ین م سـ تند بخ شی از ک تاب در شرف انتشار آشنایی با ISMS (سیستم مدیریت امنیت اطلاعات) و استانداردهای امنیتی ISO27001 و ISO27002 نوشته حیدر علی کورنگی است و مطالعه آن صرفا برای شرکت کنندگان در سمینارهای شبکه علمی مجاز است. چاپ و تکثیر این مستند غیر مجاز است . www.newtechnology.ir

استاندارد بین المللی ISO/IEC27002

نام کامل استاندارد : BS ISO/IEC 27002:2005

تاریخ آخرین اصلاحات : **۳۱ ژوئیه ۲۰۰۷**

۱- دامنه

از استاندارد بین المللی حاضر می توان به عنوان یک راهنمای عملی برای تدوین استانداردهای امنیتی سازمانی و رویه هـای مـوثر مدیریت امنیت استفاده نمود و به این ترتیب از فعالیت های بین سازمانی اطمینان حاصل نمود.

۳- استاندارد بین المللی حاضر

استاندارد حاضر مشتمل بر ۱۱ ماده درباره امنیتی است و در مجموع شامل ۳۹ مقوله اصلی امنیت و یک ماده مقدماتی است کـه در آن به معرفی ارزشیابی ریسک و نحوه مقابله و برخورد با آن پرداخته می شود.

۱-۳- مواد

هر ماده مشتمل بر چندین مقوله اصلی امنیت است. این ۱۱ ماده (به همراه تعدادی از مقولات اصلی امنیت که در هر ماده گنجانده شده است) عبارتند از :

الف) خط مشی امنیت (۱) ؛

ب) ساختار امنیت اطلاعات (۲) ؛

پ) مدیریت دارایی ها(۲) ؛

ت) امنیت منابع انسانی (۳) ؛

ث) امنیت فیزیکی و پیرامونی (۲) ؛

ج) مدیریت ارتباطات و عملیات (۱۰) ؛

ح) دسترسی (۷) ؛

خ) اکتساب سیستم های امنیت اطلاعات ، توسعه و نگهداری (۲) ؛

چ) مدیریت رویداد امنیت اطلاعات (۲) ؛

د) مدیریت استمرار تجارت (۱) ؛

ذ) انطباق (۳) .

۵- خط مشی امنیت

۱-۵- خط مشی امنیت اطلاعات

هدف : جهت بخشیدن به مدیریت و حمایت از امنیت اطلاعات بر اساس الزامات کاری و قوانین و مقررات مربوطه.
مدیریت ملزم خواهد بود تا ضمن یک سیاستگذاری مشخص بر اساس اهداف کاری ، پشتیبانی و تعهد خود امنیت اطلاعات را از طریق انتشار و پایبندی به خط مشی امنیت اطلاعات در کل سازمان به اثبات رساند.

۱-۱-۵- سند خط مشی امنیت اطلاعات

سند خط مشی امنیت اطلاعات باید توسط مدیریت تایید ، انتشار و به تمامی کارکنان و گروه های ذی ربط برون سازمانی ابلاغ گردد.

۲-۱-۵- بازنگری خط مشی امنیت اطلاعات

خط مشی امنیت اطلاعات باید در فواصل زمانی برنامه ریزی شده مورد بازنگری قرار داده شود تا اگر تغییرات قابل توجهی در آن ایجاد شده است ، از حفظ شایستگی ، کفایت و اثربخشی آن اطمینان حاصل شود.

۶- ساختار امنیت اطلاعات

۱-۶ ساختار داخلی

هدف : مدیریت امنیت اطلاعات در داخل سازمان.

هر گونه اقدام در جهت شروع و بر اجرای امنیت اطلاعات در داخل سازمان، مستلزم ایجاد یک چهارچوب مدیریتی خواهد بود. مدیریت ملزم خواهد بود تا ضمن تایید خط مشی امنیت اطلاعات ، نقش های امنیت را تعیین و اجرای امنیت در داخل سازمان را هماهنگ و مورد بازنگری قرار دهد.

بر حسب لزوم ، یک بانک اطلاعاتی حاوی مشاوره های تخصصی درباره امنیت اطلاعات باید تشکیل و ایجاد گردد و در سطح سازمان در دسترس قرار داده شود. توسعه سطح برقراری ارتباطات با متخصصین امنیت یا گروه های ذیربط در خارج از سازمان از جمله مقامات ذیربط در راستای بروز نگه داشتن روندها و روش های صنعتی، نظارت بر استانداردها و روش های ارزشیابی و پیدا کردن نقاط ارتباطی مناسب در زمان مقابله با رویدادهای امنیت اطلاعات الزامی می باشد. در این ارتباط، اتخاذ یک رویکرد چند رشته ای (multi-disciplinary) در رابطه با امنیت اطلاعات توصیه می شود.

۱-۱-۶ تعهد مدیریت به امنیت اطلاعات

مدیریت ملزم خواهد بود ضمن آن که بطور فعالانه و از طریق دستورالعمل های مشخص از امنیت در داخل سازمان حمایت و پشتیبانی می نماید ، تعهد خود را نسبت به آن به اثبات برساند و وظایف را صراحتاً تعیین نماید و مسئولیت ها در حوزه امنیت اطلاعات را مورد تایید قرار دهد.

۲-۱-۶ هماهنگی امنیت اطلاعات

فعالیت های امنیت اطلاعات باید توسط نمایندگان بخش های مختلف سازمان و با توجه به نقش ها و وظایف شغلی هماهنگ گردد.

۳-۱-۶ تعیین مسئولیت های امنیت اطلاعات

تمامی مسئولیت های امنیت اطلاعات باید به طور واضح تعریف و مشخص گردد.

۵-۱-۶ موافقت نامه های حفظ محرمانگی

الزامات مربوط به موافقت نامه های حفظ محرمانگی یا عدم افشای اطلاعات که بیانگر نیازهای سازمان به محافظت از اطلاعات می باشد باید تعیین و مشخص شده و بطور منظم مورد بازنگری قرار داده شود .

۶-۱-۶ ارتباط (تماس) با مقامات مسئول

حفظ روابط مناسب با مقامات ذیربط لازم و ضروری می باشد.

۷-۱-۶ ارتباط با گروه های ذینفع خاص

حفظ ارتباطات مناسب با گروه های ذینفع خاص یا سایر تشکیلات امنیتی تخصصی و انجمن های حرفه ای لازم و ضروری می باشد.

۶-۱-۸ بازنگری مستقل امنیت اطلاعات

رویکرد سازمان نسبت به مدیریت امنیت اطلاعات و نحوه اجرای آن (به عبارت دیگر ، اهداف کنترلی ، اقدامات کنترلی ، خط مشی ها ، فرآیندها و رویه های امنیت اطلاعات) باید به صورت مستقل و در فواصل زمانی معین و برنامه ریزی شده و یا در مواقعی که تغییرات عمده و قابل ملاحظه در اجرای امنیت ایجاد می شود ، مورد بازنگری قرار گیرد.

۶-۲ شرکای برون سازمانی

هدف : حفظ امنیت اطلاعات سازمان و مراکز پردازش اطلاعاتی که در دسترس اشخاص برون سازمانی قرار می گیرند، توسط ایشان پردازش ، منتشر یا مدیریت می شوند .

میزان امنیت اطلاعات سازمان و مراکز پردازش اطلاعات نباید بواسطه معرفی محصولات یا خدمات اشخاص برون سازمانی کاهش یابد.

چنانچه بر مبنای الزامات کاری ، لزوم همکاری با اشخاص برون سازمانی مستلزم دسترسی به اطلاعات سازمان یا مراکز پردازش اطلاعات یا مستلزم دریافت یا تامین کالا یا خدمات از سوی اشخاص برون سازمانی باشد ، انجام ارزشیابی ریسک به منظور تعیین مفاهیم و مضامین امنیت و الزامات لازم و ضروری خواهد بود. انجام اقدامات کنترلی باید در قالب یک موافقت نامه با اشخاص برون سازمانی تعریف و مورد توافق قرار گیرد.

۶-۲-۱ تشخیص ریسک های مربوط به شرکای برون سازمانی

ریسک های مترتب بر اطلاعات سازمان و مراکز پرداز اطلاعات که ناشی از فرآیندهای تجاری انجام شده توسط اشخاص برون سازمانی می باشد ، باید تعیین و قبل از هرگونه امتیاز دسترسی اقدامات کنترلی لازم به مورد اجرا گذاشته شود.

۶-۲-۲ توجه به موضوع امنیت در زمان رسیدگی به مشتریان

قبل از هرگونه اقدام در خصوص دادن مجوز دسترسی به اطلاعات یا دارایی های سازمان از سوی مشتریان، لازم خواهد بود تا تمام الزامات امنیتی شناخته شده مورد بررسی و رسیدگی قرار داده شوند.

۶-۲-۳ توجه به موضوع امنیت در قراردادهای شخص ثالث

موافقت نامه های منعقده با اشخاص ثالثی که به نحوی از انحاء در دسترسی ، پردازش ، انتشار یا مدیریت اطلاعات سازمان یا مراکز پردازش اطلاعات یا اضافه کردن محصولات یا خدمات به مراکز پردازش اطلاعات دخالت دارند باید متضمن تمامی الزامات امنیتی مربوطه باشند.

۷- مدیریت اموال

هدف : انجام اقدامات لازم در جهت محافظت از اموال سازمان.

تمامی اموال باید دارای شناسنامه بوده و دارای یک صاحب و مالک مشخص (اسمی)باشند.

صاحبان هر یک از اموال باید مشخص و مسئولیت ایشان در قبال انجام اقدامات کنترلی لازم تعیین شده باشد. صاحب هر یک از این اموال می تواند مسئولیت اجرای اقدامات کنترلی خاص را بر حسب مورد واگذار نماید ، اما این واگذاری موجب سلب مسئولیت وی در قبال محافظت صحیح از اموال نخواهد شد.

۷-۱- مسئولیت در قبال اموال

۷-۱-۱ صورت اموال

تمامی اموال باید به صورت کامل ومشخص شناسایی شده باشد و فهرستی از موجودی کلیه دارایی های مهم تنظیم و به نحو مقتضی نگهداری گردد.

۷-۱-۲ مالکیت اموال

مالکیت تمامی اطلاعات و دارایی های مربوط به مراکز پردازش اطلاعات باید توسط یک بخش مشخص از سازمان بعهده گرفته شود.

۷-۱-۳ استفاده قابل قبول از دارایی ها

قوانین مربوط به استفاده قابل قبول از اطلاعات و دارایی های مربوط به مراکز پردازش اطلاعات باید علاوه بر تعیین ، می بایست مستندسازی و به مورد اجرا گذاشته شود.

۷-۲- طبقه بندی اطلاعات

هدف : حصول اطمینان از این که اطلاعات سازمان در حد قابل قبول و به نحو مقتضی مورد محافظت قرار داده می شوند.

اطلاعات باید بگونه ای طبقه بندی شود که میزان نیاز به آنها ، اولویت ها و سطوح مورد انتظار محافظت از آنها در زمان جابجایی کاملا" مشخص باشد.

اطلاعات از سطوح مختلف حساسیت و اهمیت برخوردار هستند. برخی از این اطلاعات نیازمند محافظت بیشتر یا اعمال های خاص هستند. لذا تعریف و تعیین سطوح محافظت و بازگو کردن اهیمت بکاربردن اقدامات ویژه در زمان استفاده از اطلاعات جز از طریق طرح طبقه بندی اطلاعات میسر نخواهد گردید.

۷-۲-۱ دستورالعمل های طبقه بندی

اطلاعات باید برحسب ارزش آنها ، الزانات قانونی ، حساسیت و میزان اهمیتی که برای سازمان دارند ، طبقه بندی شوند.

۷-۲-۲ تعیین عنوان و نحوه جابجایی اطلاعات

بر اساس طرح طبقه بندی اتخاذ شده توسط سازمان لازم خواهد بود تا یک مجموعه مناسب از رویه های اجرایی برای برچسب زنی و جابجایی اطلاعات تهیه و تدوین گردد.

۸- امنیت منابع انسانی

۸-۱- قبل از استخدام

هدف: حصول اطمینان از این که کارکنان ، پیمانکاران و کاربران ثالث نسبت به مسئولیت های خویش شناخت کافی داشته و برای نقش هایی که برای ایشان در نظر گرفته شده است از هر نظر مناسب هستند و همچنین کاهش ریسک سرقت ، کلاهبرداری یا سوء استفاده از امکانات.

توجه کافی به مسئولیت های امنیتی در شرح مشاغل و بر اساس شرایط و ضوابط استخدامی قبل از هر گونه اقدام در جهت استخدام لازم و ضروری خواهد بود.

انجام گزینش متقاضیان استخدامی ، پیمانکاران و کاربران ثالث به خصوص در مورد مشاغل حساس ، الزامی خواهد بود.

کلیه کارکنان ، پیمانکاران و کاربران مراکز پردازش اطلاعات ملزم خواهند بود تا موافقت نامه مربوز به نقش ها ومسئولیت های امنیتی را به امضاء برسانند.

۸-۱-۱ نقش ها و مسئولیت ها

نقش ها و مسئولیت های امنیتی کارکنان ، پیمانکاران و کاربران باید بطور کامل تعریف و مستندات مربوط به آن بر اساس خط مشی امنیت اطلاعات سازمان تهیه گردد.

۸-۱-۲ گزینش

انجام اقدامات لازم در خصوص اخذ سوء پیشینه تمامی داوطلبین استخدامی ، پیمانکاران و کاربران ثالث باید بر اساس قوانین و مقررات مربوطه و اصول اخلاقی و متناسب با الزامات کاری ، طبقه بندی اطلاعاتی که قرار است در دسترس قرار گیرند و ریسک های شناخته شده انجام پذیرد.

۸-۱-۳ شرایط و ضوابط استخدامی

کارکنان ، پیمانکاران و کاربران ثالث ملزم خواهند بود تا به عنوان بخشی از تعهدات قراردادی شان ، مراتب موافقت خود را با شرایط و ضوابط مندرج در قرارداد استخدامی اعلام و آنرا به امضاء برسانند. در این قرارداد صراحتا" به مسئولیت های ایشان و سازمان در قبال امنیت اطلاعات اشاره شده است.

۸-۲ ضمن استخدام

هدف: حصول اطمینان از این که کارکنان ، پیمانکاران و کاربران ثالث نسبت به تهدیدات و دل نگرانی های مترتب بر امنیت اطلاعات ، مسئولیت ها و تعهدات خویش آگاه بوده و برای حمایت از خط مشی امنیت سازمانی در جریان کارهای عادی خویش به ابزار لازم تجهیز شده اند و کاهش ریسک خطای انسانی.

مسئولیت های مدیریت باید بگونه ای تعریف شود که از اعمال امنیت در جریان مراحل استخدامی یک فرد در سازمان اطمینان لازم حاصل شود.

آگاه سازی مناسب و آموزش های کافی در زمینه رویه های اجرایی امنیت و استفاده صحیح از مراکز پردازش اطلاعات به تمامی کارکنان ، پیمانکاران و کاربران ثالث به منظور کاهش ریسک های امنیتی . تعیین یک رویه رسمی انضباطی برای برخورد در موارد نقض امنیت لازم و ضروری می باشد.

۸-۲-۱ مسئولیت های مدیریت

مدیریت ملزم خواهد بود تا از کارکنان ، پیمانکاران و کاربران بخواهد تا موازین امنیتی را بر اساس خط مشی ها و رویه های اجرایی جاری در سازمان را رعایت نموده و به مورد اجرا بگذارند.

۸-۲-۲ آگاه سازی ، آموزش و کارآموزی در زمینه امنیت اطلاعات

تمامی کارکنان سازمان و بر حسب مورد پیمانکاران و کاربران ثالث ملزم خواهند بود دوره های آگاه سازی و کارآموزی در خصوص خط مشی ها و رویه های اجرایی سازمان را با توجه به میزان ارتباط یا شرح شغلی خود پشت سر بگذارند.

۸-۲-۳ رویه انضباطی

اجرای یک رویه انضباطی در مورد آندسته از کارکنانی که مرتکب نقض امنیت می شوند ، الزامی به نظر می رسد.

۸-۳ فسخ قرارداد استخدامی یا تغییر آن

هدف :حصول اطمینان از خروج کارکنان ، پیمانکاران یا کاربران ثالث از سازمان یا تغییر شرایط مندرج در قرارداد استخدامی طبق روش های جاری.

تعیین مسئولیت ها به گونه ای که اطمینان حاصل شود خروج کارکنان ، پیمانکاران یا کاربران ثالث از سازمان کاملا" با نظر مدیریت انجام شده است و عودت کلیه تجهیزات و الغای تمامی حقوق دسترسی بطور کامل انجام شده است.

تغییر مسئولیت ها و قراردادهای استخدامی در داخل یک سازمان باید به شرحی که در بخش فسخ مسئولیت یا قرارداد استخدامی تصریح شده است انجام پذیرد و هر گونه قرارداد استخدامی جدید باید به شرحی که در بند ۱-۸ آمده است ، مدیریت و اداره شود.

۸-۳-۱ لغو مسئولیت ها

مسئولیت های مربوط به اجرای فسخ قرارداد استخدامی یا تغییر شرایط مندرج در آن باید بطور کامل تعیین و به افراد ذیربط محول گردد.

۸-۳-۲ عودت دارایی ها

تمامی کارکنان ، پیمانکاران و کاربران ثالث ملزم خواهند بود تا به محض فسخ قرارداد استخدامی یا قرارداد یا موافقت نامه مربوطه ، نسبت به عودت و استرداد آندسته از دارایی های سازمان که در اختیار ایشان قرار داشته است ، اقدام نمایند.

۸-۳-۳ سلب حقوق دسترسی

کلیه حقوق دسترسی کارکنان ، پیمانکاران یا کاربران ثالث که به نحوی از انحاء از اطلاعات یا مراکز پردازش اطلاعات استفاده می نمایند، باید به محض فسخ استخدام ، قرارداد یا موافقت نامه از ایشان سلب یا بر اساس تغییرات صورت گرفته اصلاح گردد.

۹- امنیت فیزیکی و پیرامونی

۹-۱ مناطق امن

هدف : جلوگیری از هر گونه دسترسی فیزیکی غیر مجاز، خسارت و ایجاد هر گونه تداخل در پیرامون یا اطلاعات سازمان.
مکانی که برای مراکز پردازش اطلاعات حساس یا حائز اهمیت در نظر گرفته می شوند ، باید از هر حیث امن بوده و با در نظر گرفتن محیط های امنیتی و با ایجاد موانع امنیتی مناسب و کنترلی مناسب در مبادی وروی مورد محافظت قرار گیرند. در این میان لازم خواهد بود تا از این مکان ها به صورت فیزیکی در برابر هر گونه دسترسی غیر مجاز ، خسارت و تداخل محافظت شود.

۹-۱-۱ مواضع امنیت فیزیکی

برای محافظت از مناطقی که تشکیلات اطلاعاتی و مراکز پردازش اطلاعات را در خود جای داده اند، لازم است از مواضع های امنیتی (موانعی از قبیل دیوارها ، گیت های ورودی که با کارت می شوند یا واحدهای بازرسی که توسط نیروی انسانی اداره می شوند) استفاده نمود.

۹-۱-۲ موانع فیزیکی ورودی

مناطق امن باید با استفاده از موانع کنترلی مناسب در مبادی ورودی مورد محافظت قرار داده شوند تا به این ترتیب از این موضوع که تنها افراد مجاز ، حق دسترسی به این مناطق را دارند اطمینان حاصل شود.

۹-۱-۳ تامین امنیت دفاتر کار ، اتاق ها و مراکز (تاسیسات)

امنیت فیزیکی دفاتر کار ، اتاق ها و مراکز پردازش اطلاعات باید به صورت مشخص طراحی و به مورد اجرا گذاشته شود.

۹-۱-۴ محافظت در برابر تهدیدات بیرونی و امنیت فیزیکی و پیرامونی

محافظت فیزیکی در برابر خسارات ناشی از آتش سوزی ، سیلاب ، زلزله ، انفجار ، ناآرامی های داخلی و سایر بلایای طبیعی و بلایای ناشی از رفتارهای انسانی باید به صورت مشخص طراحی و به کار بسته شود.

۹-۱-۵- کار کردن در مناطق امن

امنیت فیزیکی و دستورالعمل های مربوط به کار کردن در مناطق امن باید به صورت مشخص طراحی و به اجرا گذاشته شود.

ین م ـ ـ ـ ـ ـ بخ ـ ـ ـ ـ

تدوین رویه های عملیاتی مناسب را نیز شامل می گردد.

تفکـــــــیک وظایف بر حسب مورد باید به مورد اجرا گذاشته شود تا به این ترتیب ریسک ناشی از هرگونه بی مبالاتی و سوء استفاده تعمدی از سیستم کاهش یابد.

۱۰-۱-۱ رویه های عملیاتی مستند سازی شده

رویه های عملیاتی باید ضمن آن که مستند سازی می شوند ، به نحو مقتضی نگهداری شده و در اختیار تمام کاربرانی که به نحوی از انحاء بدانها نیاز دارند ، قرار داده شود.

۱۰-۱-۲ مدیریت تغییر

هر گونه تغییر در مراکز پردازش اطلاعات و سیستم ها باید با اعمال های لازم انجام پذیرد.

۱۰-۱-۳ تفکیک وظایف

وظایف و حیطه مسئولیت ها باید تفکیک گردد تا به این ترتیب فرصت هر گونه جرح و تعدیل غیر مجاز و ناخواسته یا سوء استفاده از دارایی های سازمان کاهش یابد.

۱۰-۱-۴- تفکیک مراکز توسعه ، تست و عملیات

مراکز توسعه ، تست و عملیات باید از یکدیگر تفکیک شوند تا به این ترتیب ریسک های ناشی از دسترسی یا اعمال تغییرات غیر مجاز در سیستم عملیاتی کاهش یابد.

۱۰-۲ مدیریت خدمات ارائه شده توسط اشخاص ثالث

هدف : اجرا و حفظ سطح مناسب امنیت اطلاعات و ارائه خدمات طبق موافقت نامه های ارائه خدمات توسط اشخاص ثالث . سازمان ملزم خواهد بود تا بر حسن اجرای موافقت نامه ها نظارت داشته باشد و انطباق آنها با موافقت نامه ها را تحت نظارت خویش داشته باشد و مدیریت تغییرات را بگونه ای انجام دهد که از برآورده شدن تمامی الزامات توافق شده با اشخاص ثالث در زمینه ارائه خدمات اطمینان حاصل نماید.

۱۰-۲-۱ ارائه خدمات

حصول اطمینان از اجرا ، بکارگیری و پایبندی به اقدامات امنیت ، تعاریف خدمات و سطوح تحویل دهی مندرج در موافقت نامه ارائه خدمات توسط اشخاص ثالث ، توسط ایشان الزامی و ضروری خواهد بود.

۱۰-۲-۲ نظارت و بازنگری خدمات ارائه شده توسط اشخاص ثالث

خدمات ، گزارشات و سوابقی که توسط اشخاص ثالث در اختیار سازمان قرار داده می شود ، باید بطور منظم نظارت و مورد بازنگزی قرار داده شود و در فواصل زمانی معین ممیزی شوند.

۱۰-۲-۳ مدیریت تغییرات در خدمات ارائه شده توسط اشخاص ثالث

تغییر در تامین خدمات از جمله پایبندی و بهبود خط مشی های امنیت اطلاعات موجود ، رویه های اجرایی و اقدامات کنترلی باید به نحو مقتضی تحت مدیریت قرار گیرد ، ضمن آن که میزان اهمیت سیستم های کاری و فرآیندهای مربوطه و ارزشیابی مجدد ریسک ها نیز باید مد نظر قرار داده شود.

۱۰-۳ برنامه ریزی و پذیرش سیستم

هدف : به حداقل رساندن ریسک ناشی از خرابی های سیستم.

حصول اطمینان از دسترس بودن ظرفیت و منابع کافی برای رسیدن به عملکرد مورد انتظار از سیستم مستلزم آماده سازی و برنامـه ریزی پیشرفته می باشد.

به منظور کاهش ریسک ناشی از اضافه بار تحمیلی به سیستم ، پیش بینی الزامات ظرفیت آتی لازم و اجتناب ناپذیر خواهد بود.
تعیین ، مستندسازی و تست الزامات عملیاتی سیستم های جدید قبل از هر گونه اقدام در جهت پذیرش و استفاده از آنهـا، لازم و ضروری می باشد.

۱-۳-۱۰ مدیریت ظرفیت

استفاده از منابع باید تحت نظارت قرار گرفته ، تنظیم شده و الزامات ظرفیت آتی پیش بینی شود تا به این ترتیب از رسیدن به عملکرد مورد انتظار از سیستم اطمینان لازم حاصل گردد.

۲-۳-۱۰پذیرش سیستم

معیارهای پذیرش سیستم های اطلاعاتی جدید ، نسخه های روزآمد شده و نسخه های جدید باید تعیین شود ، ضمن آن که تست های متناسب با سیستم (ها) باید در حریان توسعه و قبل از پذیرش انجام گردد.

۴-۱۰ محافظت در برابر کد های مخرب و موبایل

هدف : محافظت و صیانت از تمامیت نرم افزار و اطلاعات.
در نظر گرفتن جنبه های تامینی برای شناسایی و جلوگیری از بکار بردن کد مخرب و کد غیر مجاز موبایل.
نرم افزار و مراکز پردازش اطلاعات در برابر ورود کد مخرب از جمله ویروس های کامپیوتری ، کرم های شبکه ، اسب های Trojan و بمب های منطقی آسیب پذیر هستند و لذا کاربران باید نسبت به ریسک های این کدهای مخرب آگاه و هوشیار باشند. لذا مدیران ملزم خواهند بود تا بر حسب مورد ، اقدامات کنترلی لازم را در جهت جلوگیری ، شناسایی و حذف کدهای مخرب و کد موبایل به مورد اجرا بگذارند.

۱-۴-۱۰ اقدامات کنترلی در برابر کدهای مخرب

شناسایی ، جلوگیری و بازسازی به منظور محافظت در برابر کدهای مخرب و اتخاذ رویه های اجرایی مناسب در جهت آگاه سازی کاربر از جمله اقداماتی می باشد که باید به مورد اجرا گذاشته شود.

۲-۴-۱۰ اقدامات کنترلی در برابر کد موبایل

در مواردی که استفاده از کد موبایل مجاز دانسته شده است ، پیکربندی باید از فعال شدن کد موبایل بر اساس یک خط مشی امنیت کاملا مشخص اطمینان حاصل نماید. در این میان باید از اجرا شدن کد موبایل غیر مجاز جلوگیری شود .

۵-۱۰ نسخه پشتیبان (Back-up)

هدف :حفظ تمامیت و در دسترس بودن اطلاعات و مراکز و امکانات پردازش اطلاعات.
تعیین رویه های اجرایی روزمره به منظور اجرای خط مشی و استراتژی مورد توافق (به بند ۱-۱۴ مراجعه نماییـد) مربـوط بـه تهیه نسخه های پشتیبان و برقرار کردن بموقع آنها لازم و ضروری می باشد.

۱-۵-۱۰ تهیه نسخه پشتیبان از اطلاعات

تهیه نسخه های پشتیبان از اطلاعات و نرم افزار و تست آنها در فواصل زمانی معین بر اساس خط مشی مورد توافق مربوط به تهیه نسخه های پشتیبان لازم و اجتناب ناپذیر می باشد.

۶-۱۰ مدیریت امنیت شبکه

هدف : حصول اطمینان از محافظت اطلاعات در شبکه ها و محافظت از زیر ساختارهای پشتیبانی.
مدیریت ایمن شبکه ها که مرزهای سازمانی را تحت پوشش قرار می دهد ، مستـــــلزم توجه دقیق به جریان داده ها ، مفـاهیم و مضامین حقوقی ، نظارت و محافظت می باشد.

به منظور محافظت از اطلاعات حساسی که از طریق شبکه های عمومی رد و بدل می شوند ، بـه تـدابیر کنترلـی بیشـتری نیـاز خواهد بود.

۱-۶-۱۰ های شبکه

برای آن که امکان محافظت از شبکه ها در برابر تهدیدات فراهم گردد و به منظور حفظ امنیت سیستم و برنامه های کاربردی که به نحوی از انحاء از شبکه استفاده می کنند (منجمله اطلاعات در حال انتقال) ، مدیریت و صحیح و مناسب شبکه ها ، لازم و اجتناب ناپذیر خواهد بود.

۲-۶-۱۰ امنیت خدمات شبکه

مشخصه های امنیتی ، سطوح خدمات و الزامات مدیریتی کلیه خدمات شبکه از جمله مواردی هستند که باید تعیین شده و به نحو مقتضی در هر یک از موافقت نامه های خدمات شبکه لحاظ گردند ، چه این خدمات در داخل و چه از طریق منابع خارجی تامین شوند.

۷-۱۰ نحوه استفاده از رسانه ها

هدف : جلوگیری از افشای غیر مجاز ، جرح و تعدیل ، حذف یا امحای دارایی ها و هر گونه اختلال در فعالیت های کاری.

رسانه ها باید تحت قرار داشته و به صورت فیزیکی مورد محافظت قرار گیرند.

تعیین رویه های عملیاتی مناسب به منظور محافظت از اسناد ، رسانه های کامپیوتری (به عنوان مثال نوارها و دیسکت ها) داده های ورودی یا خروجی و مستندات سیستم در برابر افشای غیر مجاز ، جرح و تعدیل ، حذف و امحا ، لازم و اجتناب ناپذیر می باشد.

۱-۷-۱۰ مدیریت رسانه هایی که قابل پاک شدن هستند

تعیین و اجرای رویه های مربوط به مدیریت رسانه هایی که قابل پاک شدن هستند ، لازم و ضروری هستند

۲-۷-۱۰ امحاء رسانه ها

در صورتی که دیگر نیازی به استفاده از رسانه ها نباشد ، لازم خواهد بود تا با رعایت نکات ایمنی و امنیتی و با استفاده از رویه های رسمی نسبت به امحای آنها اقدام شود.

۳-۷-۱۰ رویه های جابجایی اطلاعات

به منظور محافظت از اطلاعات در برابر افشای غیر مجاز یا هر گونه سوء استفاده ، لازم خواهد بود تا نسبت به تعیین رویه های مربوط به جابجایی و ذخیره سازی اطلاعات مبادرت نمود.

۴-۷-۱۰ امنیت مستندات سیستم

مستندات سیستم باید به نحو مقتضی در برابر هر گونه دسترسی غیر مجاز محافظت شوند.

۸-۱۰ تبادل اطلاعات

هدف : حفظ و تامین امنیت اطلاعات و نرم افزارهایی که در داخل سازمان و با هر یک از موسسات و نهادهای بـرون سـازمانی مبادله می شوند.

تبادل اطلاعات و نرم افزار بین سازمان ها باید بر اساس خط مشی تبادل اطلاعات و مطابق با موافقت نامه های مربوطه انجام پذیرد و از هر حیث باید مطابق با قوانین مربوطه باشد (به ماده ۱۵ مراجعه نمایید).

تعیین و تبیین استانداردها و رویه های اجرایی به منظور محافظت از اطلاعات و رسانه های فیزیکی حاوی اطلاعات در حال انتقال لازم و ضروری می باشد.

۱-۸-۱۰ خط مشی ها و رویه های اجرایی تبادل اطلاعات

به منظور محافظت از تبادل اطلاعات از طریق کلیه امکانات و وسایل ارتباطاتی ، لازم خواهد بود تا خط مشی های رسمی تبادل اطلاعات ، رویه های اجرایی و تدابیر کنترلی لازم تعیین و به مورد اجرا گذاشته شود.

۲-۸-۱۰ موافقت نامه های تبادل اطلاعات

تهیه و تنظیم موافقت نامه های مربوط به تبادل اطلاعات و نرم افزار بین سازمان و اشخاص برون سازمانی ، لازم و اجتناب ناپـذیر می باشد.

۳-۸-۱۰ رسانه های فیزیکی در حال جابجایی

رسانه های محتوی اطلاعات باید در حین انتقال به خارج از مرزهای فیزیکی سازمان به نحو مقتضی در برابر هر گونه دسترسی غیر مجاز ، سوء استفاده یا خراب شدن محافظت شوند.

۴-۸-۱۰ ارسال پیام به صورت الکترونیکی

اطلاعاتی که از طریق پیام الکترونیکی ارسال می شوند باید به نحو مقتضی مورد محافظت قرار گیرند.

۵-۸-۱۰سیستم های اطلاعات مربوط به داد و ستد (Business)

تعیین و اجرای خط مشی ها و رویه های اجرایی به منظور محافظت از اطلاعاتی که از طریق ارتباط بین سیستم های اطلاعاتی کاری مبادله می شوند ، لازم و اجتناب ناپذیر می باشد.

۹-۱۰ خدمات تجارت الکترونیک

هدف : حصول اطمینان از امنیت خدمات تجارت الکترونیک و استفاده ایمن از آنها .
مفاهیم امنیتی مربوط به استفاده از خدمات تجارت الکترونیک از جمله معاملات آنلاین و الزامات مربوط به اقدامات کنترلی از جمله مواردی هستند که در این حوزه باید مورد ملاحظه قرار داده شوند. تمامیت و دردسترس پذیری اطلاعاتی که از طریق سیستم های دولتی موجود به صورت الکترونیکی منتشر می شوند از دیگر مواردی است که باید مورد توجه قرار داده شوند.

۱-۹-۱۰ تجارت الکترونیک

اطلاعاتی که به نحوی از انحا در تجارت الکترونیک مورد استفاده قرار می گیرند و اشاعه آنها از طریق شبکه های عمومی صورت می پذیرد ، باید در برابر موارد کلاهبرداری ، اختلافات قراردادی و افشای غیر مجاز و جرح و تعدیل مورد محافظت قرار گیرند.

۲-۹-۱۰ معاملات آنلاین (روی خط)

اطلاعاتی که به نحوی از انحا در معاملات آنلاین مورد استفاده قرار می گیرند ، باید به نحو مقتضی مورد محافظت قرار داده شوند تا به این ترتیب از ارسال ناقص ، تحریف مسیر ، تغییر غیر مجاز پیام، افشای غیر مجاز ، تکثیر یا پخش غیر مجاز پیام جلوگیری شود.

۳-۹-۱۰ اطلاعاتی که در دسترس عموم قرار دارد

تمامیت اطلاعاتی که از طریق یک سیستم عمومی قابل دسترس ، در دسترس عموم قرار دارد ، باید به نحو مقتضی مورد محافظت قرار داده شوند تا به این ترتیب از هرگونه تغییر غیر مجاز در آنها جلوگیری گردد.

۱۰-۱۰ بازبینی (پایش)

هدف : شناسایی فعالیت های غیر مجاز در زمینه پردازش اطلاعات.
سیستم ها باید به نحو مقتضی مورد بازبینی قرار گرفته و رویدادهای مربوط به امنیت اطلاعات ، ثبت و ضبط گردد. برای حصول اطمیمان از این که مشکلات سیستم اطلاعات بدرستی تعیین و شناسایی شده اند ، استفاده از لاگ های اپراتور و ثبت نواقص و

معایب در لاگ های مربوطه ، لازم و اجتناب ناپذیر می باشد.

سازمان ملزم به رعایت کلیه الزامات قانونی مربوطه و الزامات لازم الاجرا در فعالیت های بازبینی و ثبت در لاگ های مربوطه می باشد.

بازبینی سیستم باید بگونه ای انجام شود که بتوان از نتایج آن برای اثربخشی تدابیر کنترلی اتخاذ شده و تعیین انطباق با مدل خط مشی دسترسی استفاده نمود.

۱-۱۰-۱۰ ثبت نتایج ممیزی در لاگ های مربوطه

تهیه لاگ های ممیزی جهت ثبت فعالیت های کاربر ، استثنائات و رویدادهای مربوط به امنیت اطلاعات و نگاهداری و حفظ آنها برای یک مدت معین جهت کمک به بررسی های آتی و بازبینی دسترسی لازم و اجتناب ناپذیر می باشد.

۲-۱۰-۱۰ بازبینی موارد استفاده از سیستم

رویه های اجرایی مربوط به نظارت و بازبینی موارد استفاده از مراکز پردازش اطلاعات باید به نحو مقتضی تعیین و نتایج حاصله در فواصل زمانی معین مورد بازنگری قرار داده شود.

۳-۱۰-۱۰ محافظت از اطلاعات مندرج در لاگ

امکانات مورد استفاده جهت ثبت وقایع و اطلاعات مندرج در لاگ باید در برابر هر گونه دستکاری یا دسترسی غیر مجاز مورد محافظت قرار داده شود.

۴-۱۰-۱۰ لاگ های مدیر و اپراتور

فعالیت های مربوط به اداره کننده سیستم و اپراتور سیستم باید به نحو مقتضی در لاگ های مربوطه ثبت گردد.

۵-۱۰-۱۰ ثبت شرح عیب در لاگ مربوطه

شرح عیوب باید به نحو مقتضی در لاگ های مربوطه ثبت شده ، مورد تجزیه و تحلیل قرار گرفته و اقدامات مناسب در جهت رفع آنها بعمل آید.

۶-۱۰-۱۰ سنکرون کردن ساعت

سنکرون کردن ساعت های کلیه سیستم های پردازش اطلاعات در داخل یک سازمان یا حوزه امنیتی با یک منبع زمانی دقیق مورد توافق ، لازم و ضروری می باشد.

۱۱ – دسترسی

۱-۱۱ الزامات کاری درباره دسترسی

هدف : دسترسی به اطلاعات

دسترسی به اطلاعات ، مراکز پردازش اطلاعات و فرآیندهای کاری باید بر اساس الزامات کاری و امنیتی شود.

خط مشی های مربوط به اشاعه اطلاعات و مجوزهای مربوطه باید در قوانین دسترسی لحاظ گردد.

۱-۱-۱۱ خط مشی دسترسی

تعیین سیاست و خط مشی دسترسی ، تهیه مستندات مربوطه و بازنگری آن بر اساس الزامات کاری و امنیتی مربوط به دسترسی ، لازم و ضروری می باشد.

۲-۱۱ مدیریت دسترسی کاربر

هدف : حصول اطمینان از دسترسی مجاز کاربر و ممانعت از هر گونه دسترسی غیر مجاز به سیستم های اطلاعاتی.

برای آن که امکان تعیین حقوق دسترسی به سیستم ها و سرویس های اطلاعاتی فراهم گردد ، لازم خواهد بود تا رویه های

اجرایی رسمی به مورد اجرا درآید.

این رویه ها باید بگونه ای باشند که کلیه مراحل در طول مدت زمان دسترسی کاربر ، از ثبت اولیه کاربران جدید تا خارج نمودن نام کاربران از لیست که دیگر نیازی به دسترسی به سیستم ها و سرویس های اطلاعاتی ندارند را شامل گردد. لزوم بر رویه اختصاص حقوق دسترسی ویژه که به موجب آن های سیستم در مورد کاربران اعمال نمی شود ، از جمله موضوعاتی است که بر حسب مورد باید بدان توجه خاص شود.

۱-۲-۱۱ ثبت نام کاربر

تعیین و به مورد اجرا درآوردن رویه اجرایی رسمی ثبت نام کاربر و حذف نام کاربر از فهرست ثبت نام برای اعطاء یا الغای حق دسترسی به تمامی سیستم ها و سرویس های اطلاعاتی ، لازم و ضروری می باشد.

۲-۲-۱۱ مدیریت امتیاز (حق ویژه)

تخصیص و استفاده از امتیازات باید تا حد امکان محدود و تحت قرار گیرد.

۳-۲-۱۱ مدیریت کلمه عبور کاربر

اخصاص کلمه های عبور باید از طریق یک فرآیند مدیریتی رسمی شود.

۴-۲-۱۱ بازنگری حقوق دسترسی کاربر

مدیریت ملزم خواهد بود تا با استفاده از یک فرآیند رسمی ، مبادرت به بازنگری حقوق دسترسی کاربر در فواصل زمانی منظم نماید.

۴-۲-۱۱ بازنگری حقوق دسترسی کاربر

مدیریت ملزم خواهد بود تا با استفاده از یک فرآیند رسمی ، مبادرت به بازنگری حقوق دسترسی کاربر در فواصل زمانی منظم نماید.

۳-۱۱ مسئولیت های کاربر

هدف : جلوگیری و ممانعت از هر گونه دسترسی غیر مجاز توسط کاربر و به مخاطره افتادن یا به سرقت رفتن اطلاعات و امکانات پردازشگر اطلاعات.

امنیت موثر جز در سایه همکاری کاربران مجاز با یکدیگر محقق نخواهد گردید.

کاربران باید نسبت به مسئولیت های خویش در قبال بکار گرفتن روش های دسترسی موثر و به خصوص توجه به استفاده از کلمات عبور و امنیت تجهیزات کاربر آگاه باشند.

خط مشی میز تمیز و صفحه نمایشگر پاک باید به نحو مقتضی به مورد اجرا درآید تا به این ترتیب ریسک ناشی از دسترسی غیر مجاز یا وارد آمدن خسارت به پرونده ها ، رسانه ها و امکانات پردازشگر اطلاعات کاهش یابد.

۱-۳-۱۱ استفاده از کلمه عبور

کاربران ملزم خواهند بود تا از روش های امنیتی مناسب در انتخاب و استفاده از کلمات عبور تبعیت نموده و آنها را به مورد اجرا بگذارند.

۲-۳-۱۱ تجهیزات خودکار کاربر

کاربران ملزم خواهند بود تا از تحت محافظت قرار داشتن تجهیزات خودکار (بی نیاز از متصدی) ، اطمینان حاصل نمایند.

۱۱-۳-۳ خط مشی میز تمیز و صفحه نمایش پاک

اتخاذ سیاست میز تمیز در مورد اسناد و مدارک و رسانه های ذخیره سازی قابل پاک شدن و سیاست صفحه نمایش پاک در مورد تجهیزات پردازشگر اطلاعات لازم و ضروری می باشد.

۱۱-۴ دسترسی به شبکه

هدف : ممانعت از دسترسی غیر مجاز به خدمات شبکه

دسترسی به خدمات شبکه داخلی و خارجی باید به نحو مقتضی تحت قرار داشته باشد.

دسترسی کاربر به شبکه ها یا خدمات شبکه نباید امنیت خدمات شبکه را به مخاطره بیندازد. برای حصول اطمینان از این موضوع :

الف) لازم خواهد بود تا اینترفیس های مناسب بین شبکه سازمان و شبکه سایر سازمان ها و شبکه های دولتی قرار داده شود ؛

ب) استفاده و بکار بردن مکانیزم های مناسب به منظور تعیین اعتبار کاربران و تجهیزات لازم خواهد بود ؛

پ) دسترسی کاربر به خدمات اطلاعاتی جاری باید شود.

۱۱-۴-۱ خط مشی مربوط به استفاده از خدمات شبکه

در این خصوص لازم است کاربران صرفا" به خدماتی دسترسی پیدا نمایند که بطور اختصاصی جهت استفاده از آنها مجوزهای لازم را دریافت نموده باشند.

۱۱-۴-۲ شناسایی کاربر در زمان وصل شدن به اتصال های (کانکشن های) بیرونی

به منظور دسترسی از سوی کاربران راه دور ، لازم خواهد بود تا از روش های مناسب تعیین اعتبار استفاده شود.

۱۱-۴-۳ شناسایی تجهیزات مورد استفاده در شبکه ها

شناسایی تجهیزات به صورت اتوماتیک باید به عنوان یکی از روش های تعیین اعتبار اتصال های مکان ها یا تجهیزات خاص مورد توجه قرار داده شود.

۱۱-۴-۴ محافظت از راه دور پورت پیکره بندی و تشخیصی

دسترسی فیزیکی و منطقی به پورت های پیکره بندی و تشخیصی از دیگر مواردی است که باید تحت قرار گیرد.

۱۱-۴-۵ تفکیک (جدا سازی) در شبکه ها

تفکیک و جداسازی گروه های مختلف خدمات اطلاعات ، کاربران و سیستم های اطلاعاتی در شبکه ها ، الزامی می باشد.

۱۱-۴-۶ اتصال به شبکه

امکاناتی که جهت اتصال به شبکه در اختیار کاربران قرار دارد باید بر اساس خط مشی دسترسی و الزامات برنامه های کاربردی مورد استفاده در یک حوزه کاری مشخص ، محدود شود . این محدودیت در مورد شبکه های مشترک و به خصوص شبکه هایی دامنه گسترش آنها بگونه ای است که از مرزهای سازمان نیز فراتر رفته است ، بسیار مهم و حائز اهمیت به شمار می رود.

۱۱-۴-۷ مسیریابی شبکه

مسیریابی در شبکه ها باید به مورد اجرا درآید تا به این ترتیب از عدم نقض خط مشی دسترسی برنامه های کاربردی تجاری بواسطه اتصال های کامپیوتری و جریان های اطلاعات اطمینان حاصل شود.

۱۱-۵ دسترسی به سیستم عامل

هدف : جلوگیری از دسترسی غیر مجاز به سیستم عامل.

استفاده از امکانات امنیتی به منظور محدود نمودن میزان دسترسی به سیستم های عامل بگونه ای که کاربران مجاز قادر به

دسترسی به این سیستم ها باشند ، بسیار مهم و حائز اهمیت می باشد. این امکانات باید توانایی انجام موارد ذیل را داشته باشند:

الف) تعیین اعتبار کاربران مجاز بر اساس خط مشی دسترسی که از پیش تعیین شده است

ب) ثبت تلاش های موفق و نا موفقی که در خصوص تعیین اعتبار سیستم صورت گرفته اند ؛

پ) ثبت موارد استفاده از امتیازات ویژه سیستم ؛

ت) اعلام هشدار در صورت موارد نقض خط مشی امنیت سیستم.

ث) ارائه روش های مناسب برای تعیین اعتبار؛

ج) محدود نمودن زمان اتصال کاربران بر حسب مورد.

۱۱-۵-۱ رویه های ایمن در مورد کاراندازی سیستم (log-on)

دسترسی به سیستم های عامل باید بوسیله رویه اجرایی مربوط به کاراندازی سیستم به صورت امن شود.

۱۱-۵-۲ شناسایی و تعیین اعتبار کاربر

تمامی کاربران ملزم خواهند بود تا از یک شناسه منحصربفرد (کاربر ID) برخوردار بوده و صرفا" جهت کاربردهای شخصی خویش از آن استفاده نمایند. همچنین برای اثبات هویت ادعا شده توسط یک کاربر ، لازم خواهد بود تا یک تکنیک تعیین اعتبار مناسب انتخاب و به مورد اجرا درآید.

۱۱-۵-۳ سیستم مدیریت کلمه عبور

سیستم های مدیریت کلمات عبور باید از نوع سیستم های تعاملی بوده و کلمات عبور با کیفیت را تضمین نماید.

۱۱-۵-۴ استفاده از امکانات سیستم

استفاده از برنامه های کمکی و جانبی که ممکن است از سرعت سیستم و تاثیر کنترلی برنامه های کاربردی بکاهد ، باید محدود شده و به شدت تحت قرار بگیرد.

۱۱-۵-۵ تایم اوت (انقضای مدت) جلسه

جلسات غیر فعال باید پس از مدت زمان بیکاری تعیین شده در حالت خاموش قرار داده شوند.

۱۱-۵-۶ محدودیت زمان اتصال

اعمال محدودیت در خصوص زمان اتصال به منظور تامین امنیت بیشتر برای نرم افزارهای با ریسک بالا ، لازم و ضروری خواهد بود.

۱۱-۶ دسترسی به اطلاعات و برنامه های نرم افزاری

هدف : جلوگیری از دسترسی غیر مجاز به اطلاعاتی که بر روی سیستم های کاربردی نگاهداری می شوند.

استفاده از امکانات امنیتی به منظور محدود نمودن دسترسی به سیستم های کاربردی و بداخل آنها ، لازم و اجتناب ناپذیر می باشد.

دسترسی منطقی به نرم افزارهای کاربردی و اطلاعات باید به کاربران مجاز محدود شود. سیستم های کاربردی باید :

الف) دسترسی کاربر به اطلاعات و فانکشن های سیستم کاربردی را بر اساس خط مشی دسترسی را نماید ؛

ب) محافظت لازم در برابر دسترسی غیر مجاز از سوی هر یک از امکانات ، نرم افزار سیستم عامل و نرم افزارهای مخربی که موجب کندی سرعت سیستم یا کاهش تاثیر های نرم افزار کاربردی می شوند را بعمل آورد ؛

پ) سایر سیستم هایی که مشترکا" از منابع اطلاعاتی استفاده می کنند را به مخاطره نیندازد.

۱-۶-۱۱ محدود ساختن دسترسی به اطلاعات

دسترسی کاربران و پرسنل پشتیبانی به اطلاعات و فانکشن های سیستم نرم افزار کاربردی باید بر اساس خط مشی دسترسی محدود شود.

۲-۶-۱۱ جداسازی سیستم های حساس

سیستم های حساس باید از یک محیط کامپیوتری اختصاصی (مجزا) برخوردار باشند.

۷-۱۱ کار کردن از راه دور و کامپیوترهای قابل حمل

هدف : تامین امنیت اطلاعات در زمان استفاده از امکانات محاسبات موبایل و کار کردن از راه دور یا **teleworking** .

سطح محافظت مورد نظر باید با ریسک هایی که بواسطه این نوع روش های خاص کارکردن متصور می باشد، متناسب باشد.

در هنگام استفاده از امکانات و تجهیزات محاسباتی موبایل ، ریسک های ناشی از کارکرد در یک محیط نا امن باید مورد ملاحظه قرار داشته باشد و محافظت مناسب و لازم به مورد احرا درآید. در مورد کارکردن از راه دور ، سازمان ملزم خواهد بود تا از سایتی که این نوع فعالیت در آن انجام می شود به نحو مقتضی محافظت نموده و از هماهنگی های مناسب برای این روش کار کردن اطمینان حاصل نماید.

۱-۷-۱۱ ارتباطات و محاسبات موبایل

به منظور محافظت در برابر ریسک های مربوط به استفاده از امکانات ارتباطاتی و محاسباتی سیار ، اجرای یک خط مشی رسمی و اتخاذ اقدامات امنیتی مناسب لازم و اجتناب ناپذیر خواهد بود.

۲-۷-۱۱ کار کردن از راه دور

تبیین و اجرای خط مشی ، برنامه های عملیاتی و رویه های اجرایی در مورد فعالیت هایی که در حوزه کار کردن از راه دور انجام می شود ، لازم و ضروری است.

۱۲ اکتساب (خرید)، توسعه و نگهداری سیستم های اطلاعاتی

۱-۱۲ الزامات امنیتی سیستم های اطلاعاتی

هدف : حصول اطمینان از این که امنیت ، جزء لاینفکی از سیستم های اطلاعاتی می باشد.

سیستم های اطلاعاتی متشکل از سیستم های عامل ، زیر ساختارها ، نرم افزارهای کاربردی ، محصولات غیر سفارشی و نرم افزارهای تولید شده توسط کاربر می باشد. طراحی و پیاده سازی سیستم اطلاعاتی (سیستم های اطلاعاتی که مسئولیت پشتیبانی از پروسه های کاری را برعهده دارند) ، از نقطه نظر امنیتی بسیار مهم و حائز اهمیت می باشد. لذا تعیین الزامات امنیتی و توافق در خصوص آنها قبل از مبادرت به هر گونه توسعه یا پیاده سازی سیستم های اطلاعاتی ، لازم و ضروری خواهد بود.

تعیین تمامی الزامات امنیتی در فاز تعیین الزامات پروژه ، توجیه ، توافق ، و مستندسازی الزامات امنیتی به عنوان بخشی از موارد کاری مربوط به سیستم اطلاعاتی ، لازم و ضروری خواهد بود.

۱-۱-۱۲ مشخصات و تجزیه و تحلیل الزامات امنیتی

هر گونه گزارش درباره الزامات کاری مربوط به سیستم های اطلاعاتی جدید ، یا هر گونه موارد بهبود در سیستم های اطلاعاتی موجود باید بیانگر الزامات مربوط به های امنیتی باشد.

۱۲-۲ پردازش صحیح در نرم افزارهای کاربردی

هدف : جلوگیری از هر گونه اشتباه ، خسارت ، هر گونه جرح و تعدیل غیر کجاز یا سوء استفاده از اطلاعـات موجـود در نـرم افزارهای کاربردی.

موارد کنترلی مناسب باید در نرم افزراهای کاربردی از جمله نرم افزارهای تولید شده توسط کاربر طراحی گردد تا به این ترتیب از پردازش صحیح اطمینان حاصل گردد. این موارد کنترلی ، مواردی از قبیل تایید و تصدیق داده های ورودی ، پردازش داخلی و داده های خروجی را شامل می گردد.

اتخاذ موارد کنترلی بیشتر در سیستم هایی که به نحوی از انحاء اطلاعات حساس، ارزشمند و حائز اهمیت را پردازش می نمایند و یا بر این دسته از اطلاعات تاثیر گذار هستند ، لازم و ضروری می باشد.

۱۲-۲-۱ اعتبار سنجی داده های ورودی

تصدیق داده هایی ثبت شده (وارد شده) در نرم افزارهای کاربردی باید به نحو مقتضی انجام پذیرد تا به این ترتیب از درست بودن و مناسب بودن داده ها اطمینان حاصل شود.

۱۲-۲-۲ پردازش داخلی

چک لیست تصدیق باید در داخل نرم افزارهای کاربردی تعبیه و پیش بینی شود تا به این ترتیب امکان شناسایی هر گونه خرابی اطلاعات از طریق اشتباهات پردازش یا اقدامات تعمدی فراهم گردد.

۱۲-۲-۳ درستی پیغام

تعیین الزامات مربوط به حصـول اطمینان از صحت و اعتبار و محافظت از درستی پیام در نرم افزارهای کاربردی ، تعیین موارد کنترلی مناسب و اجرای آنها ، لازم و ضروری خواهد بود.

۱۲-۲-۴ اعتبار سنجی داده های خروجی

داده های خروجی از یک برنامه کاربردی باید اعتبار سنجی شود تا به این ترتیب از اجرای درست پردازش اطلاعات ذخیره شده و مناسب بودن آن با شرایط اطمینان حاصل نمود.

۱۲-۳ انجام اقدامات کنترلی از طریق رمز نگاری

هدف : محافظت از محرمانگی ، اعتبار یا تمامیت (درستی) اطلاعات با استفاده از روش های رمزگذاری.

تبیین و تدوین خط مشی استفاده از های رمز نگاری ، لازم و اجتناب ناپذیر می باشد. در این ارتباط ، به اجرا درآوردن مدیریت کلید به منظور پشتیبانی از تکنیک های رمزگذاری توصیه می شود.

۱۲-۳-۱ خط مشی مربوط به استفاده از اقدامات کنترلی از طریق رمزگذاری

خط مشی مربوط به استفاده از های رمزگذاری جهت محافظت از اطلاعات باید تبیین و به مورد اجرا درآید.

۱۲-۳-۲ مدیریت کلید

به منظور حمایت و پشتیبانی از کاربرد و استفاده از تکنیک های رمزگذاری در سطح سازمان ، لازم خواهد بود تا مدیریت کلید به نحو مقتضی نهادینه و به مورد اجرا درآید.

۱۲-۴ امنیت فایل های سیستم

هدف: حصول اطمینان از امنیت فایل های سیستم.

دسترسی به به فایل های سیستم و کد برنامه اصلی باید به نحو مقتضی شود و پروژه های IT و فعالیت های پشتیبانی با در نظر گرفتن ملاحظات امنیتی انجام شود. در این ارتباط باید به این موضوع توجه داشت که داده های حساس در معرض محیط های

تست قرار نگیرد.

۱-۴-۱۲ نرم افزار عملیاتی

تعیین و اجرای رویه های لازم برای نصب نرم افزار برروی سیستم های عملیاتی ، ضروری و اجتناب ناپذیر می باشد.

۲-۴-۱۲ محافظت از داده های مربوط به تست سیستم

داده های تست باید بدقت انتخاب شود و به نحو مقتضی محافظت و شود.

۳-۴-۱۲ دسترسی به کد منبع برنامه

دسترسی به رمز منبع برنامه باید محدود شود.

۵-۱۲ امنیت در فرآیندهای توسعه و پشتیبانی

هدف : حفظ امنیت اطلاعات و نرم افزار سیستم برنامه کاربردی.

محیط های پروژه و پشتیبانی باید بدقت شوند.

مدیران مسئول سیستم های برنامه های کاربردی ، در قبال امنیت محیط های پروژه یا محیط پشتیبانی نیز مسئول شناخته خواهند شد. آنها باید اطمینان حاصل نمایند که تمامی تغییرات پیشنهادی جهت اعمال در سیستم مورد بازنگری قرار گرفته و بطور کامل چک شده اند و امنیت سیستم یا محیط عامل را به مخاطره نخواهند انداخت.

۱-۵-۱۲ تغییر رویه های کنترلی

اعمال و اجرای تغییرات باید با استفاده از رویه های رسمی تغییر ، به نحو مقتضی شوند.

۲-۵-۱۲ بازنگری فنی برنامه های کاربردی پس از اعمال تغییرات در سیستم عامل

هنگامی که سیستم های عامل تغییر می یابند ، لازم خواهد بود تا اقدامات لازم جهت بازنگری برنامه های کاربردی مهم و حیاتی صورت پذیرد و تست های لازم انجام شود تا به این ترتیب از مصون ماندن عملیات های سازمان یا امنیت در برابر تاثیرات سوء ناشی از این تغییرات اطمینان حاصل شود.

۳-۵-۱۲ محدودیت در اعمال تغییرات در بسته های نرم افزاری

عدم تشویق به اعمال تغییرات در بسته های نرم افزاری و محدود نمودن آنها به تغییرات ضروری ، از جمله مواردی است که باید مد نظر قرار داده شوند. در این ارتباط لازم خواهد بود تا تمامی تغییرات بدقت شوند.

۴-۵-۱۲ درز اطلاعات

جلوگیری از هر گونه فرصتی که منجر به درز اطلاعات گردد ، اکیدا" توصیه می شود.

۵-۵-۱۲ توسعه نرم افزارهای خریداری شده از خارج از کشور

توسعه نرم افزارهای تامین شده از طریق منابع خارجی باید توسط سازمان تحت نظارت و سرپرستی قرار گیرد.

۶-۱۲ مدیریت آسیب پذیری فنی

هدف: کاهش ریسک های ناشی از بهره برداری از آسیب پذیری های فنی .

مدیریت آسیب پذیری فنی باید به صورت موثر ، سیستماتیک و به صورت تکرار پذیر به مورد اجرا گذاشته شود ، ضمن آن که ملاحظات لازم برای تایید اثربخشی آن باید صورت پذیرد.سیستم های عامل و سایر برنامه های کاربردی در حال استفاده از جمله مواردی هستند که در این فرآیند باید مورد ملاحظه قرار داده شود.

۱-۶-۱۲ آسیب پذیری های فنی

اطلاعات به موقع درباره آسیب پذیری های فنی سیستم های اطلاعاتی در حال استفاده باید دریافت شود و اگر سازمانی در معرض این گونه آسیب پذیری ها قرار گرفته است ،لازم خواهد بود تا ارزیابی های لازم صورت پذیرد و اقدامات مناسب برای پرداختن به ریسک های مترتب بر آن به عمل آید.

۱۳ – مدیریت حوادث مربوط به امنیت اطلاعات

۱-۱۳ گزارش دهی حوادث مربوط به امنیت اطلاعات و نقاط ضعف آنها

هدف : حصول اطمینان از این که حوادث مربوط به امنیت اطلاعات و نقاط ضعف مربوط به سیستم های اطلاعاتی به گونه ای گزارش شده است که امکان اتخاذ اقدامات اصلاحی به موقع وجود دارد.

رویه های اجرایی تعدیل و گزارش دهی رسمی حوادث باید تعیین و به مورد اجرا درآید و کلیه کارکنان ، پیمانکاران و کاربران ثالث باید نسبت به رویه های مربوط به گزارش دهی انواع مختلف حوادث و نقاط ضعفی که می توانند به نحوی از انحا بر امنیت دارایی های سازمان تاثیر بگذارند ، شناخت و آگاهی کافی داشته باشند. ایشان ملزم خواهند بود تا حوادث مربوط به امنیت اطلاعات و نقاط ضعف موجود در نقاط تماس مشخص شده را در اسرع وقت گزارش نمایند.

۱-۱-۱۳ گزارش دهی حوادث مربوط به امنیت اطلاعات

حوادث مربوط به امنیت اطلاعات باید در اسرع وقت و از طریق سلسله مراتب مدیریتی گزارش شوند.

۲-۱-۱۳ گزارش دهی درباره نقاط ضعف امنیت

تمامی کارکنان ، پیمانکاران و کاربران ثالث سیستم ها و خدمات اطلاعاتی ملزم خواهند بود در صورت مشاهده هر گونه نقطه ضعف در سیستم یا خدمات ، موارد را گزارش نمایند.

۲-۱۳ مدیریت حوادث مربوط به امنیت اطلاعات و روش های بهبود

هدف : حصول اطمینان از اتخاذ یک رویکرد موثر و ثابت در مدیریت حوادث امنیت اطلاعات.

برای آن که شرایط لازم برای پرداختن و بررسی رویدادهای امنیت اطلاعات و نقاط ضعف آنها به صورت موثر و کارآمد مهیا گردد ، لازم خواهد بود تا مسئولیت ها و رویه های اجرایی تعیین و به مورد اجرا گذاشته شود.اجرای فرآیند بهبود مستمر در پروسه عکس العمل ، نظارت و مدیریت کلی حوادث امنیت اطلاعات ، لازم و اجتناب ناپذیر می باشد.

در مواردی که ارائه ادله و شواهد لازم دانسته شده باشد ، لازم خواهد بود تا نسبت به جمع آوری آنها اقدام و به این ترتیب از انطباق با الزامات قانونی اطمینان حاصل نمود.

۱-۲-۱۳ مسئولیت ها و رویه ها

مسئولیت های مدیریت و رویه های اجرایی باید به نحو مقتضی تعیین و تبیین شود تا به این ترتیب از واکنش سریع ، موثر و به موقع به رویدادهای امنیت اطلاعات اطمینان حاصل شود.

۳-۲-۱۳ جمع آوری مدارک و شواهد

در مواردی که اقدامات پیگیری علیه یک فرد یا سازمان پس از بروز حادث امنیت اطلاعات مستلزم یک اقدام قانونی باشد (اعم از مدنی یا جنایی) لازم خواهد بود تا شواهد و ادله کافی جمع آوری ، نگهداری و بگونه ای ارائه گردد که با قوانین مربوط به طرح ادله در مجامع قضایی مطابقت داشته باشد.

۱۴ – مدیریت تداوم فعالیت های کاری

۱۴-۱ جنبه های امنیت اطلاعات در مدیریت تداوم فعالیت های کاری

هدف : خنثی نمودن هر گونه اختلال در فعالیت های کاری و محافظت از فرآیندهای کاری حیاتی در برابر اثرات ناشی از خرابی های عمده در سیستم های اطلاعات یا آسیب های جدی در آنها و حصول اطمینان از ادامه و از سرگیری به موقع آنها.

یک فرآیند مدیریت تداوم فعالیت های کاری باید به گونه ای اجرا شود که تاثیر آن بر سازمان به حداقل کاهش یابد و امکان از سر گیری مجدد آنها پس از آسیب های وارده به دارایی های اطلاعات (که ممکن است ناشی از بلایای طبیعی ، تصادفات ، خرابی تجهیزات و اقدامات تعمدی باشد) تا حـد مورد قبول از طریق ترکیب روش های کنترلی پیشگیرانه و بازیابی فراهم گردد. تعیین فرآیندهای کاری حیاتی و مهم در این فرآیند و ادغام الزامات مدیریت امنیت اطلاعات تداوم فعالیت های کاری با سایر الزامات تداوم مربوط به سایر جنبه ها از جمله عملیات ها ، جذب پرسنل ، ماتریال ها ، حمل و نقل و تاسیسات ، لازم و ضروری می باشد.

پیامدهای ناشی از بروز بلایا ، معایب امنیتی ، از بین رفتن خدمات و در دسترس پذیری خدمات از جمله مواردی هستند که انجام تجزیه و تحلیل تاثیر کاری در مورد آنها لازم و اجتناب ناپذیر خواهد بود. برنامه های تداوم فعالیت های کاری بایـــد بگونه ای تدوین ، تبیین و به مورد اجرا درآید که اطمینان لازم در خصوص از سرگیری به موقع عملیات های اساسی حاصل گردد. در این ارتباط ، امنیت اطلاعات باید به عنوان جزء لاینفکی از فرآیند کلی تداوم فعالیت های کاری و سایر فرآیندهای مدیریتی درون سازمان در نظر گرفته شود.

مدیریت تداوم فعالیت های کاری باید روش های کنترلی جهت شناسایی ، تشخیص و کاهش ریسک ها و همچنین فرآیند کلی ارزشیابی ریسک را شامل شده و پیامدهای ناشی از رویدادهای مخرب را کاهش دهد و از دسترسی پذیری آسان اطلاعات مورد نیاز جهت فرآیندهای کاری اطمینان حاصل نماید.

۱۴-۱-۱ لحاظ نمودن امنیت اطلاعات در فرآیند مدیریت تداوم فعالیت های کاری

تعیین و اجرای یک فرآیند مدیریتی برای تداوم فعالیت های کاری در سطح سازمان ، لازم و ضروری خواهد بود. این فرآیند باید دربردارنده الزامات امنیت اطلاعات مورد نیاز برای تداوم فعالیت های کاری سازمان باشد.

۱۴-۱-۲ تداوم فعالیت های کاری و ارزشیابی ریسک

حوادثی که به نحوی از انحا می توانند باعث بروز اختلال در فرآیندهای کاری شوند باید به همراه احتمال و تاثیر این گونه اختلالات و پیامدهای ناشی از آنها در امنیت اطلاعات ، تعیین و شناسایی شوند.

۱۴-۱-۳ توسعه و اجرای طرح های استمرار با در نظر گرفتن امنیت اطلاعات

برنامه ها باید بگونه ای تبیین و به مورد اجرا درآیند که امکان حفظ یا ازسرگیری عملیات ها و حصول اطمینان از دسترسی پذیری اطلاعات در سطح مورد انتظار و در مقیاس های زمانی و پس ا اختلال در ، یا خرابی فرآیندهای کاری حیاتی و مهم وجود داشته باشد.

۱۴-۱-۴ چهارچوب برنامه ریزی تداوم فعالیت های کاری

در این بخش و به منظور حصول اطمینان از عدم مغایرت برنامه ها و این که در آنها به الزامات امنیت اطلاعات اشاره شده است و به منظور تعیین اولویت های تست و نگهداری ، توجه و رعایت یک چهارچوب مجزا از برنامه های تداوم فعالیت های کاری لازم و اجتناب ناپذیر خواهد بود.

۵-۱-۱۴ تست ، نگهداری و ارزشیابی مجدد برنامه های تداوم فعالیت های کاری

برنامه های تداوم فعالیت های کاری باید به صورت منظم تست و بروزسازی شوند تا به این ترتیب از بروز بودن و موثر بودن آنها اطمینان حاصل گردد.

۱-۱۵ انطباق با الزامات قانونی

هدف : جلوگیری از هر گونه موارد نقض قوانین ، مقررات ، آیین نامه ها یا تعهدات قراردادی و هر یک از الزامات امنیتی.

طراحی ، راه اندازی ، استفاده و نگهداری سیستم های اطلاعاتی ، تابع الزامات قانونی ، آیین نامه ای و قراردادی امنیت هستند.مشاوره با مشاورین حقوقی سازمان یا کارورزان حقوقی ذیصلاح درباره الزامات قانونی خاص ، الزامی و اجتناب ناپذیر می باشد. الزامات قانونی در هر کشور متفاوت می باشد و لذا برای هر گـــــــونه اطلاعاتی که در یک کشور ایجاد و به کشور دیگر ارسال می شود ، الزامات قانونی خاصی تعیین می شود.(به عنوان مثال جریان داده ای فرا مرزی) .

۱-۱-۱۵ تعیین قوانین لازم الاجرا

کلیه الزامات قانونی ، حقوقی و قراردادی و رویکرد سازمان در برآورده نمودن این الزامات باید به طور صریح و روشن تعریف ، مستند سازی و برای هر یک از سیستم های اطلاعاتی و سازمان های ذیربط بروز سازی شود.

۲-۱-۱۵ حقوق دارایی های معنوی (IPR)

رویه های اجرایی مناسب باید بگونه ای به مورد اجرا گذاشته شود که از انطباق آنها با الزامات قانونی ، حقوقی و قراردادی مربوط به استفاده از هر یک از مطالبی که در مورد آنهـــــا حقوق دارایی های معنوی صادق است و همچنین الزامات مربوط به استفاده از محصولات نرم افزاری اختصاصی ، اطمینان حاصل شود.

۳-۱-۱۵ محافظت از سوابق سازمانی

محافظت از سوابق مهم و حائز اهمیت در برابر هر گونه خسارت ، نابودی و تحریف باید بر اساس الزامات قانونی ، حقوقی ، قراردادی یا کاری انجام پذیرد.

۴-۱-۱۵ محافظت از داده ها و محرمانه تلقی نمودن اطلاعات فردی

حصول اطمینان درباره محافظت از داده ها و حفظ محرمانگی ، به شرحی که در قوانین ، مقررات و بر حسب مورد مفاد قرارداد مقرر گردیده است ، الزامی و اجتناب ناپذیر خواهد بود.

۵-۱-۱۵ جلوگیری از موارد سوء استفاده از مراکز پردازش اطلاعات

هر گونه استفاده از مراکز پردازش اطلاعات جهت اهداف غیر مجاز از سوی کاربران ممنوع بوده و در این خصوص لازم خواهد بود تا اقدامات کنترلی لازم برای جلوگیری از دسترسی غیر مجاز کاربران به این مراکز صورت پذیرد.

۶-۱-۱۵ تنظیم روش های کنترلی رمزگذاری

روش های کنترلی رمزگذاری باید بر اساس موافقت نامه ها ، قوانین و مقررات مربوطه مورد استفاده قرار گیرد.

۲-۱۵ انطباق با خط مشی ها و استانداردهای امنیت و انطباق فنی

هدف: حصول اطمینان از انطباق سیستم ها با خط مشی ها و استانداردهای امنیت سازمانی

امنیت سیستم های اطلاعاتی باید در فواصل زمانی معین مورد بازنگری قرار گیرد.

این گونه بازنگری ها باید بر اساس سیاست ها و خط مشی های امنیتی مناسب و پلاتفورم های فنی انجام پذیرد و سیستم های اطلاعاتی باید از حیث انطباق با استانداردهای اجرای امنیت و روش های امنیت مستند سازی شده مورد ممیزی قرار گیرد.

۱-۲-۱۵ انطباق با خط مشی ها و استانداردهای امنیت

مدیران ملزم خواهند بود تا از اجرای صحیح رویه های امنیتی در چهارچوب مسئولیت های خویش و وجود انطباق با خط مشی ها و استانداردهای امنیتی اطمینان حاصل نمایند.

۲-۲-۱۵ بازبینی (چک) انطباق فنی

سیستم های اطلاعاتی باید از حیث انطباق با استانداردهای اجرای امنیت ، در فواصل زمانی منظم چک شوند.

۳-۱۵ ملاحظات مربوط به ممیزی سیستم های اطلاعات

هدف : افزایش اثر بخشی و کاهش تداخل در فرآیند ممیزی سیستم های اطلاعاتی یا تداخل های ناشی از این فرآیند.
تعیین روش های کنترلی برای محافظت و نگاهداری از سیستم های عملیاتی و ابزارهای ممیزی در جریان ممیزی سیستم های اطلاعاتی لازم و اجتناب ناپذیر خواهد بود
به منظور محافظت از تمامیت و جلوگیری از هر گونه موارد سوء استفاده از ابزارهای میزی ، لازم خواهد بود تا روش های محافظتی لازم تعیین و به مورد اجرا گذاشته شود. .

۱-۳-۱۵ ممیزی سیستم های اطلاعات

الزامات و فعالیت های ممیزی مربوط به چک های سیستم های عملیاتی باید بدقت برنامه ریزی و مورد توافق قرار گیرد تا به این ترتیب ریسک ناشی از اختلال و وقفه در فرآیندهای کاری به حداقل کاهش یابد.

۲-۳-۱۵ محافظت از ابزارهای ممیزی سیستم های اطلاعات

دسترسی به ابزارهای ممیزی سیستم های اطلاعاتی باید بگونه ای باشد که از هر گونه سوء استفاده یا خطرات احتمالی جلوگیری شود.

www.tehranportal.org