استاندارد ملی ایران-ایزو
-آی ای سی
۲۷۰۰۱
تجدید نظر اول
۱۳۹۴

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standards Organization

INSO –ISO-IEC
27001
1st.Revision
2015

فناوری اطلاعات– فنون امنیتی- سامانه (سیستم) مدیریت امنیت اطلاعات- الزامات

Information Technology — Security techniques — Information Security Management System — Requirement

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- فنون امنیتی- سامانه (سیستم) مدیریت امنیت اطلاعات- الزامات »

رئیس:	**سمت و/ یا نمایندگی:**
سجادیه، سید علیرضا (کارشناسی‌ارشد مهندسی کامپیوتر، هوش مصنوعی و رباتیک)	مدیرعامل شرکت پردازشگران داده آرای سپاهان
دبیر:	
میر اسکندری، سید محمدرضا (کارشناسی‌ارشد مدیریت اجرایی)	مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (به ترتیب حروف الفبا)	
آریا، بهناز (دکترا فناوری اطلاعات)	مدیر آموزش موسسه فرهنگی هنری کهکشان نور
ایزدپناه، سحرالسادات (کارشناسی‌ارشد مهندسی فناوری اطلاعات، سیستم-های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
بهبهانی، فرید (کارشناسی مکانیک، طراحی جامدات)	مدیر عامل شرکت اینفو امن
تیموری، حسین (کارشناسی‌ارشد مدیریت تکنولوژی، انتقال تکنولوژی)	مدیرعامل نمایندگی شرکت niscert
طی نیا، رضا (کارشناسی‌ارشد فناوری اطلاعات، مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
عباس نژاد، علی (دکترا فن‌آوری اطلاعات)	مدیر عامل موسسه فرهنگی هنری کهکشان نور
عزیزی پور، محسن (کارشناسی‌ارشد مدیریت بازرگانی، بازاریابی)	مدیرعامل شرکت پارس آوان رایان
قسمتی، سیمین (کارشناسی‌ارشد مهندسی فناوری اطلاعات)	کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران

کیامهر، بیتا (کارشناسی‌ارشد مدیریت تکنولوژی)	معـاون مـدیرکل نظـام مـدیریت امنیـت اطلاعـات سـازمان فناوری اطلاعات ایران
محمودی، یعقوب (کارشناسی‌ارشد فن‌آوری اطلاعات)	کارشناس رسمی دادگستری
مرتضوی، محمود (دکترا مهندسی نرم افزار)	مدیرفنی شرکت پردازشگران داده آرای سپاهان
مغانی، مهدی (کارشناسی‌ارشد ریاضی کاربردی)	کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعـات سازمان فناوری اطلاعات ایران

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی-سامانه(سیستم) مدیریت امنیت اطلاعات - الزامات» اولین بار در سال ۱۳۸۷ تدوین شد. این استاندارد بر اساس پیشنهادهای رسیده و بررسی توسط سازمان فناوری اطلاعات ایران و تأیید کمیسیون‌های مربوط برای اولین بار مورد تجدیدنظر قرار گرفت و در سیصد و هفتاد و هشتمین اجلاس کمیته ملی فناوری اطلاعات مورخ ۱۳۹۴/۰۴/۱۶ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره ISIRI-ISO-IEC۲۷۰۰۱: سال ۱۳۸۷ است.

منابع و مأخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیراست:

ISO/IEC 27001: 2013, Information technology — Security techniques —Information Security Management System- Requirements

۰ مقدمه

۰-۱ کلیات

هدف از تدوین این استاندارد ملی، تعیین الزامات جهت استقرار، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات است. پذیرش سیستم مدیریت امنیت اطلاعات، تصمیمی راهبردی برای سازمان است. استقرار و پیاده‌سازی سیستم مدیریت امنیت اطلاعات تحت تأثیر نیازها و اهداف و الزامات امنیتی سازمان، فرایندهای سازمانی مورداستفاده و اندازه و ساختار سازمان است. انتظار می‌رود به‌مرورزمان، همه این عوامل تأثیرگذار، تغییر کند.

سیستم مدیریت امنیت اطلاعات از محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات با به‌کاربردن فرایند مدیریت مخاطرات محافظت می‌کند و به علاقه‌مندان اطمینان می‌دهد که مخاطرات به حد کافی مدیریت می‌شود.

مهم است که سیستم مدیریت امنیت اطلاعات، جزئی از فرایندهای سازمان و ساختار کلی مدیریتی و به‌صورت یکپارچه با آن باشد و امنیت اطلاعات در طراحی فرایندها، سامانه‌های اطلاعاتی و کنترل‌ها در نظر گرفته شود. انتظار می‌رود پیاده‌سازی سیستم مدیریت امنیت اطلاعات، متناسب با نیازهای سازمان باشد.

این استاندارد ملی، می‌تواند توسط طرف‌های درونی و بیرونی، برای ارزیابی توانایی سازمان در برآورده سازی الزامات امنیت اطلاعات خود سازمان به‌کاربرده شود.

ترتیب ارائه‌ی الزامات در این استاندارد ملی، منعکس‌کننده اهمیت یا ترتیب پیاده‌سازی آن‌ها نیست. اقلام فهرست شده، فقط برای ارجاع، شماره‌گذاری شده‌اند.

استاندارد ISO/IEC 27000[۱] مرور کلی و واژگان سیستم‌های مدیریت امنیت اطلاعات را توصیف می‌کند، که همراه با واژگان و تعاریف مرتبط، به خانواده استانداردهای سیستم مدیریت امنیت اطلاعات اشاره دارد (شامل ISO/IEC 27003[۲]، ISO/IEC 27004[۳]، ISO/IEC 27005[۴]).

۱- استاندارد ملی ایران با شماره INSO-ISO-IEC ۲۷۰۰۰ در سال ۱۳۹۴ با منبع بین‌المللی ISO/IEC 27000:2014 منتشر شده است.

۲- استاندارد ملی ایران با شماره ISIRI-ISO-IEC ۲۷۰۰۳ در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27003:2010 منتشر شده است.

۳- استاندارد ملی ایران با شماره ISIRI-ISO-IEC۱۴۰۹۶ در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27004:2009 منتشر شده است.

۴- استاندارد ملی ایران با شماره INSO-ISO-IEC ۲۷۰۰۵ در سال ۱۳۹۲ با منبع بین‌المللی ISO/IEC 27005:2011 منتشر شده است.

۰-۲ انطباق با دیگر استانداردهای سیستم‌های مدیریتی

این استاندارد ملی، ساختار سطح بالا، عناوین زیر بند یکسان، متن یکسان، عبارات مشترک، و تعاریف پایه تعریف‌شده در « پیوست SL مکمل تلفیقی ISO از قسمت ۱ رهنمودهای ISO/IEC »، را به کار می‌برد و بنابراین انطباق با دیگر استانداردهای سیستم‌های مدیریتی که پیوست SL را قبول کرده‌اند، را حفظ می‌کند.

این رویکرد مشترک که در پیوست SL تعریف‌شده است، برای آن دسته از سازمان‌هایی که در نظر دارند یک سیستم مدیریت واحد جهت برآورده سازی الزامات دو یا چند استاندارد سیستم مدیریت، عملیاتی کنند، مفید خواهد بود.

فناوری اطلاعات- فنون امنیتی- سامانه (سیستم)های مدیریت امنیت اطلاعات- الزامات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین الزاماتی برای ایجاد، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات درزمینهٔ سازمان، است. این استاندارد ملی همچنین شامل الزامات ارزیابی و برطرف‌سازی[1] مخاطرات امنیت اطلاعات است که برای نیازهای سازمان، سفارشی‌شده[2] است. الزامات بیان‌شده در این استاندارد ملی، عمومی بوده و قصد آن است که در کلیه سازمان‌ها، صرف‌نظر از نوع، اندازه و ماهیت، کاربردپذیر باشند. اگر که سازمان ادعای انطباق با این استاندارد را دارد، کنار گذاری هیچ یک از الزامات مشخص‌شده در بندهای ۴ تا ۱۰ قابل‌پذیرش نیست.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده‌شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شوند.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده‌شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده‌شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها موردنظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف ارائه‌شده در استاندارد ISO/IEC 27000 به کار می‌رود.

۴ زمینهٔ سازمان

۴-۱ درک[3] سازمان و زمینهٔ[4] آن

سازمان باید موضوعات درونی و بیرونی که مرتبط با مقصود خود است و بر قابلیت آن، جهت حصول نتایج تعیین‌شده سیستم مدیریت امنیت اطلاعات تأثیرگذار است را تعیین کند.

---

1 - Treatment
2 - Tailored
3 - Underestanding
4 - Context

یادآوری- تعیین این موضوعات به ایجاد زمینهٔ بیرونی و درونی سازمان که در بند ۵-۳ استاندارد ملی ۱۴۵۶۰ سال ۱۳۹۱ [۵] در نظر گرفته‌شده، اشاره دارد.

۴-۲ درک نیازها و انتظارات طرف‌های علاقه‌مند

سازمان باید موارد زیر را تعیین کنند:

الف- طرف‌های علاقه‌مند مرتبط با سیستم مدیریت امنیت اطلاعات؛ و

ب- الزامات طرف‌های علاقه‌مند در خصوص امنیت اطلاعات.

یادآوری- الزامات طرف‌های علاقه‌مند ممکن است شامل الزامات قانونی، مقررات تنظیمی و تعهدات قراردادی شود.

۴-۳ تعیین محدوده سیستم مدیریت امنیت اطلاعات

سازمان باید مرزها و کاربردپذیری سیستم مدیریت امنیت اطلاعات را به‌منظور استقرار محدوده خود، تعیین کند.

سازمان باید هنگام تعیین این محدوده موارد زیر را در نظر بگیرد:

الف- موارد بیرونی و درونی اشاره‌شده در بند ۴-۱؛

ب- الزامات اشاره‌شده در بند ۴-۲؛ و

پ- واسط‌ها[1] و وابستگی‌ها بین فعالیت‌هایی که توسط سازمان انجام می‌شوند و فعالیت‌هایی که توسط سازمان‌های دیگر انجام می‌شوند.

محدوده باید به‌صورت اطلاعات مستند در دسترس باشد.

۴-۴ سیستم مدیریت امنیت اطلاعات

سازمان باید سیستم مدیریت امنیت اطلاعات را مطابق با الزامات این استاندارد ملی استقرار، پیاده‌سازی، نگهداری کند و به‌طور مستمر بهبود دهد.

۵ رهبری

۵-۱ رهبری و تعهد

مدیر ارشد باید رهبری و تعهد در رابطه با سیستم مدیریت امنیت اطلاعات را توسط موارد زیر نشان[2] دهد:

الف- اطمینان از این‌که خط‌مشی امنیت اطلاعات و اهداف امنیت اطلاعات مستقرشده و سازگار با جهت-گیری راهبردی سازمان است؛

ب- اطمینان از یکپارچه شدن الزامات سیستم مدیریت امنیت اطلاعات در فرآیندهای سازمان؛

پ- اطمینان از این‌که منابع موردنیاز سیستم مدیریت امنیت اطلاعات در دسترس است؛

1 - Interfaces
2 - Demonstrate

ت- ابلاغ اهمیت مدیریت امنیت اطلاعات اثربخش و اهمیت انطباق با الزامات سیستم مدیریت امنیت اطلاعات؛

ث- اطمینان از این‌که سیستم مدیریت امنیت اطلاعات نتیجه(های) موردنظر خود را به دست می‌آورد؛

ج- هدایت و پشتیبانی افراد به‌منظور مشارکت در اثربخشی سیستم مدیریت امنیت اطلاعات؛

چ- بهبود مستمر؛ و

ح- پشتیبانی از سایر نقش‌های مدیریتی مرتبط برای نشان دادن رهبری توسط آن‌ها در حوزه‌های مسئولیتی مرتبط.

۵-۲ خط‌مشی

مدیر ارشد باید یک خط‌مشی امنیت اطلاعات ایجاد کند که؛

الف- متناسب با مقصود سازمان باشد؛

ب- شامل اهداف امنیت اطلاعات (به بند ۶-۲ مراجعه شود) بوده یا چارچوبی برای تعیین اهداف امنیت اطلاعات فراهم کند؛

پ- شامل تعهد به برآورده سازی الزامات کاربردپذیر مرتبط با امنیت اطلاعات باشد؛ و

ت- شامل تعهد به بهبود مستمر سیستم مدیریت امنیت اطلاعات باشد؛

خط‌مشی امنیت اطلاعات باید:

ث- به‌عنوان اطلاعات مستند در دسترس باشد؛

ج- درون سازمان ابلاغ‌شده باشد؛

چ- به‌طور مناسب، در دسترس طرف‌های علاقه‌مند باشد.

۵-۳ نقش‌ها، مسئولیت‌ها و اختیارات سازمانی

مدیریت ارشد باید اطمینان حاصل کند که مسئولیت‌ها و اختیارات، برای نقش‌های مرتبط با امنیت اطلاعات، اختصاص‌یافته و ابلاغ‌شده است.

مدیریت ارشد، باید مسئولیت‌ها و اختیارات را برای موارد زیر اختصاص دهد:

الف- تضمین این‌که سیستم مدیریت امنیت اطلاعات با الزامات این استاندارد ملی منطبق است؛ و

ب- گزارش‌دهی عملکرد سیستم مدیریت امنیت اطلاعات برای مدیریت ارشد؛

یادآوری- مدیریت ارشد همچنین می‌تواند مسئولیت‌ها و اختیاراتی برای گزارش‌دهی عملکرد سیستم مدیریت امنیت اطلاعات در سازمان اختصاص دهد.

۶ طرح‌ریزی

۶-۱ اقدامات جهت پرداختن[1] به مخاطرات و فرصت‌ها

۶-۱-۱ کلیات

هنگام طرح‌ریزی سیستم مدیریت امنیت اطلاعات، سازمان باید موارد اشاره‌شده در بند ۴-۱ و الزامات اشاره‌شده در بند ۴-۲ را در نظر گرفته و مخاطرات و فرصت‌هایی را با لحاظ کردن موارد زیر تعیین کند:

الف- اطمینان از این‌که سیستم مدیریت امنیت اطلاعات می‌تواند به نتایج موردنظر دست یابد؛

ب- اجتناب یا کاهش تأثیرات نامطلوب؛ و

پ- دستیابی به بهبود مستمر.

سازمان باید موارد زیر را طرح‌ریزی کند:

ت- اقدامات برای پرداختن به این مخاطرات و فرصت‌ها؛ و

ث- چگونه:

۱- یکپارچه‌سازی و پیاده‌سازی این اقدامات را در فرآیندهای سیستم مدیریت امنیت اطلاعات انجام دهد؛ و

۲- اثربخشی این اقدامات را ارزشیابی کند.

۶-۱-۲ ارزیابی مخاطرات امنیت اطلاعات

سازمان باید فرآیند ارزیابی مخاطرات را تعریف کرده و به کار گیرد که:

الف- معیارهای مخاطرات امنیت اطلاعات را تعیین و نگهداری کند که شامل موارد زیر است:

۱-معیارهای پذیرش مخاطرات؛ و

۲-معیارهایی برای انجام ارزیابی‌های مخاطرات امنیت اطلاعات؛

ب- تضمین کند که تکرار ارزیابی مخاطرات امنیت اطلاعات نتایج سازگار، معتبر و قیاس‌پذیر تولید می‌کند؛

پ- مخاطرات امنیت اطلاعات را شناسایی کند:

۱- اعمال فرآیند ارزیابی مخاطرات امنیت اطلاعات برای شناسایی مخاطرات مرتبط با از دست دادن محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات در محدوده سیستم مدیریت امنیت اطلاعات؛ و

۲- شناسایی مالکان مخاطرات؛

ت- مخاطرات امنیت اطلاعات را تحلیل کند:

---

1 - Address

۱- ارزیابی پیامدهای بالقوه که ممکن است در صورت تحقق مخاطرات شناسایی‌شده در بند پ ۶-۱-۲ رخ دهد؛

۲- ارزیابی واقع‌بینانه فرصت وقوع مخاطرات شناسایی‌شده در بند پ ۶-۱-۲؛ و

۳- تعیین سطوح مخاطرات؛

ث- مخاطرات امنیت اطلاعات را ارزشیابی کند:

۱- مقایسه نتایج تحلیل مخاطرات با معیار معین‌شده مخاطرات در بند الف ۶-۱-۲؛

۲- اولویت‌بندی مخاطرات تحلیل‌شده برای برطرف‌سازی مخاطرات؛

سازمان باید اطلاعات مستند در مورد فرآیند ارزیابی مخاطرات امنیت اطلاعات را نگهداری کند.

۶-۱-۳ برطرف‌سازی مخاطرات امنیت اطلاعات

سازمان باید فرآیند برطرف‌سازی مخاطرات امنیت اطلاعات را برای موارد زیر تعریف کرده و به کار گیرد:

الف- انتخاب گزینه‌های مناسب برطرف‌سازی مخاطرات امنیت اطلاعات با در نظر گرفتن نتایج ارزیابی مخاطرات؛

ب- تعیین همه کنترل‌هایی که برای پیاده‌سازی گزینه(های) انتخاب‌شده جهت برطرف‌سازی مخاطرات امنیت اطلاعات لازم هستند؛

یادآوری- سازمان‌ها می‌توانند کنترل‌های موردنیاز را طراحی کرده یا آن‌ها را از هر منبعی شناسایی کند.

پ- مقایسه‌ی کنترل‌های تعیین‌شده در بالا (بند ب ۶-۱-۳) با آن‌هایی که در پیوست الف هستند، و اطمینان از اینکه هیچ کنترل موردنیازی حذف نشده است.

یادآوری ۱- پیوست الف حاوی فهرست جامعی از اهداف کنترلی و کنترل‌ها است. کاربران این استاندارد ملی به استفاده از پیوست الف هدایت می‌شوند تا اطمینان حاصل شود که از هیچ کنترل لازمی چشم‌پوشی نشده است.

یادآوری ۲- اهداف کنترلی به صورت ضمنی در کنترل‌های انتخابی موجود هستند. اهداف کنترلی و کنترل‌های فهرست شده در پیوست الف، کامل نیستند و کنترل‌ها و اهداف کنترلی اضافی نیز ممکن است نیاز باشد.

ت-تهیه یک بیانیه کاربردپذیری که شامل کنترل‌های لازم (به ب و پ بند ۶-۱-۳ مراجعه شود) و توجیه برای انتخاب کنترل‌ها؛ فارغ از اینکه پیاده‌سازی شده یا نشده باشند، و توجیه برای کنترل‌های کنارگذاری-شده از پیوست الف باشد.

ث- تدوین طرح برطرف‌سازی مخاطرات امنیت اطلاعات؛ و

ج- دریافت تأیید مالکان مخاطرات برای طرح برطرف‌سازی مخاطرات امنیت اطلاعات و پذیرش مخاطرات امنیت اطلاعات باقیمانده؛

سازمان باید اطلاعات مستند در مورد فرآیند برطرف‌سازی مخاطرات امنیت اطلاعات را نگهداری کند.

یادآوری- فرآیند ارزیابی و برطرف‌سازی مخاطرات امنیت اطلاعات در این استاندارد ملی، هم‌راستا با اصول و راهنمایی‌های عمومی موجود در استاندارد ملی ۱۴۵۶۰، است.

۶-۲ اهداف امنیت اطلاعات و طرح‌ها برای دستیابی به آن‌ها

سازمان باید اهداف امنیت اطلاعات را در سطوح و کارکردهای متناسب مستقر کند.

اهداف امنیت اطلاعات باید:

الف- سازگار با خط‌مشی امنیت اطلاعات باشد؛

ب- قابل‌سنجش باشد (اگر عملی باشد)؛

پ-الزامات امنیت اطلاعات کاربردپذیر، نتایج ارزیابی مخاطرات و برطرف‌سازی مخاطرات را در نظر بگیرد؛

ت- ابلاغ شود؛ و

ث- به نحو مناسبی به‌روزرسانی شود؛

سازمان باید اطلاعات مستند از اهداف امنیت اطلاعات را نگهداری کند. زمانی که سازمان برای چگونگی تحقق اهداف امنیت اطلاعات طرح‌ریزی می‌کند، باید موارد زیر را تعیین کند:

ج- چه‌کارهایی انجام خواهد شد؛

چ- چه منابعی موردنیاز خواهد بود؛

ح- چه کسانی پاسخگو خواهند بود؛

خ-چه زمانی تکمیل خواهد شد؛ و

د- چگونه نتایج ارزشیابی خواهند شد.

۷ پشتیبانی

۷-۱ منابع

سازمان باید منابع لازم برای ایجاد، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات را تعیین و فراهم آورد.

۷-۲ شایستگی

سازمان باید:

الف- شایستگی موردنیاز افرادی که تحت کنترل سازمان کار می‌کنند، و بر روی عملکرد امنیت اطلاعات تأثیرگذار هستند را تعیین کند؛

ب- از این‌که این افراد، بر اساس تحصیلات، آموزش‌ها، یا تجربیات مناسب، شایستگی دارند، اطمینان حاصل کند؛

پ- در صورت کاربردپذیر بودن، اقداماتی برای به دست آوردن شایستگی لازم را انجام داده و اثربخشی اقدامات انجام‌گرفته را ارزشیابی کند؛ و

ت- اطلاعات مستند مناسب به‌عنوان شواهد شایستگی را نگهداری کند.

یادآوری- اقدامات کاربردپذیر می‌تواند شامل مواردی مانند:تامین آموزش‌ها، مربی‌گری، یا جابجایی کارکنان موجود، یا اشتغال یا برون‌سپاری به افراد شایسته، باشد.

۷-۳ آگاه‌سازی

کارکنانی که تحت کنترل سازمان کار می‌کنند باید از موارد زیر آگاه باشند:

الف- خط‌مشی امنیت اطلاعات؛

ب- مشارکت خود در اثربخشی سیستم مدیریت امنیت اطلاعات، شامل مزایای بهبود عملکرد امنیت اطلاعات؛ و

پ- پیامدهای عدم انطباق با الزامات سیستم مدیریت امنیت اطلاعات.

۷-۴ ارتباطات

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

الف- در مورد چه موضوعاتی ارتباط برقرار شود؛

ب-چه مواقعی ارتباط برقرار شود؛

پ-با چه کسانی ارتباط برقرار شود؛

ت- چه کسانی باید ارتباط را برقرار کنند؛ و

ث- فرآیندهایی که به‌واسطه آن‌ها باید ارتباطات برقرار شود.

۷-۵ اطلاعات مستند

۷-۵-۱ کلیات

سیستم مدیریت امنیت اطلاعات سازمان باید شامل موارد زیر باشد:

الف- اطلاعات مستند الزام شده توسط این استاندارد ملی؛ و

ب- اطلاعات مستندی که سازمان آنها را به‌عنوان موارد اجباری برای اثربخشی سیستم مدیریت امنیت اطلاعات تعیین‌کرده است.

یادآوری- گستره اطلاعات مستند برای سیستم مدیریت امنیت اطلاعات، می‌تواند از یک سازمان به سازمان دیگر بر اساس موارد زیر متفاوت باشد:

الف- اندازه سازمان و نوع فعالیت‌ها، فرآیندها، محصولات و خدمات؛

ب- پیچیدگی فرآیندها و تعاملات آن‌ها؛ و

پ-شایستگی کارکنان.

۷-۵-۲ ایجاد و به‌روزرسانی

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

الف- شناسایی و توصیف (مانند عنوان، تاریخ، نویسنده، یا شماره ارجاع)؛

ب- قالب(مانند زبان، نسخه نرم‌افزار، نگاشتاری[1]) و رسانه (مانند کاغذی، الکترونیکی)؛ و

پ- بازنگری و تأیید مناسب بودن و کفایت آن‌ها.

۷-۵-۳ کنترل اطلاعات مستند

اطلاعات مستند الزامی سیستم مدیریت امنیت اطلاعات و این استاندارد ملی باید کنترل شود تا اطمینان حاصل شود که:

الف- این اطلاعات در دسترس و مناسب برای استفاده است، در زمان و مکانی که به آن احتیاج است؛ و

ب- به‌اندازه کافی محافظت شده است (در مقابل فقدان محرمانگی، استفاده نادرست، یا از فقدان یکپارچگی).

برای کنترل اطلاعات مستند، سازمان باید به فعالیت‌های زیر، در صورت کاربردپذیر بودن، بپردازد:

پ- توزیع، دسترسی، بازیابی و استفاده؛

ت- ذخیره‌سازی و محافظت[2]، شامل حفظ خوانایی؛

ث-کنترل تغییرات (مانند کنترل نسخه)؛ و

ج- نگهداری و امحا.[3]

اطلاعات مستند با منشأ خارجی، که نیاز به آن جهت طراحی و عملیاتی سازی سیستم مدیریت امنیت اطلاعات توسط سازمان تعیین‌شده است، باید به‌صورت مناسب، شناسایی‌شده و کنترل شود.

یادآوری- دسترسی، به‌صورت ضمنی، بیانگر تصمیمی مرتبط با مجوز فقط برای مشاهده اطلاعات، یا مجوز و اختیاردهی جهت مشاهده و تغییر اطلاعات مستند و مواردی مانند آن می‌شود.

1 - Graphic
2 - preservation
3 -Disposition

۸ عملیات

۸-۱ طرح‌ریزی و کنترل عملیاتی

سازمان باید فرآیندهای لازم برای برآورده سازی الزامات امنیت اطلاعات و پیاده‌سازی فعالیت‌های تعیین‌شده در بند۶.۱ را، طرح‌ریزی، پیاده‌سازی و کنترل کند. سازمان همچنین باید طرح‌هایی را برای دستیابی به اهداف امنیت اطلاعات تعیین‌شده در بند ۶.۲، پیاده‌سازی کند.

سازمان باید اطلاعات مستند را در حد لازم برای حصول اطمینان از اینکه فرآیندها به همان صورت که طرح‌ریزی‌شده‌اند انجام می‌شود، نگهداری کند.

سازمان باید تغییرات طرح‌ریزی‌شده را کنترل کند و تبعات تغییرات ناخواسته را بازنگری کند، و در صورت لزوم، اقدامات مناسبی برای کاهش هرگونه اثرات نامطلوب انجام دهد.

سازمان باید اطمینان یابد که فرآیندهای برون‌سپاری شده، تعیین‌شده و تحت کنترل هستند.

۸-۲ ارزیابی[1] مخاطرات امنیت اطلاعات

سازمان باید در دوره‌های طرح‌ریزی‌شده یا زمان‌هایی که تغییرات عمده‌ای پیشنهاد می‌شود یا اتفاق می‌افتد، ارزیابی مخاطرات امنیت اطلاعات را با در نظر گرفتن معیار تعیین‌شده در بند الف-۶-۲-۱ انجام دهد.

سازمان باید اطلاعات مستند از نتایج ارزیابی مخاطرات امنیت اطلاعات را نگهداری کند.

۸-۳ برطرف‌سازی مخاطرات امنیت اطلاعات

سازمان باید طرح برطرف‌سازی مخاطرات امنیت اطلاعات را پیاده‌سازی کند.

سازمان باید اطلاعات مستند از نتایج برطرف‌سازی مخاطرات امنیت اطلاعات را نگهداری کند.

۹ ارزشیابی عملکرد

۹-۱ پایش، اندازه‌گیری، تحلیل و ارزشیابی

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

سازمان باید تعیین کند:

الف- چه مواردی لازم است پایش و اندازه‌گیری شود، شامل فرآیندها و کنترل‌های امنیت اطلاعات؛

ب- روش‌های پایش، اندازه‌گیری، تحلیل و ارزشیابی، به‌صورت کاربردپذیر، برای حصول اطمینان از اعتبار نتایج؛

یادآوری- روش‌هایی که انتخاب می‌شوند باید نتایج قابل‌تجدید و قیاس‌پذیر تولید کنند، تا معتبر در نظر گرفته شوند.

پ- چه زمانی پایش و سنجش باید انجام شود؛

---

1 - Assessment

توضیح شماره ۱- با توجه به دست آوردن ارزش ریسک و نه مقایسه آن از معادل ارزیابی استفاده شده است.

ت-چه کسی باید پایش و سنجش را انجام دهد؛

ث- چه زمانی نتایج پایش و سنجش باید تحلیل و ارزشیابی شود؛ و

ج- چه کسی باید نتایج را تحلیل و ارزشیابی کند.

سازمان باید اطلاعات مستند مناسب را به‌عنوان شواهد نتایج پایش و سنجش، نگهداری کند.

۹-۲ ممیزی داخلی

سازمان باید ممیزی‌های داخلی را در دوره‌های زمانی طرح‌ریزی‌شده، انجام دهد تا مشخص شود آیا سیستم مدیریت امنیت اطلاعات:

الف-منطبق است با:

۱- الزامات خود سازمان برای سیستم مدیریت امنیت اطلاعات مورداستفاده‌اش؛ و

۲- الزامات این استاندارد ملی.

ب- به‌طور مؤثری پیاده‌سازی و نگهداری می‌شود؛

سازمان باید:

پ- برنامه(های) ممیزی که شامل بسامد، روش‌ها، مسئولیت‌ها، الزامات[1] برنامه‌ریزی و گزارش‌دهی است، را طرح‌ریزی، استقرار، پیاده‌سازی و نگهداری کند. برنامه(های) ممیزی باید اهمیت فرآیندهای موردنظر و نتایج ممیزی‌های قبلی را در نظر بگیرد؛

ت- معیار ممیزی و محدوده را برای هر ممیزی تعریف کند؛

ث- ممیزان را انتخاب و ممیزی‌ها را اجرا کند که از عینی بودن و بی‌طرف بودن فرآیند ممیزی اطمینان یابد؛

ج- اطمینان یابد که نتایج ممیزی به مدیریت مرتبط گزارش می‌شود؛

چ- اطلاعات مستند را به‌عنوان شواهد برنامه(های) ممیزی و نتایج ممیزی نگهداری کند.

۹-۳ بازنگری مدیریت

مدیریت ارشد باید سیستم مدیریت امنیت اطلاعات سازمان را در دوره‌های زمانی طرح‌ریزی‌شده بازنگری کند تا از استمرار تناسب، کفایت و اثربخشی آن اطمینان حاصل کند.

بازنگری مدیریت باید شامل در نظر گرفتن موارد زیر باشد:

الف- وضعیت اقدامات از زمان بازنگری‌های قبلی مدیریت؛

---

1 - Requirements

ب- تغییرات در موضوعات درونی و بیرونی مرتبط با سیستم مدیریت امنیت اطلاعات؛

پ- بازخورد در مورد عملکرد امنیت اطلاعات، شامل روندهای:

۱-عدم انطباق‌ها و اقدامات اصلاحی؛

۲-نتایج پایش و سنجش؛

۳-نتایج ممیزی؛ و

۴- تحقق اهداف امنیت اطلاعات؛

ت-بازخورد از گروه‌های ذینفع؛

ث-نتایج ارزیابی مخاطرات و وضعیت طرح برطرف‌سازی مخاطرات؛ و

ج- فرصت‌های بهبود مستمر.

خروجی بازنگری مدیریت باید شامل تصمیمات مرتبط با فرصت‌های بهبود مستمر و هر نیازی به تغییرات در سیستم مدیریت امنیت اطلاعات باشد.

سازمان باید اطلاعات مستند را به‌عنوان شواهد نتایج بازنگری، مدیریت نگهداری کند.

۱۰ بهبود

۱-۱۰ عدم انطباق و اقدام اصلاحی

زمانی که عدم انطباق رخ می‌دهد، سازمان باید:

الف- به عدم انطباق واکنش نشان دهد و اگر کاربردپذیر باشد:

۱- فعالیتی برای کنترل و اصلاح آن انجام دهد؛ و

۲-به پیامدها رسیدگی کند.

ب- به‌منظور جلوگیری از تکرار آن عدم انطباق یا رخ دادن در جای دیگری؛ نیاز به اقدام برای حذف علت-های عدم انطباق را ارزشیابی کند، با:

۱-بازنگری عدم انطباق؛

۲- تعیین علت‌های عدم انطباق؛ و

۳- تعیین اینکه آیا عدم انطباق‌های مشابه وجود دارد، یا امکان وقوع دارد؛

پ-پیاده‌سازی هر فعالیتی که لازم است؛

ت- بازنگری اثربخشی هر اقدام اصلاحی انجام‌شده؛ و

ث- ایجاد تغییرات در سیستم مدیریت امنیت اطلاعات، اگر لازم باشد؛

اقدامات اصلاحی باید متناسب با تأثیرات عدم انطباق‌های اتفاق افتاده باشد.

سازمان باید اطلاعات مستند را به‌عنوان شواهد موارد زیر نگهداری کند:

ج- ماهیت عدم انطباق و هر اقدامی که به‌تبع آن انجام‌شده است؛ و

چ-نتایج هر اقدام اصلاحی؛

۱۰-۲ بهبود مستمر

سازمان باید به‌صورت مستمر، تناسب، کفایت و اثربخشی سیستم مدیریت امنیت اطلاعات را بهبود دهد.

پیوست الف
(الزامی)
مرجع اهداف کنترلی و کنترل‌ها

اهداف کنترلی و کنترل‌های فهرست شده در جدول الف-۱ مستقیماً از بندهای ۵ تا ۱۸ استاندارد ایزو ۲۷۰۰۲: ۱۳۹۴ گرفته‌شده و با آن‌ها هم‌راستا هستند و درزمینهٔ بند ۶-۱-۳ استفاده می‌شوند.

جدول الف-۱- اهداف کنترلی و کنترل‌ها

الف-۵ خط‌مشی‌های امنیت اطلاعات		
الف-۵-۱ جهت‌گیری مدیریت برای امنیت اطلاعات		
مقصود: جلب حمایت و جهت‌گیری مدیریت برای امنیت اطلاعات با توجه به الزامات کسب‌وکار و قوانین و آیین‌نامه‌های مرتبط.		
الف-۵-۱-۱	خط‌مشی‌های امنیت اطلاعات	کنترل یک مجموعه از خط‌مشی‌ها برای امنیت اطلاعات باید توسط مدیریت تعریف، تصویب، منتشر و به اطلاع همه کارکنان و طرف‌های مرتبط بیرونی برسد.
الف-۵-۱-۲	بازنگری خط‌مشی‌های امنیت اطلاعات	کنترل خط‌مشی‌های امنیت اطلاعات باید در فواصل زمانی طرح‌ریزی‌شده یا درصورتی‌که تغییرات بارزی رخ دهد، به‌منظور حصول اطمینان از تداوم تناسب، کفایت و اثربخشی آن‌ها، بازنگری شود.
الف-۶ سازمان امنیت اطلاعات		
الف-۶-۱ سازمان داخلی		
مقصود: ایجاد یک چارچوب مدیریتی جهت راه‌اندازی و کنترل پیاده‌سازی و عملیات امنیت اطلاعات در درون سازمان.		

جدول الف-۱ (ادامه)

الف-۶-۱-۱	نقش‌ها و مسئولیت-های امنیت اطلاعات	کنترل تمامی مسئولیت‌های امنیت اطلاعات باید تعریف و تخصیص داده شود.
الف-۶-۱-۲	تفکیک وظایف	کنترل به‌منظور کاهش فرصت‌های دست‌کاری غیر عمد یا غیرمجاز، یا سوءاستفاده از دارائی‌های سازمان، باید وظایف متداخل و حدود مسئولیت‌ها، تفکیک شوند.
الف-۶-۱-۳	برقراری ارتباط با مراجع دارای اختیار	کنترل باید ارتباطات مناسبی با مراجع دارای اختیار مرتبط، برقرار و حفظ شود.
الف-۶-۱-۴	برقراری ارتباط با گروه‌های دارای علاقه‌مندی‌های خاص	کنترل باید ارتباطات مناسبی با گروه‌های دارای علاقه‌مندی‌های خاص یا سایر انجمن‌های حرفه‌ای در حوزه امنیت، برقرار و حفظ شود.
الف-۶-۱-۵	امنیت اطلاعات در مدیریت پروژه	کنترل صرف‌نظر از نوع پروژه، باید در مدیریت پروژه، به امنیت اطلاعات پرداخته شود.
الف-۶-۲ افزاره‌های سیار و دورکاری		
مقصود: اطمینان از امنیت دورکاری و استفاده از افزاره‌های سیار		
الف-۶-۲-۱	خط‌مشی افزاره سیار	کنترل به‌منظور مدیریت مخاطرات ناشی از استفاده از افزاره‌های سیار، باید یک خط-مشی و اقدامات امنیتی پشتیبان، به کار گرفته شود.
الف-۶-۲-۲	دورکاری	کنترل به‌منظور حفاظت از اطلاعاتی که در محل دورکاری، مورد دسترسی، پردازش یا ذخیره قرار می‌گیرد، باید یک خط‌مشی و اقدامات امنیتی پشتیبان، پیاده-سازی شود.
الف-۷ امنیت منابع انسانی		
الف-۷-۱ پیش از اشتغال		

جدول الف-۱ (ادامه)

مقصود: حصول اطمینان از اینکه کارکنان و پیمانکاران مسئولیت‌هایشان را درک کرده و برای نقش‌هایی که برای آن‌ها در نظر گرفته‌شده‌اند، مناسب می‌باشند.		
الف-۷-۱-۱	گزینش	کنترل بررسی‌های درستی‌سنجی سوابق تمامی داوطلبین اشتغال باید با توجه به قوانین، آئین‌نامه‌ها و اصول اخلاقی مرتبط انجام شوند و باید متناسب با الزامات کسب‌وکار، طبقه‌بندی اطلاعاتی که در دسترس قرار می‌گیرد و مخاطرات قابل‌تصور، باشد.
الف-۷-۱-۲	ضوابط و شرایط اشتغال	کنترل توافق‌نامه‌های قراردادی با کارکنان و پیمانکاران، باید بیانگر مسئولیت‌های ایشان و سازمان در قبال امنیت اطلاعات باشد.
الف-۷-۲ در حین خدمت		
مقصود: حصول اطمینان از اینکه کارکنان و پیمانکاران از مسئولیت‌هایشان در مورد امنیت اطلاعات آگاه بوده و آن را انجام می‌دهند.		
الف-۷-۲-۱	مسئولیت‌های مدیریت	کنترل مدیریت باید همه کارکنان و پیمانکاران را برای به‌کارگیری امنیت اطلاعات با توجه به خط‌مشی‌ها و روش‌های اجرایی ایجادشده سازمان، ملزم کند.
الف-۷-۲-۲	آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات	کنترل تمامی کارکنان سازمان و در صورت لزوم پیمانکاران، درجایی که به کارکرد شغلی ایشان مرتبط است، باید در خصوص خط‌مشی‌ها و روش‌های اجرایی سازمان، آگاه‌سازی، تحصیل و آموزش مناسب دیده و به‌طور منظم به‌روز شوند.
الف-۷-۲-۳	فرآیند انضباطی	کنترل باید یک فرآیند انضباطی رسمی و ابلاغ‌شده برای اقدام در مقابل کارکنانی که مرتکب یک نقض امنیتی اطلاعات می‌شوند، وجود داشته باشد.
الف-۷-۳ خاتمه و تغییر اشتغال		
مقصود: حفاظت از منافع سازمان به‌عنوان بخشی از فرآیند تغییر یا خاتمه اشتغال.		
الف-۷-۳-۱	مسئولیت‌های خاتمه یا تغییر	کنترل

جدول الف-۱ (ادامه)

	اشتغال	مسئولیت‌ها و وظایف امنیت اطلاعات که بعد از خاتمه یا تغییر در شغل، معتبر باقی می‌مانند، باید تعریف‌شده و به کارکنان یا پیمانکاران، ابلاغ و اجبار شود.
الف-۸ مدیریت دارایی		
الف-۸-۱ مسئولیت دارایی‌ها		
مقصود: شناسایی دارایی‌های سازمان و تعریف مسئولیت‌های مناسب برای حفاظت.		
الف-۸-۱-۱	فهرست دارایی‌ها	کنترل اطلاعات، دیگر دارایی‌های مرتبط با اطلاعات و تسهیلات پردازش اطلاعات باید شناسایی‌شده و فهرستی از این دارایی‌ها باید تنظیم و نگهداری شود.
الف-۸-۱-۲	مالکیت دارایی‌ها	کنترل دارایی‌های نگهداری شده در فهرست باید دارای مالک باشد.
الف-۸-۱-۳	استفاده قابل قبول از دارایی-ها	کنترل باید قواعدی برای استفاده قابل قبول از اطلاعات و دارایی‌های مرتبط با اطلاعات و تسهیلات پردازش اطلاعات، شناسایی، مستند و پیاده‌سازی شود.
الف-۸-۱-۴	بازگرداندن دارایی‌ها	کنترل تمامی کارکنان و کاربران شخص ثالث، باید تمامی دارایی‌های سازمان را که در اختیارشان است، به‌محض خاتمه اشتغال، قرارداد یا توافقنامه‌شان، به سازمان بازگردانند.
الف-۸-۲ طبقه‌بندی اطلاعات		
مقصود: حصول اطمینان از اینکه اطلاعات، با توجه به اهمیتشان برای سازمان از سطح حفاظت مناسبی برخوردارند.		
الف-۸-۲-۱	طبقه‌بندی اطلاعات	کنترل اطلاعات باید با توجه به الزامات قانونی، ارزش، بحرانی‌بودن و حساسیت در برابر افشای غیرمجاز یا تغییرات، طبقه‌بندی شوند.
الف-۸-۲-۲	علامت‌گذاری اطلاعات	کنترل برای علامت‌گذاری اطلاعات، باید مجموعهٔ مناسبی از روش‌های اجرایی با توجه به طرح طبقه‌بندی پذیرفته‌شدهٔ سازمان، ایجاد و مستقر شوند.

جدول الف-۱ (ادامه)

الف-۸-۲-۳	اداره کردن دارایی‌ها	کنترل باید روش‌های اجرایی برای ادارهٔ دارایی‌ها با توجه به طرح طبقه‌بندی اطلاعات پذیرفته‌شدهٔ سازمان، ایجاد و پیاده‌سازی شوند.
الف-۸-۳ اداره کردن رسانه‌های ذخیره‌سازی		
مقصود: پیشگیری از افشاء، دست‌کاری، خروج یا تخریب غیرمجاز اطلاعات ذخیره‌شده در رسانه.		
الف-۸-۳-۱	مدیریت رسانه-های ذخیره‌سازی قابل‌جابه‌جایی	کنترل برای مدیریت رسانه‌های ذخیره‌سازی قابل‌جابه‌جایی با توجه به طرح طبقه‌بندی اتخاذشده توسط سازمان باید روش‌های اجرایی پیاده‌سازی شود.
الف-۸-۳-۲	امحای رسانه‌های ذخیره‌سازی	کنترل رسانه‌های ذخیره‌سازی که دیگر موردنیاز نیستند، باید با به‌کارگیری روش‌های اجرایی رسمی، به صورتی امن، امحاء شوند.
الف-۸-۳-۳	انتقال رسانه‌های ذخیره‌سازی فیزیکی	کنترل رسانه‌های ذخیره‌سازی حاوی اطلاعات باید در هنگام حمل‌ونقل در برابر دسترسی غیرمجاز، استفادهٔ نابجا یا صدمه، محافظت شوند.
الف-۹ کنترل دسترسی		
الف-۹-۱ الزامات کسب‌وکار کنترل دسترسی		
مقصود: محدودسازی دسترسی به اطلاعات و امکانات پردازش اطلاعات.		
الف-۹-۱-۱	خط‌مشی کنترل دسترسی	کنترل یک خط‌مشی کنترل دسترسی باید بر مبنای الزامات کسب‌وکار و الزامات امنیت اطلاعات ایجاد، تدوین و بازنگری شود.
الف-۹-۱-۲	دسترسی به شبکه و خدمات شبکه	کنترل کاربران باید تنها به شبکه و خدمات شبکه که مشخصاً استفاده از آن‌ها برایشان مجاز شده، دسترسی داشته باشند.
الف-۹-۲ مدیریت دسترسی کاربر		

جدول الف-۱ (ادامه)

مقصود: حصول اطمینان از دسترسی کاربر مجاز شده و پیشگیری از دسترسی غیرمجاز به سیستم‌ها و خدمات.		
الف-۹-۲-۱	ثبت و حذف کاربر	کنترل جهت فراهم نمودن امکان تخصیص حقوق دسترسی باید یک فرآیند رسمی ثبت و حذف کاربر پیاده‌سازی شود.
الف-۹-۲-۲	تأمین دسترسی کاربر	کنترل برای واگذاری یا لغو حقوق دسترسی برای انواع کاربران به همه سیستم‌ها و خدمات، باید یک فرآیند رسمی تأمین دسترسی کاربر پیاده‌سازی شود.
الف-۹-۲-۳	مدیریت حقوق ویژه دسترسی	کنترل تخصیص و به‌کارگیری حقوق ویژه دسترسی ، باید محدود و کنترل‌شده باشد.
الف-۹-۲-۴	مدیریت اطلاعات محرمانه اصالت‌سنجی کاربران	کنترل تخصیص اطلاعات محرمانه اصالت‌سنجی ، باید از طریق یک فرآیند مدیریتی رسمی، کنترل شود.
الف-۹-۲-۵	بازنگری حقوق دسترسی کاربر	کنترل مالکان دارایی باید حقوق دسترسی کاربران را در فواصل زمانی منظم بازنگری کنند.
الف-۹-۲-۶	حذف یا تنظیم حقوق دسترسی	کنترل حقوق دسترسی تمامی کارکنان و کاربران طرف‌های بیرونی به اطلاعات و امکانات پردازش اطلاعات، باید به‌محض خاتمه خدمت، قرارداد یا توافقنامه‌شان، حذف‌شده یا به‌محض تغییر شغل، تنظیم شود.
الف-۹-۳ مسئولیت‌های کاربر		
مقصود: مسئول ساختن کاربران برای حفاظت از اطلاعات اصالت‌سنجی‌شان.		
الف-۹-۳-۱	استفاده از اطلاعات اصالت‌سنجی	کنترل کاربران باید به تبعیت از شیوه‌های سازمان در استفاده از اطلاعات محرمانه اصالت‌سنجی ملزم شوند.

جدول الف-۱ (ادامه)

الف-۹-۴ کنترل دسترسی به برنامه‌های کاربردی و سامانه‌ها[1]		
مقصود: پیشگیری از دسترسی غیرمجاز به سامانه‌ها و برنامه‌های کاربردی		
الف-۹-۴-۱	محدودسازی دسترسی به اطلاعات	کنترل مطابق با خط‌مشی کنترل دسترسی، باید دسترسی به اطلاعات و کارکردهای سامانه کاربردی، محدود شود.
الف-۹-۴-۲	روش‌های اجرایی ورود امن	کنترل در مواردی که خط‌مشی کنترل دسترسی الزام کرده است، دسترسی به سامانه‌ها باید از طریق یک روش اجرایی ورود امن به سامانه، کنترل شود.
الف-۹-۴-۳	سیستم مدیریت کلمات عبور	کنترل سیستم‌های مدیریت کلمات عبور، باید تعاملی بوده و باید کیفیت کلمات عبور را تضمین کنند.
الف-۹-۴-۴	استفاده از برنامه‌های کمکی ویژه	کنترل استفاده از برنامه‌های کمکی سامانه که ممکن است دارای قابلیت ابطال کنترل‌های سامانه و برنامهٔ کاربردی باشد، باید محدود و به‌شدت کنترل شوند.
الف-۹-۴-۵	کنترل دسترسی به کد منبع برنامه	کنترل دسترسی به کد منبع برنامه، باید محدود شود.
الف-۱۰ رمزنگاری		
الف-۱۰-۱ کنترل‌های رمزنگاری		
مقصود: حصول اطمینان از استفاده مناسب و مؤثر رمزنگاری برای حفاظت از محرمانگی، اصالت و یا یکپارچگی اطلاعات.		
الف-۱۰-۱-۱	خط‌مشی استفاده از کنترل‌های	برای حفاظت از اطلاعات، باید یک خط‌مشی استفاده از کنترل‌های رمزنگاری، ایجاد و پیاده‌سازی شود.

۱- درجایی که سیستم به‌عنوان ابزار است (برای نرم افزار و سخت افزار و شبکه) از معادل سامانه استفاده می‌شود

جدول الف-۱ (ادامه)

	رمزنگاری	
الف-۱۰-۱-۲	مدیریت کلید	خط‌مشی برای استفاده، محافظت و طول عمر کلیدهای رمزنگاری در سراسر چرخه عمر آن، باید ایجاد و پیاده‌سازی شود.
الف-۱۱ امنیت فیزیکی و محیطی		
الف-۱۱-۱ نواحی امن		
مقصود: پیشگیری از دسترسی فیزیکی غیرمجاز، خسارت و تعارض به اطلاعات و امکانات پردازش اطلاعات سازمان.		
الف-۱۱-۱-۱	حصار امنیت فیزیکی	کنترل حصارهای امنیتی باید برای حفاظت نواحی حاوی اطلاعات حساس یا حیاتی و امکانات پردازش اطلاعات، تعریف و استفاده شوند.
الف-۱۱-۱-۲	کنترل‌های ورودی فیزیکی	کنترل نواحی امن، به‌منظور حصول اطمینان از اینکه فقط کارکنان مجاز، اجازه دسترسی دارند، باید توسط کنترل‌های ورودی مناسب، حفاظت شوند.
الف-۱۱-۱-۳	امن سازی دفاتر، اتاق‌ها و امکانات	کنترل امنیت فیزیکی برای دفاتر، اتاق‌ها و امکانات، باید طراحی و به کار گرفته شود.
الف-۱۱-۱-۴	محافظت در برابر تهدیدهای بیرونی و محیطی	کنترل برای مقابله با فاجعه طبیعی، حملات مخرب یا سوانح ، باید حفاظت فیزیکی طراحی و به کار گرفته شود.
الف-۱۱-۱-۵	کار در نواحی امن	کنترل برای کار در نواحی امن، باید روش‌های اجرایی طراحی و به کار گرفته شود.
الف-۱۱-۱-۶	نواحی تحویل و بارگیری	کنترل نقاط دسترسی از قبیل نواحی تحویل و بارگیری و سایر نقاطی که افراد غیرمجاز امکان ورود به محوطه را دارند، باید تحت کنترل قرارگرفته و در صورت امکان، برای جلوگیری از دسترسی غیرمجاز، از امکانات پردازش اطلاعات، مجزا شوند.

جدول الف-۱ (ادامه)

الف-۱۱-۲ تجهیزات		
مقصود: پیشگیری از اتلاف، زیان، سرقت یا به خطر افتادن دارایی‌ها و ایجاد وقفه در عملیات سازمان.		
الف-۱۱-۲-۱	استقرار و حفاظت تجهیزات	کنترل تجهیزات باید به‌گونه‌ای مستقر یا محافظت شوند تا مخاطرات ناشی از تهدیدها و خطرات محیطی و فرصت‌های دسترسی غیرمجاز، کاهش یابند.
الف-۱۱-۲-۲	امکانات پشتیبانی	کنترل تجهیزات باید در برابر قطع برق و سایر اختلالات ناشی از نقص‌های امکانات پشتیبانی، محافظت شوند.
الف-۱۱-۲-۳	امنیت کابل-کشی	کنترل کابل‌کشی‌های برق و ارتباطات مورداستفاده برای انتقال داده یا پشتیبانی از خدمات اطلاعاتی، باید در برابر قطع شدن، تداخل یا وارد آمدن خسارت محافظت شوند.
الف-۱۱-۲-۴	نگهداری تجهیزات	کنترل تجهیزات باید به‌منظور حصول اطمینان از تداوم دسترس‌پذیری و یکپارچگی-شان، به‌درستی نگهداری شوند.
الف-۱۱-۲-۵	خروج دارایی	کنترل تجهیزات، اطلاعات یا نرم‌افزار، نباید بدون مجوز قبلی، از محوطه خارج شوند.
الف-۱۱-۲-۶	امنیت تجهیزات خارج از ابنیه	کنترل برای دارایی‌های خارج از محوطه، باید با توجه به مخاطرات مختلف ناشی از انجام کار در خارج از مرز فیزیکی سازمان، امنیت برقرار شود.
الف-۱۱-۲-۷	امحاء یا استفاده مجدد از تجهیزات به‌صورت امن	کنترل تمام اجزای تجهیزاتی که دارای رسانهٔ ذخیره‌سازی می‌باشند، باید به‌منظور حصول اطمینان از اینکه هر داده حساس و نرم‌افزار دارای حق امتیاز، پیش از امحاء یا استفاده مجدد، حذف یا به شیوه امنی بازنویسی شده، تأیید شوند.
الف-۱۱-۲-۸	تجهیزات بدون مراقبت	کنترل کاربران باید اطمینان داشته باشند که تجهیزات بدون مراقبت، حفاظت مناسبی

جدول الف-۱ (ادامه)

	کاربر	دارند.
الف-۱۱-۲-۹	خط‌مشی میز پاک و صفحه پاک	کنترل یک خط‌مشی میز پاک برای کاغذها و محیط‌های ذخیره‌سازی قابل‌جابه‌جایی و یک خط‌مشی صفحه پاک برای امکانات پردازش اطلاعات، باید به کار گرفته شود.
الف-۱۲ امنیت عملیات		
الف-۱۲-۱ مسئولیت‌ها و روش‌های اجرایی عملیاتی		
مقصود: حصول اطمینان از کارکرد صحیح و امن امکانات پردازش اطلاعات.		
الف-۱۲-۱-۱	روش‌های اجرایی عملیاتی مستند	کنترل روش‌های اجرایی عملیاتی، باید مستند شده، و در دسترس تمام کاربرانی که به آن‌ها نیاز دارند قرار بگیرد.
الف-۱۲-۱-۲	مدیریت تغییر	کنترل تغییرات در سازمان، فرآیند کسب‌وکار، امکانات و سیستم‌های پردازش اطلاعات، که بر امنیت اطلاعات تأثیر دارد باید تحت کنترل باشد.
الف-۱۲-۱-۳	مدیریت ظرفیت	کنترل استفاده از منابع باید پایش شده، تنظیم‌شده، و ظرفیت موردنیاز در آینده به‌گونه‌ای پیش‌بینی شود که از عملکرد موردنیاز سیستم، اطمینان حاصل شود.
الف-۱۲-۱-۴	جداسازی محیط توسعه، آزمون و عملیاتی	کنترل باید محیط‌های توسعه، آزمون و عملیاتی، به‌منظور کاهش مخاطرات ناشی از دسترسی غیرمجاز یا تغییرات در محیط‌های عملیاتی، تفکیک شوند.
الف-۱۲-۲ حفاظت در برابر بدافزار[1]		
مقصود: حصول اطمینان از محافظت از اطلاعات و تسهیلات پردازش اطلاعات در برابر بدافزار.		

[1] Malware

جدول الف-۱ (ادامه)

الف-۱۲-۲-۱	کنترل‌هایی در برابر بدافزار	کنترل کنترل‌های لازم برای تشخیص، پیشگیری و ترمیم به‌منظور محافظت در برابر بدافزار، همراه با آگاه‌سازی مناسب کاربر باید پیاده‌سازی شوند.
الف-۱۲-۳ نسخه‌های پشتیبان		
مقصود: محافظت در برابر از دست دادن داده‌ها.		
الف-۱۲-۳-۱	ایجاد پشتیبان از اطلاعات	کنترل نسخه‌های پشتیبان از اطلاعات، نرم‌افزارها و رونوشت[1]های سامانه‌ها، باید با توجه به یک خط‌مشی توافق شدهٔ نسخه‌های پشتیبان، به‌صورت منظم تهیه و آزمایش شوند.
الف-۱۲-۴ واقعه‌نگاری[2] و پایش		
مقصود: ثبت رویدادها و تولید شواهد.		
الف-۱۲-۴-۱	واقعه‌نگاری رویداد	کنترل سوابق وقایع رویدادها شامل فعالیت‌های کاربر، استثناها، خرابی‌ها و رویدادهای امنیت اطلاعات، باید ایجاد، نگهداری و به‌طور منظم بازنگری شوند.
الف-۱۲-۴-۲	حفاظت از اطلاعات ثبت‌شده وقایع	کنترل تسهیلات واقعه‌نگاری و اطلاعات ثبت‌شدهٔ وقایع، باید در برابر دست‌کاری و دسترسی غیرمجاز، حفاظت شوند.
الف-۱۲-۴-۳	ثبت وقایع سرپرست و بهره‌بردار سیستم	کنترل وقایع فعالیت‌های سرپرست و بهره‌بردار سیستم باید ثبت شود و این وقایع محافظت و به‌طور منظم بازنگری شود.
الف-۱۲-۴-۴	هم‌زمان‌سازی ساعت‌ها	کنترل ساعت‌های تمامی سیستم‌های پردازش اطلاعات مرتبط در درون یک سازمان یا

[1] Images
[2] Logging

جدول الف-۱ (ادامه)

		دامنه امنیتی، باید با یک منبع زمانی مرجع واحد، هم‌زمان شوند.
الف-۱۲-۵ کنترل نرم‌افزارهای عملیاتی		
مقصود: حصول اطمینان از یکپارچگی سامانه‌های عملیاتی.		
الف-۱۲-۵-۱	نصب نرم‌افزار بر سامانه‌های عملیاتی	کنترل به‌منظور کنترل نصب نرم‌افزار بر سامانه‌های عملیاتی، باید روش‌های اجرایی پیاده‌سازی شوند.
الف-۱۲-۶ مدیریت آسیب‌پذیری فنی		
مقصود: جلوگیری از سوءاستفاده از آسیب‌پذیری‌های فنی		
الف-۱۲-۶-۱	مدیریت آسیب‌پذیری-های فنی	کنترل اطلاعات در خصوص آسیب‌پذیری‌های فنی سامانه‌های اطلاعاتی مورداستفاده، باید به هنگام کسب شود، قرارگرفتن سازمان در معرض چنین آسیب‌پذیری-هایی ارزشیابی شود، و اقدامات مناسبی برای مخاطرات مرتبط، اجرا شوند.
الف-۱۲-۶-۲	محدودسازی در نصب نرم-افزار	کنترل باید قواعدی حاکم بر نصب نرم‌افزار توسط کاربر، ایجاد و پیاده‌سازی شود.
الف-۱۲-۷ ملاحظات ممیزی سامانه‌های اطلاعاتی		
مقصود: کمینه کردن پیامد فعالیت‌های ممیزی بر روی سامانه‌های عملیاتی.		
الف-۱۲-۷-۱	کنترل‌های ممیزی سامانه‌های اطلاعاتی	کنترل الزامات و فعالیت‌های ممیزی مرتبط با بررسی‌های سامانه‌های عملیاتی، باید به‌دقت طرح‌ریزی و موردتوافق قرار گیرند تا اختلال در فرآیندهای کسب‌وکار، کمینه شوند.
الف-۱۳- امنیت ارتباطات		
الف-۱۳-۱- مدیریت امنیت شبکه		
مقصود: حصول اطمینان از حفاظت اطلاعات در شبکه‌ها و امکانات پشتیبانی کننده پردازش اطلاعات.		
الف-۱۳-۱-۱	کنترل شبکه‌ها	کنترل

جدول الف-۱ (ادامه)

		شبکه‌ها باید به‌منظور محافظت اطلاعات در سامانه‌ها و برنامه‌های کاربردی مدیریت و کنترل شود.
الف-۱۳-۱-۲	امنیت خدمات شبکه	کنترل سازوکارهای امنیتی، سطوح خدمت، و الزامات مدیریتی تمامی خدمات شبکه، باید شناسایی‌شده و در هر توافقنامهٔ خدمات شبکه، اعم از اینکه این خدمات در داخل مهیا شده یا برون‌سپاری شده‌اند، لحاظ شوند.
الف-۱۳-۱-۳	تفکیک در شبکه‌ها	کنترل گروه‌های خدمات اطلاعاتی، کاربران و سامانه‌های اطلاعاتی، باید در شبکه‌ها تفکیک شوند.
الف-۱۳-۲ انتقال اطلاعات		
مقصود: حفظ امنیت اطلاعات انتقال‌یافته در درون سازمان و با هر هستار بیرونی.		
الف-۱۳-۲-۱	خط‌مشی‌ها و روش‌های اجرایی انتقال اطلاعات	کنترل برای حفاظت انتقال اطلاعات به‌واسطهٔ استفاده از تمام انواع امکانات ارتباطی، باید خط‌مشی‌ها، روش‌های اجرایی و کنترل‌های انتقال رسمی ایجاد شوند.
الف-۱۳-۲-۲	توافق‌نامه‌های انتقال اطلاعات	کنترل توافق‌نامه‌ها باید به انتقال امن اطلاعات کسب‌وکار بین سازمان و طرف‌های بیرونی بپردازند.
الف-۱۳-۲-۳	پیام‌رسانی الکترونیکی	کنترل اطلاعات موجود در پیام‌رسانی الکترونیکی باید به‌صورت مناسبی حفاظت شوند.
الف-۱۳-۲-۴	توافق‌نامه‌های محرمانگی یا عدم افشاء	کنترل الزاماتی برای توافق‌نامه‌های محرمانگی یا عدم افشاء که منعکس‌کنندهٔ نیازهای سازمان به حفاظت از اطلاعات است باید شناسایی و به‌طور منظم بازنگری و مدون شود.
الف-۱۴ اکتساب، توسعه و نگهداری سامانه		
الف-۱۴-۱ الزامات امنیتی سامانه‌های اطلاعاتی		
مقصود: حصول اطمینان از اینکه امنیت، یک جزء جدایی‌ناپذیر از سامانه‌های اطلاعاتی در تمام چرخه حیات است.		

جدول الف-۱ (ادامه)

همچنین شامل الزاماتی برای سامانه‌های اطلاعاتی که بر روی شبکه‌های همگانی ارائه خدمات می‌کنند.		
الف-۱۴-۱-۱	تحلیل و تعیین الزامات امنیت اطلاعات	کنترل الزامات مرتبط با امنیت اطلاعات باید در الزامات سامانه‌های اطلاعاتی جدید یا ارتقا سامانه‌های اطلاعاتی فعلی، موجود باشد.
الف-۱۴-۱-۲	امن سازی خدمات کاربردی در شبکه‌های همگانی	کنترل اطلاعات مورداستفاده در خدمات کاربردی که از شبکه‌های عمومی عبور می‌کنند، باید در برابر فعالیت‌های کلاه‌برداری، اختلاف نظر در قرارداد، و افشاء و دست‌کاری غیرمجاز محافظت شوند.
الف-۱۴-۱-۳	محافظت از تراکنش‌های خدمات کاربردی	کنترل اطلاعات مورداستفاده در تراکنش‌های خدمات کاربردی، باید به‌منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه، تغییر یافتن غیرمجاز پیغام، افشای غیرمجاز، بازخوانی یا کپی شدن غیرمجاز پیغام، حفاظت شوند.
الف-۱۴-۲ امنیت در فرآیندهای توسعه و پشتیبانی		
مقصود: حصول اطمینان از اینکه امنیت درون چرخه توسعه سامانه‌های اطلاعاتی، طراحی و پیاده‌سازی شده است.		
الف-۱۴-۲-۱	خط‌مشی توسعه امن	کنترل باید قواعدی برای توسعه نرم‌افزار و سامانه‌های ایجادشده و برای توسعه‌های درون سازمان به‌کارگیری شود.
الف-۱۴-۲-۲	روش‌های اجرایی کنترل تغییر سامانه	کنترل تغییرات در سامانه‌های درون چرخه توسعه، باید با استفاده از روش‌های اجرایی رسمی کنترل تغییر، کنترل شوند.
الف-۱۴-۲-۳	بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات بسترهای نرم-افزاری	کنترل در هنگام تغییر بسترهای نرم‌افزاری، به‌منظور حصول اطمینان از عدم وجود تأثیر سوء بر عملیات یا امنیت سازمانی، نرم‌افزارهای کاربردی حیاتی کسب‌وکار باید بازنگری و آزمایش شوند.
الف-۱۴-۲-۴	محدودسازی	کنترل

جدول الف-۱ (ادامه)

	در اعمال تغییرات در بسته‌های نرم-افزاری	باید از دست‌کاری در بسته‌های نرم‌افزاری، اجتناب شده، محدود به تغییرات ضروری باشد، و تمامی تغییرات باید به‌شدت کنترل شوند.
الف-۱۴-۲-۵	اصول مهندسی نرم-افزار امن	کنترل باید اصولی برای مهندسی سیستم‌های امن استقرار یابد، مستند شده، نگهداری شده و برای هرگونه پیاده‌سازی سامانه اطلاعاتی به‌کارگیری شود.
الف-۱۴-۲-۶	محیط توسعه امن	کنترل سازمان‌ها باید محیط‌های توسعه امن را جهت توسعه و یکپارچه‌سازی سامانه که کل چرخه توسعه سامانه را در برمی‌گیرد، مستقر و به‌طور مناسب حفاظت کنند.
الف-۱۴-۲-۷	توسعهٔ برون‌سپاری شده	کنترل سازمان باید فعالیت توسعه سامانه به‌صورت برون‌سپاری شده را، نظارت و پایش کند.
الف-۱۴-۲-۸	آزمون امنیت سامانه	کنترل باید آزمون کارکرد امنیتی، در طول توسعه انجام شود.
الف-۱۴-۲-۹	آزمون پذیرش سامانه	کنترل برنامه‌های آزمون پذیرش و معیارهای مرتبط برای سامانه‌های اطلاعاتی جدید، ارتقاها و ویرایش‌های جدید، باید ایجاد شود.
الف-۱۴-۳ داده آزمون		
مقصود: حصول اطمینان از محافظت داده مورداستفاده برای آزمایش.		
الف-۱۴-۳-۱	حفاظت از داده‌های آزمایشی	کنترل داده‌های آزمایشی، باید به‌دقت انتخاب‌شده، محافظت و کنترل شوند.
الف-۱۵ روابط تأمین‌کنندگان		
الف-۱۵-۱ امنیت اطلاعات در روابط تأمین‌کنندگان		
مقصود: حصول اطمینان از حفاظت دارایی‌های سازمان که در دسترس تأمین‌کنندگان است.		

جدول الف-۱ (ادامه)

الف-۱۵-۱-۱	خط‌مشی امنیت اطلاعات برای روابط تأمین-کنندگان	کنترل الزامات امنیت اطلاعات برای کاهش مخاطرات مربوط به دسترسی تأمین-کنندگان به دارایی‌های سازمان باید با تأمین‌کنندگان توافق شده و مستند شود.
الف-۱۵-۱-۲	پرداختن به امنیت درون توافقنامه‌های تأمین‌کننده	کنترل تمامی الزامات امنیت اطلاعات، باید با هر تأمین‌کننده که امکان دسترسی، پردازش، ذخیره، مبادله یا تهیه اجزاء زیرساخت فناوری اطلاعات برای اطلاعات سازمان را دارد، ایجاد و توافق شود.
الف-۱۵-۱-۳	زنجیره تأمین فناوری اطلاعات و ارتباطات	کنترل توافق‌نامه‌ها با تأمین‌کنندگان باید شامل الزاماتی برای پرداختن به مخاطرات امنیت اطلاعات مربوط به زنجیره تأمین خدمات و محصولات فناوری اطلاعات باشد.
الف-۱۵-۲ مدیریت تحویل خدمت تأمین‌کننده		
مقصود: نگهداری یک سطح موردتوافق امنیت اطلاعات و تحویل خدمت، در راستای توافق‌نامه‌های تأمین‌کننده.		
الف-۱۵-۲-۱	پایش و بازنگری خدمات تأمین-کننده	کنترل سازمان‌ها باید تحویل خدمت تأمین‌کننده را به‌صورت قاعده‌مند پایش، بازنگری و بازرسی کنند.
الف-۱۵-۲-۲	مدیریت تغییرات در خدمات تأمین‌کننده	کنترل تغییرات در ارائه خدمات توسط تأمین‌کننده، شامل نگهداری و بهبود خط-مشی‌های امنیت اطلاعات، روش‌های اجرایی و کنترل موجود، باید با توجه به میزان بحرانی بودن اطلاعات کسب‌وکار، سیستم‌ها و فرآیندهای مرتبط و برآورد مجدد مخاطرات، مدیریت شوند.
الف-۱۶ مدیریت رخداد امنیت اطلاعات		
الف-۱۶-۱ مدیریت رخدادهای امنیت اطلاعات و بهبودها		
مقصود: حصول اطمینان از رویکردی استوار و مؤثر برای مدیریت رخدادهای امنیت اطلاعات، شامل ارتباط در مورد		

جدول الف-۱ (ادامه)

رویدادهای امنیتی و ضعف‌ها.		
الف-۱۶-۱-۱	مسئولیت‌ها و روش‌های اجرایی	کنترل به‌منظور حصول اطمینان از یک پاسخ سریع، مؤثر و منظم به رخدادهای امنیت اطلاعات، مسئولیت‌های مدیریتی و روش‌های اجرایی باید ایجاد شوند.
الف-۱۶-۱-۲	گزارش‌دهی رویدادهای امنیت اطلاعات	کنترل رویدادهای امنیت اطلاعات باید در کوتاه‌ترین زمان ممکن، از طریق مجاری مدیریتی مناسب، گزارش شوند.
الف-۱۶-۱-۳	گزارش‌دهی ضعف‌های امنیتی	کنترل کارکنان و پیمانکارانی که از سیستم‌ها و خدمات اطلاعاتی سازمان استفاده می‌کنند، باید نسبت به توجه و گزارش‌دهی هر ضعف امنیتی مشاهده‌شده یا مورد سوءظن در سیستم‌ها یا خدمات، ملزم شوند.
الف-۱۶-۱-۴	ارزیابی و تصمیم برای رویدادهای امنیت اطلاعات	کنترل رویدادهای امنیت اطلاعات باید ارزیابی شود و باید تصمیم‌گیری شود که در صورت نیاز، به‌عنوان رخدادهای امنیت اطلاعات طبقه‌بندی شوند.
الف-۱۶-۱-۵	پاسخ به رخدادهای امنیت اطلاعات	کنترل به رخدادهای امنیت اطلاعات باید مطابق با روش‌های اجرایی مستند، پاسخ داده شود.
الف-۱۶-۱-۶	یادگیری از رخدادهای امنیت اطلاعات	کنترل دانش به‌دست‌آمده از تحلیل و برطرف کردن رخدادهای امنیت اطلاعات باید برای کاهش احتمال یا تأثیر رخدادهای آینده، استفاده شود.
الف-۱۶-۱-۷	گردآوری شواهد	کنترل سازمان باید روش‌های اجرایی برای شناسایی، جمع‌آوری، اکتساب و حفاظت از اطلاعات، که می‌تواند به‌عنوان شواهد استفاده شود را، تعریف و به کار برد.
الف-۱۷ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار		
الف-۱۷-۱ تداوم امنیت اطلاعات		
مقصود: تداوم امنیت اطلاعات باید در سیستم‌های مدیریت تداوم کسب‌وکار سازمان گنجانده شود.		

جدول الف-۱ (ادامه)

الف-۱۷-۱-۱	طرح‌ریزی تداوم امنیت اطلاعات	کنترل سازمان باید نیازهای خود را برای امنیت اطلاعات و تداوم مدیریت امنیت اطلاعات در موقعیت‌های ناسازگار، به‌طور مثال در طول یک بحران یا فاجعه، تعیین کند.
الف-۱۷-۱-۲	پیاده‌سازی تداوم امنیت اطلاعات	کنترل برای حصول اطمینان از سطح موردنیاز تداوم امنیت اطلاعات در حین یک موقعیت ناسازگار، سازمان باید فرآیندها، روش‌های اجرایی و کنترل‌هایی ایجاد، مستندسازی، پیاده‌سازی و نگهداری کند.
الف-۱۷-۱-۳	بررسی، بازنگری و ارزشیابی تداوم امنیت اطلاعات	کنترل سازمان باید کنترل‌های تداوم امنیت اطلاعات ایجاد و پیاده‌سازی شده را به‌منظور حصول اطمینان از معتبر و مؤثربودنشان در حین موقعیت‌های ناسازگار، در بازه‌های زمانی منظم بررسی کند.
الف-۱۷-۲ افزونگی‌ها		
مقصود: حصول اطمینان از دسترس‌پذیری امکانات پردازش اطلاعات.		
الف-۱۷-۲-۱	دسترس‌پذیری امکانات پردازش اطلاعات	کنترل امکانات پردازش اطلاعات، باید برای برآورده ساختن الزامات دسترس‌پذیری، با افزونگی کافی پیاده‌سازی شوند.
الف-۱۸ انطباق		
الف-۱۸-۱ انطباق با الزامات قانونی و قراردادی		
مقصود: پرهیز از نقض هر نوع قانون، مقررات، تعهدات آئین‌نامه‌ای یا قراردادی مرتبط با امنیت اطلاعات و هر الزام امنیتی.		
الف-۱۸-۱-۱	شناسایی الزامات قانونی و قراردادی قابل‌اجرا	کنترل تمامی مقررات قانون گزاری، الزامات آئین‌نامه‌ای، قراردادی مرتبط و رویکرد سازمان نسبت به برآورده سازی این الزامات، باید برای هر سامانه اطلاعاتی و سازمان، به‌وضوح شناسایی‌شده، تدوین‌شده و به‌روز نگه‌داشته شوند.
الف-۱۸-۱-۲	حقوق دارایی فکری	کنترل به‌منظور حصول اطمینان از انطباق با الزامات قانون‌گزار، الزامات آئین‌نامه‌ای

جدول الف-۱ (ادامه)

		و قراردادی در مورد حقوق مالکیت معنوی و استفاده از محصولات نرم‌افزاری، روش‌های اجرایی مناسب، باید پیاده‌سازی شوند.
الف-۱۸-۱-۳	حفاظت از سوابق	کنترل سوابق، باید با توجه به الزامات قانونی، آئین‌نامه‌ای، قراردادی و کسب‌وکار، در برابر گم‌شدن، تخریب، تحریف، دسترسی غیرمجاز و پخش غیرمجاز محافظت شوند.
الف-۱۸-۱-۴	حریم خصوصی و حفاظت از اطلاعات قابل‌شناسایی شخصی	کنترل حریم خصوصی و حفاظت از اطلاعات قابل‌شناسایی شخصی باید آن‌گونه که در قوانین و آئین‌نامه‌های مرتبط الزام شده و همچنین کاربردپذیر است، تضمین شود.
الف-۱۸-۱-۵	قواعد کنترل‌های رمزنگاری	کنترل کنترل‌های رمزنگاری باید در انطباق با تمامی توافقنامه‌ها، قوانین و آئین‌نامه-های مرتبط، به کار گرفته شوند.
الف-۱۸-۲ بازنگری‌های امنیت اطلاعات		
مقصود: حصول اطمینان از اینکه امنیت اطلاعات مطابق با خط‌مشی‌ها و روش‌های اجرایی سازمانی پیاده‌سازی و اجراشده.		
الف-۱۸-۲-۱	بازنگری مستقل امنیت اطلاعات	کنترل رویکرد سازمان به مدیریت امنیت اطلاعات و پیاده‌سازی آن (به‌عنوان‌مثال اهداف کنترلی، کنترل‌ها، خط‌مشی‌ها، فرآیندها و روش‌های اجرایی امنیت اطلاعات)، باید در فواصل زمانی طرح‌ریزی‌شده یا هنگامی‌که تغییرات عمده-ای رخ دهد، به‌صورت مستقل بازنگری شود.
الف-۱۸-۲-۲	انطباق با خط-مشی‌ها و استانداردهای امنیتی	کنترل مدیران باید به‌طور منظم انطباق پردازش اطلاعات و روش‌های اجرایی در حیطهٔ مسئولیتشان را با خط‌مشی‌های امنیتی مناسب، استانداردها و الزامات امنیتی دیگر، بازنگری کنند.
الف-۱۸-۲-۳	بررسی انطباق فنی	کنترل به‌منظور انطباق با خط‌مشی‌ها و استانداردهای امنیت اطلاعات سازمان، باید

جدول الف-۱ (ادامه)

		سامانه‌های اطلاعاتی به‌صورت منظم بازنگری شود.

کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۲۷۰۰۳: سال ۱۳۸۹، فناوری اطلاعات – فنون امنیتی – راهنمای اجرای سیستم مدیریت امنیت اطلاعات

[۲] استاندارد ملی ایران شماره ۲۷۰۰۴: سال ۱۳۸۹، فناوری اطلاعات – فنون امنیتی – مدیریت امنیت اطلاعات - سنجش

[۳] استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت مخاطرات امنیت اطلاعات

[۴] استاندارد ملی ایران شماره ۱۴۵۶۰: سال ۱۳۹۱، مدیریت مخاطرات – تکنیک های ارزیابی مخاطرات

[5] ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls

[6] ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012