محمد مهدی واعظی نژاد

ترجمه استاندارد

ISO/IEC 27001:2022

www.Mvaezi.ir

به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید؛ از روح خود در او دمید و او را خلیفه خویش در زمین قرار داد و پیامبرانش را با دلایل آشکار فرو فرستاد تا انسان‌ها را به سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.

فهرست مطالب

مقدمه

امنیت اطلاعات و نگهداشت امن دارایی‌های اطلاعاتی در برابر مخاطرات و تهدیداتی همچون تخریب، تغییر، حذف، افشا و دسترسی غیرمجاز، همواره یکی از مهمترین چالش‌های عصر فناوری اطلاعات محسوب می‌شود. حفاظت از دارایی‌ها و سیستم‌های اطلاعاتی برای تمامی سازمان‌ها دیگر یک امر حیاتی بوده و مستلزم مدیریتی اثربخش است. فراهم‌آوری صحت و تمامیت اطلاعات به گونه‌ای که در زمان مناسب، اطلاعات در دسترس افراد مجازی قرار گیرد که نیازمند آن هستند عاملی است که علاوه بر اثربخشی فرایندهای کسب‌وکار، موجب تداوم فعالیت‌های کلیدی آن نیز می‌شود. این موضوع در سال‌های اخیر، با افزایش تهدیدات و حملات سایبری به سازمان‌ها و روند رو به گسترش آن با وجود تمام پیشرفت‌هایی که در زمینه امنیت فناوری اطلاعات صورت گرفته، مورد توجه جدی مدیران ارشد سازمان‌ها و کارشناسان مربوطه قرار گرفته است.

از سوی دیگر، در دو دهه گذشته با ایجاد نگرش استانداردی به مبحث امنیت اطلاعات، استانداردهای مفیدی در این حوزه تدوین شده است. استاندارد ISO/IEC 27001 که مهمترین و پرمراجعه‌ترین استاندارد در این خصوص است، زمینه مناسبی را برای طراحی، پیاده‌سازی، استقرار و بهبود مستمر سیستم مدیریت امنیت اطلاعات در شرکت‌ها و سازمان‌ها و همچنین بهره‌گیری از منافع این رویکرد فراهم کرده است.

کتابچه حاضر، ترجمه استاندارد ISO/IEC 27001 ویرایش ۲۰۲۲ است که در راستای نگاه سیستمی به مقوله امنیت اطلاعات در کشور عزیزمان تهیه شده و در اختیار علاقه‌مندان قرار گرفته است.

خدایا چنان کن سرانجام کار
تو خشنود باشی و ما رستگار

محمد مهدی واعظی نژاد

پاییز ۱۴۰۱

پیشگفتار

ISO (سازمان بین‌المللی استاندارد) و IEC (کمیسیون بین‌المللی الکتروتکنیک)، یک سیستم تخصصی را جهت استانداردسازی در سطح جهان ایجاد کرده‌اند. نهادهای ملی عضو ISO یا IEC از طریق کمیته‌های فنی که از طرف سازمان مربوطه‌شان برای پرداختن به زمینه‌های خاص فعالیت‌های فنی ایجاد شده‌اند، در توسعه استانداردهای بین‌المللی مشارکت دارند. کمیته‌های فنی ISO و IEC در زمینه‌هایی با منافع مشترک با یکدیگر همکاری می‌کنند. سایر سازمان‌های بین‌المللی، دولتی یا غیردولتی در ارتباط با ISO و IEC نیز در این کار مشارکت دارند.

رویه‌های مورد استفاده برای توسعه این سند و روش‌هایی که برای حفظ بیشتر آن در نظر گرفته شده‌اند، در قسمت ۱ دستورالعمل‌های ISO/IEC توضیح داده شده است. به ویژه، به معیارهایی جهت تأییدیه موارد مورد نیاز برای سندهای مختلف نیز باید توجه داشت. این سند مطابق با قسمت ۲ قوانین ویراستاری دستورالعمل‌های ISO/IEC تهیه شده است (به www.iso.org/directives یا www.iec.ch/members_experts/refdocs مراجعه کنید).

به این احتمال که ممکن است بعضی موارد مطرح شده در این سند، تحت قوانین حق ثبت اختراع باشند هم توجه شده است. ISO و IEC مسئولیتی در قبال شناسایی هر یک یا همه این حقوق ندارند. جزئیات حق ثبت اختراع‌های شناسایی شده در طول تدوین این سند، در مقدمه و/ یا در فهرست ISO از اعلامیه‌های ثبت اختراع دریافت شده (به www.iso.org/patents مراجعه کنید) یا فهرست IEC اظهارنامه‌های ثبت اختراع دریافتی (به ttps://patents.iec.ch نگاه کنید) بیان شده است.

هر نام تجاری استفاده شده در این سند، صرفاً جنبه اطلاعاتی داشته و برای راحتی کاربران ارایه شده و به منزله تأیید آن نیست.

برای توضیح ماهیت داوطلبانه استانداردها، معنای اصطلاح‌ها و عبارت‌های خاص ISO مربوط به ارزیابی انطباق و همچنین اطلاعاتی در خصوص پایبندی ISO به اصول سازمان تجارت جهانی (WTO) در موانع فنی تجارت (TBT) به www.iso.org/iso/foreword.html مراجعه کنید. در IEC نیز می‌توان به www.iec.ch/understanding مراجعه کرد.

این سند توسط کمیته فنی مشترک ISO/IEC JTC 1، فناوری اطلاعات، کمیته فرعی SC 27، امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی تهیه شده است.

این ویرایش سوم، جایگزین و باطل‌کننده ویرایش دوم (ISO/IEC 27001:2013) است که از نظر فنی مورد بازنگری قرار گرفته بود. همچنین ISO/IEC 27001:2013/Cor 1:2014 و ISO/IEC 27001:2013/Cor 2:2015 تصحیح فنی شده‌اند.

تغییرات اصلی به شرح زیر است:

- متن سند، با ساختار هماهنگ شده استانداردهای سیستم‌های مدیریتی و ISO/IEC 27002:2022 یکسان شده است.

هرگونه بازخورد یا سؤالی در مورد این سند باید به سازمان استاندارد ملی کاربر که از آن تبعیت می‌کند، ارسال شود. فهرست کامل این نهادها را می‌توان در www.iso.org/members.html و www.iec.ch/national committees مشاهده کرد.

۰. مقدمه

۱,۰ کلیات

این سند به منظور ارایه الزاماتی برای استقرار، پیاده‌سازی، نگهداری و بهبود مستمر یک سیستم مدیریت امنیت اطلاعات تهیه شده است. پذیرش سیستم مدیریت امنیت اطلاعات، یک تصمیم راهبردی برای هر سازمانی است. استقرار و پیاده‌سازی سیستم مدیریت امنیت اطلاعات در یک سازمان، تحت تأثیر نیازها و اهداف سازمان، الزامات امنیتی، فرایندهای سازمانی مورد استفاده و اندازه و ساختار آن قرار دارد. انتظار می‌رود 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 دسترس‌پذیری اطلاعات محافظت کرده و به طرف‌های ذینفع این اطمینان را می‌دهد که مخاطرات، به میزان کافی مدیریت می‌شوند.

توجه داشته باشید که سیستم مدیریت امنیت اطلاعات، بخشی از فرایندها و ساختار مدیریتی کلان سازمان بوده و با آن یکپارچه شده باشد و امنیت اطلاعات در طراحی فرایندها، سیستم‌های اطلاعاتی و کنترل‌ها لحاظ شود. انتظار می‌رود پیاده‌سازی سیستم مدیریت امنیت اطلاعات، با نیازهای سازمان تطابق داشته باشد.

این سند می‌تواند توسط طرف‌های داخلی و بیرونی، به منظور ارزیابی توانایی سازمان در برآوردن الزامات امنیت اطلاعات خود مورد استفاده قرار گیرد.

ترتیب ارایه الزامات در این سند، بیانگر اهمیت یا ترتیب پیاده‌سازی آنها نیست. موارد گفته شده، به منظور ارجاع‌های بعدی ذکر شده‌اند.

ISO/IEC 27000، نمای کلی و واژگان سیستم مدیریت امنیت اطلاعات را توصیف کرده و مرجع خانواده استانداردهای سیستم مدیریت امنیت اطلاعات (شامل ISO/IEC 27003) به همراه اصطلاح‌ها و تعاریف مرتبط با آن است.

۲,۰ سازگاری با سایر استانداردهای سیستم مدیریت

این سند از ساختار سطح بالا، عنوان‌های فرعی مشابه، متن یکسان، اصطلاح‌های مشترک و تعاریف اصلی موجود در پیوست SL بخش ۱ دستورالعمل‌های ISO/IEC، مکمل‌های تلفیقی ISO استفاده می‌کند و در نتیجه با سایر استانداردهای سیستم مدیریت که بر اساس پیوست SL تدوین شده‌اند، سازگار است.

این رویکرد مشترک که در پیوست SL تعریف شده است، برای آن دسته از سازمان‌هایی که در نظر دارند یک سیستم مدیریتی واحد را در راستای فراهم‌آوری الزامات دو یا چند استاندارد سیستم مدیریت اجرا کنند، مفید خواهد بود.

امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی – سیستم‌های مدیریت امنیت اطلاعات – الزامات

۱. قلمرو

این سند، الزاماتی را برای استقرار، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات در چارچوب یک سازمان بیان می‌کند. این سند همچنین شامل الزاماتی برای ارزیابی و برطرف‌سازی مخاطرات امنیت اطلاعات، متناسب با نیازهای سازمان است. الزامات تعیین شده در این سند، عمومی بوده و در تمام سازمان‌ها صرف‌نظر از نوع، اندازه یا ماهیت آنها کاربرد دارد. کنارگذاری هر یک از الزامات گفته شده در بندهای ۴ تا ۱۰، چنانچه یک سازمان ادعای تطابق با این سند را داشته باشد، قابل قبول نیست.

۲. مراجع اصلی

به اسناد زیر به گونه‌ای در متن ارجاع داده شده که محتوای بعضی یا تمام آنها الزامات این سند را تشکیل می‌دهد. برای مراجعی که تاریخ در آنها گفته شده فقط همان ویرایش مدنظر است. مراجعی که بدون ذکر تاریخ، ارجاع داده شده‌اند آخرین ویرایش سند اشاره شده (شامل همه اصلاحیه‌ها) مورد استناد است.

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

۳. اصطلاحات و تعاریف

در راستای اهداف این سند، اصطلاح‌ها و تعریف‌های گفته شده در ISO/IEC 27000 به کار می‌روند.

ISO و IEC، پایگاه داده‌های اصطلاحات را به منظور استفاده در استانداردسازی در آدرس‌های زیر نگهداری می‌کنند:

- پلتفرم مرور آنلاین ISO: در https://www.iso.org/obp موجود است.
- الکتروپدیای IEC: در https://www.electropedia.org وجود دارد.

۴. چارچوب سازمان

۱,۴ شناخت سازمان و چارچوب آن

سازمان باید مسایل درونی و بیرونی مرتبط با اهداف سازمان و موارد تأثیرگذار در امکان دستیابی به نتایج مورد انتظار سیستم مدیریت امنیت اطلاعات را شناسایی کند.

نکته: تعیین این مسایل به استقرار چارچوب درونی و بیرونی سازمان که در بند ۵,۴,۱ استاندارد ISO 31000:2018 مطرح شده است، اشاره دارد.

۲,۴ شناخت نیازها و انتظارات طرف‌های ذینفع

سازمان باید موارد زیر را مشخص کند:

الف) طرف‌های ذینفع مرتبط با سیستم مدیریت امنیت اطلاعات؛

ب) الزامات مربوط به این طرف‌های ذینفع؛

ج) کدام یک از این الزامات با اجرای سیستم مدیریت امنیت اطلاعات محقق خواهد شد.

نکته: الزامات طرف‌های ذینفع ممکن است شامل الزامات قانونی، حقوقی، مقرراتی و تعهدات قراردادی باشد.

۳,۴ تعیین قلمرو سیستم مدیریت امنیت اطلاعات

سازمان باید مرزها و کاربردپذیری سیستم مدیریت امنیت اطلاعات را به منظور تعیین قلمرو آن مشخص کند.

سازمان باید هنگام مشخص کردن قلمرو، موارد زیر را در نظر بگیرد:

الف) مسایل درونی و بیرونی اشاره شده در بند ۱,۴؛

ب) الزامات اشاره شده در بند ۲,۴؛

ج) ارتباطات و وابستگی‌های بین فعالیت‌های انجام شده توسط سازمان و فعالیت‌هایی که توسط سازمان‌های دیگر انجام می‌شوند.

قلمرو باید به صورت اطلاعات مستند، در دسترس باشد.

۴,۴ سیستم مدیریت امنیت اطلاعات

سازمان باید یک سیستم مدیریت امنیت اطلاعات، شامل فرایندهای مورد نیاز و تعاملات بین آنها را مطابق با الزامات این سند ایجاد، پیاده‌سازی و نگهداری کرده و آن را به طور مستمر بهبود بخشد.

۵. رهبری

۱,۵ رهبری و تعهد

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

الف) حصول اطمینان از ایجاد خط‌مشی امنیت اطلاعات و اهداف امنیت اطلاعات و سازگاری آنها با مسیر راهبردی سازمان؛

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

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 نتایج مورد انتظار دست می‌یابد.

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

ز) ترویج بهبود مستمر؛ و

ح) پشتیبانی از سایر نقش‌های مدیریتی مرتبط جهت نشان‌دهی رهبری آنها به نحوی که در محدوده‌های مسئولیتی‌شان اعمال گردد.

نکته: ارجاع به «کسب‌وکار» در این سند را می‌توان به صورت عام به معنای آن دسته از فعالیت‌هایی دانست که هسته اصلی اهداف وجودی سازمان را تشکیل می‌دهند.

۲,۵ خط‌مشی

مدیریت ارشد باید یک خط‌مشی امنیت اطلاعات ایجاد کند که:

الف) متناسب با هدف سازمان باشد.

ب) شامل اهداف امنیت اطلاعات بوده (به بند ۲,۶ مراجعه شود) یا چارچوبی را برای تعیین اهداف امنیت اطلاعات در نظر بگیرد.

ج) شامل تعهدی مبنی بر تأمین الزامات کاربردپذیر مرتبط با امنیت اطلاعات باشد؛

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

خط‌مشی امنیت اطلاعات باید:

ه) به صورت اطلاعات مستند، در دسترس باشد.

و) در داخل سازمان ابلاغ شود؛

ز) در صورت نیاز، در اختیار طرف‌های ذینفع قرار گیرد.

۳,۵ نقش‌های سازمانی، مسئولیت‌ها و اختیارات

مدیریت ارشد باید اطمینان حاصل کند که مسئولیت‌ها و اختیارات لازم برای ایفای نقش‌های امنیت اطلاعات، تعیین و ابلاغ شده‌اند.

مدیریت ارشد باید مسئولیت‌ها و اختیارات لازم را به منظور تحقق موارد زیر تعیین کند:

الف) حصول اطمینان از انطباق سیستم مدیریت امنیت اطلاعات با الزامات این سند؛

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

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

۶. طرح‌ریزی

۱,۶ اقداماتی برای مدیریت مخاطرات و فرصت‌ها

۱,۱,۶ کلیات

سازمان در هنگام طراحی سیستم مدیریت امنیت اطلاعات باید مسایل اشاره شده در بند ۱,۴ و الزامات بیان شده در بند ۲,۴ را مدنظر قرار داده و مخاطرات و فرصت‌هایی که نیازمند توجه هستند، در راستای موارد زیر تعیین کند:

الف) حصول اطمینان از اینکه سیستم مدیریت امنیت اطلاعات می‌تواند به نتایج مطلوب خود دست یابد.

ب) از بروز اثرات ناخواسته جلوگیری کرده یا آنها را تا حد امکان کاهش دهد؛

ج) به بهبود مستمر دست یابد.

سازمان باید موارد زیر را طرح‌ریزی کند:

د) اقدام‌هایی برای مقابله با این مخاطرات و در نظر گرفتن فرصت‌ها؛ و

ه) چگونگی:

۱. گنجاندن و پیاده‌سازی این اقدام‌ها در فرایندهای سیستم مدیریت امنیت اطلاعات خود؛ و

۲. ارزیابی اثربخشی این اقدامات.

۲,۱,۶ ارزیابی مخاطره امنیت اطلاعات

سازمان باید یک فرایند ارزیابی مخاطره امنیت اطلاعات را تعریف و اجرا کرده تا بتواند:

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

۱. معیارهای پذیرش مخاطرات؛ و

۲. معیارهایی برای انجام ارزیابی مخاطرات امنیت اطلاعات.

ب) اطمینان دهد که ارزیابی‌های مکرر مخاطرات امنیت اطلاعات، نتایج نامتناقض، معتبر و مقایسه‌پذیر تولید می‌کنند.

ج) مخاطرات امنیت اطلاعات را شناسایی کند:

۱. به کارگیری فرایند ارزیابی مخاطره امنیت اطلاعات برای شناسایی مخاطرات مربوط به از دست رفتن محرمانگی، صحت و دسترس‌پذیری 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 واقع‌گرایانه احتمال وقوع مخاطرات شناسایی شده در بند ۲,۱,۶ - ج - ۱؛

۳. تعیین سطوح مخاطرات.

ه) مخاطرات امنیت اطلاعات را ارزیابی کند:

۱. مقایسه نتایج تحلیل مخاطرات با معیارهای مخاطره تعیین شده در بند ۱,۲,۶ - الف؛ و

۲. اولویت‌بندی مخاطرات تحلیل شده برای برطرف‌سازی آنها.

سازمان باید اطلاعات مستندی را در خصوص فرایند ارزیابی مخاطره امنیت اطلاعات نگهداری کند.

۳,۱,۶ برطرف‌سازی مخاطره امنیت اطلاعات

سازمان باید فرایندی را برای برطرف‌سازی مخاطره امنیت اطلاعات، تعریف و اجرا کرده تا بتواند:

الف) با در نظر گرفتن نتایج ارزیابی مخاطره، گزینه‌های مناسب جهت برطرف‌سازی مخاطرات امنیت اطلاعات را انتخاب کند.

ب) تمامی کنترل‌های ضروری به منظور پیاده‌سازی گزینه(های) انتخابی برطرف‌سازی مخاطرات امنیت اطلاعات را تعیین کند.

نکته ۱: سازمان‌ها می‌توانند در صورت لزوم، کنترل‌هایی طراحی کرده یا آنها را از هر منبع دیگری شناسایی کنند.

ج) کنترل‌های تعیین شده در بند ۳,۱,۶ ب را با کنترل‌های پیوست الف مقایسه کرده و بررسی کند که هیچ یک از کنترل‌های ضروری از قلم نیافتاده است.

نکته ۲: پیوست الف شامل فهرستی از کنترل‌های احتمالی امنیت اطلاعات است. استفاده‌کنندگان از این سند برای حصول اطمینان از اینکه هیچ یک از کنترل‌های ضروری نادیده گرفته نشده است، به پیوست الف ارجاع داده می‌شوند.

نکته ۳: کنترل‌های امنیت اطلاعات فهرست شده در پیوست الف، جامع نبوده و ممکن است کنترل‌های امنیت اطلاعات دیگری هم لازم باشد.

د) یک بیانیه کاربردپذیری تدوین کند که شامل:

- کنترل‌های ضروری (به بند ۳،۱،۶، زیربند ب و زیربند ج مراجعه کنید)؛

- دلیل استفاده از آنها؛

- اینکه کنترل‌های ضروری پیاده‌سازی شده‌اند یا خیر؛ و

- توجیه کنارگذاری هر یک از کنترل‌های پیوست الف.

ه) یک طرح برطرف‌سازی مخاطرات امنیت اطلاعات را تدوین کند؛ و

و) تأییدیه طرح برطرف‌سازی مخاطرات امنیت اطلاعات و پذیرش مخاطرات امنیت اطلاعات باقی‌مانده را از مالکان مخاطرات اخذ کند.

سازمان باید اطلاعات مستندی را در خصوص فرایند برطرف‌سازی مخاطرات امنیت اطلاعات نگهداری کند.

نکته ۴: فرایند ارزیابی و برطرف‌سازی مخاطرات امنیت اطلاعات در این سند، با اصول و رهنمودهای کلی ارایه شده در ISO 31000 مطابقت دارد.

۲،۶ اهداف امنیت اطلاعات و برنامه‌ریزی برای دستیابی به آنها

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

اهداف امنیت اطلاعات باید:

الف) با خط‌مشی امنیت اطلاعات سازگار باشند.

ب) قابل اندازه‌گیری باشند (در صورت عملی بودن)؛

ج) الزامات قابل اجرای امنیت اطلاعات و نتایج ارزیابی و برطرف‌سازی مخاطرات را در نظر بگیرند.

د) پایش شوند؛

ه) ابلاغ شوند؛

و) در صورت نیاز به‌روزرسانی شوند.

ز) به عنوان اطلاعات مستند در دسترس باشند.

سازمان باید اطلاعات مستندی را درباره اهداف امنیت اطلاعات نگهداری کند.

سازمان هنگام برنامه‌ریزی نحوه دستیابی به اهداف امنیت اطلاعات باید موارد زیر را تعیین کند:

ح) چه کاری انجام خواهد شد.

ط) به چه منابعی نیاز است.

ی) چه شخصی مسئول است.

ک) چه زمانی انجام خواهد شد؛ و

ل) نتایج، چگونه ارزیابی می‌شوند.

۳,۶ برنامه‌ریزی تغییرات

هنگامی که سازمان نیاز به انجام تغییرات در سیستم مدیریت امنیت اطلاعات را تشخیص می‌دهد، تغییرات باید به صورت برنامه-ریزی شده اجرا شوند.

۷. پشتیبانی

۱,۷ منابع

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

۲,۷ صلاحیت

سازمان باید:

الف) صلاحیت‌های مورد نیاز شخص یا افرادی که تحت کنترل سازمان کار می‌کنند و بر روی عملکرد امنیت اطلاعات تأثیرگذار هستند را تعیین کند.

ب) اطمینان حاصل کند که این افراد بر اساس سطح تحصیلات، آموزش‌ها یا تجربیات مناسب از صلاحیت لازم برخوردار هستند.

ج) هر جا که امکان‌پذیر است، اقدام‌هایی را به منظور کسب صلاحیت لازم انجام داده و اثربخشی اقدام‌های انجام شده را ارزیابی کند؛ و

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

نکته: اقدامات امکان‌پذیر، به عنوان مثال می‌تواند شامل ارایه آموزش، مشاوره یا جابه‌جایی کارکنان فعلی یا استخدام یا قرارداد همکاری با افراد شایسته باشد.

۳,۷ آگاهی‌رسانی

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

الف) خط‌مشی 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.

۴,۷ ارتباطات

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

الف) در چه زمینه‌ای ارتباط برقرار شود.

ب) چه زمانی ارتباط برقرار شود.

ج) با چه کسی باید ارتباط برقرار شود.

د) چگونه ارتباط برقرار شود.

۵,۷ اطلاعات مستند

۱,۵,۷ کلیات

سیستم مدیریت امنیت اطلاعات سازمان باید شامل موارد زیر باشد:

الف) اطلاعات مستند مورد نیاز این سند؛ و

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

نکته: گستره مستندسازی اطلاعات سیستم مدیریت امنیت اطلاعات می‌تواند به دلایل زیر برای هر سازمانی متفاوت باشد:

۱. اندازه سازمان و نوع فعالیت‌ها، فرایندها، محصولات و خدمات آن؛
۲. پیچیدگی فرایندها و تعاملات آنها؛ و
۳. صلاحیت افراد.

۲,۵,۷ ایجاد و به‌روزرسانی

هنگام ایجاد و به‌روزرسانی 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 نرم‌افزار، گرافیک) و رسانه (مثلاً کاغذی، الکترونیکی)؛ و

ج) بازنگری و تصویب جهت سازگاری و کفایت.

۳,۵,۷ کنترل اطلاعات مستند

اطلاعات مستند مورد نیاز سیستم مدیریت امنیت اطلاعات و این سند باید کنترل شوند تا اطمینان حاصل شود که:

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

ب) به میزان کافی حفاظت می‌شوند (به عنوان مثال در برابر از دست رفتن محرمانگی، استفاده نادرست یا فقدان صحت).

به منظور کنترل اطلاعات مستند، سازمان باید در صورت قابلیت اجرا فعالیت‌های زیر را انجام دهد:

ج) توزیع، دسترسی، بازیابی و استفاده؛

د) ذخیره‌سازی و نگهداری، شامل حفظ خوانایی؛

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

و) نگهداری و امحا.

اطلاعات مستند با منشأ بیرونی که از سوی سازمان برای طرح‌ریزی و اجرای سیستم مدیریت امنیت اطلاعات ضروری تشخیص داده شده‌اند باید به نحوی مناسب، شناسایی و کنترل شوند.

نکته: دسترسی، صرفاً به معنای تصمیم در خصوص اجازه مشاهده اطلاعات مستند یا اجازه و اختیار جهت مشاهده و تغییر اطلاعات مستند و غیره است.

۸. عملیات

۱,۸ برنامه‌ریزی و کنترل عملیاتی

سازمان باید فرایندهای مورد نیاز برای برآوردن الزامات و انجام اقدام‌های تعیین شده در بند ۶ را طرح‌ریزی، پیاده‌سازی و کنترل کند؛ به وسیله:

- تعیین معیارها برای فرایندها؛
- اجرای کنترل فرایندها بر اساس قوانین.

اطلاعات مستند باید تا حدی در دسترس باشند که اطمینان حاصل شود فرایندها مطابق با برنامه‌ریزی صورت گرفته انجام می‌شوند.

سازمان باید در صورت لزوم، تغییرات طرح‌ریزی شده را کنترل کرده و پیامدهای تغییرات ناخواسته را بررسی نموده تا هرگونه عوارض جانبی کاهش یابد.

سازمان باید اطمینان حاصل کند که فرایندها، محصولات یا خدمات برون‌سپاری شده سیستم مدیریت امنیت اطلاعات کنترل می‌شوند.

۲,۸ ارزیابی مخاطره امنیت اطلاعات

سازمان باید ارزیابی مخاطره امنیت اطلاعات را در بازه‌های زمانی طرح‌ریزی شده یا هنگام وقوع تغییرات مهم یا تغییرات پیشنهادی، با در نظر گرفتن معیارهای تعیین شده در بند ۲,۱,۶ الف انجام دهد.

سازمان باید اطلاعات مستندی را در خصوص نتایج ارزیابی مخاطرات امنیت اطلاعات نگهداری کند.

۳,۸ برطرف‌سازی مخاطره امنیت اطلاعات

سازمان باید طرح برطرف‌سازی مخاطره امنیت اطلاعات را اجرا کند.

سازمان باید اطلاعاتی مستند را در خصوص نتایج برطرف‌سازی مخاطرات امنیت اطلاعات نگهداری کند.

۹. ارزیابی عملکرد

۱,۹ پایش، اندازه‌گیری، تحلیل و ارزیابی

سازمان باید موارد زیر را مشخص کند:

الف) چه چیزهایی به پایش و اندازه‌گیری نیاز دارند، از جمله فرایندها و کنترل‌های امنیت اطلاعات؛

ب) روش‌هایی را برای پایش، اندازه‌گیری، تحلیل و ارزیابی به منظور حصول اطمینان از معتبر بودن نتایج مشخص کند. روش‌های انتخابی باید نتایج قابل قیاس و تکرارپذیر تولید کرده تا معتبر شناخته شوند.

ج) چه زمانی باید پایش و اندازه‌گیری انجام شود.

د) چه شخصی باید پایش و اندازه‌گیری را انجام دهد.

ه) چه زمانی نتایج حاصل از پایش و اندازه‌گیری باید تحلیل و ارزیابی شوند؛ و

و) چه شخصی باید این نتایج را تحلیل و ارزیابی کند.

اطلاعات مستند باید به عنوان شواهدی از نتایج نگهداری شوند.

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

۲,۹ ممیزی داخلی

۱,۲,۹ کلیات

سازمان باید ممیزی‌های داخلی را در فاصله‌های 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؛

۲. الزامات این سند؛

ب) به طور اثربخش، اجرا و نگهداری می‌شود.

۲,۲,۹ برنامه ممیزی داخلی

سازمان باید برنامه(های) ممیزی شامل دفعات تکرار، روش‌ها، مسئولیت‌ها، الزامات طرح‌ریزی و گزارش‌دهی را طرح‌ریزی، استقرار، پیاده‌سازی و نگهداری کند.

سازمان در هنگام ایجاد برنامه(های) ممیزی داخلی باید اهمیت فرایندهای مربوطه و نتایج ممیزی‌های قبلی را در نظر بگیرد.

سازمان باید:

الف) معیارهای ممیزی و قلمرو ممیزی را مشخص کند.

ب) در انتخاب ممیزان و انجام ممیزی‌ها از واقع‌بینی و بی‌طرفی فرایند ممیزی اطمینان حاصل کند.

ج) اطمینان یابد که نتایج ممیزی به مدیریت مربوطه گزارش داده می‌شوند؛ و

د) اطلاعات مستند را به عنوان شواهد اجرای برنامه(های) ممیزی و نتایج ممیزی نگهداری کند.

۳,۹ بازنگری مدیریت

۱,۳,۹ کلیات

مدیریت ارشد باید سیستم مدیریت امنیت اطلاعات سازمان را در فاصله‌های زمانی طرح‌ریزی شده بررسی کرده تا از تداوم سازگاری، کفایت و اثربخشی آن اطمینان حاصل کند.

۲,۳,۹ ورودی‌های بازنگری مدیریت

در بازنگری مدیریت باید موارد زیر در نظر گرفته شوند:

الف) وضعیت انجام اقدامات در بازنگری‌های قبلی مدیریت؛

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

ج) تغییرات در نیازها و انتظارت طرف‌های ذینفع سیستم مدیریت امنیت اطلاعات؛

د) بازخوردها درباره عملکرد امنیت اطلاعات، شامل روند:

۱. عدم انطباق‌ها و اقدام‌های اصلاحی؛

۲. نتایج پایش و اندازه‌گیری؛

۳. نتایج ممیزی؛

۴. تحقق اهداف امنیت اطلاعات.

ه) بازخوردهای طرف‌های ذینفع؛

و) نتایج ارزیابی مخاطره و وضعیت طرح برطرف‌سازی مخاطرات؛

ز) فرصت‌های بهبود مستمر.

۳,۳,۹ نتایج بازنگری مدیریت

خروجی‌های بازنگری مدیریت باید شامل تصمیم‌های مربوط به فرصت‌های بهبود مستمر و هرگونه نیاز به انجام تغییرات در سیستم مدیریت امنیت اطلاعات باشد.

اطلاعات مستند باید به عنوان شواهد نتایج بازنگری‌های مدیریت نگهداری شوند.

۱۰. بهبود

۱,۱۰ بهبود مستمر

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

۲,۱۰ عدم انطباق و اقدام اصلاحی

هنگام وقوع یک عدم انطباق، سازمان باید:

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

۱. برای کنترل و اصلاح آن اقدام کند؛

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 جایی دیگر، از طریق موارد زیر تعیین کند:

۱. بررسی عدم انطباق؛

۲. تعیین علل عدم انطباق؛ و

۳. شناسایی وجود عدم انطباق‌های مشابه یا احتمال وقوع آنها.

ج) اقدام‌های مورد نیاز را اجرا کند.

د) اثربخشی تمام اقدام‌های اصلاحی انجام شده را بررسی کند؛ و

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

اقدام‌های اصلاحی باید متناسب با پیامدهای عدم انطباق‌های مشاهده شده باشند.

اطلاعات مستند باید به عنوان مدرک برای موارد زیر نگهداری شوند:

و) ماهیت عدم انطباق‌ها و تمام اقدام‌های انجام شده متعاقب آنها؛ و

ز) نتایج هر یک از اقدام‌های اصلاحی.

پیوست الف

(الزامی)

مرجع کنترل‌های امنیت اطلاعات

کنترل‌های امنیت اطلاعات گفته شده در جدول الف.۱، به طور مستقیم از بندهای ۵ تا ۸ استاندارد ISO/IEC 27002:2022 و منطبق با آنها برگرفته شده‌اند و در چارچوب بند ۳،۱،۶ مورد استفاده قرار خواهند گرفت.

جدول الف.۱ - کنترل‌های امنیت اطلاعات

۵	**کنترل‌های سازمانی**	
۱،۵	خط‌مشی‌های امنیت اطلاعات	**کنترل** خط‌مشی امنیت اطلاعات و خط‌مشی‌های موضوعی خاص باید تدوین شده، توسط مدیریت تأیید و منتشر شده، به اطلاع و تصدیق کارکنان و طرف‌های ذینفع مربوطه رسیده و در بازه‌های زمانی برنامه‌ریزی شده یا هر زمان که تغییرات مهمی رخ داد، بازنگری شوند.
۲،۵	نقش‌ها و مسئولیت‌های امنیت اطلاعات	**کنترل** نقش‌ها و مسئولیت‌های امنیت اطلاعات باید بر اساس نیازهای سازمان، تعریف و تخصیص داده شوند.
۳،۵	تفکیک وظایف	**کنترل** وظایف کاری و حوزه‌های مسئولیتی متناقض باید از یکدیگر تفکیک شوند.
۴،۵	مسئولیت‌های مدیریت	**کنترل** مدیریت باید تمام کارکنان را به رعایت امنیت اطلاعات، مطابق با خط‌مشی منتشر شده امنیت اطلاعات، خط‌مشی‌های موضوعی خاص و رویه‌های سازمانی ملزم کند.
۵،۵	ارتباط با مراجع معتبر	**کنترل** سازمان باید با مراجع معتبر ارتباط برقرار کرده و آن را حفظ کند.
۶،۵	ارتباط با گروه‌های ذینفع ویژه	**کنترل** سازمان باید با گروه‌های ذینفع ویژه یا سایر انجمن‌های تخصصی امنیت سایبری و

		اتحادیه‌های حرفه‌ای ارتباط برقرار کرده و آن را حفظ کند.
۷,۵	هوش تهدید	**کنترل** اطلاعات مربوط به تهدیدهای امنیت اطلاعات باید به منظور ایجاد هوش تهدید، جمع‌آوری و تحلیل شوند.
۸,۵	امنیت اطلاعات در مدیریت پروژه	**کنترل** امنیت اطلاعات باید در مدیریت پروژه لحاظ شود.
۹,۵	موجودی اطلاعاتی و سایر دارایی‌های مربوطه	**کنترل** یک فهرست از اطلاعات و سایر دارایی‌های مرتبط با آنها از جمله مالکان‌شان باید تهیه و نگهداری شود.
۱۰,۵	استفاده پسندیده از اطلاعات و دارایی‌ها	**کنترل** باید قوانینی برای استفاده قابل قبول و رویه‌هایی برای مدیریت اطلاعات و دارایی‌ها مشخص، مستند و اجرا شود.
۱۱,۵	بازگرداندن دارایی‌ها	**کنترل** کارکنان و سایر طرف‌های ذینفع باید به محض تغییر سمت یا خاتمه همکاری، قرارداد یا توافقنامه کاری‌شان، دارایی‌های سازمان که در اختیارشان است را بازگردانند.
۱۲,۵	طبقه‌بندی اطلاعات	**کنترل** اطلاعات باید مطابق با نیازمندی‌های امنیت اطلاعات سازمان و بر اساس الزامات محرمانگی، صحت، دسترس‌پذیری و همچنین الزامات مربوط به اشخاص ذینفع طبقه‌بندی شوند.
۱۳,۵	برچسب‌گذاری اطلاعات	**کنترل** مجموعه مناسبی از رویه‌ها برای برچسب‌گذاری اطلاعات باید ایجاد شده و مطابق با طرح طبقه‌بندی اطلاعات سازمان اجرا شود.
۱۴,۵	تبادل اطلاعات	**کنترل** برای همه امکانات تبادل اطلاعات در سازمان و بین سازمان و طرف‌های دیگر باید

		قوانین، رویه‌ها و توافقنامه‌های تبادل اطلاعات وجود داشته باشد.
۱۵،۵	کنترل دسترسی	**کنترل** قوانین کنترل دسترسی منطقی و فیزیکی به اطلاعات و سایر دارایی‌های مرتبط باید بر اساس الزامات کسب‌وکار و امنیت اطلاعات ایجاد و اجرا شوند.
۱۶،۵	مدیریت هویت	**کنترل** چرخه عمر هویت‌ها باید به صورت کامل مدیریت شود.
۱۷،۵	اطلاعات احراز هویت	**کنترل** تخصیص و مدیریت اطلاعات احراز هویت باید توسط یک فرایند مدیریتی، از جمله آموزش کارکنان در خصوص نحوه مدیریت مناسب اطلاعات احراز هویت کنترل شود.
۱۸،۵	حقوق دسترسی	**کنترل** حقوق دسترسی به اطلاعات و سایر دارایی‌های مرتبط باید مطابق با خط‌مشی موضوعی خاص و قوانین کنترل دسترسی سازمان اعطا، بازنگری، بررسی، اصلاح و لغو شود.
۱۹،۵	امنیت اطلاعات در روابط با تأمین‌کنندگان	**کنترل** فرایندها و رویه‌هایی برای مدیریت مخاطرات امنیت اطلاعات مرتبط با استفاده از محصولات یا خدمات تأمین‌کننده باید تعریف و اجرا شوند.
۲۰،۵	لحاظ کردن امنیت اطلاعات در توافقنامه‌های با تأمین‌کنندگان	**کنترل** الزامات امنیت اطلاعات مربوطه باید بر اساس نوع ارتباط با تأمین‌کننده، با هر تأمین-کننده‌ای مشخص شده و مورد توافق قرار گیرد.
۲۱،۵	مدیریت امنیت اطلاعات در زنجیره تأمین ICT	**کنترل** فرایندها و رویه‌هایی برای مدیریت مخاطرات امنیت اطلاعات مرتبط با زنجیره تأمین محصولات و خدمات ICT باید تعریف و اجرا شوند.
۲۲،۵	پایش، بازنگری و مدیریت تغییر خدمات تأمین‌کننده	**کنترل** سازمان باید به طور مرتب تغییرات در رویه‌های امنیت اطلاعات و ارایه خدمات

		تأمین‌کننده را پایش، بررسی، ارزیابی و مدیریت کند.
۲۳،۵	امنیت اطلاعات در استفاده از خدمات ابری	**کنترل** فرایندهای اکتساب، استفاده، مدیریت و خاتمه خدمات ابری باید مطابق با الزامات امنیت اطلاعات سازمان ایجاد شوند.
۲۴،۵	برنامه‌ریزی و آمادگی برای مدیریت رخدادهای امنیت اطلاعات	**کنترل** سازمان باید با تعریف، ایجاد و اطلاع‌رسانی فرایندها، نقش‌ها و مسئولیت‌های مدیریت رخدادهای امنیت اطلاعات، برای مدیریت حوادث امنیت اطلاعات برنامه‌ریزی کرده و آماده شود.
۲۵،۵	ارزیابی و تصمیم‌گیری درباره رویدادهای امنیت اطلاعات	**کنترل** سازمان باید رویدادهای امنیت اطلاعات را ارزیابی کرده و تصمیم بگیرد که آیا می‌توان آنها را به عنوان رخدادهای امنیت اطلاعات دسته‌بندی کرد یا خیر.
۲۶،۵	پاسخ به رخدادهای امنیت اطلاعات	**کنترل** به رخدادهای امنیت اطلاعات باید مطابق با رویه‌های مستند شده، پاسخ داده شود.
۲۷،۵	یادگیری از رخدادهای امنیت اطلاعات	**کنترل** دانش به دست آمده از رخدادهای امنیت اطلاعات باید برای ارتقا و بهبود کنترل‌های امنیت اطلاعات مورد استفاده قرار گیرد.
۲۸،۵	جمع‌آوری شواهد	**کنترل** سازمان باید رویه‌هایی را برای شناسایی، جمع‌آوری، اکتساب و حفظ شواهد مربوط به رویدادهای امنیت اطلاعات، ایجاد و اجرا کند.
۲۹،۵	امنیت اطلاعات در هنگام اختلال	**کنترل** سازمان باید نحوه حفظ امنیت اطلاعات را در سطح مناسب، در هنگام وقوع اختلال طرح‌ریزی کند.
۳۰،۵	آمادگی ICT برای تداوم کسب-وکار	**کنترل** آمادگی ICT باید بر اساس اهداف تداوم کسب‌وکار و الزامات تداوم ICT طرح‌ریزی،

		پیاده‌سازی، حفظ و آزمایش شود.
۳۱،۵	الزامات قانونی، حقوقی، مقرراتی و قراردادی	**کنترل** الزامات قانونی، حقوقی، مقرراتی و قراردادی مربوط به امنیت اطلاعات و رویکرد سازمان برای برآورده ساختن این الزامات باید شناسایی، مستند و به‌روز نگه داشته شود.
۳۲،۵	حقوق مالکیت معنوی	**کنترل** سازمان باید رویه‌های مناسبی را برای حفاظت از حقوق مالکیت معنوی ایجاد کند.
۳۳،۵	حفاظت از سوابق	**کنترل** سوابق باید در برابر گم شدن، تخریب، جعل، دسترسی و انتشار غیرمجاز محافظت شوند.
۳۴،۵	حریم خصوصی و حفاظت از اطلاعات هویت شخصی	**کنترل** سازمان باید الزامات مربوط به حفظ حریم خصوصی و حفاظت از اطلاعات هویت شخصی را مطابق با قوانین و مقررات قابل اجرا و الزامات قراردادی، شناسایی و برآورده کند.
۳۵،۵	بازنگری مستقل امنیت اطلاعات	**کنترل** رویکرد سازمان نسبت به مدیریت امنیت اطلاعات و اجرای آن از جمله افراد، فرایندها و فناوری‌ها باید به طور مستقل، در فواصل زمانی برنامه‌ریزی شده یا هر زمان تغییرات قابل توجهی رخ داد، بازنگری شود.
۳۶،۵	انطباق با خط‌مشی‌ها، قوانین و استانداردهای امنیت اطلاعات	**کنترل** انطباق با خط‌مشی امنیت اطلاعات سازمان، خط‌مشی‌های موضوعی خاص، قوانین و استانداردها باید به طور منظم بررسی شود.
۳۷،۵	رویه‌های عملیاتی مدون	**کنترل** رویه‌های عملیاتی مرتبط با امکانات پردازش اطلاعات باید مدون شده و در دسترس کارکنانی که به آنها نیاز دارند، قرار گیرد.

۶	کنترل‌های فردی	
۱,۶	گزینش	**کنترل** بررسی‌های تأیید پیشینه تمام داوطلبان استخدام باید قبل از پیوستن آنها به سازمان، به صورت مستمر و با در نظر گرفتن قوانین، مقررات و اصول اخلاقی قابل اجرا انجام شده و متناسب با الزامات کسب‌وکاری، طبقه‌بندی اطلاعاتی که باید مورد دسترس قرار گیرند و مخاطرات شناسایی شده باشد.
۲,۶	شرایط و ضوابط استخدام	**کنترل** در قراردادهای کاری باید مسئولیت‌های کارکنان و سازمان در قبال امنیت اطلاعات گفته شود.
۳,۶	آگاهی‌بخشی، تحصیل و آموزش امنیت اطلاعات	**کنترل** کارکنان سازمان و طرف‌های ذینفع مربوطه باید آگاهی‌بخشی، تحصیل و آموزش مناسب را در زمینه امنیت اطلاعات دیده و به صورت منظم در جریان به‌روزرسانی خط‌مشی امنیت اطلاعات، خط‌مشی‌های موضوعی خاص و رویه‌های سازمان متناسب با وظایف شغلی‌شان قرار گیرند.
۴,۶	فرایند انضباطی	**کنترل** یک فرایند انضباطی باید تدوین و ابلاغ شده تا اقدام‌های لازم در خصوص کارکنان و سایر طرف‌های ذینفعی که مرتکب نقض خط‌مشی امنیت اطلاعات می‌شوند، صورت گیرد.
۵,۶	مسئولیت‌های پس از خاتمه یا تغییر شغل	**کنترل** مسئولیت‌ها و وظایف امنیت اطلاعات که پس از خاتمه یا تغییر شغل همچنان معتبر باقی می‌مانند باید تعریف و اجرا شده و به اطلاع تمام کارکنان و طرف‌های ذینفع مربوطه برسد.
۶,۶	توافقنامه‌های محرمانگی یا عدم افشا	**کنترل** توافقنامه‌های محرمانگی یا عدم افشا که منعکس‌کننده نیازهای سازمان برای حفاظت

		از اطلاعات هستند باید شناسایی و مدون شده، به صورت مرتب بازنگری شده و توسط کارکنان و سایر طرف‌های ذینفع مربوطه امضا شوند.
۷,۶	دورکاری	**کنترل** هنگامی که کارکنان از راه دور کار می‌کنند باید تدابیر امنیتی لازم برای حفاظت از اطلاعات قابل دسترس، پردازش یا ذخیره شده در خارج از محیط سازمان اجرا شوند.
۸,۶	گزارش‌دهی رویداد امنیت اطلاعات	**کنترل** سازمان باید سازوکاری برای کارکنان فراهم کند تا رویدادهای امنیت اطلاعات مشاهده شده یا مشکوک را از طریق روش‌های مناسب، به موقع گزارش دهند.
۷	**کنترل‌های فیزیکی**	
۱,۷	حصارهای امنیت فیزیکی	**کنترل** حصارهای امنیتی برای محافظت از مناطقی که حاوی اطلاعات و دارایی‌های مرتبط هستند باید ایجاد و اجرا شوند.
۲,۷	ورودی فیزیکی	**کنترل** نواحی امن باید با کنترل‌های ورودی و نقاط دسترسی مناسب محافظت شوند.
۳,۷	امن‌سازی دفاتر، اتاق‌ها و امکانات	**کنترل** امنیت فیزیکی برای دفاتر، اتاق‌ها و امکانات باید طراحی و اجرا شود.
۴,۷	پایش امنیت فیزیکی	**کنترل** اماکن باید به صورت مداوم از لحاظ دسترسی فیزیکی غیرمجاز کنترل شوند.
۵,۷	حفاظت در برابر تهدیدات فیزیکی و محیطی	**کنترل** حفاظت در برابر تهدیدات فیزیکی و محیطی مانند بلایای طبیعی و سایر تهدیدات فیزیکی عمدی یا سهوی برای زیرساخت‌ها باید طراحی و اجرا شود.
۶,۷	کار در نواحی امن	**کنترل** اقدام‌های امنیتی برای کار در نواحی امن باید طراحی و اجرا شوند.
۷,۷	میز پاک و صفحه نمایش پاک	**کنترل**

		قوانین میز پاک برای مدارک و رسانه‌های ذخیره‌سازی قابل حمل و قوانین صفحه نمایش پاک برای امکانات پردازش اطلاعات باید تعریف شده و به نحو مناسب اجرا شوند.
۸,۷	استقرار و حفاظت از تجهیزات	**کنترل** تجهیزات باید به صورت امن انتخاب و حفاظت شوند.
۹,۷	امنیت دارایی‌های خارج از سازمان	**کنترل** از دارایی‌های خارج از سازمان باید محافظت شود.
۱۰,۷	رسانه ذخیره‌سازی	**کنترل** رسانه‌های ذخیره‌سازی باید در طول چرخه عمر اکتساب، استفاده، انتقال و امحای آنها مطابق با طرح طبقه‌بندی سازمان و الزامات استفاده از آنها مدیریت شوند.
۱۱,۷	امکانات پشتیبانی	**کنترل** امکانات پردازش اطلاعات باید در برابر قطعی برق و سایر اختلالات ناشی از خرابی امکانات پشتیبانی محافظت شوند.
۱۲,۷	امنیت کابل‌کشی	**کنترل** کابل‌های برق، داده یا سرویس‌های اطلاعاتی پشتیبان باید در برابر شنود، تداخل یا آسیب حفاظت شوند.
۱۳,۷	نگهداری از تجهیزات	**کنترل** تجهیزات باید به درستی نگهداری شده تا از دسترس‌پذیری، صحت و محرمانگی اطلاعات اطمینان حاصل شود.
۱۴,۷	امحا یا استفاده دوباره امن از تجهیزات	**کنترل** تجهیزات دارای رسانه ذخیره‌ساز باید قبل از امحا یا استفاده دوباره، به صورت کامل بررسی شده تا اطمینان حاصل شود که داده‌های حساس و نرم‌افزارهای دارای مجوز، حذف یا به روشی امن رونویسی شده‌اند.
۸	**کنترل‌های فنی**	

۱,۸	دستگاه کاربر نهایی	**کنترل** اطلاعات ذخیره شده، پردازش شده یا قابل دسترس از طریق دستگاه کاربر نهایی باید حفاظت شوند.
۲,۸	حقوق دسترسی ویژه	**کنترل** تخصیص و استفاده از حقوق دسترسی ویژه باید محدود و مدیریت شود.
۳,۸	محدودسازی دسترسی به اطلاعات	**کنترل** دسترسی به اطلاعات و دارایی‌ها باید مطابق با خط‌مشی موضوعی خاص تدوین شده در خصوص کنترل دسترسی محدود شود.
۴,۸	دسترسی به کد منبع	**کنترل** دسترسی خواندن و نوشتن به کد منبع، ابزارهای توسعه و کتابخانه‌های نرم‌افزاری باید به طور مناسب مدیریت شود.
۵,۸	احراز هویت امن	**کنترل** فناوری‌ها و رویه‌های احراز هویت امن باید بر اساس محدودیت‌های دسترسی به اطلاعات و خط‌مشی موضوعی خاص در مورد کنترل دسترسی پیاده‌سازی شوند.
۶,۸	مدیریت ظرفیت	**کنترل** استفاده از منابع باید مطابق با نیازمندی‌های ظرفیت فعلی و مورد انتظار، تحت پایش قرار گرفته و تنظیم شود.
۷,۸	حفاظت در برابر بدافزار	**کنترل** حفاظت در برابر بدافزار باید با آگاهی‌رسانی مناسب کاربر، اجرا و پشتیبانی شود.
۸,۸	مدیریت آسیب‌پذیری‌های فنی	**کنترل** اطلاعات مربوط به آسیب‌پذیری‌های فنی سیستم‌های اطلاعاتی در حال استفاده باید جمع‌آوری شده، وضعیت سازمان در برابر این آسیب‌پذیری‌ها ارزیابی شده و اقدام‌های مناسب انجام شود.
۹,۸	مدیریت پیکربندی	**کنترل**

		پیکربندی‌ها از جمله تنظیمات امنیتی سخت‌افزارها، نرم‌افزارها، سرویس‌ها و شبکه‌ها باید مشخص، مستند، پیاده‌سازی، نظارت و بازنگری شوند.
۱۰،۸	پاک‌سازی اطلاعات	**کنترل** اطلاعات ذخیره شده در سیستم‌های اطلاعاتی، دستگاه‌ها یا هر رسانه ذخیره‌ساز باید مواقعی که دیگر به آنها نیازی نیست، پاک شوند.
۱۱،۸	داده پوشانی	**کنترل** پوشاندن داده‌ها باید با در نظر گرفتن قوانین قابل اجرا و متناسب با خط‌مشی موضوعی خاص سازمان در زمینه کنترل دسترسی و سایر خط‌مشی‌های موضوعی خاص مرتبط و نیز الزامات کسب‌وکاری انجام شود.
۱۲،۸	جلوگیری از نشت داده‌ها	**کنترل** تدابیر جلوگیری از نشت داده‌ها باید برای سیستم‌ها، شبکه‌ها و هر دستگاه دیگری که اطلاعات حساس را پردازش، ذخیره یا انتقال می‌دهد، اعمال شود.
۱۳،۸	پشتیبان‌گیری از اطلاعات	**کنترل** نسخه‌های پشتیبان از اطلاعات، نرم‌افزارها و سیستم‌ها باید مطابق با خط‌مشی موضوعی خاص توافق شده در زمینه پشتیبان‌گیری، تهیه شده و به طور منظم آزمایش شوند.
۱۴،۸	افزونگی امکانات پردازش اطلاعات	**کنترل** امکانات پردازش اطلاعات باید از افزونگی کافی برای برآورده ساختن الزامات دسترس-پذیری برخوردار باشند.
۱۵،۸	واقعه‌نگاری	**کنترل** لاگ‌هایی که فعالیت‌ها، موارد استثنا، خطاها و سایر رویدادهای مربوطه را ثبت می‌کنند باید تولید، ذخیره، حفاظت و تحلیل شوند.
۱۶،۸	فعالیت‌های نظارتی	**کنترل** شبکه‌ها، سیستم‌ها و برنامه‌ها باید از نظر رفتار غیرعادی، تحت نظارت قرار گرفته و

		اقدام‌های مناسب برای ارزیابی رخدادهای احتمالی امنیت اطلاعات انجام شود.
۱۷،۸	همزمان‌سازی ساعت‌ها	**کنترل** ساعت‌های سیستم‌های پردازش اطلاعات مورد استفاده در سازمان باید با مراجع زمانی معتبر همزمان‌سازی شوند.
۱۸،۸	استفاده از برنامه‌های کمکی ویژه	**کنترل** استفاده از برنامه‌های کمکی که امکان نقض کنترل‌های سیستم و برنامه را دارند باید محدود شده و به شدت کنترل شود.
۱۹،۸	نصب نرم‌افزار در سیستم‌های عملیاتی	**کنترل** رویه‌ها و تدابیری برای مدیریت امن نصب نرم‌افزار در سیستم‌های عملیاتی باید وجود داشته باشد.
۲۰،۸	امنیت شبکه	**کنترل** شبکه‌ها و دستگاه‌های شبکه باید امن‌سازی، مدیریت و کنترل شده تا از اطلاعات سیستم‌ها و برنامه‌ها حفاظت شود.
۲۱،۸	امنیت سرویس‌های شبکه	**کنترل** سازوکارهای امنیتی، سطوح سرویس‌دهی و الزامات سرویس‌های شبکه باید شناسایی، پیاده‌سازی و پایش شوند.
۲۲،۸	تفکیک شبکه‌ها	**کنترل** در شبکه‌های سازمان باید گروه‌های سرویس‌های اطلاعاتی، کاربران و سیستم‌های اطلاعاتی از یکدیگر تفکیک شوند.
۲۳،۸	فیلترینگ وب	**کنترل** دسترسی به وب‌سایت‌های بیرونی برای کاهش میزان قرار گرفتن در معرض محتوای مخرب باید مدیریت شود.
۲۴،۸	استفاده از رمزنگاری	**کنترل** قوانینی برای استفاده اثربخش از رمزنگاری، از جمله مدیریت کلید رمزنگاری باید

		تعریف و اجرا شود.
۲۵،۸	چرخه عمر توسعه امن	**کنترل** قوانینی برای توسعه امن نرم‌افزار و سیستم‌ها باید ایجاد و اجرا شود.
۲۶،۸	الزامات امنیتی برنامه‌های کاربردی	**کنترل** الزامات امنیت اطلاعات در هنگام خرید یا توسعه برنامه‌های کاربردی باید شناسایی، مشخص و تأیید شوند.
۲۷،۸	اصول معماری و مهندسی امن سیستم‌ها	**کنترل** اصول مهندسی امن سیستم‌ها باید مشخص، مستند و نگهداری شده و برای انجام هرگونه فعالیتی در خصوص توسعه سیستم‌های اطلاعاتی اجرا شوند.
۲۸،۸	کدنویسی امن	**کنترل** در هنگام توسعه یک نرم‌افزار باید اصول کدنویسی امن در نظر گرفته شود.
۲۹،۸	ارزیابی امنیتی در مراحل توسعه و پذیرش	**کنترل** فرایندهای ارزیابی امنیتی باید در چرخه عمر توسعه، تعریف و اجرا شوند.
۳۰،۸	توسعه برون‌سپاری شده	**کنترل** سازمان باید فعالیت‌های مرتبط با توسعه سیستم برون‌سپاری شده را هدایت، نظارت و بازنگری کند.
۳۱،۸	جداسازی محیط‌های توسعه، آزمون و عملیات	**کنترل** محیط‌های توسعه، آزمون و عملیات باید از یکدیگر تفکیک و امن شوند.
۳۲،۸	مدیریت تغییر	**کنترل** هرگونه تغییر در امکانات پردازش اطلاعات و سیستم‌های اطلاعاتی باید بر اساس رویه‌های مدیریت تغییر انجام شود.
۳۳،۸	اطلاعات آزمون	**کنترل** اطلاعات آزمون باید به طور مناسب انتخاب، حفاظت و مدیریت شوند.
۳۴،۸	حفاظت از سیستم‌های اطلاعاتی	**کنترل**

	در حین آزمون‌های ممیزی	آزمون‌های ممیزی و سایر فعالیت‌های اطمینان‌بخش که شامل ارزیابی سیستم‌های عملیاتی هستند باید بین آزمونگر و سطح مدیریتی مناسب، برنامه‌ریزی شده و مورد توافق قرار گیرند.

کتابنامه

۱- ISO/IEC 27002:2022، امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی – کنترل‌های امنیت اطلاعات

۲- ISO/IEC 27003، فناوری اطلاعات – فنون امنیتی – سیستم‌های مدیریت امنیت اطلاعات – راهنمایی

۳- ISO/IEC 27004، فناوری اطلاعات – فنون امنیتی – مدیریت امنیت اطلاعات – پایش، سنجش، تحلیل و ارزیابی

۴- ISO/IEC 27005، امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی – راهنمایی برای مدیریت مخاطرات امنیت اطلاعات

۵- ISO 31000:2018، مدیریت مخاطره – اصول و راهنماها