انتقال اطلاعات ضروری می باشد.

[56]- On-line Transactions

[57]- Service Level Agreement

- لازم است از پروتکل ها و جداول مسیریابی مناسب به منظور پیشگیری از اشتباه های منجر به ارسال اطلاعات به آدرس های اشتباهی یا دریافت اطلاعات از آدرس های اشتباهی استفاده شود.
- در محیط های شبکه پیچیده به منظور جلوگیری از ارسال ترافیک به بخش های غیرضروری و حفظ سرعت ارتباطات بین بخش های مختلف شبکه و تعیین بهترین مسیر ارسال داده و مدیریت ارتباط کامپیوترهای فرستنده و گیرنده باید از مسیریابی (Router) که به درستی پیکربندی شده است استفاده شود.
- لازم است از دسترسی افراد غیرمجاز به اطلاعات مربوط به آدرس دهی شبکه و جداول مسیریابی در مسیریاب ها جلوگیری به عمل آید.
- لازم است در شبکه هایی که برای تبادل پیام های برخط مورد استفاده واقع می شوند، از پروتکل ها و تجهیزاتی که از مسیریابی پشتیبانی می کنند استفاده شود.
- لازم است اقدامات لازم به منظور جلوگیری از دسترسی غیرمجاز، اعمال نفوذ و یا تغییر در پیام، انکار پیام و ایجاد پیام جعلی انجام شود.
- انجام اقدامات لازم به منظور حفظ یکپارچگی یا تمامیت پیام، محرمانگی، تصدیق صحت و انکارناپذیری پیام ضروری می باشد.
- کلیه فرآیندهای ارسال و دریافت پیغام باید در قالب «پیغام امن» انجام شود.
- به منظور جلوگیری از تغییر محتوای پیام و عدم انکار هویت فرستنده بکاربردن رمزنگاری اطلاعات و امضای الکترونیکی ضروری می باشد.
- در الگوریتم های رمزنگاری باید از کلیدهایی استفاده شود که توسط یک منبع تصادفی قابل اطمینان و یا یک مولد بیت شبه تصادفی امن تولید شود. همچنین کلیدهای ضعیف الگوریتم رمزنگاری مورد استفاده باید تا حد امکان حذف شوند و یا مشخص باشند تا در هنگام تولید و انتخاب کلیدها استفاده نگردند.

- استفاده از سیستم های پیام رسانی فوری (IM)[58] مثل پیام رسان یاهو[59]، پیام رسان MSN[60]، گفتگوی گوگل[61]، سرویس Netmeeting و... برای تبادل پیام های دارای طبقه بندی حفاظتی و یا تبادل های مالی یا تعهدآور ممنوع است. در مراکز حساس و حیاتی استفاده از این سیستم ها بطور کلی ممنوع می‌باشد.
- لازم است از عملکرد صحیح وب سایت و سیستم های اطلاعاتی و پایگاه های داده وب سایت در مقابل خرابی های احتمالی اطمینان حاصل شود.
- لازم است از وجود کنترل های اضافی برای حفاظت از وب سایت ها، اطلاعات و پایگاه های داده در مقابل نرم افزارهای مضر و حملات احتمالی اطمینان حاصل شود.
- لازم است مسئولیت های مرتبط با امنیت اطلاعات در داد و ستدهای برخط و مسئولیت های شغلی تعیین شود.
- لازم است ضرورت حفظ امنیت و محرمانگی اطلاعات در مقابل دسترسی های غیرمجاز به تمامی کارکنان آموزش داده شود.
- لازم است از افشاء یا تغییر اطلاعات از طریق اعمال اتفاقی یا بی توجهی در داد و ستدها در مقابل افراد یا سازمان های غیرمجاز جلوگیری به عمل آید.
- پاسخگویی به تمامی نیازهای قانونی، قراردادی و داخلی مرتبط با امنیت داد و ستدها و وب سایت و همچنین امنیت دارایی های اطلاعاتی و داده های الکترونیکی ضروری می باشد.
- حمایت از امنیت اطلاعات الکترونیکی شرکای تجاری یا اداری، شرکت ها و سازمان های تابعه در محدوده سیستم های اطلاعاتی سازمان ضروری است.

58- Instant Messaging

59- Yahoo Messenger

60- MSN Messenger

61- Google talk

- لازم است عملیات مانیتور کردن اطلاعات کاربر شامل شناسایی پست الکترونیک، ترافیک اینترنت و تماس های تلفنی (در صورت وجود VOIP) منطبق بر الزامات قانونی حفظ حریم خصوصی افراد به اجراء گذاشته شود.
- لازم است عملیات مانیتورینگ خودکار از طریق سیستم های شناسایی نفوذ و یا سایر دستگاه ها و یا نرم افزارهای مربوطه به صورت جداگانه تعیین و تعریف شود.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

- در ابتدا الزامات امنیتی و روش های امن سازی داد و ستدهای برخط تدوین می شود. در صورتی که سازمان دارای الزامات و روش های اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.
- پس از تدوین الزامات و روش ها در این مرحله متقاضی استفاده از سرویس مورد نظر بایستی از روش های تدوین شده موارد مورد نظر خود را انتخاب نماید.
- در صورتی که روش انتخاب شده مورد تایید (((نهاد متصدی امنیت اطلاعات))) باشد مجوز بهره برداری از سرویس برای متقاضی صادر می شود. در غیر اینصورت مرحله انتخاب روش مجدداً اجرا می شود.
- پس از صدور مجوز مکانیزم ها و امکانات مورد نیاز مانند الگوریتم های رمزنگاری مناسب و سیستم مانیتورینگ تامین می شوند.
- در این مرحله به پیاده سازی مکانیزم و اجرای کلیه الزامات و روش های تدوین شده اقدام می شود.

- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۵ بازگشت.

۴۴- رسانه های ذخیره سازی فیزیکی حین حمل و نقل:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی حفاظت از رسانه های ذخیره سازی فیزیکی حین حمل و نقل می باشد.

الزامات:

در صورت نیاز به انتقال داده ها و اطلاعات از طریق رسانه های فیزیکی مثل کاغذ، نوار مغناطیسی، دیسک مغناطیسی، دیسک نوری، حافظه فلش و یا سایر رسانه ها لازم است نکات زیر رعایت شود:

- برای انتقال داده های دارای طبقه بندی حفاظتی فقط از پیک معتمد استفاده شود.
- تدابیر لازم برای جلوگیری از صدمه خوردن رسانه حین حمل و نقل در اثر عوامل سهوی یا طبیعی مثل ضربه، لرزش، گرما، سرما، رطوبت و تشعشع در نظر گرفته شود.
- در خصوص داده های عادی حتی الامکان از روش های رمزنگاری و در خصوص داده های دارای طبقه بندی از روش های مستحکم رمزنگاری (برای جلوگیری از افشاء) استفاده شود.
- به حمل کننده اخطارهای لازم در خصوص نوع اطلاعات و الزامات حفاظت از آن داده شود.
- قبل از ارسال باید از اطلاعات، نسخه پشتیبان تهیه شود.
- به حمل کننده آموزش های لازم در خصوص چگونگی مواجهه با سرقت رسانه ها یا جلوگیری از دستیابی افراد غیرمجاز به رسانه داده شود.
- روش مناسبی برای اطمینان از هویت دریافت کننده و دریافت رسانه در مقصد اتخاذ شود.

- قبل از ارسال فهرستی از داده های موجود در رسانه تهیه و به عنوان سوابق سازمانی نگهداری شود.
- فرآیندهای لازم برای چگونگی مقابله با پیامدها یا محدودسازی اثرات ضربه ناشی از سرقت رسانه یا افشای داده های موجود در آن وجود داشته باشد.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا طبقه بندی حفاظتی اطلاعات موجود بر روی رسانه های ذخیره سازی مورد بررسی قرار می‌گیرد. این بررسی در مراحل بعدی و بخصوص تدوین الزامات و روش ها بسیار تاثیرگذار می‌باشد.

۲- الزامات امنیتی و روش های امن حمل و نقل رسانه های ذخیره سازی متناسب با طبقه بندی اطلاعات درون آن تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۳- در این مرحله مکانیزم ها و امکانات مورد نیاز از قبیل تجهیزات سخت افزاری و یا فرم های مورد نیاز تهیه و تدوین می شوند.

۴- در این مرحله حمل و نقل رسانه ذخیره سازی و همچنین روش های تدوین شده مورد ارزیابی قرار گرفته و ریسک حاصل از انجام آن برآورد می شود.

۵- در صورتی که ریسک برآورد شده غیرقابل پذیرش باشد از حمل و نقل رسانه جلوگیری شده و فرآیند خاتمه می یابد.

۶- در صورت قابل پذیرش بودن ریسک از اطلاعات درون رسانه مطابق با دستورالعمل تهیه نسخه پشتیبان، پشتیبان گیری به عمل می آید.

۷- پیش از ارسال باید به حمل کننده رسانه ذخیره سازی، آموزش های لازم در خصوص جلوگیری از دستیابی افراد غیرمجاز به رسانه و چگونگی مواجهه با سرقت رسانه ارائه شود.

۸- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد مجوز ارسال و حمل و نقل رسانه توسط (((**نهاد متصدی امنیت اطلاعات**))) صادر می شود. در غیر اینصورت بایستی به مرحله ۳ فرآیند بازگشت.

۹- پس از صدور مجوز، رسانه ذخیره سازی توسط فرد مجاز ارسال می شود.

۴۵- روش های اجرایی مدیریت و نگهداری اطلاعات:

هدف از تدوین این دستورالعمل ملزم نمودن کلیه واحدهای جمع‌آوری و تولید کننده اطلاعات **سازمان** به رعایت نمودن الزامات امنیتی در ایجاد و بکارگیری رویه‌های مدیریت و نگهداری اطلاعات (جمع‌آوری، نگهداری، ذخیره‌سازی و بازخوانی) برای حفاظت در برابر افشاء غیرمجاز یا استفاده نابجا می باشد.

الزامات:

- لازم است نحوه جمع‌آوری، کسب و دسته‌بندی اطلاعات منطبق بر نیازهای از پیش تعیین شده باشد.

- پس از تولید اطلاعات باید آنها را به شکل صحیح طبقه‌بندی کرده و سطح دسترسی هر دسته از اطلاعات به دقت مشخص شود.

- لازم است رسانه های ذخیره اطلاعات طبقه‌بندی شده با علامت‌ها و برچسب‌های لازم علامت گذاری شوند به نحوی که به آسانی قابل تشخیص باشند.

- برای انجام عمل طبقه‌بندی بایستی معیارهای غیرقابل تفسیر و از پیش تعیین شده مورد استفاده قرار گیرند.

- برای پردازش اطلاعات باید به سطح طبقه‌بندی هر دسته از اطلاعات توجه کرد و اطلاعات با هر سطح طبقه‌بندی فقط به افرادی که اجازه دسترسی به آن سطح را دارا می‌باشند تحویل داده شود.

- باید توجه داشت سطح طبقه‌بندی اطلاعات پس از پردازش در چه درجه‌ای می‌باشد و اگر پردازش موجب تولید اطلاعاتی با سطح طبقه‌بندی سخت گیرانه‌تر شود باید الزامات مدیریت آن دسته از اطلاعات رعایت گردد.

- لازم است اطلاعات پس از پردازش و قبل از عمل ذخیره‌سازی به دقت مورد بررسی قرار گیرد که در آن ایراد و اشتباهی صورت نگیرد.

- بعد از اتمام مراحل پردازش بایستی اطمینان حاصل شود تغییرات در تمامی نسخه‌های موجود اطلاعات اعمال شود.

- اطلاعات باید برای ذخیره‌سازی در محل امن قرار گیرد به طوری که دسترسی به آنها برای افراد غیرمجاز امکان‌پذیر نباشد.

- برای اطمینان از عدم لطمه ناخواسته به اطلاعات باید از آنها نسخه پشتیبان تهیه شود.

- بایستی از اطلاعات در مقابل تهدیدات ناشی از حوادث طبیعی و غیرطبیعی بر اساس سطح حساسیت سازمان (طبق دسته بندی سازمان پدافند غیرعامل) تا آنجا که ممکن است محافظت شود.

- در مراکز حساس و حیاتی، محل نگهداری اطلاعات باید در مقابل بلایایی از قبیل سیل، زلزله، آتش‌سوزی، انفجار، اغتشاشات اجتماعی و مانند آن کاملاً ایمن باشد.

- تا آنجا که ممکن است رسانه ذخیره‌سازی طوری انتخاب شود که در صورت خرابی برخی قطعات به صورت ناخواسته، امکان بازیابی اطلاعات از رسانه وجود داشته باشد.

- بعد از استفاده کامل از اطلاعات و اطمینان از عدم نیاز همیشگی به اطلاعات باید اطلاعات به صورت کامل از بین برده شود.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا به تبیین اهداف و نیازهای جمع آوری اطلاعات پرداخته می شود. این بررسی بر طراحی، نحوه جمع آوری، دسته بندی و دیگر مراحل این فرآیند موثر می باشد. همچنین در این مرحله الزامات امنیتی مدیریت و نگهداری اطلاعات در مراحل تولید، پردازش، ذخیره‌سازی و امحاء اطلاعات تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- در این مرحله جمع آوری و یا تولید اطلاعات انجام می شود.

۳- پس از تولید یا جمع آوری اطلاعات آنها را به شکل صحیح و مطابق با دستورالعمل طبقه بندی حفاظتی دارایی های اطلاعاتی طبقه بندی کرده و سطح دسترسی به آنها مشخص می شود.

۴- در این مرحله بر روی اطلاعات اولیه پردازش های لازم صورت می گیرد. این پردازش می تواند توسط رایانه و یا افراد صورت پذیرد. به عنوان مثال امضای نماینده حراست بر روی برگه مشخصات فردی پرسنل شرکت نیز خود به عنوان پردازش محسوب می شود.

۵- در صورتی که پس از پردازش سطح طبقه بندی حفاظتی اطلاعات تغییر یابد تعیین طبقه بندی اطلاعات مجدداً صورت می پذیرد. در اینصورت باید به مرحله ۳ فرآیند بازگشت.

۶- در این مرحله ذخیره سازی اطلاعات مطابق با الزامات امنیتی تدوین شده صورت می پذیرد. همچنین بایستی اطمینان حاصل شود تغییرات صورت گرفته در اطلاعات بر روی تمامی نسخه های موجود اعمال می شود.

۷- در صورتی که کلیه الزامات تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله طبقه بندی اطلاعات (مرحله ۳) بازگشت.

۴۶- رویه‌های عملیاتی مستند:

هدف از تدوین این دستورالعمل الزام کلیه ارائه دهندگان خدمات رایانه ای **سازمان** اعم از ارائه دهندگان درون سازمانی و یا طرف های قرارداد برون سپاری خدمات رایانه ای به رعایت الزامات مستند نمودن کلیه رویه‌های اجراء و امن‌سازی عملیات رایانه ای، نگهداری مستندات و دسترس پذیر بودن برای کاربرانی که به آن نیاز دارند می‌باشد.

الزامات:

- کلیه رویه‌های عملیاتی امن سازی باید مستند بوده و روش‌های انجام آنها به صورت دوره‌ای و یا در صورت نیاز مورد بازنگری قرار گیرند.

- رعایت الزامات امنیت اطلاعات در تدوین هر رویه و دستورالعملی الزامی است.

- رویه‌های عملیاتی بایستی بر اساس استاندارد مرجع مدیریت امنیت اطلاعات (به عنوان مثال ISO/IEC-27001) تدوین شوند.

- ضروری است مستندات لازم برای برنامه‌ریزی، اجرا، کنترل کارا و مؤثر فرآیندهای سازمان به تناسب کاربرد در سازمان تهیه شود.

- لازم است یک نسخه پشتیبان از کلیه مستندات تدوین شده تهیه شده و توسط نهاد ذیربط بایگانی شود.

- مستندات می‌بایست شامل اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات سازمان باشد.

- فرمت مستندات تولید شده باید بر اساس دستورالعمل تولید و کنترل تعیین شود.

- لازم است حداقل مستندات زیر به صورت مدون تهیه و به اجراء گذاشته شود:

- سند (بیانیه) مدون خط مشی نظام مدیریت امنیت اطلاعات و اهداف آن

- قلمرو (حوزه) استقرار نظام مدیریت امنیت اطلاعات : تعیین قلمرو پیاده سازی سامانه مدیریت امنیت اطلاعات)

- روش های اجرایی و مکانیزم های کنترلی پشتیبانی نظام مدیریت امنیت اطلاعات و اهداف آن

- تشریح روش برآورد مخاطرات (تحلیل ریسک) : ارزیابی ریسک)

- گزارش مخاطرات شناسایی شده (گزارش تحلیل ریسک)

- طرح مدیریت و مقابله با ریسک (برطرف سازی مخاطرات)

- روش های اجرایی مدون شده ای که برای حصول اطمینان از موثر بودن طرح ریزی، اجرا و کنترل فرآیندهای امنیت اطلاعات و تشریح میزان اثربخشی مکانیزم های کنترلی در سازمان به کارگرفته خواهند شد.

- سوابقی که توسط استاندارد مرجع (به عنوان مثال ISO/IEC-27001) الزام شده اند. (بخصوص سوابق وقایع مهم و حوادث رایانه ای)

- بیانیه کاربردپذیری

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۸- ابتدا لازم است الزامات امنیتی مربوط به مستند نمودن کلیه رویه های اجرا و امن سازی عملیات رایانه‌ای، نگهداری مستندات و دسترس پذیر بودن آن برای کاربران مجاز تدوین شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۹- در این مرحله به تهیه فهرستی از رویه ها و مستنداتی که باید تدوین شوند اقدام می شود. نمونه ای از این مستندات عبارتند از:

- سند (بیانیه) مدون خط مشی نظام مدیریت امنیت اطلاعات و اهداف آن
- روش های اجرایی و مکانیزم های کنترلی پشتیبانی نظام مدیریت امنیت اطلاعات و اهداف آن
- سوابقی که توسط استاندارد مرجع (به عنوان مثال ISO/IEC-27001) الزام شده اند.

۱۰-پس از تهیه لیست مذکور در این مرحله به تدوین رویه ها و مستندات بیان شده در لیست پرداخته می شود.

۱۱-در صورتی که کلیه رویه ها و مستندات ضروری تدوین نشده باشند لازم است به مرحله ۲ بازگشت.

۱۲-پس از تدوین کلیه مستندات، باید از مستندات تدوین شده حفاظت و نگهداری مناسب به عمل آید.

۴۷- کنترل کدهای سیار :

هدف از تدوین این دستورالعمل محافظت از اطلاعات در مقابل تهدیدهای ناشی از بکارگیری کدهای سیار[۶۲] می باشد.

الزامات:

- لازم است روش های استفاده از کدهای سیار که در شبکه ارتباطی به کار گرفته می شود مطالعه شده و بر اساس نیازهای موجود یا آینده سیاست ها و پیکربندی های ضروری برای امن سازی بهره برداری از کدهای سیار تدوین شده و بر روی ماشین های میزبانی که نیاز به استفاده از آن دارند نصب شود. به عنوان مثال اگر از زبان برنامه نویسی جاوا استفاده می شود لازم است تحلیل ریسک امنیتی بکارگیری ماشین مجازی جاوا روی ایستگاه های کاری انجام شود.
- از آنجا که روش های حفاظت از میزبان ها در مقابل تهدیدات ناشی از کدهای سیار و یا حفاظت از کدهای سیار در مقابل عملکرد میزبان های آلوده نیاز به سطح بالایی از دانش تخصصی برنامه نویسی (در سطح سیستم) دارد استفاده از مشاوره فنی نهادهای تخصصی در این زمینه ضروری است.
- در بخش سیاست گذاری لازم است در خصوص صدور مجوز استفاده از قابلیت های Java ، Java Scripts ، Activex و مانند آن در هر یک از مرورگرهای وب نصب شده بر روی ایستگاه‌های کاری تصمیم گیری شود. نتیجه تصمیم باید اعمال یکی از سیاست های زیر باشد:
  - قابلیت های فوق غیرفعال (Disable) شوند.
  - قابلیت های فوق فقط هنگام ارتباط با سرورهای داخلی فعال باشند.
  - قابلیت های فوق فقط هنگام ارتباط با سرورهای معتمد (Trusted) فعال باشند.

---

[62] - Mobile Code

- قابلیت های فوق هنگام ارتباط با هر نوع سروری فعال باشد.

- محصولاتی که برای حفاظت در مقابل تهدیدات ناشی از کدهای سیار به کار گرفته می شوند لازم است خود دارای گواهینامه های امنیتی مربوط که بر اساس استانداردهای مرتبط صادر شده اند باشند. (به عنوان مثال بر اساس معیارهای معرفی شده در CC[۶۳] یا NIST Sp800-23 ارزیابی و سطح بندی شده باشند) البته لازم است توجه شود رعایت الزامات این استانداردها به معنی امن بودن کامل محصول نیست زیرا برخی از محصولاتی که در کشورهای غربی (بخصوص ایالات متحده) تولید و یا عرضه می شوند ملزم به رعایت شرط هایی هستند که ممکن است ناقض اصل محرمانگی در سایر کشورها باشند. بنابراین در مراکز حساس و حیاتی لازم است قبل از استفاده از این گونه ابزار امنیتی ارزیابی داخلی در خصوص آنها به عمل آید.
- ممیزی پیکربندی مرورگرهای وب به منظور اطمینان از رعایت سیاست گذاری پذیرش کدهای سیار به طور مرتب باید انجام شود.
- کنترل نسخه[۶۴]و مدیریت وصله های نرم افزاری[۶۵] باید به عنوان بخشی از برنامه کنترل کدهای سیار محسوب شده و به اجراء گذاشته شود.
- در شرایطی که اصولاً نیازی به دریافت کد سیار نمی باشد (مثل کامپیوترهایی که خطوط تولید را کنترل می نمایند و یا به فرآیند خاصی تخصیص داده شده اند) لازم است از روش جداسازی (منطقی یا فیزیکی) استفاده شود تا ریسک ناشی از تهدیدات کد سیار به طور کامل حذف گردد.

---

[63] -Common Criteria for Information Technology Security Evaluation

[64]- Version Control

[65]- Patch Management

- برای کاهش ریسک تهدیدات ناشی از کدهای سیار تا حدی که امکان دارد باید از نصب نرم‌افزارهای متعدد روی یک ایستگاه کاری جلوگیری شود. هر چه نرم افزارهای نصب شده روی یک ایستگاه بیشتر باشد احتمال پیکربندی نادرست افزایش می یابد.
- به هر نرم افزار فقط باید حق دسترسی در حد مورد نیاز آن اعطاء شود. به عنوان مثال در سیستم عامل یونیکس نرم افزارهایی که با حقوق دسترسی ممتاز (مثل کاربر Root) اجراء می شوند می‌توانند بسیار خطرناک باشند.
- لازم است نرم افزارهای کاربردی قابل استفاده در سیستم های مدیریت اطلاعات بر اساس مدل «دفاع عمقی[۶۶]» طراحی شده باشند تا در صورت کرنش سیستم عامل در مقابل حملات، بتوانند از داده های خود حفاظت نمایند.
- لازم است رویه های پاسخ به حوادث حاوی دستورالعمل های مقابله با حوادث ناشی از عملکرد کدهای سیار و چگونگی محدودسازی اثرات آن باشد[۶۷].

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا مطالعه ای بر روی انواع مختلف کد های سیار و بخصوص انواع جدید آن صورت گرفته و فهرستی از گونه های کد سیار تهیه می شود.

۲- در صورتی که نیاز به دریافت کد سیار نباشد این فرآیند خاتمه می یابد.

[66]- Defense in Depth

[67] مراجعه شود. NIST Sp800-28v2 -برای آگاهی از الزامات فنی مقابله با تهدیدات ناشی از عملکرد کدهای سیار به متن

۳- در صورت نیاز به دریافت کد سیار بایستی ریسک امنیتی استفاده از این کدها مورد ارزیابی قرار گرفته و مخاطرات آن برآورد شود.

۴- پس از تحلیل ریسک، در این مرحله الزامات امنیتی و سیاست های امن سازی بهره برداری از کدهای سیار در راستای حذف، کاهش یا مدیریت مخاطرات تدوین می شود.

۵- در این مرحله مکانیزم ها و ابزار مورد نیاز جهت برآورده ساختن الزامات و سیاست ها تامین می‌شود.

۶- پس از تامین مکانیزم ها و ابزار به پیاده سازی مکانیزم ها و اجرای کلیه الزامات و سیاست های تدوین شده اقدام شود.

۷- در صورتی که کلیه الزامات کنترل کدهای سیار تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۶ بازگشت.

۴۸- کنترل کدهای مخرب:

هدف از تدوین این دستورالعمل محافظت از کلیه دارایی های اطلاعاتی نرم افزاری و سخت افزاری در مقابل تهدیدهای ناشی از عملکرد کدهای مخرب[68] می‌باشد.

الزامات:

- تمام ایستگاه‌های کاری و سرورها باید به وسیله نرم‌افزارهای ضد بدافزار که توانایی شناسایی بدافزارها و پاکسازی آنها را دارند حفاظت شوند.

- غیرفعال کردن نرم‌افزار ضد بدافزار توسط کاربران ممنوع است.

[68] - Malicious Codes

- باید اطمینان حاصل شود که تمام ایستگاه‌های کاری خارج از ابنیه و یا نصب شده در سایت های دور و ایستگاه های کاری یا سرورهای متعلق به کارکنان، پیمانکاران و اشخاص ثالث که به شبکه های سازمانی دسترسی دارند به وسیله ضد بدافزار محافظت می شوند.

- نرم‌افزار ضد بدافزار باید در تمام شبکه (بی‌سیم و باسیم)، ایستگاه‌های کاری یا سرویس دهنده ها نصب و پیکربندی شود. پیکربندی آن باید حدقل موارد زیر را شامل شود:

- نرم‌افزار باید به طور خودکار و مرتب به هنگام سازی[۶۹] شود.

- هر داده ای که از یک منبع خارجی مثل اینترنت و یا رسانه های ذخیره سازی داده مثل فلاپی دیسک، CD-Rom، USB/flash (حافظه‌های ذخیره‌سازی) و مانند آن یا هر وسیله ارتباطی پیاده‌سازی می‌شود قبلاً از لحاظ عاری بودن از کدهای مخرب بررسی شده و در صورت مشکوک بودن رفع عیب شده یا از انتقال آن جلوگیری شود.

- هر فایلی که قابلیت توسعه و دسترسی به آن (بوجود آوردن، جابجا کردن، کپی کردن و یا اجرا کردن) وجود دارد باید به طور خودکار و دوره ای بررسی شود.

- هر فایل دریافت شده از سرویس دهنده های شبکه در ایستگاه‌های کاری و یا انتقال یافته از ایستگاه های کاری به سرویس دهنده ها باید از لحاظ عاری بودن از کدهای مخرب به صورت خودکار پویش[۷۰] شود و در صورت آلوده بودن، پاکسازی و در غیر این صورت از انتقال آن جلوگیری به عمل آید.

---

[69] - Update

[70] - Scan

-نرم‌افزار ضد بدافزار باید بر روی تمامی ایستگاه‌های کاری که به طور مستقل کار می‌کنند و تمام وسایل قابل حمل (اعم از متصل یا غیرمتصل به شبکه) نصب شود.

- مدیر ارشد شبکه باید کلیه مشتریان، کاربران و سایر افراد درگیر کار با دارایی های اطلاعاتی نرم‌افزاری و سخت افزاری را از وظیفه خود در مقابل قرنطینه کردن و پاک کردن نرم‌افزارهای آلوده در ایستگاه‌های کاری، ایستگاه های غیرمتصل به شبکه و دستگاه‌های قابل حمل آگاه سازد.

- تمامی Email های دریافتی شامل ضمائم[۷۱] برای وجود بدافزارها یا کدهای مخرب بررسی شوند.

- لازم است بدافزارها و کدهای مخرب به محض کشف، ریشه‌کن شوند (کد مربوط بطور کامل پاک شده و آثار آن نیز از کلیه مکان های محتمل مثل Boot Sector، FAT، NFS، فایل های رجیستری حذف شود).

-اکثر سرویس‌های پیام رسان فوری[۷۲]، IRC[۷۳] و اشتراک فایل نقطه به نقطه[۷۴] دارای پتانسیل تجاوز از راه دور هستند. استفاده از این سرویس ها ممنوع است و باید از روی کلیه ایستگاه های کاری حذف شوند مگر آنکه وجود آنها کاملاً ضروری تشخیص داده شود و ریسک حاصل از استفاده از آنها ارزیابی شود. اکثر این سرویس‌ها کوچک بوده و یا سرویس‌های امنیتی بر روی آنها نصب نمی باشد و از پروتکل‌های اختصاصی استفاده می‌کنند.

-نصب سرویس‌های پیام رسان فوری، IRC، اشتراک فایل نقطه به نقطه، تبادل پست الکترونیک و یا هر سرویس غیرضروری دیگر بر روی سرورها ممنوع است.

---

71 - Attachments

72 - Instant Messaging

73 - Internet Relay Chat

74 - Peer to Peer File Sharing

- در صورت نیاز به استفاده از سرویس‌های پیام رسان فوری، IRC و تبادل ضمیمه های پست الکترونیک یا فایل لازم است داده های مربوطه از دیواره آتش و یا دروازه های امنیتی عبور داده شده و برای عاری بودن از کدهای مخرب بررسی شوند.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا کلیه الزامات امنیتی در خصوص کنترل کد های مخرب تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- در این مرحله مکانیزم ها و ابزار لازم اعم از تجهیزات سخت افزاری و نرم افزارها تامین خواهند شد. نمونه ای از این ابزار عبارتند از:

- نرم افزار ضد بد افزار
- UTM[۷۵]
- دیواره آتش

۳- پس از تامین مکانیزم ها و ابزار لازم به پیاده سازی موارد مذکور مانند نصب بدافزار و دیواره آتش اقدام می شود.

۴- پس از نصب ابزار و پیاده سازی مکانیزم ها بایستی پیکربندی های مناسب بر روی هر یک از آنها تنظیم و اجرا گردد.

[75]- Unified Threat Management

۵- در صورتی که کلیه الزامات کنترل کدهای مخرب تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد در غیر اینصورت بایستی به مرحله ۳ بازگشت.

۴۹- کنترل های شبکه:

هدف از تدوین این دستورالعمل بیان ضرورت مدیریت کارا و کنترل اجزای شبکه های رایانه‌ای و زیرساخت‌های ارتباطی موجود در قلمرو پیاده سازی نظام مدیریت امنیت اطلاعات از طریق حفاظت از آن در مقابل تهدیدات می‌باشد.

الزامات:

- طراحی معماری شبکه باید با توجه به سطح طبقه‌بندی حفاظتی اطلاعات جاری در آن و دسته‌بندی سازمان بهره‌بردار از دیدگاه سازمان پدافند غیرعامل و نیازمندی های امنیتی در جهت جلوگیری از اختلال در شبکه به دلایل تخریب فیزیکی یا حمله های رایانه‌ای انجام شود. این طرح باید با نگرش به ضرورت‌های زیر تدوین گردد:

-افراز[۷۶] بخش های مختلف شبکه از یکدیگر بر اساس ماموریت سازمانی بخش ها و کارکرد اجزای شبکه.

- تعبیه خطوط اتصال بخش های مختلف شبکه بر اساس سیاست گذاری اتصال.

- تعبیه نقطه امن در نقاط اتصال .

[76] - Segmentation

- سد دسترسی آزاد از یک ایستگاه کاری به ایستگاه کاری دیگر و اعطای حقوق دسترسی بر اساس نیازهای کاری و تهیه فهرست های کنترل دسترسی[۷۷].

- جداسازی فیزیکی ایستگاه های کاری یا شبکه هایی که لزومی به اتصال آن به شبکه اصلی سازمان وجود ندارد و یا به دلایل حفاظتی باید جدا نگهداشته شوند.

هنگام طراحی پلان معماری شبکه باید (حداقل) بخش های زیر در نظر گرفته شده و در مورد حفاظت و تامین آنها تصمیم گیری شود:

- ناحیه کاملاً امن (برای استقرار تجهیزات حاوی اطلاعات بسیار مهم مانند کلیدهای رمزنگاری، اطلاعات کارت های اعتباری، بایگانی اطلاعات پیکربندی تجهیزات مهم و اسرار سازمانی).

- ناحیه امن عملیاتی (برای استقرار تجهیزات، نرم افزارها و اطلاعات مهم سازمانی مانند سرورهای برنامه های کاربردی و بانک های اطلاعاتی مهم).

- ناحیه امن ارتباطی (برای استقرار تجهیزات مسیریابی و کنترل شبکه).

- نواحی کاری افراز شده (محل استقرار ایستگاه های کاری بر اساس ماموریت سازمانی).

- ناحیه کاربران راه دور قابل اعتماد (برای اتصال کاربرانی که از طریق شبکه های راه دور غیراینترنت و از طریق خطوط پهن باند به شبکه سازمان متصل می شوند).

- ناحیه کاربران راه دور تلفنی (برای اتصال کاربرانی که از طریق خطوط تلفنی عادی[۷۸] به شبکه سازمان متصل می شوند).

---

[77] - ACLs: Access Control Lists

[78] - PSTN: Public Switched Telephone Network

- ناحیه DMZ[۷۹] (برای استقرار تجهیزات برقراری ارتباط کاربران داخلی با شبکه های اطلاع رسانی عمومی مثل اینترنت و یا ارائه سرویس غیرمستقیم سازمان به این نوع شبکه ها)

- اتصال فیزیکی بین ناحیه کاملاً امن و سایر نواحی بجز ناحیه امن عملیاتی ممنوع است.

- اتصال فیزیکی بین هریک از بخش های فوق با شبکه باید از طریق مکانیزم نقطه امن (بر اساس دستورالعمل ۷-۱-۱: سیاست گذاری کنترل دسترسی) محافظت شود.

- دسترسی به تجهیزات مدیریت یا مسیریابی شبکه باید با توجه به سطح طبقه بندی حفاظتی و با استفاده از قفل‌های مکانیکی و مکانیزم های کنترل دسترسی منطقی محدود شود.

- اطلاعات دسترسی به تجهیزات مدیریت یا مسیریابی شبکه شامل زمان دسترسی، مکان و شناسه کاربری مورد استفاده باید به نحو مناسب ثبت و نگهداری گردد. در صورتیکه هدف از جمع آوری این اطلاعات استفاده از آنها در مراجع قانونی باشد مستندات مذکور می‌بایست به صورت محکمه پسند گردآوری و نگهداری شود.

- لازم است در مراکز حساس و حیاتی جهت مقابله با شنود خطوط انتقال، حتی‌الامکان از کابل‌های فیبر نوری استفاده شود و شبکه های این گونه مراکز به صورت تصادفی و در فواصل زمانی معین مورد بررسی قرار گیرند.

- باید در فواصل زمانی منظم و یا زمانی که پیکربندی تجهیزات تغییر می‌یابد، از پرونده‌های پیکربندی تجهیزات، نسخه پشتیبان تهیه شود.

-می‌بایست کلیه دارایی‌های اطلاعاتی مورد استفاده در فرآیند احراز هویت [۸۰] در مقابل دسترسی‌های غیرمجاز محافظت شوند.

---

79 - Demilitarized Zone

80- Authentication

- لازم است به روز رسانی ضد بدافزارها در همه ایستگاه های کاری و سرورها طبق برنامه زمانی منظم اجرا گردد.

-آخرین وصله‌های امنیتی و به روز رسانی امنیتی سیستم عامل و سرویس‌های موجود در شبکه باید به صورت مداوم صورت گیرد. در این مرحله علاوه بر اقدامات ذکر شده لازم است کلیه سرورها، سوئیچ‌ها، مسیریاب‌ها و سایر تجهیزاتی که دارای سیستم عامل هستند با ابزارهای شناسایی حفره‌های امنیتی بررسی شوند تا علاوه بر شناسایی و رفع حفره‌های امنیتی، سرویس‌های غیرضروری هم شناسایی و غیرفعال شوند.

-می‌بایست طبق دستورالعمل‌های تأمین امنیت محیطی و فیزیکی تمهیدات لازم در خصوص امن‌سازی فیزیکی اجزای شبکه انجام گیرد.

- ضروری است برای جلوگیری از بروز وقفه در فعالیت مراکزی که از نظر سازمان پدافند غیرعامل جزء مراکز حیاتی دسته بندی شده‌اند، مشابه شبکه در حال کار (از بعد تجهیزات و کارکرد)، شبکه ثانویه‌ای در محلی که از نظر جغرافیایی با شبکه اول دارای فاصله مطمئن است، ایجاد و عملیاتی گردد.

- برای تأمین امنیت شبکه و مقابله با حملاتی نظیر پیکربندی غیرمجاز سیستم و حملات DoS، لازم است امنیت سرویس‌های شبکه و کنترل تجهیزات شبکه (همچون مسیریاب‌ها، سوئیچ‌ها، دیواره‌های آتش و سایر ابزارهای مسیریابی و امنیتی) بررسی و کنترل گردد.

- ضروری است فعالیت‌های کاربران در جهت مقابله با تخلفاتی نظیر نصب هرگونه نرم‌افزار پویش پورت، پویش شبکه، عبور از فیلترهای اینترنتی و نفوذگری در سیستم‌های فردی- شبکه‌ای کنترل و بررسی شود.

-از ضرورت‌های ایجاد امنیت پایدار برای شبکه متصل به اینترنت، اجرای نرم‌افزارهای ضد جاسوسی[۸۱] و ضد برنامه های مزاحم تبلیغاتی[۸۲] به صورت منظم می‌باشد.

-نصب نرم‌افزارهای جدید باید نخست با هماهنگی مدیر ارشد شبکه به صورت آزمایشی بر روی یک دستگاه یا در صورت حساس و یا حیاتی بودن سازمان بهره‌بردار روی یک شبکه آزمایشی جداگانه انجام شود و سپس در صورت تأیید نهاد ذیربط بر روی ایستگاه های کاری مورد نظر نصب شود.

-بازدید از صفحات وب در اینترنت فقط مختص وظایف سازمانی و علایق کاری متخصص مربوط و فقط در قلمرو عملیات سازمان مجاز است. ضروری است عملکرد کاربران در این زمینه کنترل شود. همچنین لازم است این موضوع قبلاً به اطلاع کلیه کاربران رسیده باشد.

-می‌بایست با تهیه نسخ پشتیبان، در هنگام بروز اختلال در کارایی تجهیزاتی که می‌تواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه‌ترین زمان ممکن با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه به آخرین حالت بی‌نقص پیش از اختلال بازگردانده شود. مراحل بازگشت به آخرین وضعیت پایدار قبلی بر اساس طرح احیای سیستم(DRP)[۸۳] و حداکثر زمان مجاز خارج از سرویس بودن شبکه یا برخی از اجزای آن بر اساس الزامات طرح پیوستگی عملیات(BCP)[۸۴] معین خواهد گردید.

- می‌بایست سرویس‌های قابل ارائه توسط هر رایانه کنترل و بررسی گردد و سرویس‌های غیرضروری نظیر اشتراک فایل و چاپگر غیرفعال شود.

81- Anti Spyware

82- Anti Adware

83- Disaster recovery plan

84- Business continuity plan

- لازم است مدیر شبکه جهت امور روزانه از یک شناسه کاربری با سطح دسترسی عادی استفاده کرده و تنها در جهت انجام فعالیت‌هایی که نیاز به سطح دسترسی بالاتری می باشد، از شناسه کاربری خاص مدیریتی (حق دسترسی ممتاز) استفاده نماید.

- ردیابی و مشاهده فعالیت‌ها و ارتباطات کاربران باید برای دیگر کاربران غیرممکن باشد و همچنین پیام‌هایی که در شبکه ارسال و یا دریافت می‌شود باید به صورت مناسب برای جلوگیری از شنود رمزگذاری شود.

- هنگام ارسال پیام می‌بایست کاربران از صحت هویت و اصالت طرف مقابل اطمینان حاصل نمایند و مطمئن شوند که کاربری که با آن تماس گرفته‌اند واقعاً همان فردی است که انتظارش را داشته‌اند. همچنین ارسال کننده یک پیام نباید بتواند پیامی را که فرستاده انکار نماید. در صورتیکه تبادل پیام منجر به ایجاد تعهد قانونی برای طرفین تبادل شود لازم است اصالت طرفین، صحت پیام و عدم انکار از طریق استفاده از امضای الکترونیکی قابل پذیرش توسط مراجع قانونی وتجارت الکترونیک تضمین گردد.

- لازم است کلیدهای رمزنگاری اطلاعات در فواصل زمانی از پیش تعیین شده تغییر پیدا کند تا از افشاء و دسترسی غیرمجاز به اطلاعات جلوگیری گردد. همچنین لازم است از کلیدهای رمزنگاری فاقد اعتبار همانند کلیدهای رمزنگاری معتبر حفاظت و نگهداری شود زیرا ممکن است برای دسترسی مجدد به داده‌های رمزنگاری شده قدیمی مجدداً به آنها نیاز باشد.

- ممکن است سیاست‌های امنیتی، ابلاغ دستورالعمل و بخشنامه‌ها توسط کارکنان فرصت‌طلب یا سهل‌انگار با بی‌توجهی مواجه شود. به همین دلیل می‌بایست با بکارگیری ابزارهای احتمالی که نفوذگر برای نفوذ به شبکه استفاده می‌کند علیه شبکه، تجهیزات و سرویس دهنده‌های آسیب‌پذیر کشف گردند. ضروری است فرآیند فوق طی زمانبندی معین و با رعایت جنبه های قانونی، حقوقی و مدیریتی تکرار پذیرد.

- در مراکز حساس و حیاتی لازم است تمام رایانه‌ها و تجهیزات شبکه پلمپ شده و شماره‌گذاری شوند. افراد غیرمجاز حق باز کردن بدنه رایانه‌ها و تجهیزات شبکه را به هر منظوری ندارند.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا دسته بندی سازمان از دیدگاه پدافند غیرعامل مورد بررسی قرار می گیرد. همچنین در این مرحله به بررسی طبقه بندی حفاظتی و ارزش دارایی های اطلاعاتی در بخش های مختلف شبکه سازمان پرداخته می شود.

۲- بر اساس بررسی های صورت گرفته در مراحل قبل الزامات امنیتی در خصوص معماری شبکه، پیاده سازی و کنترل های لازم تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۳- با توجه به الزامات تدوین شده و همچنین بررسی های صورت گرفته در مرحله اول این فرآیند، پلان معماری شبکه طراحی می گردد. در این طراحی باید الزامات بیان شده در این سند (و احتمالاً الزامات اختصاصی سازمان) مورد توجه قرار گیرد.

۴- در این مرحله تامین مکانیزم ها، امکانات، تجهیزات مورد نیاز از قبیل فضا، سخت افزار، نرم افزار و ... بمنظور برآورده ساختن الزامات تدوین شده و پیاده سازی معماری طراحی شده صورت می‌پذیرد.

۵- پس از تامین موارد فوق در این مرحله معماری طراحی شده پیاده سازی و کلیه مکانیزم ها و الزامات تدوین شده اجرا خواهند شد.

۶- در صورتی که کلیه الزامات کنترل شبکه تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۵ بازگشت.

۵۰- مدیریت تغییرات:

هدف از تدوین این دستورالعمل مدیریت و کنترل تغییرات در وضعیت دارایی‌های اطلاعاتی موجود در قلمرو پیاده سازی سیستم امنیت اطلاعات اعم از جابجایی، تغییر متصدی، ارتقاء یا کاهش ظرفیت و یا تغییر در روش های کنترل دسترسی، مدیریت، راهبری و بهره برداری می‌باشد.

الزامات:

- لازم است تغییراتی که بنا به دلایل موجه یا به اجبار در وضعیت دارایی‌های اطلاعاتی اعم از نرم‌افزارها، سخت‌افزارها، زیرساخت‌های شبکه‌ای، فرآیندهای پردازشی، الگوهای رمزنگاری، سامانه‌های مدیریتی و منابع انسانی انجام می‌شود کنترل و با هماهنگی متصدی یا تحویل گیرنده دارایی اعمال شود.

-باید قبل از اعمال تغییرات در وضعیت دارایی‌های اطلاعاتی تحلیل ریسک مربوط به تغییر شرایط یا وضعیت ناشی از اعمال تغییرات ,ارزیابی ریسک صورت پذیرد. فقط در صورتی که نتایج تحلیل ریسک مثبت باشد انجام تغییرات مجاز خواهد بود.

- لازم است کلیه مراحل این دستورالعمل مستند شده و یک نسخه از آن بایگانی شود. این الزام حتی در مواردی که دستورالعمل در مراحل پیش از تغییر خاتمه می یابد نیز باید رعایت شود.

- در مراکزی که از نظر سازمان پدافند غیرعامل به عنوان مراکز مهم، حساس و یا حیاتی دسته‌بندی می‌شوند همه تغییرات باید رسماً در برگه درخواست تغییر، ثبت و جهت کسب موافقت به نهاد ذیربط ارسال شود.

فرآیند:

مراحل اجرای دستورالعمل مدیریت تغییرات به شرح زیر می باشد:

۱- در بررسی موضوعات ابتدا باید مشخص شود چه چیزی تغییر می‌کند و سپس به شناسایی تغییر اقدام نمود. درخواست کننده تغییر باید مطابق نمونه فرم تغییر یا تعویض در بخش پیوست مشخصات دارایی اطلاعاتی مورد نظر را بیان نماید. همچنین دلایل توجیهی درخواست تغییر بایستی اعلام و ثبت شود. این دلایل شامل مواردی نظیر حجم کار، موانع و مشکلات، عوامل انسانی و ... می‌باشد.

۲- باید در نظر داشت درخواست تغییر از جانب چه بخشی و یا چه کسی مطرح شده و چه دلایلی برای تغییر اعلام شده است. لازم است قبلاً افرادی که دارای مسئولیت و حق اعلام نظر در خصوص پذیرش یا عدم پذیرش تغییرات می باشند مشخص شده و کلیه تغییرات به تایید ایشان برسد. دلایل تأیید یا رد درخواست تغییرات باید در قالب گزارشی رسمی ثبت و سوابق آن نگهداری شود. همچنین فاکتورهایی نظیر تاثیر زمان بر شرایط تغییر و تاثیر تغییر بر موقعیت سازمان باید در نظر گرفته شود. در صورت عدم تایید تغییر خواسته شده باید اقدامات انجام شده تا این مرحله مستند شده و فرآیند خاتمه می یابد.

۳- در صورت تایید انجام تغییر توسط مراجع ذیصلاح باید ریسک حاصل از پیامدهای احتمالی تغییر بررسی شود. سپس در صورت قابل پذیرش بودن ریسک مجوز انجام تغییر صادر می‌شود. در صورت غیرقابل پذیرش بودن ریسک باید اقدامات انجام شده تا این مرحله مستند شده و فرآیند خاتمه می یابد.

۴- در گام بعد باید به چگونگی انجام تغییرات پرداخت، اینکه تغییرات مورد نظر نیاز به چه امکانات و تجهیزاتی دارد. بنابراین لازم است مراحل اجرای تغییرات برنامه‌ریزی شود. ممکن است فرآیند تغییر بخش بزرگی از دارایی‌های اطلاعاتی را در برگیرد و یا بر بخش بزرگی از دارایی‌های اطلاعاتی تأثیر گذارد. لازم است برنامه‌ریزی مدون و مکتوب شده و به امضای افراد ذیربط برسد. در صورتی که نیاز

به تغییر در نوع بهره برداری یا مشخصه های هر یک از دارایی‌های اطلاعاتی سازمان باشد باید هماهنگی لازم با مسئول یا متصدی آن دارایی اطلاعاتی انجام شود.

۵- در این مرحله به تامین امکانات و تجهیزاتی که برای انجام تغییر به آنها نیاز می‌باشد اقدام می‌گردد.

۶- در این مرحله تغییر مورد نظر انجام خواهد شد.

۷- پس از انجام تغییر باید رفتار سیستم تا مدت معینی که در تحلیل ریسک تعیین می شود پایش و کنترل شود.

۸- در صورتی که وضعیت پس از تغییر مطلوب ارزیابی شده و مورد قبول باشد و کلیه الزامات تدوین شده برآورده شده باشد باید کلیه مراحل انجام شده مستند سازی شده و پس از آن فرآیند خاتمه می یابد. در غیر اینصورت بایستی مرحله ۶ مجددا به اجرا درآید.

بطور کلی نهاد متصدی تغییرات به عنوان واحد مسئول تغییرات با استناد به مقررات، مصوبات، الزامات قانونی و نیز تغییرات محیطی، اقدامات لازم را در مورد بازنگری در وضعیت دارایی‌های اطلاعاتی درخواست می‌نماید. درخواست‌های ارائه شده باید متناسب با حجم فعالیت‌ها و نیازهای واقعی واحد مربوطه بوده و برای رفع مشکلات موقتی و ارتقاء شخصی نباشد.

۵۱- مدیریت تغییرات در خدمات اشخاص ثالث:

هدف از تدوین این دستورالعمل بیان ضرورت و چگونگی مدیریت تغییر در مدیریت شخص ثالث و همچنین تغییرات در نحوه ارائه، کیفیت و کمیت خدمات خریداری شده از اشخاص ثالث جهت ارائه یا پشتیبانی خدمات حوزه فناوری اطلاعات و ارتباطات می‌باشد.

الزامات:

- تغییر در کیفیت، کمیت و روش ارائه خدماتی که طی قرارداد مکتوب دریافت می شوند یا روش های اندازه گیری آنها و همچنین تغییر در مدیریت شخص ثالث باید به صورت مکتوب مستند شده و به امضای نمایندگان قانونی کارفرما و ارائه دهنده خدمات (که در قراردادها یا موافقتنامه ها به آنها اشاره می شود) برسد.

- لازم است هرگونه تغییر در کیفیت، کمیت و روش ارائه خدمات و همچنین تغییر در مدیریت شخص ثالث قبل از اجرایی شدن مورد ارزیابی قرار گرفته و اثرات احتمال آن در قالب تحلیل ریسک ارزیابی شود.

- در مراکز حیاتی (از دیدگاه سازمان پدافند غیرعامل) و فعالیتهای حیاتی مراکز حساس لازم است قبل از انجام هرگونه تغییر در نحوه ارائه خدمات، گزارش مکتوب ارزیابی ریسک تهیه و پس از کسب موافقت نهاد ذیربط به اجرا گذاشته شود.

- در صورتیکه لازم باشد اعمال تغییر به صورت اضطراری به اجرا گذاشته شود باید بلافاصله موافقت نهاد ذیربط و حداقل یک نفر از اعضای کمیته امنیت اطلاعات مطلع شده و به محض رفع شرایط اضطرار گزارش مکتوب به همراه ارزیابی ریسک تهیه و ارسال گردد.

- هنگام انجام هرگونه تغییر در نحوه ارائه خدمات لازم است تاثیر تغییر بر سایر فرآیندها و روش های ارائه خدمات و همچنین تاثیرپذیری بهره برداران و یا ارباب رجوع از خدمات تغییر یافته یا فرآیندها و روش هایی که تحت تاثیر قرار می گیرند مورد بررسی قرار گیرد.

- پس از انجام هرگونه تغییر لازم است رفتار سیستم تا مدت معینی (که بر اساس سطح ریسک تعیین خواهد شد) تحت کنترل مداوم باشد تا در صورت تشخیص احتمال وقوع شرایط ناخواسته اقدامات لازم به اجرا گذاشته شود.

- تاثیر هرگونه تغییر بر عناصر اصلی امنیت (محرمانگی، جامعیت و دسترسی پذیری) باید به صورت مجزا مورد ارزیابی قرار گیرد.

- لازم است روش های پایش خدمات به نحوی باشد که علاوه بر کیفیت و مقدار ارائه خدمات، نحوه ارائه خدمات را نیز تحت کنترل قرار داده و در صورت تغییر خارج از کنترل، اخطارهای لازم صادر شود.
- نحوه تنظیم قراردادهای برون سپاری یا خرید خدمات نباید به گونه ای باشد که امکان سوء استفاده از تفاوت جایگاه مراجع مختلف نظارتی (در خصوص تغییر روش های ارائه خدمات) وجود داشته باشد. به عنوان مثال لازم است مرجع تصویب صورت وضعیتها و پرداخت به پیمانکار همان باشد که صدور اجازه تغییر در نحوه ارائه خدمات، در حوزه وظایف وی قرار می گیرد.
- اطمینان یافتن از کفایت روشهای تهیه نسخه پشتیبان و بازگشت به حالت قبلی پیش از انجام تغییرات ضروری است.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در صورت نیاز به تغییر در کیفیت، کمیت و روش ارائه خدمات و یا روش های اندازه گیری آنها و همچنین تغییر در مدیریت شخص ثالث بایستی ریسک انجام تغییرات مورد نظر ارزیابی شده و مخاطرات آن برآورد شود. در ارزیابی ریسک باید به تاثیر تغییر بر دیگر فرآیندها، بهره برداران و یا ارباب رجوع توجه شود.

۲- در صورت غیرقابل پذیرش بودن ریسک ارزیابی شده تغییر مورد نظر انجام نیافته، مستندات مربوط به تحلیل ریسک تهیه شده و فرآیند خاتمه می یابد.

۳- در صورتی که ریسک انجام تغییر قابل پذیرش باشد پیش از تغییر باید از کلیه داده های مربوط به خدمت مورد نظر نسخه پشتیبان و قابل بازگشت تهیه نمود بنحوی که از قابلیت بازگشت به حالت پیش از تغییر اطمینان باشد.

۴- پس از پشتیبان گیری از اطلاعات و اطمینان از قابلیت بازگشت در این مرحله تغییرات مورد نظر اعمال خواهد شد.

۵- پس از انجام لازم است تغییر رفتار سیستم تا مدت معینی که بر اساس سطح ریسک تعیین می شود مورد پایش و کنترل قرار گیرد.

۶- اگر وضعیت پس از تغییر مورد قبول نباشد:

- در صورتی که قابل اصلاح باشد اصلاحات لازم در خصوص آن انجام شده و مجدداً وضعیت، مورد پایش و کنترل قرار می گیرد.
- در غیر اینصورت به حالت پیش از تغییر بازگشته، اقدامات صورت گرفته مستند شده و فرآیند خاتمه می یابد.

همچنین در صورت مقبول بودن وضعیت پس از تغییر، باید کلیه مراحل این فرآیند مستند شده و برای بهره برداری های آتی احتمالی نگهداری شود.

۵۲- مدیریت رسانه های ذخیره سازی اطلاعات:

هدف از تهیه این دستورالعمل استفاده از مجموعه‌ای از سیاست‌ها و راهکارها، ابزارها، سخت‌افزار و نرم‌افزار برای فراهم کردن محیط عاری از تهدید برای رسانه‌های ذخیره‌سازی اطلاعاتی می‌باشد.

الزامات:

-به منظور محافظت از اطلاعات در برابر افشای غیرمجاز یا هرگونه سوءاستفاده لازم است رویه‌های مربوط به حمل و نقل، جابجایی و ذخیره‌سازی اطلاعات در رسانه‌های ذخیره‌سازی مثل نوارهای مغناطیسی، دیسک‌های مغناطیسی، دیسک‌های نوری، حافظه‌های سخت و تراشه‌های ذخیره اطلاعات، تدوین شود و به اطلاع بهره‌برداران از این نوع دارایی‌های اطلاعاتی برسد.

- ضروری است نسبت به حفظ و تأمین امنیت رسانه‌های ذخیره‌سازی اطلاعات، که در داخل سازمان و یا هر یک از مؤسسات و نهادهای برون سازمانی مبادله می‌شود، اقدام گردد.

-می‌بایست دسترسی به رسانه‌های ذخیره‌سازی اطلاعات بر اساس الزامات کاری و امنیتی باشد. خط مشی‌های مربوط به اشاعه اطلاعات و محورهای مربوط باید در قوانین کنترل و دسترسی لحاظ گردد. همچنین لازم است کلیه رویه‌ها و سطوح مجوزدهی به دقت مستندسازی شود.

- تعیین و اجرای رویه‌های کنترل و نظارت مضاعف بر نگهداری و مدیریت رسانه‌هایی که قابل پاک شدن یا بازنویسی هستند، لازم و ضروری است.

-لازم است در مراکز حساس و حیاتی هر یک از رسانه‌های ذخیره‌سازی اطلاعات از هنگام تهیه (برای استفاده در سازمان) دارای شناسنامه بوده و به یک فرد معین (تحویل گیرنده، متصدی، مالک) تحویل شود.

-ضروری است کلیه اطلاعات بر اساس دستورالعمل طبقه‌بندی دارایی‌های اطلاعات طبقه‌بندی شده و اطلاعات دارای طبقه‌بندی حفاظتی موجود در رسانه‌های ذخیره‌سازی اطلاعات رمزنگاری شود و تنها کسانی که جازه دسترسی به ابزار گشاینده رمز مورد نظر را دارند، بتوانند به آن اطلاعات دسترسی داشته باشند.

-می‌بایست رسانه‌های ذخیره‌سازی حاوی اطلاعات دارای طبقه‌بندی، هنگام تعمیر تحت نظارت باشند و در هنگام دور انداختن رسانه‌های ذخیره‌سازی اطلاعات باید هرگونه اطلاعات صرف نظر از حساس بودن یا نبودن پاک شود و یا از بین برود.

-ضروری است از اطلاعات موجود در رسانه‌های ذخیره‌سازی قبل از جابجایی پشتیبان‌گیری انجام شود تا در صورت تخریب اطلاعات به هر دلیل بلافاصله امکان جایگزین نمودن اطلاعات پشتیبان‌گیری شده وجود داشته

باشد. تهیه نسخه پشتیبان باید با توجه به رعایت دستورالعمل طبقه‌بندی دارایی‌های اطلاعاتی و پشتیبان‌گیری نجام شود.

- لازم است محل نگهداری رسانه‌های ذخیره‌سازی قابل جابجایی به صورت فیزیکی در برابر هرگونه دسترسی غیرمجاز، خسارت و تداخل محافظت گردد.

- باید برای دسترسی و استفاده از اطلاعات دارای طبقه‌بندی حفاظتی موجود روی دستگاه‌های ذخیره‌سازی قابل جابجایی همواره از کلمه عبور استفاده شود.

- ضروری است کلیه عملیات ورود اطلاعات، مشاهده اطلاعات و عملیات مدیریت و امنیت اطلاعات بر روی رسانه‌های ذخیره‌سازی اطلاعات و نظایر آن به شکل یک تراکنش (Log) در سیستم ثبت شود، بنحوی که بعداً قابل پیگیری باشد که چه کسانی و در چه زمانهایی، چه عملیاتی را انجام داده و چه اطلاعاتی را بر روی رسانه مورد نظر تغییر داده‌اند. بازبینی سوابق دسترسی به رسانه‌های ذخیره‌سازی اطلاعات می‌بایست بر طبق فواصل زمانی از پیش تعیین شده صورت گیرد.

- لازم است درخواست خرید، ایجاد و یا تغییرات سخت‌افزار و نرم‌افزارهای در ارتباط با رسانه‌های ذخیره‌سازی اطلاعات از دیدگاه امنیت شبکه، آسیب‌پذیری‌های سیستم و یا سرویس موردنظر و مشکلات امنیتی ناشی از بکارگیری آن در سایر بخش‌ها و در نهایت تصمیم‌گیری در خصوص تأیید یا رد درخواست اقدامات لازم صورت گیرد.

- کلیه رسانه‌های ذخیره‌سازی باید تحت شرایط ایمنی تعیین شده از طرف سازنده نگهداری شوند و امنیت مکان نگهداری تأمین شود.

-انتقال رسانه‌های ذخیره‌سازی قابل حمل به خارج از محیط کاری یا رسانه‌های ذخیره‌سازی متعلق به خارج از سازمان به داخل محیط کاری بایستی تحت کنترل بوده و به صورت مستند ثبت شود.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا الزامات امنیتی و رویه های مدیریت رسانه های ذخیره سازی اعم از نگهداری، حمل و نقل، جابجایی و ذخیره سازی اطلاعات در آنها تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- پس از تدوین الزامات و رویه ها در این مرحله به تامین مکانیزم ها، امکانات و تجهیزات مورد نیاز از قبیل سخت افزارها و نرم افزارهای لازم جهت برآورده ساختن الزامات و رویه های تدوین شده اقدام می شود.

۳- در این مرحله پیاده سازی مکانیزم ها و اجرای کلیه الزامات و رویه های تدوین شده صورت می‌پذیرد.

۴- در صورتی که کلیه الزامات مدیریت رسانه های ذخیره سازی تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر این صورت بایستی به مرحله ۳ بازگشت.

۵۳- مدیریت ظرفیت:

هدف از تدوین این دستورالعمل اطمینان از کارایی دارایی‌های اطلاعاتی موجود در قلمرو پیاده سازی نظام مدیریت امنیت اطلاعات در پاسخگویی به تقاضاهای موجود و آینده کاربران برای پردازش، ذخیره‌سازی و یا انتقال داده و همچنین مدیریت ظرفیت[۸۵] به منظور حفظ پایداری سیستم در کلیه شرایط کاری می باشد.

الزامات:

- هنگام برآورد ظرفیت، لازم است الزامات طرح پیوستگی عملیات (BCP) در نظر گرفته شده و رعایت شود.

- لازم است بر اساس طرح پیوستگی عملیات (BCP)[۸۶] و با توجه به نیازهای از پیش تعیین شده فعلی و آتی انتخاب صحیحی از موارد زیر انجام شود:

- ظرفیت پردازش شامل:

- توان پردازش مورد نیاز (سرعت پردازنده)

- پهنای باند داده‌ها (گذرگاه داده)

- ظرفیت رسانه ذخیره‌سازی شامل:

- ذخیره سازی دائم:

- مغناطیسی مثل دیسک نرم، دیسک سخت، فلش

- نوری مثل سی‌دی، دی وی دی و بلو- ری

[85]- Capacity Management

[86] - Business Continuity Plan

- ذخیره سازی موقت:

- حافظه نهان

- RAM

- ظرفیت مخابراتی (پهنای باند) شامل:

- ظرفیت لازم برای ایجاد شبکه محلی (LAN)

- ظرفیت لازم برای اتصال به شبکه‌های عمومی (مثل اینترنت)

- ظرفیت لازم جهت اتصال دو یا چند شبکه محلی

- ظرفیت‌های فضا: استقرار و حفاظت تجهیزات)

- ظرفیت‌های تهویه:(امکانات پشتیبانی)

- ظرفیت تامین توان الکتریکی: امکانات پشتیبانی)

- برای مشخص کردن ظرفیت های مورد نیاز لازم است به موارد زیر دقت شود:

- نیاز متوسط فعلی: متوسط نیاز به ازای هر کاربر

- نیاز کلی فعلی: مجموع متوسط نیازهای فعلی

- پیش‌بینی نیازهای امنیتی: مقدار نیاز اضافی کاربران برای ایجاد امنیت

- پیش‌بینی اوج مصرف: پیش‌بینی حداکثر تعداد کاربران × حداکثر نیاز کاربران

- پیش‌بینی تقاضای آینده: پیش‌بینی افزایش تعداد کاربران در آینده و یا افزایش تقاضای ایشان بر اساس برنامه های توسعه‌ای

- لازم است ظرفیت های تخمین زده شده در اسرع وقت تامین گردد. در صورت عدم امکان تامین سریع ظرفیت، لازم است برنامه زمانبندی شده آن توسط (((**مدیر ارشد شبکه**))) تهیه و برای تصویب به کمیته امنیت اطلاعات تسلیم گردد.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- در ابتدا لازم است لیستی از دارایی های اطلاعاتی که ظرفیت آنها باید بررسی شود تهیه گردد. نمونه ای از این دارایی ها عبارتند از:

- دارایی های پردازشی
- رسانه های ذخیره سازی
- کانال های ارتباطی
- فضا

۲- بمنظور تخمین دقیق تر از ظرفیت های لازم باید طرح پیوستگی عملیات مطالعه شده و نیازهای از پیش تعیین شده مورد توجه قرار گیرد.

۳- در این مرحله ظرفیت دارایی های اطلاعاتی و تسهیلات پشتیبانی آنها توسط مدیر ارشد شبکه تخمین زده و برآوردی از میزان آن محاسبه می گردد.

۴- در صورتی که ظرفیت تخمین زده شده مورد تایید کمیته امنیت اطلاعات نباشند باید مرحله ۳ مجددا به اجرا در آید.

۵- پس از تایید کمیته امنیت اطلاعات، در صورتی که همه ظرفیت های لازم و تسهیلات پشتیبانی آنها تخمین زده شده باشند این فرآیند خاتمه می یابد در غیر اینصورت بایستی مجددا به مرحله ۱ بازگشت.

۵۴- واقعه نگاری خرابی:

هدف از تدوین این دستورالعمل بیان ضرورت ثبت و رسیدگی به خطاهای نرم افزاری یا خرابی های تجهیزات موجود در قلمرو پیاده سازی نظام مدیریت امنیت اطلاعات به منظور پیشگیری از تبدیل وقایع کوچک به بحران های بزرگ می باشد.

الزامات:

- لازم است کلیه اشتباهات[۸۸]، خرابی ها[۸۹] و خطاهای[۹۰] بروز یافته هنگام بکارگیری دارایی های اطلاعاتی تحت کنترل قرار گرفته و بر اساس سیاست گذاری مدیریت حوادث امنیت اطلاعات مورد رسیدگی قرار گیرد.
- سوابق کلیه خطاها باید به صورت رسمی ثبت شده و مراحل رسیدگی و رفع آنها مستند شود.
- به دلیل آنکه ممکن است خطا به دلیل کوتاهی افراد در انجام فعالیت های محوله و یا در اثر صدمه عمدی به سیستم حادث شود لازم است در مراکز و سازمان های حساس و حیاتی و یا بخش های حساس و حیاتی سایر مراکز و سازمان ها، مراحل و روش های ثبت سوابق مربوط به آن منطبق بر الزامات قانونی باشد تا بتوان هنگام مراجعه به مراجع قضایی به آنها استناد نمود.

فرآیند:

88 - Error

89 - Failure

90 - Faults

۱- در ابتدا کلیه الزامات در خصوص چگونگی و مراحل ثبت، گزارش و رسیدگی به خطا تدوین می‌شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- پس از تدوین الزامات، مکانیزم‌ها و امکانات مورد نیاز از قبیل تجهیزات سخت‌افزاری و نرم‌افزارها تامین می شوند. همچنین در صورت نیاز فرم های مربوط نیز در این مرحله تدوین می شوند.

۳- در صورت وقوع خرابی، مطابق با الزامات تدوین شده، خرابی ثبت می گردد.

۴- پس از ثبت خرابی بایستی گزارش مربوط به مراجع ذیصلاح همچون مدیر ارشد شبکه ارائه گردد.

۵- با توجه به امکان وجود چندین خرابی در یک زمان رسیدگی به خطاها تعیین اولویت می شوند که این کار توسط مدیر ارشد شبکه صورت می گیرد.

۶- در این مرحله بایستی خطای رخ داده بررسی شده و مورد تحلیل قرار گیرد و علل رخداد، چگونگی رفع آن و دیگر موارد مربوط به آن شناسایی و مشخص گردند.

۷- پس از تحلیل بایستی اقدام مناسب در جهت رفع یا اصلاح خطا صورت پذیرد.

۸- در صورتی که کلیه الزامات واقعه نگاری خرابی های تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد باید اقدامات صورت گرفته در کلیه مراحل ثبت واقعه، گزارش، رسیدگی و رفع خطا مستند شده و سوابق آنها نگهداری شود. در غیر اینصورت بایستی به مرحله ۵ بازگشت.

۵۵- واقعه نگاری ممیزی:

هدف از تدوین این دستورالعمل الزام سازمان به ثبت[۹۱] و نگهداری رویدادهای سیستم، فعالیت کاربران و وقایع امنیت اطلاعات برای یک بازه زمانی توافق شده است تا از وجود روشی برای پیگیری و بررسی تراکنش های

1- Logging

کاربران و سامانه ها به منظور ممیزی[۹۲] و یافتن دلایل وقایع و حوادث ناقض امنیت دارایی های اطلاعاتی اطمینان حاصل شود.

الزامات

- کلیه وقایع دیجیتالی و غیردیجیتالی مهم مرتبط با فعالیت و بهره برداری از دارایی های اطلاعاتی اعم از موارد زیر باید ثبت شود:

- نصب یا برداشتن نرم افزارها یا قطعات
- پیکربندی نرم افزارها، سخت افزارها و یا شبکه ها
- دسترسی، صدور و یا ابطال مجوزهای آن
- نگهداری، خرابی یا تعمیر دارایی های اطلاعاتی
- ورود و خروج دارایی های اطلاعاتی
- ورود و خروج افراد به مراکز داده یا مکان‌های نگهداری دارایی‌های اطلاعاتی دارای طبقه‌بندی حفاظتی
- آغاز یا پایان کار دارایی های اطلاعاتی
- تهیه نسخه پشتیبان یا بازخوانی اطلاعات
- نصب یا عزل متصدیان کار با دارایی های اطلاعاتی بخصوص افرادی که دارای دسترسی ممتاز[۹۳] به هر یک از دارایی های اطلاعاتی می باشند
- تبادل اطلاعات هر دارایی اطلاعاتی با سایر دارایی های اطلاعاتی

[2-] Audit

[93]- Privilege Access

- کمیته امنیت اطلاعات باید وقایع دیجیتالی و غیردیجیتالی مهم را با توجه به نیازهای سازمانی و دسته بندی سازمان از دیدگاه پدافند غیرعامل تعیین نماید.

- فرم های لازم جهت ثبت وقایع دیجیتال و یا غیر دیجیتالی باید با توجه به نیازهای سازمانی و دسته بندی سازمان از دیدگاه پدافند غیرعامل تدوین شود.

- در مراکزی که از طرف سازمان پدافند غیرعامل به عنوان مراکز حساس و حیاتی دسته بندی می شوند باید کلیه تجهیزات و نرم افزارهایی که برای ارائه خدمات رایانه ای به کار گرفته می شوند مجهز به قابلیت ثبت وقایع باشند و یا از طریق طرح معماری شبکه یا سیستم کنترل دسترسی به نحوی پشتیبانی شوند که امکان رهگیری دسترسی و فعالیت آنها وجود داشته باشد.

- روش های ثبت و پایش فعالیت ها باید منطبق بر قوانین کشور جمهوری اسلامی ایران، به خصوص مواد مرتبط با حفظ حریم خصوصی افراد باشد.

- در صورتیکه بهره برداری از دارایی های اطلاعاتی به صورت مشترک (بین سازمانی) انجام می شود لازم است توافقنامه های تبادل اطلاعات به نحوی تنظیم شوند تا اولاً مفاد دستورالعمل ۲-۱-۷(ارتباط با سایر مراجع، سازمان ها و نهادهای دارای اشتراک منافع) رعایت شده و ثانیاً همه طرف ها ملزم به ثبت وقایع بر اساس روشی توافق شده باشند.

- لازم است قبلاً در خصوص ثبت فعالیت کاربران و پایش فعالیت های ایشان، اطلاع رسانی کافی انجام شود، به طوری که کاربران از پایش فعالیت های خود آگاه باشند.

- به منظور نظارت بر استفاده از دارایی‌های اطلاعاتی باید فرآیندهایی جهت پایش[۹۴] ایجاد شوند و اطلاعات ثبت شده بر اساس آن بطور منظم مرور شوند.

- برای پاسخگویی کاربران در برابر عملکردشان، ثبت فعالیت‌های آنان ضروری است. روش ثبت فعالیت باید به نحوی باشد که عدم انکار[۹۵] آن تضمین شود.

- ممیزی سیستم می بایست به نحوی باشد تا منجر به شناسایی هرگونه حملات موفق یا غیرموفق علیه امنیت اطلاعات شود. بررسی رویدادهای ناموفق برای دنبال کردن رد نفوذ و حمله اهمیت دارد.

- روش شناسایی، نگهداری، حفظ و ارائه مدارک ثبت شده، باید به نحوی باشد که بر اساس آنها ثبت وقایع به نحوی مدیریت شود که اطلاعات قابل استناد و در طول دوره توافق شده (همچنین در صورت بایگانی شدن در طول دوره بایگانی) در دسترس، قابل استخراج و حفاظت شده در برابر هرگونه صدمات سهوی یا عمدی باشند.

- ساعت کلیه تجهیزات و رایانه ها باید به منظور ثبت دقیق وقایع، براساس دستور العمل ۶-۱۰-۶ (همزمان‌سازی[۹۶] ساعت ها) تنظیم شده باشند.

- جامعیت اطلاعات ثبت شده در کلیه مراحل واقعه نگاری ممیزی باید از طریق مکانیزم های حفاظتی مثل رمزنگاری یا امضای الکترونیک گواهی شده تضمین شود.

- در صورتی که واقعه نگاری برای کاربردهای درون سازمانی انجام می شود، استحکام و کفایت الگوریتم های مورد استفاده در رمزنگاری باید قبلاً به تایید کمیته امنیت اطلاعات رسیده باشد.

[4-] Monitoring

[95]- Non-repudiation

[96]- Synchronize

- در صورتی که واقعه نگاری برای کاربردهای برون سازمانی انجام می شود و یا هدف از آن بهره برداری احتمالی در مراجع قضایی باشد لازم است روش جمع آوری و حفاظت داده ها منطبق بر قانون تجارت الکترونیک در خصوص داده پیام و امضای الکترونیک باشد.

- لازم است دسترسی به اطلاعات ثبت شده برای واقعه نگاری ممیزی از طریق رویه های کنترل دسترسی محدود و مدیریت شود.

- در مراکز حساس و حیاتی لازم است ثبت رویدادها بر اساس نیازهای ممیزی دسته بندی شود تا در آینده بررسی، پایش و رسیدگی به اطلاعات ثبت شده کاراتر باشد.

- ضروری است به منظور حفظ امنیت در برابر دسترسی های غیرمجاز، فقط افرادی که دارای کلمه عبور هستند، مجاز به دستیابی به واسط های ورود به سیستم و مشاهده اطلاعات واقعه نگاری باشند.

- اطلاعات مندرج در گزارش‌ها یا فهرست ثبت وقایع سیستم باید طبقه‌بندی شوند. رده حفاظتی گزارش یا فهرست ثبت وقایع باید حداقل یک رده سخت‌گیرانه‌تر از دارایی های اطلاعاتی موضوع گزارش گیری باشند.

فرآیند

مراحل اجرای این دستورالعمل به شرح زیر می باشد:

۶- در مرحله اول این فرآیند لازم است کلیه فعالیت هایی که باید ثبت شوند شناسایی و لیستی از آنها تهیه شود.

۷- مشخص کردن سطح مناسب ثبت وقایع و ممیزی سیستم بخش مهمی از تدوین استراتژی امنیتی را تشکیل می‌دهد که در این مرحله انجام می شود. علاوه بر این در این مرحله کلیه الزاماتی که در این فرآیند باید رعایت شوند تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی خود باشد الزامات مورد نظر نیز به موارد بیان شده در این سند افزوده خواهند شد.

۸- پس از تدوین الزامات و سطح ثبت واقعه نگاری در این مرحله به تامین مکانیزم ها و امکانات مورد نیاز و تدوین فرم های لازم جهت برآورده سازی الزامات اقدام می شود.

۹- در این مرحله بر اساس مکانیزم های تامین شده و در راستای برآورده نمودن الزامات تدوین شده ثبت واقعه صورت می پذیرد.

۱۰- پس از ثبت وقایع، آنها را بر اساس نیازهای ممیزی دسته بندی کرده تا در آینده بررسی، پایش و رسیدگی به اطلاعات ثبت شده کاراتر باشد.

۱۱-در این مرحله با توجه به واقعه ثبت شده گزارش های تحلیلی تهیه و برای بررسی در اختیار مسئولین مربوطه قرار می گیرد. گزارش های تحلیلی مسئولین مربوط را قادر می سازند تا در صورت مشاهده موارد مشکوک و غیرعادی بتوانند به اطلاعات لازم برای یافتن دلایل وقایع یا حوادث امنیت اطلاعات دست یابند.

۱۲-پس از بررسی در صورت مشاهده موارد مشکوک لازم است تا اقدامات لازم انجام شود.

۱۳-در صورتی که پس از بررسی مشخص شود کلیه الزامات تدوین شده برآورده شده است فرآیند خاتمه می یابد در غیر اینصورت نیاز است جهت برآورده نمودن کلیه الزامات به مرحله ۴ بازگشت.

۵۶- همزمان سازی ساعت ها:

هدف از تدوین دستورالعمل فوق الزام به یکسان سازی ساعت‌های تمامی سیستم‌های پردازش اطلاعات موجود در شبکه بر اساس یک منبع زمانی دقیق و توافق شده می‌باشد.

الزامات:

- لازم است جهت صحت گزارش فعالیت‌های انجام شده در شبکه (log گیری)، ساعت‌های سیستم با منبعی موثق و توافق شده همزمان گردد.

- در صورت احتمال استفاده از گزارش‌های تولید شده در پیگردهای قضایی لازم است منبع مرکزی اعلان زمان (ساعتی که ساعت تجهیزات پردازشی بر اساس آن تنظیم می‌شود) به نحوی انتخاب و مدیریت شود که صحت آن مورد قبول مراجع قضایی یا قانونی باشد.

- ضروری است تدابیری در جهت جلوگیری از تغییر ساعت سیستم‌ها در نظر گرفته و از مکانیزمی استفاده شود که در صورت دستکاری یا تغییر سهوی یا عمدی زمان، نهاد ذیربط مطلع گردد.

- لازم است ساعت سیستم‌ها طبق زمانبندی تعیین شده ممیزی و در صورت عدم تطابق با ساعت مرکزی، مراتب جهت تنظیم ساعت و بررسی علت به اطلاع نهاد ذیربط برسد.

- می‌بایست پروتکل‌های وابسته به همزمانی ساعت همانند NTP در برابر انواع حملات خرابکارانه از بیرون یا داخل مرکز حفاظت گردد.

- امکان تنظیم اتوماتیک یا دستی ساعت سیستم توسط کاربر باید غیرفعال گردد.

- ساعت سیستم‌های پردازش اطلاعات باید تنها توسط سرویس دهنده مرکزی ساعت قابل تغییر باشد.

فرآیند:

مراحل انجام این دستورالعمل به شرح زیر می باشد:

۱- ابتدا الزامات امنیتی همزمان سازی ساعت سیستم های سازمان تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

۲- انتخاب منبع زمانی دقیق یکی از مهمترین مراحل اجرای این فرآیند می باشد لذا باید یک منبع زمانی دقیق توسط مدیر ارشد شبکه شناسایی شده و پس از انجام توافقات لازم با نهاد ذیربط منبع زمانی تامین شود.

۳- پس از انتخاب منبع زمانی دقیق در این مرحله مکانیزم ها و امکانات مورد نیاز اعم از تجهیزات سخت افزاری یا نرم افزارهای مورد نیاز جهت برآورده ساختن الزامات تدوین شده و همچنین بکارگیری منبع زمانی تامین می شود.

۴- پس از تامین مکانیزم ها و امکانات در این مرحله به پیاده سازی مکانیزم ها و بهره برداری از منبع زمانی اقدام می شود.

۵- در صورتی که کلیه الزامات همزمان سازی ساعت های تدوین شده (بیان شده در این سند و الزامات اختصاصی سازمان) برآورده شده باشد این فرآیند خاتمه می یابد. در غیر اینصورت بایستی به مرحله ۴ بازگشت.

من الله التوفیق