مرکز مشاوره و اطلاع رسانی

سیستم کاران

سیستم مدیریت امنیت اطلاعات

ISO/IEC 27001:2013

تهیه کننده :

مرکز مشاوره و اطلاع رسانی سیستم کاران

WWW.SYSTEMKARAN.COM

پیشگفتار

سازمان بین المللی استاندارد (ISO) و کمیسیون بین المللی الکتروتکنیک (IEC) ، سیستمی تخصصی را جهت استانداردسازی در

سطح دنیا ایجاد نموده اند . نهادهای ملی عضو ISO یا IEC ، توسط کمیته های فنی تدوین شده از سوی سازمان مربوطه شان ، در تدوین استانداردهای بین المللی مشارکت می کنند و به زمینه های خاص فعالیت های فنی می پردازند. کمیته های فنی ISO و IE ، در زمینه هایی با منافع مشترک ، با همدیگر همکاری میکنند . سایر سازمان های بین المللی ، دولتی یا غیردولتی وابسته به ISO و IEC نیز در این زمینه مشارکت دارند . ISO و IEC ، کمیته فنی مشترکی را در حوزه فناوری اطلاعات تحت عنوان ISO/IEC JTC 1 تشکیل داده اند .

پیشنویس استانداردهای بین المللی ، مطابق با قوانین مندرج در بخش ۲ دستورالعمل های ISO/IEC تهیه شده است . وظیفه اصلی کمیته فنی مشترک ، آماده سازی استانداردهای بین المللی است . پیشنویس استانداردهای بین المللی مورد تأیید کمیته فنی مشترک ، برای رأی گیری در اختیار نهادهای ملی قرار می گیرد . انتشار به عنوان استاندارد بین المللی منوط به تأیید حداقل ۷۵٪ نهادهای ملی رأی دهنده است .

به این احتمال که ممکن است برخی عناصر این سند ، تحت حقوق ثبت اختراع باشند هم توجه شده است . ISO وIEC مسئولیتی در قبال شناسایی هر یک یا همه این حقوق ندارند .

ISO/IEC 27001 توسط کمیته فرعی SC 27 ، فنون امنیتی فناوری اطلاعات ، زیرمجموعه کمیته فنی مشترک ISO/IEC JTC 1، فناوری اطلاعات ، تهیه شده است .

این ویرایش دوم ، جایگزین و باطل کننده ویرایش اول (ISO/IEC 27001:2005) است که از نظر فنی مورد بازنگری قرار گرفته

است .

۰. مقدمه

۱.۰ کلیات

این استاندارد بین المللی ، به منظور ارئه الزاماتی برای استقرار ، پیاده سازی ، نگهداری و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات تهیه شده است . پذیرش یک سیستم مدیریت امنیت اطلاعات ، یک تصمیم استراتژیک برای یک سازمان است . استقرار و پیاده سازی سیستم مدیریت امنیت اطلاعات در یک سازمان ، تحت تأثیر نیازها و اهداف سازمان ، الزامات امنیتی ، فرایندهای سازمانی به کار گرفته شده و اندازه و ساختار سازمان قرار دارد . انتظار می رود تمامی این عوامل اثرگذار ، در طول زمان دچار تغییر شوند .

سیستم مدیریت امنیت اطلاعات ، با به کارگیری یک فرایند مدیریت مخاطرات ، از محرمانگی ، صحت و دسترس پذیری اطلاعات محافظت می کند و به طرف های ذینفع این اطمینان را می دهد که مخاطرات ، به میزان کافی مدیریت می شوند .

توجه داشته باشید که سیستم مدیریت امنیت اطلاعات ، با فرایندهای سازمان و ساختار مدیریتی کلان ، یکپارچه بوده و بخشی از

آنها است و همچنین امنیت اطلاعات در طراحی ، فرایندها ، سیستم های اطلاعاتی و کنترل ها لحاظ می شود . انتظار می رود که

پیاده سازی یک سیستم مدیریت امنیت اطلاعات ، منطبق با نیازهای سازمان باشد .

این استاندارد بین المللی می تواند توسط طرفهای درونی و بیرونی ، به منظور ارزیابی توانایی یک سازمان در فراهم آوری الزامات امنیت اطلاعات خود ، مورد استفاده قرار گیرد .

ترتیب ارایه الزامات در این استاندارد بین المللی ، بیان کننده اهمیت یا ترتیب پیاده سازی آنها نیست . موارد فهرست

شده ، به

منظور ارجاع های بعدی ذکر شده اند .

استاندارد ISO/IEC 27000 ، نمای کلی و واژگان سیستم های مدیریت امنیت اطلاعات را توصیف نموده و مرجع خانواده استاندارد

سیستم مدیریت امنیت اطلاعات (شامل ISO/IEC 27003[2] ، ISO/IEC 27004[3] و ISO/IEC 27005[4]) به همراه اصطلاحات و تعاریف مرتبط با آن است .

۲.۰ سازگاری با سایر استانداردهای سیستم مدیریت

این استاندارد بین المللی از ساختار سطح بالا ، عناوین یکسان در بندهای فرعی ، متن یکسان ، اصطلاحات مشترک و تعاریف اصلی

موجود در پیوست SL بخش ۱ دستورالعمل های ISO/IEC ، مکمل های تلفیقی ISO استفاده می کند و در نتیجه با سایر استانداردهای سیستم مدیریت که پیوست SL را پذیرفته اند ، سازگار است .

این رویکرد مشترک که در پیوست SL تعریف شده است ، برای آن دسته از سازمان هایی که درنظر دارند یک سیستم مدیریت

واحد را در راستای فراهم آوری الزامات دو یا چند استاندارد سیستم مدیریت اجرا کنند ، مفید خواهد بود .

فناوری اطلاعات – فنون امنیتی – سیستم های مدیریت امنیت اطلاعات – الزامات

۱. قلمرو

این استاندارد بین المللی ، الزاماتی را برای استقرار ، پیاده سازی ، نگهداری و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات در چارچوب سازمان ، مشخص می کند . این استاندارد بین المللی ، همچنین شامل الزاماتی برای ارزیابی و برطرف سازی مخاطرات امنیت اطلاعات ، متناسب با نیازهای سازمان است . الزامات تعیین شده در این استاندارد بین المللی ، عمومی بوده و در تمام سازمان ها ، صرفنظر از نوع ، اندازه یا ماهیت آنها ، قابل اعمال است . کنارگذاری هر یک از الزامات مشخص شده در بندهای ٤ تا ۱۰، چنانچه یک سازمان ادعای تطابق با این استاندارد بین المللی را داشته باشد ، مورد پذیرش نخواهد بود.

۲. مراجع اصلی

اسناد زیر، به صورت کلی و جزئی ، در این سند به صورت الزامی ، مورد ارجاع قرار گرفته اند و در راستای کاربرد این سند ، مراجعی که با ذکر تاریخ ، ارجاع داده شده اند فقط همان ویرایش ، و مراجعی که بدون ذکر تاریخ ، ارجاع داده شده اند آخرین ویرایش سند اشاره شده (شامل همه اصاحیه ها) مورد استناد است .

ISO/IEC 27000 ، فناوری اطلاعات – فنون امنیتی – سیستم های مدیریت امنیت اطلاعات – نمای کلی و واژگان

۳. اصطلاحات و تعاریف

در راستای اهداف این سند ، اصطلاحات و تعاریف ذکر شده در ISO/IEC 27000 به کار می روند .

٤. چارچوب سازمان

۱.٤ شناخت سازمان و چارچوب آن

سازمان باید مسایل درونی و بیرونی مرتبط با اهداف سازمان و مسایل تأثیرگذار در امکان دستیابی به نتایج مورد نظر سیستم

مدیریت امنیت اطلاعات را شناسایی کند .

نکته : تعیین این مسایل به استقرار چارچوب بیرونی و درونی سازمان که در بند ۵و۳ از استاندارد[۵] ISO 31000:2009 مطرح شده

است ، اشاره دارد .

۲.٤ شناخت نیازها و انتظارات طرف های ذینفع

سازمان باید موارد زیر را مشخص کند :

الف) طرف های ذینفع مرتبط با سیستم مدیریت امنیت اطلاعات ؛ و

ب) الزامات این طرف های ذینفع در ارتباط با امنیت اطلاعات .

نکته : الزامات طرف های ذینفع ، ممکن است شامل الزامات قانونی ، مقرراتی و تعهدات قراردادی باشد .

۳.٤ تعیین قلمرو سیستم مدیریت امنیت اطلاعات

سازمان باید مرزها و کاربردپذیری سیستم مدیریت امنیت اطلاعات را به منظور استقرار قلمرو خود ، شناسایی کند .

سازمان باید هنگام تعیین قلمرو ، موارد زیر را درنظر بگیرد :

الف) مسایل بیرونی و درونی اشاره شده در بند ۱.٤ ؛

ب) الزامات اشاره شده در بند ۲.٤ ؛ و

ج) واسط ها و وابستگی های بین فعالیت های انجام شده توسط سازمان و فعالیت هایی که توسط سازمان های دیگر انجام می شوند .

قلمرو باید به صورت اطلاعات مستند ، در دسترس باشد .

٤.٤ سیستم مدیریت امنیت اطلاعات

سازمان باید یک سیستم مدیریت امنیت اطلاعات را مطابق با الزامات این استاندارد بین المللی ، ایجاد ، پیاده سازی و نگهداری کند .

و آن را به طور مستمر بهبود بخشد .

۵. رهبری

۱.۵ رهبری و تعهد

مدیریت ارشد باید رهبری و تعهد خود را نسبت به سیستم مدیریت امنیت اطلاعات ، از طریق موارد زیر نشان دهد :

الف) حصول اطمینان از اینکه خط مشی امنیت اطلاعات و اهداف امنیت اطلاعات ، ایجاد شده و با مسیر استراتژیک سازمان سازگار هستند .

ب) حصول اطمینان از اینکه الزامات سیستم مدیریت امنیت اطلاعات در فرایندهای سازمان گنجانده شده اند .

ج) حصول اطمینان از اینکه منابع مورد نیاز سیستم مدیریت امنیت اطلاعات ، در دسترس هستند .

د) ابلاغ اهمیت مدیریت امنیت اطلاعات اثربخش و تطابق با الزامات سیستم مدیریت امنیت اطلاعات ؛

ه) اطمینان از اینکه سیستم مدیریت امنیت اطلاعات به نتیجه (نتایج) مورد انتظار دست می یابد .

و) هدایت و پشتیبانی از افراد برای کمک به اثربخشی سیستم مدیریت امنیت اطلاعات ؛

ز) ترویج بهبود مستمر ؛ و

ح) پشتیبانی از سایر نقش های مدیریتی مرتبط جهت نشان دادن رهبری آنها ، به نحوی که در محدوده های مسئولیتی آنها اعمال گردد .

۲.۵ خط مشی

مدیریت ارشد باید یک خط مشی امنیت اطلاعات ایجاد کند که :

الف) متناسب با هدف سازمان باشد .

ب) شامل اهداف امنیت اطلاعات باشد (به بند ۲.۶ مراجعه شود) یا چارچوبی را برای تعیین اهداف امنیت اطلاعات ارایه دهد .

ج) شامل تعهدی مبنی بر فراهم آوری الزامات کاربردپذیر مرتبط با امنیت اطلاعات باشد .

د) شامل تعهدی مبنی بر بهبود مستمر سیستم مدیریت امنیت اطلاعات باشد .

خط مشی امنیت اطلاعات باید :

ه) به صورت اطلاعات مستند ، در دسترس باشد .

و) در داخل سازمان اباغ شود ؛ و

ز) در صورت نیاز ، در اختیار طرف های ذینفع قرار گیرد .

۳.۵ نقش های سازمانی ، مسئولیت ها و اختیارات

مدیریت ارشد باید اطمینان حاصل کند که مسئولیت ها و اختیارات برای نقش های مرتبط با امنیت اطلاعات ، تعیین و ابلاغ شده اند .

مدیریت ارشد باید مسئولیت و اختیارات را برای موارد زیر تعیین کند :

الف) حصول اطمینان از انطباق سیستم مدیریت امنیت اطلاعات با الزامات این استاندارد بین المللی ؛ و

ب) گزارش عملکرد سیستم مدیریت امنیت اطلاعات به مدیریت ارشد .

نکته : مدیریت ارشد ممکن است مسئولیت ها و اختیاراتی را نیز برای گزارش عملکرد سیستم مدیریت امنیت اطلاعات در درون سازمان تعیین کند .

۶. طرح ریزی

۱.۶ اقداماتی برای درنظر گرفتن مخاطرات و فرصت ها

۱.۱.۶ کلیات

هنگام طراحی سیستم مدیریت امنیت اطلاعات ، سازمان باید مسایل اشاره شده در بند ۱.٤ و الزامات اشاره شده در بند ۲.٤ را مدنظر قرار داده و مخاطرات و فرصت هایی را که نیازمند مقابله هستند ، در راستای موارد زیر تعیین کند :

الف) حصول اطمینان از اینکه سیستم مدیریت امنیت اطلاعات می تواند به نتیجه (نتایج) مطلوب خود دست یابد .

ب) از بروز اثرات ناخواسته ممانعت نموده یا آنها را کاهش دهد ؛ و

ج) به بهبود مستمر دست یابد .

سازمان باید موارد زیر را طرح ریزی کند :

د) اقدام هایی برای مقابله با این مخاطرات و فرصت ها ؛ و

ه) چگونگی

۱. گنجاندن و پیاده سازی این اقدام ها در فرایندهای سیستم مدیریت امنیت اطلاعات سازمان ؛ و

۲. ارزشیابی اثربخشی این اقدامات .

۲.۱.۶ ارزیابی مخاطرات امنیت اطلاعات

سازمان باید یک فرایند ارزیابی مخاطرات امنیت اطلاعات را تعریف نموده و به کار گیرد که :

الف) معیارهایی را برای مخاطرات امنیت اطلاعات ، ایجاد و نگهداری کند که شامل موارد زیر باشد :

۱. معیارهای پذیرش مخاطرات ؛ و

۲. معیارهایی برای انجام ارزیابی مخاطرات امنیت اطلاعات .

ب) اطمینان دهد که ارزیابی های مکرر مخاطرات امنیت اطلاعات ، نتایج نامتناقض ، معتبر و مقایسه پذیر تولید می کنند .

ج) مخاطرات امنیت اطلاعات را شناسایی کند :

۱. به کارگیری فرایند ارزیابی مخاطرات امنیت اطلاعات برای شناسایی مخاطرات مربوط به فقدان محرمانگی ، صحت و

دسترس پذیری اطلاعات در قلمرو سیستم مدیریت امنیت اطلاعات ؛ و

۲. شناسایی مالکان مخاطره .

د) مخاطرات امنیت اطلاعات را تحلیل کند :

۱. ارزیابی پیامدهای احتمالی وقوع مخاطرات شناسایی شده در بند ۲.۱.۶ - ج -۱؛

۲. ارزیابی احتمال واقع گرایانه وقوع مخاطرات شناسایی شده در بند ۲.۱.۶ - ج - ۱؛

۳. مشخص نمودن سطوح مخاطرات .

ه) مخاطرات امنیت اطلاعات را ارزشیابی کند :

۱. مقایسه نتایج تحلیل مخاطرات با معیارهای مخاطرات ایجاد شده در بند ۱.۲.۶ – الف ؛ و

۲. اولویت بندی مخاطرات تحلیل شده برای برطرف سازی مخاطرات .

سازمان باید اطلاعاتی مستند درباره فرایند ارزیابی مخاطرات امنیت اطلاعات نگهداری کند.

۳.۱.۶ برطرف سازی مخاطرات امنیت اطلاعات

سازمان باید یک فرایند برطرف سازی مخاطرات امنیت اطلاعات را تعریف و اعمال کند تا بتواند :

الف) با درنظر گرفتن نتایج ارزیابی مخاطرات ، گزینه های مناسب جهت برطرف سازی مخاطرات امنیت اطلاعات را انتخاب نماید .

ب) تمامی کنترل های ضروری به منظور پیاده سازی گزینه (های) انتخابی برطرف سازی مخاطرات امنیت اطلاعات را تعیین کند .

نکته : سازمان ها می توانند در صورت لزوم ، کنترل هایی طراحی کنند یا آنها را از هر منبع دیگری شناسایی کنند .

ج) کنترل های تعیین شده در بند ۳.۱.۶ ب در بالا را با کنترل های موجود در پیوست الف ، مقایسه کرده و بررسی کند که هیچ

یک از کنترل های ضروری از قلم نیافتاده است .

نکته ۱: پیوست الف شامل فهرست جامعی از اهداف کنترلی و کنترل ها است . استفاده کنندگان از این استاندارد بین المللی برای

حصول اطمینان از اینکه هیچ یک از کنترل های ضروری نادیده گرفته نشده است ، به پیوست الف ارجاع داده می شوند .

نکته ۲ : کنترل های انتخاب شده به طور ضمنی شامل اهداف کنترلی هستند . اهداف کنترلی و کنترل های فهرست شده در

پیوست الف ، جامع نبوده و ممکن است اهداف کنترلی و کنترل های اضافی هم مورد نیاز باشد .

د) یک بیانیه کاربست پذیری که شامل کنترل های ضروری (مراجعه به بند ۳.۱.۶ زیر بند ب و زیر بند ج) و دلیل استفاده از آنها بدون درنظر گرفتن اینکه پیاده سازی شده یا نشده اند و توجیه کنارگذاری کنترل های پیوست الف باشد ، ایجاد نماید .

ه) یک طرح برطرف سازی مخاطرات امنیت اطلاعات را تدوین نماید ؛ و

و) طرح برطرف سازی مخاطرات امنیت اطلاعات و پذیرش مخاطرات امنیت اطلاعات باقی مانده را از مالکان مخاطرات

اخذ نماید .

سازمان باید اطلاعاتی مستند درباره فرایند برطرف سازی مخاطرات امنیت اطلاعات ، نگهداری کند .

نکته : فرایند ارزیابی و برطرف سازی مخاطرات امنیت اطلاعات در این استاندارد بین المللی ، با اصول و رهنمودهای کلی / عمومی موجود در ISO 31000[5] مطابقت دارد .

۲.۶ اهداف امنیت اطلاعات و طرحریزی برای دستیابی به آنها

سازمان باید اهداف امنیت اطلاعات را برای کارکردها و سطوح مرتبط ایجاد کند .

اهداف امنیت اطلاعات باید :

الف) با خط مشی امنیت اطلاعات ، سازگار باشند .

ب) قابل اندازه گیری باشند (در صورت عملی بودن) ؛

ج) الزامات قابل اجرای امنیت اطلاعات ، و نتایج ارزیابی مخاطرات و نتایج برطرف سازی مخاطرات را درنظر بگیرند .

د) ابلاغ شوند ؛ و

ه) در صورت نیاز ، به روزرسانی شوند .

سازمان باید اطلاعاتی مستند را درباره اهداف امنیت اطلاعات ، نگهداری کند .

سازمان باید هنگام طرح ریزی نحوه دستیابی به اهداف امنیت اطلاعات ، موارد زیر را تعیین کند :

و) چه چیزی انجام خواهد شد .

ز) چه منابعی مورد نیاز خواهند بود .

ح) چه افرادی مسئول خواهند بود .

ط) چه زمانی تکمیل خواهد شد ؛ و

ی) نتایج ، چگونه ارزشیابی خواهند شد .

۷. پشتیبانی

۱.۷ منابع

سازمان باید منابع مورد نیاز به منظور استقرار ، پیاده سازی ، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات را تعیین و فراهم کند .

۲.۷ صلاحیت

سازمان باید :

الف) صاحیت های مورد نیاز افرادی که تحت کنترل سازمان کار می کنند و بر روی عملکرد امنیت اطلاعات تأثیرگذار هستند را

تعیین کند .

ب) اطمینان حاصل کند که این افراد ، بر اساس تحصیلات ، آموزش ها یا تجربیات مناسب ، صلاحیت دارند .

ج) هر جا که امکانپذیر است ، اقدام هایی را به منظور کسب صلاحیت لازم انجام داده و اثربخشی اقدام های انجام شده را ارزشیابی کند ؛ و

د) اطلاعات مستند مناسب را به عنوان مدرکی مبنی بر صلاحیت ، نگهداری کند .

نکته : اقدامات امکانپذیر ، به طور مثال می توانند شامل ارایه آموزش ، مشاوره یا جابجایی کارکنان فعلی ، یا استخدام یا قرارداد با افراد شایسته باشد .

۳.۷ آگاه سازی

افرادی که تحت کنترل سازمان فعالیت می کنند باید نسبت به موارد زیر آگاه باشند :

الف) خط مشی امنیت اطلاعات ؛

ب) سهم آنها در اثربخشی سیستم مدیریت امنیت اطلاعات ، شامل منافع حاصل از بهبود عملکرد امنیت اطلاعات ؛ و

ج) پیامدهای عدم انطباق با الزامات سیستم مدیریت امنیت اطلاعات .

٤.٧ ارتباطات

سازمان باید نیاز به ارتباطات درونی و بیرونی را در رابطه با سیستم مدیریت امنیت اطلاعات تعیین کند که شامل موارد زیر

میشود :

الف) در چه زمینه ای ارتباط برقرار شود .

ب) چه زمانی ارتباط برقرار شود .

ج) با چه کسی ارتباط برقرار شود .

د) چه کسی باید ارتباط را برقرار کند ؛ و

ه) فرایندهایی که ارتباط باید از طریق آن انجام شود .

٥.٧ اطلاعات مستند

١.٥.٧ کلیات

سیستم مدیریت امنیت اطلاعات سازمان باید شامل این موارد باشد :

الف) اطلاعات مستند مورد نیاز این استاندارد بین المللی ؛ و

ب) اطلاعات مستندی که از سوی سازمان برای اثربخشی سیستم مدیریت امنیت اطلاعات ، ضروری تشخیص داده شده است .

نکته : گستره مستندسازی سیستم مدیریت امنیت اطلاعات می تواند به دایل زیر برای هر سازمان متفاوت باشد :

١. اندازه سازمان و نوع فعالیت ها ، فرایندها ، محصولات و خدمات آن ؛

٢. پیچیدگی فرایندها و تعاملات آنها ؛ و

٣. صلاحیت افراد .

٢.٥.٧ ایجاد و به روزرسانی

هنگام ایجاد و به روزرسانی اطلاعات مستند ، سازمان باید از مناسب بودن موارد زیر اطمینان حاصل کند :

الف) شناسایی و توصیف (مثلاً یک عنوان، تاریخ، نگارنده یا شماره ارجاع) ؛

ب) قالب (مثلاً زبان ، نسخه نرم افزار ، گرافیک) و رسانه (مثلاً کاغذی ، الکترونیکی) ؛ و

ج) بازنگری و تصویب جهت سازگاری و کفایت .

٣.٥.٧ کنترل اطلاعات مستند

اطلاعات مستند مورد نیاز سیستم مدیریت امنیت اطلاعات و این استاندارد بین المللی باید کنترل شوند تا اطمینان حاصل شود :

الف) در مکان و زمانی که برای استفاده ، مورد نیاز هستند ، در دسترس و مناسب هستند ؛ و

ب) به میزان کافی حفاظت می شوند (به عنوان مثال در برابر فقدان محرمانگی ، استفاده نادرست یا فقدان صحت) .

به منظور کنترل اطلاعات مستند ، سازمان باید در صورت قابلیت اجرا ، فعالیت های زیر را مورد رسیدگی قرار دهد :

ج) توزیع ، دسترسی ، بازیابی و استفاده ؛

د) ذخیره سازی و محافظت ، شامل حفظ خوانایی ؛

ه) کنترل تغییرات (برای مثال کنترل نسخه) ؛ و

و) نگهداشتن و از بین بردن .

اطلاعات مستند با منشأ بیرونی که سازمان برای طرح ریزی و اجرای سیستم مدیریت امنیت اطلاعات ضروری تشخیص داده است باید به نحوی مناسب ، شناسایی و کنترل شوند .

نکته : دسترسی به معنای تصمیم درباره صرفاً اجازه مشاهده اطلاعات مستند یا اجازه و اختیار جهت مشاهده و تغییر اطلاعات

مستند و غیره است .

۸. عملیات

۱.۸ طرح ریزی و کنترل عملیات

سازمان باید فرایندهای مورد نیاز برای فراهم آوری الزامات امنیت اطلاعات را طرحریزی ، پیاده سازی و کنترل نموده و اقدام های مشخص شده در بند ۱.۶ را پیاده سازی کند . سازمان همچنین باید طرح هایی را برای دستیابی به اهداف امنیت اطلاعات مشخص شده در بند ۲.۶ پیاده سازی نماید .

سازمان باید اطلاعات مستند تا حدی ضروری را برای حصول اطمینان از اینکه فرایندها مطابق با طرح ها پیشروی داشته اند ،

نگهداری کند .

سازمان باید در صورت لزوم ، اقدام هایی را برای کاهش هرگونه عوارض جانبی انجام دهد تا تغییرات طرح ریزی شده را کنترل و پیامدهای تغییرات ناخواسته را بازنگری نماید و سازمان باید اطمینان حاصل کند که فرایندهای برون سپاری شده ، شناسایی و کنترل می شوند .

۲.۸ ارزیابی مخاطرات امنیت اطلاعات

سازمان باید ارزیابی مخاطرات امنیت اطلاعات را در بازه های زمانی طرحریزی شده یا هنگام وقوع تغییرات مهم یا تغییرات

پیشنهاد شده ، با درنظر گرفتن معیار ایجاد شده در بند ۲.۱.۶ الف ، انجام دهد .

سازمان باید اطلاعاتی مستند را درباره نتایج ارزیابی های مخاطرات امنیت اطلاعات ، نگهداری کند .

۳.۸ برطرف سازی مخاطرات امنیت اطلاعات

سازمان باید طرح برطرف سازی مخاطرات امنیت اطلاعات را پیاده سازی کند .

سازمان باید اطلاعاتی مستند را درباره نتایج برطرف سازی مخاطرات امنیت اطلاعات ، نگهداری کند .

۹. ارزشیابی عملکرد

۱.۹ پایش ، اندازه گیری ، تحلیل و ارزشیابی

سازمان باید عملکرد امنیت اطلاعات و اثربخشی سیستم مدیریت امنیت اطلاعات را ارزشیابی کند .

سازمان باید موارد زیر را مشخص کند :

الف) چه چیزهایی به پایش و اندازه گیری نیاز دارند ، از جمله فرایندها و کنترل های امنیت اطلاعات ؛

ب) در صورت قابلیت اعمال ، روش هایی برای پایش ، اندازه گیری ، تحلیل و ارزشیابی ، به منظور حصول اطمینان از معتبر بودن

نتایج ؛

نکته : روش های انتخابی باید نتایج قابل قیاس و تکرارپذیر تولید کنند تا معتبر شناخته شوند .

ج) چه زمانی باید پایش و اندازه گیری انجام شود .

د) چه کسی باید پایش و اندازه گیری را انجام دهد .

ه) چه زمانی نتایج حاصل از پایش و اندازه گیری باید مورد تحلیل و ارزشیابی قرار گیرند ؛ و

و) چه کسی باید این نتایج را تحلیل و ارزشیابی کند .

سازمان باید اطلاعات مستند مناسب را به عنوان مدرک پایش و اندازه گیری نتایج ، نگهداری کند .

۲.۹ ممیزی داخلی

سازمان باید ممیزی های داخلی را در فاصله های زمانی طرحریزی شده انجام دهد تا اطلاع حاصل شود که آیا سیستم مدیریت

امنیت اطلاعات :

الف) با موارد زیر انطباق دارد :

۱. الزامات خود سازمان برای سیستم مدیریت امنیت اطلاعات ؛ و

۲. الزامات این استاندارد بین المللی ؛

ب) به طور اثربخش ، پیاده سازی و نگهداری می شود .

سازمان باید :

ج) برنامه (های) ممیزی شامل دفعات تکرار ، روش ها ، مسئولیت ها ، الزامات طرح ریزی و گزارش دهی را طرح ریزی ، مستقر ، پیاده سازی و نگهداری کند . برنامه (های) ممیزی باید اهمیت فرایندهای مورد نظر و نتایج ممیزی های قبلی را درنظر بگیرند .

د)معیارهای ممیزی و قلمرو هر ممیزی را تعریف کند .

ه) در انتخاب ممیزان و انجام ممیزی ها ، از واقع بینی و بی طرفی فرایند ممیزی اطمینان حاصل نماید .

و) اطمینان حاصل کند که نتایج ممیزی ها به مدیریت مربوطه گزارش داده می شوند ؛ و

ز) اطلاعات مستند را به عنوان مدرک برنامه (های) ممیزی و نتایج ممیزی ، نگهداری کند .

۳.۹ بازنگری مدیریت

مدیریت ارشد باید سیستم مدیریت امنیت اطلاعات سازمان را در فاصله های زمانی طرحریزی شده ، بازنگری کند تا از تداوم

سازگاری ، کفایت و اثربخشی آن اطمینان حاصل نماید .

در بازنگری مدیریت ، باید موارد زیر درنظر گرفته شود :

الف) وضعیت اقدامات در بازنگری های قبلی مدیریت ؛

ب) تغییرات در مسایل بیرونی و درونی مرتبط با سیستم مدیریت امنیت اطلاعات ؛

ج) بازخوردها درباره عملکرد امنیت اطلاعات ، شامل روند :

۱. عدم انطباقها و اقدام های اصاحی ؛

۲. نتایج پایش و اندازه گیری ؛

۳. نتایج ممیزی ؛ و

٤. تحقق اهداف امنیت اطلاعات .

د) بازخورد از طرف های ذینفع ؛

ه) نتایج ارزیابی مخاطرات و وضعیت طرح برطرف سازی مخاطرات ؛ و

و) فرصت ها برای بهبود مستمر .

خروجی های بازنگری مدیریت باید دربرگیرنده تصمیمات مربوط به فرصت های بهبود مستمر و هرگونه نیاز به تغییر در سیستم مدیریت امنیت اطلاعات باشد .

سازمان باید اطلاعات مستند را به عنوان مدرک نتایج بازنگری های مدیریت ، نگهداری کند .

۱۰. بهبود

۱.۱۰ عدم انطباق و اقدام اصالحی

هنگام وقوع یک عدم انطباق ، سازمان باید :

الف) نسبت به عدم انطباق ، واکنش نشان داده و در صورت مقتضی :

۱. برای کنترل و اصلاح آن اقدام کند ؛ و

۲. با پیامدهای آن مقابله کند .

ب) نیاز به اقدام برای رفع علل عدم انطباق را به منظور جلوگیری از تکرار یا بروز آن در جای دیگر ، از طریق موارد زیر تعیین

کند :

۱. بازنگری عدم انطباق ؛

۰. تعیین علل عدم انطباق ؛ و

۲. شناسایی وجود عدم انطباق های مشابه یا احتمال وقوع آنها .

ج) اقدام های مورد نیاز را پیاده سازی کند .

د) اثربخشی تمام اقدام های اصلاحی انجام شده را بازنگری کند ؛ و

ه) در صورت لزوم ، تغییراتی را در سیستم مدیریت امنیت اطلاعات ایجاد کند .

اقدام های اصلاحی باید متناسب با اثرات عدم انطباق های مشاهده شده باشند .

سازمان باید اطلاعات مستند را به عنوان مدرک برای موارد زیر نگهداری کند :

و) ماهیت عدم انطباق ها و تمام اقدام های انجام شده متعاقب آن ؛ و

ز) نتایج هر یک از اقدام های اصلاحی .

۲.۱۰ بهبود مستمر

سازمان باید به طور مستمر ، سازگاری ، کفایت و اثربخشی سیستم مدیریت امنیت اطلاعات را بهبود بخشد .

پیوست الف

(الزامی)

کنترل ها و اهداف کنترلی مرجع

اهداف کنترلی و کنترل های فهرست شده در جدول الف.۱ ، به طور مستقیم از بندهای ۵ تا ۱۸ استاندارد [1] ISO/IEC 27002:2013 و منطبق با آنها برگرفته شده اند و در چارچوب بند ۳.۱.۶ مورد استفاده قرار خواهند گرفت .

جدول الف.۷ – اهداف کنترلی و کنترلها

الف.۵ : خط مشی های امنیت اطلاعات		
الف ۱,۵ : هدایت مدیریت برای امنیت اطلاعات		
هدف : تأمین هدایت و پشتیبانی مدیریت از تطابق امنیت اطلاعات ، مطابق با الزامات کسب و کار و قوانین و آیین نامه های مرتبط		
الف .۱,۱,۵	خط مشی های امنیت اطلاعات	کنترل : مجموعه ای از خط مشی های امنیت اطلاعات ، باید تعریف و توسط مدیریت تصویب شود ، منتشر شده و به اطلاع کارکنان و طرف های مرتبط بیرونی برسد .
الف.۲,۱,۵	بازنگری خط مشی های امنیت	کنترل : خط مشی های امنیت اطلاعات باید در فواصل زمانی طرح ریزی شده یا در صورتی که تغییرات مهمی رخ دهد ، به منظور حصول اطمینان از تداوم سازگاری ، کفایت و اثربخشی آنها بازنگری شوند .
الف.۶ : سازمان امنیت اطلاعات		
الف.۱,۶ : سازمان داخلی		
هدف : ایجاد یک چارچوب امنیتی به منظور شروع و کنترل پیاده سازی و اجرای امنیت اطلاعات در درون سازمان		
الف.۱,۱,۶	نقش ها و مسئولیت های امنیت اطلاعات	کنترل : کلیه مسئولیت های امنیت اطلاعات ، باید تعریف و محول شوند .
الف.۲,۱,۶	تفکیک وظایف	کنترل : به منظور کاهش فرصت های دستکاری غیرمجاز یا غیرعمد ، یا سوءاستفاده از دارایی های سازمان ، باید وظایف و حدود مسئولیت های مغایر ، تفکیک شوند .
الف.۳,۱,۶	ارتباط با مراجع معتبر	کنترل : ارتباطات مقتضی با مراجع معتبر مرتبط باید حفظ شود .
الف.٤,۱,۶	ارتباط با گروه های ذینفع ویژه	کنترل : ارتباطات مقتضی با گروه های ذینفع ویژه یا سایر انجمن های امنیتی متخصص و انجمن های حرفه ای باید حفظ شود .
الف.۵,۱,۶	امنیت اطلاعات در مدیریت پروژه	کنترل : امنیت اطلاعات باید در مدیریت پروژه ، صرف نظر از نوع پروژه ، لحاظ شود .
الف.۲,۶ : دستگاه های قابل حمل و دورکاری		
هدف : حصول اطمینان از امنیت دورکاری و استفاده از دستگاه های قابل حمل		
الف.۱,۲,۶	خط مشی دستگاه های قابل حمل	کنترل : یک خط مشی و اقدامات امنیتی پشتیبان ، به منظور مدیریت مخاطرات ایجاد شده به دلیل استفاده از دستگاه های قابل حمل ، باید اتخاذ گردد .
الف.۲,۲,۶	دورکاری	کنترل : یک خط مشی و اقدامات امنیتی پشتیبان ، به منظور حفاظت از اطلاعات قابل دسترس ، پردازش یا ذخیره شده در محل های دورکاری ، باید پیاده سازی شود .

الف .۷ : امنیت منابع انسانی		
الف.۱,۷ : پیش از اشتغال		
هدف : حصول اطمینان از اینکه کارکنان و پیمانکاران ، مسئولیت هایشان را درک کرده و برای نقش های در نظر گرفته شده برای ایشان مناسب هستند .		
الف.۱,۱,۷	گزینش	کنترل : پیشینه تمام داوطلبان استخدام ، باید مطابق با قوانین مرتبط ، آیین نامه ها و اصول اخلاقی ، بررسی گردد و متناسب با الزامات کسب و کار ، طبقه بندی اطلاعاتی که در دسترس قرار می گیرند و مخاطرات بالقوه باشند .
الف.۲,۱,۷	ضوابط و شرایط استخدام	کنترل : توافق های قردادی با کارکنان وپیمانکاران باید بیانگر مسئولیت های ایشان و سازمان ، در قبال امنیت اطلاعت باشد .
الف .۲,۷ : حین خدمت		
هدف : حصول اطمینان از اینکه کارکنان و پیمانکاران از مسئولیت های امنیت اطلاعات خود ، آگاه بوده و آنها را به انجام می رسانند .		
الف.۱,۲,۷	مسئولیت های مدیریت	کنترل : مدیریت باید تمامی کارکنان و پیمانکاران را به بکارگیری امنیت اطلاعات ، مطابق با خط مشی ها و رویه های ایجاد شده سازمان ، الزام نماید .
الف.۲,۲,۷	آگاه سازی ، تحصیل و آموزش امنیت اطلاعات	کنترل : تمامی کارکنان سازمان ، و در صورت لزوم پیمانکاران ، باید به صورت مناسب ، در خصوص خط مشی ها و رویه های سازمان ، تحصیل و آموزش آگاه سازانه ببینند و به طور منظم به روز شوند ، به طوری که کارکرد شغلی ایشان مرتبط باشد .
الف . ۳,۲,۷	فرایند انضباطی	کنترل : باید برای اقدام در برابر کارکنانی که مرتکب نقض امنیت اطلاعات شده اند یک فرایند انضباطی رسمی و ابلاغ شده ، وجود داشته باشد .
الف . ۳,۷ : خاتمه اشتغال یا تغییر شغل		
هدف : محافظت از منافع سازمان ، به عنوان بخشی از فرایند تغییر یا خاتمه اشتغال		
الف .۱,۳,۷	مسئولیت های خاتمه اشتغال یا تغییر شغل	کنترل : مسئولیت ها و وظایف امنیت اطلاعات که پس از خاتمه اشتغال یا تغییر شغل ، معتبر باقی می مانند باید تعریف شده ، به کارکنان یا پیمانکاران ابلاغ و اجبار شوند .
الف .۸ : مدیریت دارایی ها		
الف .۱,۸: مسئولیت دارایی ها		
هدف : شناسایی دارایی های سازمانی و تعریف مسئولیت های حفاظت مناسب		
الف .۱,۱,۸	سیاهه اموال	کنترل : دارایی های مرتبط با اطلاعات و امکانات پردازش اطلاعات باید شناسایی شده و سیاهه ای از این دارایی ها تنظیم و نگهداری شود .
الف.۲,۱,۸	مالکیت دارایی ها	کنترل : دارایی های نگهداری شده در سیاهه باید دارای مالک باشند .
الف.۳,۱,۸	استفاده پسندیده از دارایی ها	کنترل : قوانینی برای استفاده پسندیده از اطلاعات و دارایی های مرتبط با اطلاعات و امکانات پردازش اطلاعات ، باید شناسایی ، مدون و پیاده سازی شوند .
الف.٤,۱,۸	عودت دارایی ها	کنترل : تمامی کارکنان و کاربران طرف بیرونی باید کلیه دارایی های سازمانی را که در اختیار دارند ، به محض خاتمه اشتغال ، قرداد یا توافق نامه ، عودت دهند .
الف. ۲,۸ : طبقه بندی اطلاعات		
هدف : حصول اطمینان از اینکه اطلاعات ، با توجه به اهمیت آن برای سازمان ، به سطح حفاظتی مناسب رسیده است .		

الف.۱,۲,۸	طبقه بندی اطلاعات	کنترل : اطلاعات باید با توجه به الزمات قانونی ، ارزش ، بحرانی بودن و حساس بودن نسبت به افشا یا دستکاری غیر مجاز ، طبقه بندی شوند .
الف.۲,۲,۸	برچسب گذاری اطلاعات	کنترل : باید مجوعه مناسبی از رویه هایی برای برچسب گذاری اطلاعات ، با توجه به الگوی طبقه بندی اطلاعات پذیرفته شده توسط سازمان ، ایجاد و پیاده سازی شود .
الف.۳,۲,۸	اداره کردن دارایی	کنترل : باید رویه هایی برای اداره کردن دارایی ها ، با توجه به الگوی طبقه بندی اطلاعات پذیرفته شده توسط سازمان ، ایجاد و پیاده سازی شود .
الف.۳,۸ : اداره کردن رسانه ها		
هدف : پیشگیری از افشا ، دستکاری ، حذف یا تخریب غیرمجاز اطلاعات ذخیره شده در رسانه ها		
الف.۱,۳,۸	مدیریت رسانه های جداشدنی	کنترل : باید رویه هایی برای مدیریت رسانه های جداشدنی ، با توجه به الگوی طبقه بندی پذیرفته شده توسط سازمان ، ایجاد و پیاده سازی شود .
الف.۲,۳,۸	امحاءِ رسانه	کنترل : رسانه ها باید زمانی که دیگر مورد نیاز نیستند ، به صورت امن و با استفاده از رویه هایی رسمی ، امحا شوند .
الف.۳,۳,۸	انتقال رسانه فیزیکی	کنترل : رسانه های حاوی اطلاعات باید در حین انتقال ، در برابر دسترسی غیرمجاز ، سوءِ استفاده یا خرابی ، محافظت شوند .
الف.۹ : کنترل دسترسی		
الف.۱,۹ : الزامات کسب و کار برای کنترل دسترسی		
هدف : محدودسازی دسترسی به اطلاعات و امکانات پردازش اطلاعات		
الف.۱,۱,۹	خط مشی کنترل دسترسی	کنترل : باید خط مشی کنترل دسترسی ، بر مبنای الزامات کسب و کار و امنیت اطلاعات ، ایجاد ، مدون و بازنگری شود .
الف.۲,۱,۹	دسترسی به شبکه ها و سرویس های شبکه	کنترل : کاربران فقط باید به شبکه و سرویس هایی از شبکه دسترسی داشته باشند که بطور مشخص ، مجوز استفاده از آنها را داشته باشند .
الف.۲,۹ : مدیریت دسترسی کاربر		
هدف : حصول اطمینان از دسترسی کاربر مجاز شده و جلوگیری از دسترسی غیرمجاز به سیستم ها و سرویس ها		
الف.۱,۲,۹	ثبت و حذف کاربر	کنترل : باید فرایندی رسمی برای ثبت و حذف کاربر ، به منظور ایجاد امکان اعطای حقوق دسترسی ، پیاده سازی شود .
الف.۲,۲,۹	تامین مجوز دسترسی کاربر	کنترل : باید یک فرایند رسمی تامین مجوز دسترسی کاربر ، جهت اعطا یا لغو حقوق دسترسی برای کلیه انواع کاربران به تمامی سیستم ها و سرویس ها ، پیاده سازی شود .
الف.۳,۲,۹	مدیریت حق دسترسی ویژه	کنترل : تخصیص اطلاعات محرمانه احراز هویت ، باید از طریق یک فرایند رسمی مدیریتی ، کنترل شود .
الف.٤,۲,۹	مدیریت اطلاعات محرمانه احراز هویت کاربران	کنترل : تخصیص اطلاعات محرمانه احراز هویت ، باید از طریق یک فرایند رسمی مدیریتی ، کنترل شود .
الف.۵,۲,۹	بازنگری حقوق دسترسی	کنترل : مالکان دارایی ها باید حقوق دسترسی کاربران را در فواصل زمانی منظم

	کاربر	بازنگری کنند .
الف.۶,۲,۹	حذف یا اصلاح حقوق دسترسی	کنترل : حقوق دسترسی تمامی کارکنان و کاربران طرف بیرونی به اطلاعات و امکانات پردازش اطلاعات ، باید به محض خاتمه اشتغال ، قرارداد یا توافق نامه آنها حذف شده ، و در صورت تغییر وضعیت ، اصلاح شوند .
الف.۳,۹ : مسئولیت های کاربر		
هدف : پاسخگو بودن کاربران در برابر حفاظت از اطلاعات احراز هویت خود		
الف.۱,۳,۹	استفاده از اطلاعات محرمانه احراز هویت	کنترل : کاربران باید به پیروی از دستورالعمل های سازمانی جهت استفاده از اطلاعات محرمانه احراز هویت ، ملزم شوند .
الف.٤,۹ : کنترل دسترسی به سیستم و برنامه		
هدف : جلوگیری از دسترسی غیرمجاز به سیستم ها و برنامه ها		
الف.۱,٤,۹	محدودیت دسترسی به اطلاعات	کنترل : دسترسی به اطلاعات و کارکردهای سیستم برنامه ، باید مطابق با خط مشی کنترل دسترسی ، محدود شود .
الف.۲,٤,۹	رویه های ورود امن	کنترل : دسترسی به سیستم ها و برنامه ها ، در صورت الزام در خط مشی کنترل دسترسی ، باید توسط یک رویه ورود امن ، کنترل شود .
الف.۳,٤,۹	سیستم مدیریت کلمه عبور	کنترل : سیستم های مدیریت کلمه عبور باید تعاملی بوده و کیفیت کلمات عبور را تضمین نمایند .
الف.٤,٤,۹	استفاده از برنامه های کمکی	کنترل : استفاده از برنامه های کمکی که ممکن است قادر به ابطال کنترل های سیستم و برنامه ها باشند ، باید محدود شده و به شدت کنترل شود .
الف.۵,٤,۹	کنترل دسترسی به کد منبع برنامه	کنترل : دسترسی به کد منبع برنامه ، باید محدود شود .
الف.۱۰ : رمزنگاری		
هدف : حصول اطمینان از استفاده بجا و اثربخش از رمزنگاری ، به منظور حفاظت از محرمانگی ، اصالت یا صحت اطلاعات		
الف.۱,۱,۱۰	خط مشی استفاده از کنترل های رمزنگاری	کنترل : بایدخط مشی استفاده از کنترل های رمزنگاری ، برای حفاظت از اطلاعات ، ایجاد و پیاده سازی شود .
الف.۲,۱,۱۰	مدیریت کلید	کنترل : خط مشی استفاده ، حفاظت و طول عمر کلیدهای رمزنگاری ، باید ایجاد و در کل چرخه حیات آنها پیاده سازی شود .
الف.۱۱ : امنیت فیزیک و محیطی		
الف.۱,۱۱ : نواحی امن		
هدف : جلوگیری از دسترسی فیزیکی غیر مجاز ، خسارت و مداخله در اطلاعات و امکانات پردازش اطلاعات سازمان		
الف.۱,۱,۱۱	حصار امنیت فیزیکی	کنترل : حصارهای امنیتی باید برای حفاظت از نواحی حاوی اطلاعات و امکانات پردازش اطلاعات حساس یا حیاتی ، تعیین شده و استفاده شوند .

الف.۲,۱,۱۱	کنترل های مداخل فیزیکی	کنترل : نواحی امن ، به منظور حصول اطمینان از اینکه فقط کارکنان مجاز ، اجازه دسترسی دارند ، باید توسط کنترل های مداخل مناسب ، حفاظت شوند .
الف.۳,۱,۱۱	امن سازی دفاتر ، اتاق ها و امکانات	کنترل : امنیت فیزیکی برای دفاتر ، اتاق ها و امکانات ، باید طراحی شده و به کار گرفته شود .
الف.٤,۱,۱۱	محافظت در برابر تهدیدهای بیرونی و محیطی	کنترل : حفاظت فیزیکی در برابر بلایای طبیعی ، سوانح و حملات خرابکارانه ، باید طراحی شده و به کار گرفته شود .
الف.٥,۱,۱۱	نواحی تحویل و بارگیری	کنترل : نقاط دسترسی مانند نواحی تحویل و بارگیری و سایر نقاطی که افراد متفرقه ممکن است وارد محوطه ها شوند ، باید تحت کنترل قرار گیرند ، و در صورت امکان ، برای جلوگیری از دسترسی غیر مجاز ، از امکانات پردازش اطلاعات ، مجزا شوند .
الف.۲,۱۱ : تجهیزات		
هدف : جلوگیری از فقدان ، آسیب ، سرقت یا به خطر افتادن دارایی ها و ایجاد وقفه در فعالیت های سازمان		
الف.۱,۲,۱۱	استقرار و حفاظت از تجهیزات	کنترل : تجهیزات باید (در محل مناسب) مستقر و محافظت شوند تا مخاطرات ناشی از تهدیدها و خطرات محیطی و فرصت های دسترسی غیرمجاز ، کاهش یابند .
الف.۲,۲,۱۱	امکانات پشتیبانی	کنترل : تجهیزات باید در برابر خرابی برق و سایر اختلالات ناشی از خرابی امکانات پشتیبانی ، محافظت شوند .
الف.۳,۲,۱۱	امنیت کابل کشی	کنترل : کابل کشی های برق و مخابرات مورد استفاده برای انتقال داده یا پشتیبانی از سرویس های اطلاعاتی ، باید در برابر قطع شدن ، ایجاد تداخل یا آسیب ، محافظت شوند .
الف.٤,۲,۱۱	نگهداری تجهیزات	کنترل : تجهیزات باید به منظور حصول اطمینان از تداوم دسترس پذیری و صحت شان ، به درستی نگهداری شوند .
الف.٥,۲,۱۱	خروج دارایی ها	کنترل : تجهیزات ، اطلاعات یا نرم افزار ، نباید بدون مجوز قبلی از محل خارج شوند .
الف.٦,۲,۱۱	امنیت تجهیزات و دارایی های خارج از محوطه	کنترل : برای دارایی های خارج از محوطه ، باید با توجه به مخاطرات مختلف ناشی از انجام کار در خارج از محوطه های سازمان ، امنیت برقرار شوند .
الف.۷,۲,۱۱	امحا یا استفاده مجدد از تجهیزات به صورت امن	کنترل تمام اجزای تجهیزاتی که دارای رسانه ذخیره سازی هستند ، باید به منظور حصول اطمینان از اینکه کلیه داده های حساس و نرم افزارهای دارای حق امتیاز ، پیش از محا یا استفاده مجدد ، حذف شده یا به شیوه امنی بازنویسی شده اند ، بررسی شوند .
الف.۸,۲,۱۱	تجهیزات بدون مراقبت	کنترل : کاربران باید اطمینان حاصل کنند که تجهیزات بدون مراقبت ، حفاظت مناسبی دارند .

	کاربر	
الف.۹,۲,۱۱	خط مشی میز پاک و صفحه پاک	کنترل : خط مشی میز پاک برای اوراق و رسانه های ذخیره سازی جداشدنی ، و خط مشی صفحه پاک برای امکانات پردازش اطلاعات ، باید اتخاذ شوند .
الف.۱۲ : امنیت عملیات		
الف.۱,۱۲ : رویه های عملیاتی و مسئولیت ها		
هدف : حصول اطمینان از کارکرد صحیح و امن امکانات پردازش اطلاعات		
الف.۱,۱,۱۲	رویه های عملیاتی مدون	کنترل : رویه های عملیاتی باید مدون شوند و در دسترس همه کاربرانی که به آنها نیاز دارند ، قرار گیرند .
الف.۲,۱,۱۲	مدیریت تغییر	کنترل : تغییرات در سازمان ، فرایندها ی کسب و کار ، امکانات و سیستم های پردازش اطلاعات که بر امنیت اطلاعات تاثیرگذار هستند ، باید کنترل شوند .
الف.۳,۱,۱۲	مدیریت ظرفیت	کنترل : استفاده از منابع ، باید پایش و تنظیم شده و پیش بینی ظرفیت مورد نیاز آینده جهت حصول اطمینان از کارایی الزامات سیستم ، انجام شود .
الف.٤,۱,۱۲	جداسازی محیط های توسعه ، آزمایش و عملیاتی	کنترل : محیط های توسعه ، آزمایش و عملیاتی ، باید به منظور کاهش مخاطرات ناشی از دسترسی یا تغییر غیرمجاز در محیط عملیاتی ، از یکدیگر جدا شوند .
الف.۲,۱۲ : حفاظت در برابر بدافزارها		
هدف : حصول اطمینان از اینکه اطلاعات و امکانات پردازش اطلاعات در برابر بدافزارها حفاظت می شوند .		
الف.۱,۲,۱۲	کنترل ها در برابر بدافزارها	کنترل : کنترل های تشخیص ، جلوگیری و بازیابی ، به منظور حفاظت در برابر بدافزارها ، باید پیاده سازی شده و با آگاه سازی مناسب کاربر همراه شوند .
الف.۳,۱۲ : پشتیبان گیری		
هدف : حفاظت در برابر فقدان داده ها		
الف.۱,۳,۱۲	پشتیبان گیری از اطلاعات	کنترل : نسخه های پشتیبانی از اطلاعات ، نرم افزار و تصاویر سیستم ، باید با توجه به خط مشی مورد توافق پشتیبان گیری ، تهیه و به صورت منظم آزمایش شوند .
الف.٤,۱۲ : ثبت پایش		
هدف : ثبت رویدادها و ایجاد شواهد		
الف.۱,٤,۱۲	ثبت رویداد	کنترل : ثبت رویدادها شامل ثبت فعالیت های کاربر ، استثناءها ، خطاها و رویدادهای امنیت اطلاعات ، باید ایجاد ، نگهداری و به صورت منظم بازنگری شوند .
الف.۲,٤,۱۲	حفاظت از اطلاعات ثبت شده رویدادها	کنترل : امکانات ثبت رویداد و اطلاعات ثبت شده ، باید در برابر دستکاری و دسترسی غیرمجاز حفاظت شوند .
الف.۳,٤,۱۲	ثبت رویدادهای مدیر و اپراتور سیستم	کنترل : فعالیت های مدیر سیستم و اپراتور سیستم باید ثبت شوند و رویدادهای ثبت شده باید محافظت و به صورت منظم ، بازنگری شوند .
الف.٤,٤,۱۲	همزمان سازی ساعت ها	کنترل : ساعت های تمامی سیستم های پردازش اطلاعات مرتبط در درون یک سازمان یا دامنه اطلاعاتی ، باید با یک منبع زمانی مرجع واحد ، همزمان شوند .
الف.۵,۱۲ : کنترل نرم افزارهای عملیاتی		

هدف : حصول اطمینان از صحت سیستم های عملیاتی		
الف.۱,۵,۱۲	نصب نرم افزار بر روی سیستم های عملیاتی	کنترل : رویه هایی برای کنترل نصب نرم افزار بر روی سیستم های عملیاتی باید پیاده سازی شوند .
الف.۶,۱۲ : مدیریت آسیب پذیری فنی		
الف.۱,۱۶ : مدیریت و بهبود رخدادهای امنیت اطلاعات		
هدف : حصول اطمینان از بکارگیری رویکردی استوار و اثربخش برای مدیریت رخدادهای امنیت اطلاعات ، شامل اعلان رویدادهای امنیتی و نقاط ضعف		
الف.۱,۱,۱۶	مسئولیت ها و رویه ها	کنترل : مسئولیت های مدیریتی و رویه ها ، به منظور حصول اطمینان از پاسخگویی سریع ، موثر و منظم به رخدادهای امنیت اطلاعت ، باید وضع شوند .
الف.۲,۱,۱۶	گزارش دهی رویدادهای امنیت اطلاعات	کنترل : رویدادهای امنیت اطلاعات باید از طریق مجاری مدیریتی مناسب ، در کوتاه ترین زمان ممکن گزارش شوند .
الف.۳,۱,۱۶	گزارش دهی نقاط ضعف امنیت اطلاعات	کنترل : کارکنان و پیمانکارانی که از سیستم ها و سرویس های اطلاعاتی سازمان استفاده می کنند ، باید نسبت به یادداشت برداری و گزارش دهی هر گونه ضعف امنیت اطلاعات مشاهده شده یا مشکوک در سیستم ها یا سرویس ها ، ملزم شوند .
الف.٤,۱,۱۶	ارزیابی و تصمیم گیری درباره رویدادهای امنیت اطلاعات	کنترل : رویدادهای امنیت اطلاعات ، باید ارزیابی شوند و در خصوص اینکه لازم است به عنوان رخدادهای امنیت اطلاعات طبقه بندی شوند ، تصمیم گیری شود .
الف.۵,۱,۱۶	پاسخ به رخدادهای امنیت اطلاعات	کنترل : باید به توجه به رویه های مدون ، به رخدادهای امنیت اطلاعات پاسخ داده شود .
الف.۷,۱,۱۶	جمع آوری شواهد	کنترل : سازمان باید رویه هایی را برای شناسایی ، جمع آوری ، اکتساب و حفظ اطلاعاتی که می توانند به عنوان شواهد مورد استفاده قرار گیرند ، تعریف نموده و به کار گیرد .
الف.۱۷ : جوانب امنیت اطلاعات در مدیریت تداوم کسب و کار		
الف.۱,۱۷ : تداوم امنیت اطلاعات		
هدف : تداوم امنیت اطلاعات باید در سیستم های مدیریت تداوم کسب و کار سازمان ، لحاظ شود .		
الف.۱,۱,۱۷	طرح ریزی تداوم امنیت اطلاعات	کنترل : سازمان باید الزاماتش را برای امنیت اطلاعات و تداوم مدیریت امنیت اطلاعات در وضعیت های نامطلوب ، به عنوان مثال هنگام بحران یا فاجعه ، تعیین کند .
الف.۲,۱,۱۷	پیاده سازی تداوم امنیت اطلاعات	کنترل : به منظور حصول اطمینان از سطح الزامی تداوم برای امنیت اطلاعات در هنگام یک موقعیت نامطلوب ، سازمان باید فرایندها ، رویه ها و کنترل هایی را وضع ، مدون ، پیاده سازی و نگهداری کند .
الف.۳,۱,۱۷	بررسی ، بازنگری و ارزیابی تداوم امنیت اطلاعات	کنترل : سازمان باید کنترل های تدوام امنیت اطلاعات را که وضع و پیاده سازی شده اند ، در فواصل زمانی منظم بررسی کند تا اطمینان حاصل شود این کنترل ها در هنگام وضعیت های نامطلوب ، معتبر و موثر هستند .
الف.۲,۱۷ : جایگزین ها		
هدف : حصول اطمینان از دسترس پذیری امکانات پردازش اطلاعات		

الف.۱,۲,۱۷	دسترس پذیری امکانات پردازش اطلاعات	کنترل : امکانات پردازش اطلاعات باید با جایگزین های کافی جهت برآورده سازی الزامات دسترس پذیری ، پیاده سازی شوند .
الف.۱۸ : انطباق		
الف.۱,۱۸ : انطباق با الزامات قانونی و قراردادی		
هدف : پرهیز از نقض تعهدات قانونی ، حقوقی ، مقرراتی یا قراردادی مرتبط با امنیت اطلاعات و هر الزام امنیتی		
الف.۱,۱,۱۸	شناسایی الزامات قانونی و قراردادی قابل اجرا	کنترل : تمامی الزامات قانونی ، حقوقی ، مقرراتی ، قراردادی مرتبط و رویکرد سازمان نسبت به تحقق این الزامات ، باید برای هر یک از سیستم های اطلاعاتی و سازمان ، به وضوح شناسایی ، مدون و به روز نگهداشته شوند .
الف.۲,۱,۱۸	حقوق مالکیت معنوی	کنترل : رویه های مناسب ، به منظور حصول اطمینان از انطباق با الزامات قانونی ، مقرراتی و قراردادی مرتبط با حقوق مالکیت معنوی و استفاده از محصولات نرم افزاری دارای حقوق مالکیت ، باید پیاده سازی شوند .
الف.۳,۱,۱۸	حفاظت از سوابق	کنترل : سوابق باید مطابق با الزامات قانونی ، مقرراتی ، قراردادی و الزامات کسب و کار در برابر فقدان ، تخریب ، تحریف ، دسترسی غیرمجاز و افشای غیرمجاز محافظت شوند .
الف.٤,۱,۱۸	حریم خصوصی و حفاظت از اطلاعات هویت شخصی	کنترل : در صورت قابلیت پیاده سازی حریم خصوصی و حفاظت از اطلاعات هویتی شخصی باید همانگونه که در قوانین و مقررات مرتبط الزام شده است ، تضمین شود .
الف.۵,۱,۱۸	قواعد کنترل های رمزنگاری	کنترل : کنترل های رمزنگاری باید منطبق با تمامی توافق نامه ها ، قوانین و مقررات مرتبط ، به کار گرفته شوند .
الف.۲,۱۸ : بازنگری های امنیت اطلاعات		
هدف : حصول اطمینان از اینکه امنیت اطلاعات ، مطابق با خط مشی ها و رویه های سازمانی ، پیاده سازی و اجرا می شوند .		
الف.۱,۲,۱۸	بازنگری مستقل امنیت اطلاعات	کنترل : رویکرد سازمان نسبت به مدیریت امنیت اطلاعات و پیاده سازی آن (به عنوان مثال اهداف کنترلی ، کنترل ها ، خط مشی ها ، فرایندها و رویه های امنیت اطلاعات) ، باید در فواصل زمانی طرح ریزی شده یا هنگامی که تغییرات مهمی رخ می دهد ، به طور مستقل بازنگری شود .
الف.۲,۲,۱۸	انطباق با خط مشی ها و استانداردهای امنیتی	کنترل : مدیران باید انطباق پردازش اطلاعات و رویه ها را در حیطه مسئولیت شان ، با خط مشی ها و استانداردهای امنیتی مناسب و دیگر الزامات امنیتی ، به طور منظم بازنگری کنند .
الف.۳,۲,۱۸	بازنگری انطباق فنی	کنترل : سیستم های اطلاعاتی باید به منظور انطباق با خط مشی ها و استانداردهای امنیت اطلاعات سازمان ، به طور منظم بازنگری شوند .