

INSO –ISO-IEC

27001

1st.Revision

2015



جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization



استاندارد ملی ایران-ایزو

آی ای سی

۲۷۰۰۱

تجدید نظر اول

۱۳۹۴

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

مؤسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه 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 و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف کنندگان، 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 می شود و پس از دریافت نظرها و پیشنهادات در کمیته 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 در کمیته ملی طرح و بررسی و در صورت 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 شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)^۱، کمیسیون بین المللی الکتروتکنیک (IEC)^۲ و سازمان بین المللی اندازه شناسی قانونی (OIML)^۳ است و به عنوان تنها رابط^۴ کمیسیون کدکس غذایی (CAC)^۵ 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 بین المللی بهره گیری می شود.

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 درجه بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) و 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، گواهینامه تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) و وسایل سنجش، تعیین عبار 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
(کارشناسی ارشد مهندسی کامپیوتر، هوش مصنوعی و
رباتیک)

مدیرعامل شرکت پردازشگران داده آرای سپاهان

دبیر:

میر اسکندری، سید محمدرضا
(کارشناسی ارشد 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

ایزدینپناه، سحرالسادات
(کارشناسی ارشد 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
(کارشناسی ارشد مدیریت تکنولوژی، انتقال تکنولوژی)

مدیرعامل نمایندگی شرکت niscert

طی نیا، رضا
(کارشناسی ارشد فناوری اطلاعات، مدیریت فناوری
اطلاعات)

مدیر عامل شرکت کاربرد سیستم

عباس نژاد، علی
(دکترا فن آوری اطلاعات)

مدیر عامل موسسه فرهنگی هنری کهکشان نور

عزیزی پور، محسن
(کارشناسی ارشد مدیریت بازرگانی، بازاریابی)

مدیرعامل شرکت پارس آوان رایان

قسمتی، سیمین
(کارشناسی ارشد مهندسی فناوری اطلاعات)

کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعات
سازمان فناوری اطلاعات ایران

معاون مدیرکل نظام مدیریت امنیت اطلاعات سازمان
فناوری اطلاعات ایران

کارشناس رسمی دادگستری

مدیرفنی شرکت پردازشگران داده آرای سپاهان

کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعات
سازمان فناوری اطلاعات ایران

کیامهر، بیتا
(کارشناسی ارشد مدیریت تکنولوژی)

محمودی، یعقوب
(کارشناسی ارشد فن آوری اطلاعات)

مرتضوی، محمود
(دکترای مهندسی نرم افزار)

مغانی، مهدی
(کارشناسی ارشد ریاضی کاربردی)

فهرست مندرجات

صفحه		عنوان
ب		آشنایی با سازمان ملی استاندارد ایران
ج		کمیسیون فنی تدوین استاندارد
ز		پیش‌گفتار
ح	۰	مقدمه
ح	۱-۰	کلیات
ط	۲-۰	انطباق با دیگر استانداردهای سیستم‌های مدیریتی
۱	۱	هدف و دامنه کاربرد
۱	۲	مراجع الزامی
۱	۳	اصطلاحات و تعاریف
۱	۴	زمینه سازمان
۱	۱-۴	درک سازمان و زمینه آن
۲	۲-۴	درک نیازها و انتظارات طرف‌های علاقه‌مند
۲	۳-۴	تعیین محدوده سیستم مدیریت امنیت اطلاعات
۲	۴-۴	سیستم مدیریت امنیت اطلاعات
۲	۵	رهبری
۲	۱-۵	رهبری و تعهد
۳	۲-۵	خط‌مشی
۳	۳-۵	نقشه‌ها، مسئولیت‌ها و اختیارات سازمانی
۴	۶	طرح‌ریزی
۴	۱-۶	اقدامات جهت پرداختن به مخاطرات و فرصت‌ها
۴	۱-۱-۶	کلیات
۴	۲-۱-۶	ارزیابی مخاطرات امنیت اطلاعات
۵	۳-۱-۶	برطرف‌سازی مخاطرات امنیت اطلاعات
۶	۲-۶	اهداف امنیت اطلاعات و طرح‌ها برای دستیابی به آن‌ها
۶	۷	پشتیبانی
۶	۱-۷	منابع
۶	۲-۷	شایستگی
۷	۳-۷	آگاه‌سازی
۷	۴-۷	ارتباطات
۷	۵-۷	اطلاعات مستند

۷	۱-۵-۷ کلیات
۸	۲-۵-۷ ایجاد و به‌روزرسانی
۸	۳-۵-۷ کنترل اطلاعات مستند
۹	۸ عملیات
۹	۱-۸ طرح‌ریزی و کنترل عملیات
۹	۲-۸ ارزیابی مخاطرات امنیت اطلاعات
۹	۳-۸ برطرف‌سازی مخاطرات امنیت اطلاعات
۹	۹ ارزشیابی عملکرد
۹	۱-۹ پایش، اندازه‌گیری، تحلیل و ارزشیابی
۱۰	۲-۹ ممیزی داخلی
۱۰	۳-۹ بازنگری مدیریت
۱۱	۱۰ بهبود
۱۱	۱-۱۰ عدم انطباق و اقدام اصلاحی
۱۲	۲-۱۰ بهبود مستمر
۱۳	پیوست الف (الزامی) مرجع اهداف کنترلی و کنترل‌ها
۳۳	کتاب‌نامه

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 ۲۷۰۰۱-ISIRI-ISO-IEC: سال ۱۳۸۷ است.

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

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

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

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

۳- استاندارد ملی ایران با شماره ۱۴۰۹۶ ISIRI-ISO-IEC در سال ۱۳۸۹ با منبع بین‌المللی ISO/IEC 27004:2009 منتشر شده است.

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

۲-۰ انطباق با دیگر استانداردهای سیستم‌های مدیریتی

این استاندارد ملی، ساختار سطح بالا، عناوین زیر بند یکسان، متن یکسان، عبارات مشترک، و تعاریف پایه تعریف شده 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 تعریف شده 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 در زمینه سازمان، است. این استاندارد ملی همچنین شامل الزامات ارزیابی و برطرف‌سازی^۱ مخاطرات امنیت اطلاعات است که برای نیازهای سازمان، سفارشی‌شده^۲ است. الزامات بیان شده 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 مشخص شده 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 داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده 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 ارائه شده در استاندارد ISO/IEC 27000 به کار می‌رود.

۴ زمینه سازمان

۱-۴ درک^۳ سازمان و زمینه^۴ آن

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

1 - Treatment

2 - Tailored

3 - Understanding

4 - Context

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

۲-۴ 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.

۳-۴ تعیین محدوده سیستم مدیریت امنیت اطلاعات

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

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

الف- موارد بیرونی و درونی اشاره شده در بند ۴-۱؛

ب- الزامات اشاره شده در بند ۴-۲؛ و

پ- واسط‌ها^۱ و وابستگی‌ها بین فعالیت‌هایی که توسط سازمان انجام می‌شوند و فعالیت‌هایی که توسط سازمان‌های دیگر انجام می‌شوند.

محدوده باید به صورت 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 به طور مستمر بهبود دهد.

۵ رهبری

۱-۵ رهبری و تعهد

مدیر ارشد باید رهبری و تعهد در رابطه با سیستم مدیریت امنیت اطلاعات را توسط موارد زیر نشان^۲ دهد:

الف- اطمینان از این که خط‌مشی امنیت اطلاعات و اهداف امنیت اطلاعات مستقر شده و سازگار با جهت-گیری راهبردی سازمان است؛

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

پ- اطمینان از این که 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 این که سیستم مدیریت امنیت اطلاعات نتیجه(های) موردنظر خود را به دست می آورد؛

ج- هدایت و پشتیبانی افراد به منظور 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.

۲-۵ 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- به عنوان اطلاعات مستند در دسترس باشد؛

ج- درون سازمان ابلاغ شده باشد؛

چ- به طور مناسب، در دسترس طرف‌های علاقه‌مند باشد.

۳-۵ نقش‌ها، مسئولیت‌ها و اختیارات سازمانی

مدیریت ارشد باید اطمینان حاصل کند که مسئولیت‌ها و اختیارات، برای نقش‌های مرتبط با امنیت اطلاعات، اختصاص یافته و ابلاغ شده است.

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

الف- تضمین این که 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

۱-۶ اقدامات جهت پرداختن^۱ به مخاطرات و فرصت‌ها

۱-۱-۶ 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.

۲-۱-۶ 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:

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

۲- ارزیابی واقع‌بینانه فرصت وقوع مخاطرات شناسایی شده 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 معین شده مخاطرات در بند الف ۶-۱-۲؛

۲- اولویت‌بندی مخاطرات تحلیل شده 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 کنند.

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- چه کارهایی 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

۱-۷ منابع

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

۲-۷ 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 انجام گرفته را ارزشیابی کند؛ و

ت- اطلاعات مستند مناسب به عنوان شواهد شایستگی را نگهداری کند.

یادآوری- اقدامات کاربردپذیر می تواند شامل مواردی مانند: تامین آموزش ها، مربی گری، یا جابجایی کارکنان موجود، یا اشتغال یا برون سپاری به افراد شایسته، باشد.

۳-۷ آگاه سازی

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

الف- خط مشی 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.

۴-۷ 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 به واسطه آنها باید ارتباطات برقرار شود.

۵-۷ اطلاعات مستند

۱-۵-۷ 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 به عنوان موارد اجباری برای اثربخشی سیستم مدیریت امنیت اطلاعات تعیین کرده است.

یادآوری- گستره اطلاعات مستند برای سیستم مدیریت امنیت اطلاعات، می تواند 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^۱) 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- به اندازه 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^۲، شامل حفظ خوانایی؛

ث- کنترل تغییرات (مانند کنترل نسخه)؛ و

ج- نگهداری و امحا^۳.

اطلاعات مستند با منشأ خارجی، که نیاز به آن جهت طراحی و عملیاتی سازی سیستم مدیریت امنیت اطلاعات توسط سازمان تعیین شده است، باید به صورت مناسب، شناسایی شده و کنترل شود.

یادآوری- دسترسی، به صورت 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

۱-۸ طرح ریزی و کنترل عملیاتی

سازمان باید فرآیندهای لازم برای برآورده سازی الزامات امنیت اطلاعات و پیاده سازی فعالیت های تعیین شده در بند ۶.۱ را، طرح ریزی، پیاده سازی و کنترل کند. سازمان همچنین باید طرح هایی را برای دستیابی به اهداف امنیت اطلاعات تعیین شده در بند ۶.۲، پیاده سازی کند.

سازمان باید اطلاعات مستند را در حد لازم برای حصول اطمینان از اینکه فرآیندها به همان صورت که طرح ریزی شده اند انجام می شود، نگهداری کند.

سازمان باید تغییرات طرح ریزی شده 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 برون سپاری شده، تعیین شده و تحت کنترل هستند.

۲-۸ ارزیابی^۱ مخاطرات امنیت اطلاعات

سازمان باید در دوره های طرح ریزی شده یا زمان هایی که تغییرات عمده ای پیشنهاد می شود یا اتفاق می افتد، ارزیابی مخاطرات امنیت اطلاعات را با در نظر گرفتن معیار تعیین شده در بند الف-۶-۲-۱ انجام دهد.

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

۳-۸ برطرف سازی مخاطرات امنیت اطلاعات

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

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

۹ ارزشیابی عملکرد

۱-۹ پایش، اندازه گیری، 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 اندازه گیری شود، شامل فرآیندها و کنترل های امنیت اطلاعات؛

ب- روش های پایش، اندازه گیری، تحلیل و ارزشیابی، به صورت کاربردپذیر، برای حصول اطمینان از اعتبار نتایج؛

یادآوری- روش هایی که انتخاب می شوند باید نتایج قابل تجدید و قیاس پذیر 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.

۲-۹ ممیزی داخلی

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

الف-منطبق است با:

۱- الزامات خود سازمان برای سیستم مدیریت امنیت اطلاعات مورد استفاده‌اش؛ 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^۱ برنامه‌ریزی و گزارش‌دهی است، را طرح‌ریزی، **استقرار**، پیاده‌سازی و نگهداری کند. برنامه(های) ممیزی باید اهمیت فرآیندهای مورد نظر 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.

۳-۹ بازنگری مدیریت

مدیریت ارشد باید سیستم مدیریت امنیت اطلاعات سازمان را در دوره‌های زمانی طرح‌ریزی شده 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؛

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 انجام شده است؛ و

چ- نتایج هر اقدام اصلاحی؛

۲-۱۰ بهبود مستمر

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

پیوست الف

(الزامی)

مرجع اهداف كنترلی و كنترل‌ها

اهداف كنترلی و كنترل‌های فهرست شده در جدول الف-۱ مستقیماً از بندهای ۵ تا ۱۸ استاندارد ایزو ۲۷۰۰۲:۱۳۹۴ گرفته شده و با آنها هم‌راستا هستند و درزمینه بند ۶-۱-۳ استفاده می‌شوند.

جدول الف-۱- اهداف كنترلی و كنترل‌ها

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	كنترل 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	كنترل خط‌مشی‌های امنیت اطلاعات باید در فواصل زمانی طرح‌ریزی شده یا در صورتی که تغییرات بارزی رخ دهد، به منظور 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 كنترل پیاده‌سازی و عملیات امنیت اطلاعات در درون سازمان.		

جدول الف-۱ (ادامه)

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

جدول الف-۱ (ادامه)

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

جدول الف-۱ (ادامه)

کنترل	اداره کردن دارایی‌ها	الف-۸-۳
باید روش‌های اجرایی برای اداره دارایی‌ها با توجه به طرح طبقه‌بندی اطلاعات پذیرفته‌شده 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.		
کنترل	مدیریت رسانه- های ذخیره‌سازی قابل جابه‌جایی	الف-۸-۳-۱
برای مدیریت رسانه‌های ذخیره‌سازی قابل جابه‌جایی با توجه به طرح طبقه‌بندی اتخاذشده توسط سازمان باید روش‌های اجرایی پیاده‌سازی شود.		
کنترل	امحای رسانه‌های ذخیره‌سازی	الف-۸-۳-۲
رسانه‌های ذخیره‌سازی که دیگر موردنیاز نیستند، باید با به‌کارگیری روش‌های اجرایی رسمی، به صورتی امن، امحاء شوند.		
کنترل	انتقال رسانه‌های ذخیره‌سازی فیزیکی	الف-۸-۳-۳
رسانه‌های ذخیره‌سازی حاوی اطلاعات باید در هنگام حمل‌ونقل در برابر دسترسی غیرمجاز، استفاده 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.		
کنترل	خط‌مشی کنترل دسترسی	الف-۹-۱-۱
یک خط‌مشی کنترل دسترسی باید بر مبنای الزامات کسب‌وکار و الزامات امنیت اطلاعات ایجاد، تدوین و بازنگری شود.		
کنترل	دسترسی به شبکه و خدمات شبکه	الف-۹-۱-۲
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.		
کنترل	ثبت و حذف کاربر	الف-۹-۲-۱
جهت فراهم نمودن امکان تخصیص حقوق دسترسی باید یک فرآیند رسمی ثبت و حذف کاربر پیاده‌سازی شود.		
کنترل	تأمین دسترسی کاربر	الف-۹-۲-۲
برای واگذاری یا لغو حقوق دسترسی برای انواع کاربران به همه سیستم‌ها و خدمات، باید یک فرآیند رسمی تأمین دسترسی کاربر پیاده‌سازی شود.		
کنترل	مدیریت حقوق ویژه دسترسی	الف-۹-۲-۳
تخصیص و به‌کارگیری حقوق ویژه دسترسی، باید محدود و کنترل شده باشد.		
کنترل	مدیریت اطلاعات محرمانه اصالت‌سنجی کاربران	الف-۹-۲-۴
تخصیص اطلاعات محرمانه اصالت‌سنجی، باید از طریق یک فرآیند مدیریتی رسمی، کنترل شود.		
کنترل	بازنگری حقوق دسترسی کاربر	الف-۹-۲-۵
مالکان دارایی باید حقوق دسترسی کاربران را در فواصل زمانی منظم بازنگری کنند.		
کنترل	حذف یا تنظیم حقوق دسترسی	الف-۹-۲-۶
حقوق دسترسی تمامی کارکنان و کاربران طرف‌های بیرونی به اطلاعات و امکانات پردازش اطلاعات، باید به‌محض خاتمه خدمت، قرارداد یا توافق‌نامه‌شان، حذف شده یا به‌محض تغییر شغل، تنظیم شود.		
الف-۹-۳ مسئولیت‌های کاربر		
مقصود: مسئول ساختن کاربران برای حفاظت از اطلاعات اصالت‌سنجی‌شان.		
کنترل	استفاده از اطلاعات اصالت‌سنجی	الف-۹-۳-۱
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 ^۱		
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 سامانه-ها 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 کنترل-های سامانه و برنامه کاربردی باشد، باید محدود و به شدت 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	
خط‌مشی برای استفاده، محافظت و طول عمر کلیدهای رمزنگاری در سراسر چرخه عمر آن، باید ایجاد و پیاده‌سازی شود.	مدیریت کلید	الف-۱۰-۲
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.		
کنترل حصارهای امنیتی باید برای حفاظت نواحی حاوی اطلاعات حساس یا حیاتی و امکانات پردازش اطلاعات، تعریف و استفاده شوند.	حصار امنیتی فیزیکی	الف-۱۱-۱-۱
کنترل نواحی امن، به‌منظور حصول اطمینان از اینکه فقط کارکنان مجاز، اجازه دسترسی دارند، باید توسط کنترل‌های ورودی مناسب، حفاظت شوند.	کنترل‌های ورودی فیزیکی	الف-۱۱-۲
کنترل امنیت فیزیکی برای دفاتر، اتاق‌ها و امکانات، باید طراحی و به کار گرفته شود.	امن سازی دفاتر، اتاق‌ها و امکانات	الف-۱۱-۳
کنترل برای مقابله با فاجعه طبیعی، حملات مخرب یا سوانح، باید حفاظت فیزیکی طراحی و به کار گرفته شود.	محافظت در برابر تهدیدهای بیرونی و محیطی	الف-۱۱-۴
کنترل برای کار در نواحی امن، باید روش‌های اجرایی طراحی و به کار گرفته شود.	کار در نواحی امن	الف-۱۱-۵
کنترل نقاط دسترسی از قبیل نواحی تحویل و بارگیری و سایر نقاطی که افراد غیرمجاز امکان ورود به محوطه را دارند، باید تحت کنترل قرار گرفته و در صورت امکان، برای جلوگیری از دسترسی غیرمجاز، از امکانات پردازش اطلاعات، مجزا شوند.	نواحی تحویل و بارگیری	الف-۱۱-۶

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 به گونه‌ای 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 مورد استفاده 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 به منظور حصول اطمینان از تداوم دسترس‌پذیری و یکپارچگی-شان، به درستی 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 به صورت امن	کنترل تمام اجزای تجهیزاتی که دارای رسانه ذخیره‌سازی می‌باشند، باید به منظور 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)

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

^۱ Malware

جدول الف-۱ (ادامه)

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

¹ Images

² Logging

جدول الف-۱ (ادامه)

دامنه امنیتی، باید با یک منبع زمانی مرجع واحد، همزمان شوند.		
الف-۱۲-۵ کنترل نرم افزارهای عملیاتی		
مقصود: حصول اطمینان از یکپارچگی سامانه‌های عملیاتی.		
الف-۱۲-۵-۱	نصب نرم افزار بر سامانه‌های عملیاتی	کنترل به منظور کنترل نصب نرم افزار بر سامانه‌های عملیاتی، باید روش‌های اجرایی پیاده‌سازی شوند.
الف-۱۲-۶ مدیریت آسیب پذیری فنی		
مقصود: جلوگیری از سوءاستفاده از آسیب‌پذیری‌های فنی		
الف-۱۲-۶-۱	مدیریت آسیب‌پذیری‌های فنی	کنترل اطلاعات در خصوص آسیب‌پذیری‌های فنی سامانه‌های اطلاعاتی مورد استفاده، باید به هنگام کسب شود، قرار گرفتن سازمان در معرض چنین آسیب‌پذیری‌هایی 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 نرم افزار 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 به دقت طرح‌ریزی و مورد توافق قرار گیرند تا اختلال در فرآیندهای کسب و کار، 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 به منظور محافظت اطلاعات در سامانه‌ها و برنامه‌های کاربردی مدیریت و کنترل شود.		
کنترل سازوکارهای امنیتی، سطوح خدمت، و الزامات مدیریتی تمامی خدمات شبکه، باید شناسایی شده و در هر توافقنامه خدمات شبکه، اعم از اینکه این خدمات در داخل مهیا شده یا برون‌سپاری شده‌اند، لحاظ شوند.	امنیت خدمات شبکه	الف-۱۳-۱-۲
کنترل گروه‌های خدمات اطلاعاتی، کاربران و سامانه‌های اطلاعاتی، باید در شبکه‌ها تفکیک شوند.	تفکیک در شبکه‌ها	الف-۱۳-۱-۳
الف-۱۳-۲ انتقال اطلاعات		
مقصود: حفظ امنیت اطلاعات انتقال یافته در درون سازمان و با هر هستار بیرونی.		
کنترل برای حفاظت انتقال اطلاعات به واسطه استفاده از تمام انواع امکانات ارتباطی، باید خط‌مشی‌ها، روش‌های اجرایی و کنترل‌های انتقال رسمی ایجاد شوند.	خط‌مشی‌ها و روش‌های اجرایی انتقال اطلاعات	الف-۱۳-۲-۱
کنترل توافق‌نامه‌ها باید به انتقال امن اطلاعات کسب‌وکار بین سازمان و طرف‌های بیرونی پردازند.	توافق‌نامه‌های انتقال اطلاعات	الف-۱۳-۲-۲
کنترل اطلاعات موجود در پیام‌رسانی الکترونیکی باید به صورت مناسبی حفاظت شوند.	پیام‌رسانی الکترونیکی	الف-۱۳-۲-۳
کنترل الزاماتی برای توافق‌نامه‌های محرمانگی یا عدم افشاء که منعکس‌کننده نیازهای سازمان به حفاظت از اطلاعات است باید شناسایی و به‌طور منظم بازنگری و مدون شود.	توافق‌نامه‌های محرمانگی یا عدم افشاء	الف-۱۳-۲-۴
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	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-۱۴-۲	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 دست کاری غیرمجاز محافظت شوند.
الف-۱۴-۳	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 به کارگیری 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 نرم‌افزاری	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)

باید از دست‌کاری در بسته‌های نرم‌افزاری، اجتناب شده، محدود به تغییرات ضروری باشد، و تمامی تغییرات باید به‌شدت کنترل شوند.	در اعمال تغییرات در بسته‌های نرم‌افزاری	
کنترل باید اصولی برای مهندسی سیستم‌های امن استقرار یابد، مستند شده، نگهداری شده و برای هرگونه پیاده‌سازی سامانه اطلاعاتی به‌کارگیری شود.	اصول مهندسی نرم‌افزار امن	الف-۱۴-۲-۵
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.	محیط توسعه امن	الف-۱۴-۲-۶
کنترل سازمان باید فعالیت توسعه سامانه به‌صورت برون‌سپاری شده را، نظارت و پایش کند.	توسعه برون‌سپاری شده	الف-۱۴-۲-۷
کنترل باید آزمون کارکرد امنیتی، در طول توسعه انجام شود.	آزمون امنیت سامانه	الف-۱۴-۲-۸
کنترل برنامه‌های آزمون پذیرش و معیارهای مرتبط برای سامانه‌های اطلاعاتی جدید، ارتقاها و ویرایش‌های جدید، باید ایجاد شود.	آزمون پذیرش سامانه	الف-۱۴-۲-۹
الف-۱۴-۳ داده آزمون		
مقصود: حصول اطمینان از محافظت داده مورد استفاده برای آزمایش.		
کنترل داده‌های آزمایشی، باید به‌دقت انتخاب شده، محافظت و کنترل شوند.	حفاظت از داده‌های آزمایشی	الف-۱۴-۳-۱
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)

کنترل	خطمشی امنیت اطلاعات برای روابط تأمین- کنندگان	الف-۱۵-۱
کنترل	پرداختن به امنیت درون توافقنامه‌های تأمین کننده	الف-۱۵-۲
کنترل	زنجیره تأمین فناوری اطلاعات و ارتباطات	الف-۱۵-۳
الف-۱۵-۲ مدیریت تحویل خدمت تأمین کننده		
مقصود: نگهداری یک سطح مورد توافق امنیت اطلاعات و تحویل خدمت، در راستای توافق نامه‌های تأمین کننده.		
کنترل	پایش و بازنگری خدمات تأمین- کننده	الف-۱۵-۲-۱
کنترل	مدیریت تغییرات در خدمات تأمین کننده	الف-۱۵-۲-۲
الف-۱۶ مدیریت رخدادهای 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.		
کنترل	مسئولیت‌ها و روش‌های اجرایی	الف-۱۶-۱-۱
به‌منظور حصول اطمینان از یک پاسخ سریع، مؤثر و منظم به رخدادهای امنیت اطلاعات، مسئولیت‌های مدیریتی و روش‌های اجرایی باید ایجاد شوند.		
کنترل	گزارش‌دهی رویدادهای امنیت اطلاعات	الف-۱۶-۱-۲
رویدادهای امنیت اطلاعات باید در کوتاه‌ترین زمان ممکن، از طریق مجاری مدیریتی مناسب، گزارش شوند.		
کنترل	گزارش‌دهی ضعف‌های امنیتی	الف-۱۶-۱-۳
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.		
کنترل	ارزیابی و تصمیم‌گیری برای رویدادهای امنیت اطلاعات	الف-۱۶-۱-۴
رویدادهای امنیت اطلاعات باید ارزیابی شود و باید تصمیم‌گیری شود که در صورت نیاز، به‌عنوان رخدادهای امنیت اطلاعات طبقه‌بندی شوند.		
کنترل	پاسخ به رخدادهای امنیت اطلاعات	الف-۱۶-۱-۵
به رخدادهای امنیت اطلاعات باید مطابق با روش‌های اجرایی مستند، پاسخ داده شود.		
کنترل	یادگیری از رخدادهای امنیت اطلاعات	الف-۱۶-۱-۶
دانش به‌دست‌آمده از تحلیل و برطرف کردن رخدادهای امنیت اطلاعات باید برای کاهش احتمال یا تأثیر رخدادهای آینده، استفاده شود.		
کنترل	گردآوری شواهد	الف-۱۶-۱-۷
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)

کنترل	طرح‌ریزی تداوم امنیت اطلاعات	الف-۱۷-۱
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.		
کنترل	پیاده‌سازی تداوم امنیت اطلاعات	الف-۱۷-۲
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.		
کنترل	بررسی، بازنگری و ارزشیابی تداوم امنیت اطلاعات	الف-۱۷-۳
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 افزودنی‌ها		
مقصود: حصول اطمینان از دسترسی‌پذیری امکانات پردازش اطلاعات.		
کنترل	دسترسی‌پذیری امکانات پردازش اطلاعات	الف-۱۷-۲-۱
امکانات پردازش اطلاعات، باید برای برآورده ساختن الزامات دسترسی‌پذیری، با افزودنی 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.		
کنترل	شناسایی الزامات قانونی و قراردادی قابل اجرا	الف-۱۸-۱-۱
تمامی مقررات قانون‌گذاری، الزامات آئین‌نامه‌ای، قراردادی مرتبط و رویکرد سازمان نسبت به برآورده سازی این الزامات، باید برای هر سامانه اطلاعاتی و سازمان، به‌وضوح شناسایی شده، تدوین شده و به‌روز نگاه‌داشته شوند.		
کنترل	حقوق دارایی فکری	الف-۱۸-۲
به‌منظور حصول اطمینان از انطباق با الزامات قانون‌گذار، الزامات آئین‌نامه‌ای		

جدول الف-۱ (ادامه)

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

جدول الف-۱ (ادامه)

سامانه‌های اطلاعاتی به صورت 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