INSO-ISO-IEC

27002
1st.Revision
Endorsement of
ISO/IEC 27002:2013 +
Cor1:2014
2015

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران –ایزو –آی ای سی
۲۷۰۰۲
تجدیدنظر اول
۱۳۹۴

فناوری اطلاعات- فنون امنیتی- آیین کار برای کنترل‌های امنیت اطلاعات

Information technology - Security techniques - Code of practice for information security controls

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- آیین کار برای کنترل‌های امنیت اطلاعات»

« تجدید نظر اول»

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)	
ایزدپناه، سحر سادات (فوق‌لیسانس مهندسی فناوری اطلاعات، سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
بهبهانی، فرید (کارشناسی مکانیک، طراحی جامدات)	مدیرعامل شرکت اینفو امن
تیموری، حسین (کارشناسی ارشد مدیریت تکنولوژی، انتقال تکنولوژی)	مدیرعامل نمایندگی شرکت niscert
دوست محمدی، وحید (فوق لیسانس مهندسی صنایع،فناوری اطلاعات)	کارشناس مرکز مدیریت راهبردی افتا
طی نیا، رضا (کارشناسی‌ارشد فناوری اطلاعات، مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
عزیزی پور، محسن (کارشناسی ارشد مدیریت بازرگانی)	مدیرعامل شرکت پارس آوان رایان
قسمتی، سیمین (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
کیامهر، بیتا (کارشناسی ارشد مدیریت تکنولوژی)	معاون مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران

محمدیان، بهزاد (فوق لیسانس مهندسی برق، مخابرات	کارشناس مرکز مدیریت راهبردی افتا
مرتضوی، محمود (دکترا مهندسی نرم‌افزار)	مدیر فنی شرکت پردازشگران داده آرای سپاهان
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس اداره تدوین استانداردهای حوزه فناوری اطلاعـات سازمان فناوری اطلاعات ایران

فهرست مندرجات

پیشگفتار

استاندارد «فناوری اطلاعات - فنون امنیتی- آیین کار برای کنترل‌های امنیت اطلاعات» که نخستین‌بار در سال ۱۳۸۷ تدوین و منتشر شد، بر اساس پیشنهادهای دریافتی 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 اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۴/۹/۳۰ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران به شماره ISIRI-ISO/IEC 27002 سال ۱۳۸۷ است.

منبع و مأخذی که برای تهیه این استاندارد مورداستفاده قرارگرفته به شرح زیر است:

ISO/IEC 27002:2013 + Cor1:2014, Information technology — Security techniques — Code of practice for information security controls

۰ مقدمه

۰-۱ پیشینه و زمینه

این استاندارد ملی، برای سازمان‌ها طراحی‌شده است تا به‌عنوان یک مرجع برای انتخاب کنترل‌ها در فرایند پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) بر اساس ISO/IEC 27001 [۱۰] مورداستفاده قرار گیرد یا به‌عنوان یک سند راهنما برای سازمان‌هایی که کنترل‌های متعارف امنیت اطلاعات را پیاده‌سازی می‌کنند، به کار گرفته شود. این استاندارد همچنین جهت توسعه راهنماهای امنیت اطلاعات خاص یک صنعت و خاص یک سازمان با مدنظر قرار دادن محیط (های) مخاطرات امنیت اطلاعات ویژه آن‌ها، به‌کارگرفته می‌شود.

سازمان‌ها از هر نوع و اندازه (ازجمله بخش عمومی و خصوصی، تجاری و غیرانتفاعی) جمع‌آوری، پردازش، ذخیره و انتقال اطلاعات را در شکل‌های مختلف ازجمله الکترونیکی، فیزیکی و کلامی (به‌عنوان‌مثال گفتگوها و ارائه‌ها) انجام می‌دهند.

ارزش اطلاعات فراتر از کلمات نوشته‌شده، اعداد و تصاویر است: دانش، مفاهیم، ایده‌ها، علائم تجاری، نمونه-هایی از اشکال نامحسوس اطلاعات هستند. در جهانی به‌هم‌پیوسته، اطلاعات و فرآیندهای مرتبط، سامانه‌ها، شبکه‌ها و کارکنان دست‌اندرکار در عملیات اداره و حفاظت آن‌ها، دارایی‌هایی هستند که مشابه سایر دارایی-های ارزشمند سازمان، برای کسب‌وکار سازمان باارزش است و درنتیجه شایسته یا نیازمند محافظت در مقابل خطرهای مختلف، است.

دارایی‌ها در معرض هر دو نوع تهدید عمدی و تصادفی هستند درحالی‌که فرآیندهای مرتبط، سامانه‌ها، شبکه‌ها و افراد، دارای آسیب‌پذیری‌های ذاتی هستند. تغییرات در فرآیندهای کسب‌وکار و سامانه‌ها، یا دیگر تغییرات خارجی (مانند قوانین و مقررات جدید) ممکن است مخاطرات جدید امنیت اطلاعات را ایجاد کنند. ازآنجاکه راه‌های زیادی وجود دارد که در آن تهدیدات می‌توانند با استفاده از آسیب‌پذیری‌ها به سازمان لطمه برسانند، مخاطرات امنیت اطلاعات همیشه وجود دارند. امنیت اطلاعات مؤثر، این مخاطرات را با حفاظت از سازمان در برابر تهدیدات و آسیب‌پذیری‌ها و درنتیجه اثرات روی دارایی‌ها، کاهش می‌دهد.

امنیت اطلاعات با اجرای یک مجموعه مناسب از کنترل‌ها، ازجمله خط‌مشی‌ها، فرآیندها، روش‌های اجرایی، ساختارهای سازمانی و کارکردهای نرم‌افزاری و سخت‌افزاری محقق می‌شود. نیاز است که این کنترل‌ها در صورت لزوم، مستقر، پیاده‌سازی، پایش، بازنگری شده و بهبود یابند تا اطمینان حاصل شود که اهداف خاص امنیت و کسب‌وکار سازمان محقق شده است. ISMS همان‌طور که در ISO/IEC 27001 [۱۰] مشخص‌شده است، یک نگاه هماهنگ و کل‌نگر به مخاطرات امنیت اطلاعات سازمان دارد تا یک مجموعه جامع از کنترل-های امنیت اطلاعات در چارچوب کلی یک سیستم مدیریت منسجم، پیاده‌سازی شود.

بسیاری از سامانه‌های اطلاعاتی با توجه به مفاهیم ISO/IEC 27001 [۱۰] و این استاندارد به‌صورت امن طراحی نشده‌اند. امنیتی که از طریق ابزارهای فنی به دست می‌آید محدود است و توصیه می‌شود توسط مدیریت و روش‌های اجرایی مناسب حمایت شود. شناسایی کنترل‌های توصیه شده برای به کار گرفته شدن،

نیازمند برنامه‌ریزی دقیق و توجه به جزئیات است. موفقیت ISMS، نیازمند حمایت همه کارکنان سازمان است. همچنین ممکن است به مشارکت سهامداران، تأمین‌کنندگان و یا سایر طرف‌های بیرونی نیاز باشد. علاوه بر این، ممکن است نیاز به مشاوره‌ی تخصصی از طرف‌های بیرونی باشد.

در یک مفهوم کلی‌تر، امنیت اطلاعات مؤثر، همچنین به مدیریت و سایر ذینفعان اطمینان می‌دهد که دارایی‌های سازمان به‌صورت منطقی، امن و در برابر آسیب محافظت‌شده‌اند و درنتیجه به‌عنوان یک توانمند ساز کسب‌وکار عمل می‌کند.

۰-۲ الزامات امنیت اطلاعات

ضروری است که سازمان الزامات امنیتی خود را شناسایی کند. سه منبع اصلی برای الزامات امنیتی وجود دارد:

الف- از طریق ارزیابی مخاطرات سازمان با در نظر گرفتن راهبرد و اهداف کلی کسب‌وکار سازمان، ارزیابی مخاطرات، تهدیدات بر دارایی‌های شناسایی‌شده، آسیب‌پذیری‌ها و فرصت وقوع را ارزشیابی کرده و تأثیر بالقوه را برآورد می‌کند؛

ب- الزامات قانونی، مقرراتی، آئین‌نامه‌ای و قراردادی که سازمان، شرکای کاری، پیمانکاران و ارائه‌دهندگان خدمات، ملزم به برآورده سازی آن هستند و محیط اجتماعی- فرهنگی آن‌ها؛

پ- مجموعه‌ای از اصول، اهداف و نیازهای کسب وکار برای تبادل، پردازش، ذخیره‌سازی، برقراری ارتباط و آرشیو اطلاعات که سازمان برای پشتیبانی از عملیات خود، توسعه داده است؛

نیاز است که بین منابع بکار گرفته‌شده در اجرای کنترل و آسیبی که به کسب‌وکار به‌واسطه مسائل امنیتی ناشی از نبود کنترل ایجاد می‌شود، تعادل برقرار شود. نتایج ارزیابی مخاطرات برای راهنمایی و تعیین اقدامات مدیریتی مناسب و اولویت‌بندی در مدیریت مخاطرات امنیت اطلاعات و پیاده‌سازی کنترل‌هایی که برای محافظت در برابر این مخاطرات، انتخاب‌شده‌اند، کمک خواهد کرد.

استاندارد ISO/IEC 27005 [۱۱] راهنمایی‌هایی جهت مدیریت مخاطرات شامل راهنمای ارزیابی مخاطرات، برطرف سازی مخاطرات، پذیرش مخاطرات، تبادل مخاطرات، پایش و بازنگری مخاطرات فراهم می‌کند.

۰-۳ انتخاب کنترل

کنترل را می‌توان از این استاندارد و یا از دیگر مجموعه کنترل‌ها انتخاب کرد و یا کنترل جدید را به‌طور مناسب برای لحاظ کردن نیازهای خاص، طراحی کرد.

انتخاب کنترل وابسته به تصمیمات سازمانی بر اساس معیارهای پذیرش مخاطرات، گزینه‌های برطرف سازی مخاطرات و رویکرد کلی سازمان برای مدیریت مخاطرات است و همچنین توصیه می‌شود پایبند به تمام

قوانین و مقررات ملی و بین‌المللی باشد. انتخاب کنترل همچنین به شیوه‌ی تعامل کنترل‌ها با یکدیگر جهت ایجاد دفاع در عمق[1]، بستگی دارد.

برخی از کنترل‌ها در این استاندارد را می‌توان به‌عنوان اصول راهنما برای مدیریت امنیت اطلاعات در نظر گرفت و قابل‌استفاده برای اکثر سازمان‌ها است. در ادامه، کنترل‌ها با جزئیات بیشتر به همراه راهنمایی پیاده-سازی توضیح داده‌شده است. اطلاعات بیشتر در مورد انتخاب کنترل و سایر گزینه‌های برطرف سازی مخاطرات را می‌توان در استاندارد ISO/IEC 27005[۱۱] یافت.

۰-۴ توسعه راهنمایی‌های مربوط به خود

این استاندارد بین‌المللی ممکن است به‌عنوان نقطه شروع برای توسعه راهنمایی‌های خاص سازمان در نظر گرفته شود. همه کنترل‌ها و راهنمایی‌ها در این آئین کار ممکن است قابل‌اجرا نباشد. علاوه بر این، کنترل-های اضافی و راهنمایی‌هایی که در این استاندارد قرار ندارد ممکن است، موردنیاز باشد. هنگامی‌که اسناد حاوی دستورالعمل یا کنترل‌های اضافه توسعه داده می‌شوند، ممکن است ارجاع متقابل به بندهای این استاندارد به‌منظور تسهیل بررسی انطباق توسط ممیزان و شرکای کسب‌وکار مناسب باشد.

۰-۵ ملاحظات چرخه حیات

اطلاعات دارای چرخه حیات است، از ایجاد و نشأت گرفتن[2] و سپس ذخیره‌سازی، پردازش، استفاده و انتقال تا تخریب و یا از بین رفتن تدریجی آن. ارزش و مخاطرات دارایی ممکن است در طول عمر دارایی متفاوت باشد (به‌عنوان‌مثال افشای غیرمجاز و یا سرقت اطلاعات حساب‌های مالی یک شرکت، پس از انتشار رسمی آن اطلاعات، به‌مراتب از اهمیت کمتری برخوردار است)؛ اما امنیت اطلاعات در تمام مراحل تا حدی مهم است.

سامانه‌های اطلاعاتی دارای چرخه حیات هستند که در آن درک شده، مشخص شده، طراحی شده، توسعه یافته، آزمایش شده، پیاده‌سازی شده، استفاده و نگهداری شده و درنهایت از خدمت، کنار گذاشته‌شده و از بین می‌روند. توصیه می شود امنیت اطلاعات در همه مراحل در نظر گرفته شود. توسعه سامانه‌های جدید و تغییرات سامانه‌های موجود، فرصت‌هایی را برای سازمان‌ها، جهت به‌روزآوری و بهبود کنترل‌های امنیتی با در نظر گرفتن رخدادهای واقعی و مخاطرات امنیت اطلاعات فعلی و مورد انتظار، ایجاد می‌کند.

۰-۶ استانداردهای مرتبط

درحالی‌که این استاندارد، راهنمایی‌هایی در طیف گسترده‌ای از کنترل‌های امنیت اطلاعات که معمولاً در بسیاری از سازمان‌های مختلف قابل‌اعمال است، ارائه می‌دهد؛ سایر استانداردهای خانواده ISO/IEC 27000، راهنمایی‌های تکمیلی و یا الزاماتی را برای سایر جنبه‌های فرایند کلی مدیریت امنیت اطلاعات ارائه می‌کنند.

1 - Defence in Depth
2 - Origination

برای معرفی کلی ISMS و خانواده استاندارد آن به ISO/IEC 27000 مراجعه شود. ISO/IEC 27000 اکثر واژگان که در کل خانواده ISO/IEC 27000 مورداستفاده قرار می‌گیرد را به‌طور رسمی بیان کرده و دامنه و اهداف برای هر یک از اعضای خانواده استانداردها را توصیف می‌کند.

فناوری اطلاعات- فنون امنیتی- آیین کار برای کنترل‌های امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، تعیین و ارائه راهنمایی‌هایی برای استانداردهای امنیت اطلاعات سازمانی و شیوه‌های مدیریت امنیت اطلاعات ازجمله انتخاب، اجرا و مدیریت کنترل‌ها با در نظر گرفتن محیط مخاطرات امنیت اطلاعات سازمان است.

این استاندارد ملی برای سازمان‌هایی طراحی‌شده است که قصد دارند:

الف- درروند اجرای سامانه (سیستم) مدیریت امنیت اطلاعات بر اساس استاندارد ISO/IEC 27001 [۱۰] کنترل‌هایی را انتخاب کنند؛

ب- کنترل‌های عموماً پذیرفته‌شده‌ی امنیت اطلاعات را پیاده‌سازی کنند؛

پ- راهنمایی‌های خود جهت مدیریت امنیت اطلاعات را توسعه دهند.

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 مرجع زیر برای این استاندارد الزامی است:

استاندارد ISO/IEC 27000، فناوری اطلاعات- فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات – مرور کلی و واژگان

۳ اصطلاحات و تعاریف

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

۴ ساختار این استاندارد

این استاندارد شامل ۱۴ بند کنترل امنیتی است که درمجموع شامل ۳۵ گروه اصلی امنیت و ۱۱۴ مورد کنترل است.

۴-۱ بندها

هر بند، کنترل‌های امنیتی که شامل یک یا چند گروه اصلی امنیت هستند را تعریف می‌کند. ترتیب بندها در این استاندارد نشان‌دهنده اهمیت آن‌ها نیست. بسته به شرایط، کنترل‌های امنیتی از هر یا همه بندها می-

تواند مهم باشد، بنابراین هر سازمان که این استاندارد را بکار می‌گیرد، توصیه می‌شود، کنترل‌های قابل به‌کارگیری را شناسایی کرده و میزان اهمیت و کاربردپذیری هر یک را نسبت به فرآیندهای سازمانی خود تعیین کند. علاوه بر این، فهرست در این استاندارد به ترتیب اولویت نیست.

۲-۴ دسته‌بندی کنترل‌ها

هر دسته اصلی کنترل امنیتی شامل موارد زیر است:

الف- هدف کنترلی که آنچه باید به دست آید را بیان می‌کند؛

ب- یک یا چند کنترل که می‌تواند برای رسیدن به آن هدف کنترلی بکار گرفته شود.

ساختار توصیف کنترل به شرح زیر است:

کنترل

عبارت خاص کنترل را برای برآوردن هدف کنترلی تعریف می‌کند؛

راهنمای پیاده‌سازی

اطلاعات جزئی‌تر جهت پشتیبانی از پیاده‌سازی کنترل و تحقق هدف کنترلی را بیان می‌کند. راهنمایی‌ها ممکن است در تمام شرایط کاملاً مناسب و یا کافی نباشند و ممکن است الزامات خاص سازمان را برای آن کنترل، پوشش ندهند.

اطلاعات دیگر

اطلاعات بیشتری که ممکن است نیاز به توجه داشته باشد را فراهم می‌کند؛ به‌عنوان‌مثال ملاحظات قانونی[1] و ارجاع به استانداردهای دیگر. اگر اطلاعات دیگری برای ارائه وجود نداشته باشد، این بخش نمایش داده نمی‌شود.

۵ خط‌مشی‌های امنیت اطلاعات

۵-۱ جهت‌گیری مدیریت برای امنیت اطلاعات

قصد: جلب حمایت و جهت‌گیری مدیریت برای امنیت اطلاعات با توجه به الزامات کسب‌وکار و قوانین و آیین‌نامه‌های مرتبط.

۵-۱-۱ خط‌مشی‌های امنیت اطلاعات

کنترل

توصیه می‌شود، مجموعه‌ای از خط‌مشی‌ها برای امنیت اطلاعات توسط مدیریت تعریف، تصویب، منتشر و به اطلاع همه کارکنان و طرف‌های مرتبط بیرونی برسد.

1- Legal

راهنمای پیاده‌سازی

توصیه می‌شود در بالاترین سطح، سازمان‌ها یک «خط‌مشی امنیت اطلاعات» تدوین کنند که مورد تصویب مدیریت قرارگرفته و رویکرد سازمان نسبت به مدیریت اهداف امنیت اطلاعات خود را تعیین کند.

توصیه می‌شود، سند خط‌مشی امنیت اطلاعات دربرگیرنده الزاماتی باشد که به‌واسطه موارد زیر ایجادشده است:

الف- راهبرد کسب‌وکار؛

ب- مقررات[1]، قوانین[2] و قراردادها[3]؛

پ- محیط تهدید امنیت اطلاعات حال حاضر و پیش‌بینی شده موردنظر[4].

توصیه می‌شود، خط‌مشی امنیت اطلاعات شامل عبارت‌هایی در خصوص موارد زیر باشد:

الف- تعریفی از امنیت اطلاعات، اهداف و اصولی برای هدایت تمامی فعالیت‌های مرتبط با امنیت اطلاعات؛

ب- واگذاری مسئولیت‌های عمومی و اختصاصی مدیریت امنیت اطلاعات به نقش‌های تعریف‌شده؛

پ- فرآیندهای ساماندهی[5] انحراف‌ها[6] و استثناءها[7].

توصیه می‌شود، در سطح پایین‌تر، خط‌مشی امنیت اطلاعات با خط‌مشی‌های با موضوع خاص پشتیبانی شود که توسط آن‌ها، پیاده‌سازی کنترل‌های امنیت اطلاعات، الزام شده و معمولاً به‌گونه‌ای ساختار داده شود که نیازهای گروه‌های هدف[8] مشخص درون سازمان یا موضوعات مشخص را پوشش دهد.

نمونه‌هایی از موضوعات چنین خط‌مشی‌هایی عبارت‌اند از:

الف- کنترل دسترسی (به بند ۹ مراجعه شود)؛

ب- طبقه‌بندی (و اداره کردن) اطلاعات (به بند ۸-۲ مراجعه شود)؛

پ- امنیت فیزیکی و محیطی (به بند ۱۱ مراجعه شود)؛

ت- موضوعات با محوریت کاربر[9] نهایی مانند:

۱- استفاده صحیح از دارایی‌ها (به بند ۸-۱-۳ مراجعه شود)؛

1- regulations
2- legislation
3- contracts
4- Projected
5- Handeling
6- deviations
7- exceptions
8- Target groups
9- User oriented

۲- میز پاک و صفحه‌نمایش پاک (به بند ۱۱-۲-۹ مراجعه شود)؛
۳- انتقال اطلاعات (به بند ۱۳-۲-۱ مراجعه شود)؛
۴- تجهیزات سیار و دورکاری (به بند ۶-۲ مراجعه شود)؛
۵- محدودیت در نصب و استفاده نرم‌افزار (به بند ۱۲-۶-۲ مراجعه شود)؛

ث- پشتیبان‌گیری (به بند ۱۲-۳ مراجعه شود)؛

ج- انتقال اطلاعات (به بند ۱۳-۲ مراجعه شود)؛

چ- حفاظت در برابر بدافزار (به بند ۱۲-۲ مراجعه شود)؛

ح- مدیریت آسیب‌پذیری‌های فنی (به بند ۱۲-۶-۱ مراجعه شود)؛

خ- کنترل‌های رمزنگاری (به بند ۱۰ مراجعه شود)؛

د- امنیت ارتباطات (به بند ۱۳ مراجعه شود)؛

ذ- حریم خصوصی و حفاظت اطلاعات شخصی قابل‌شناسایی (به بند ۱۸-۱-۴ مراجعه شود)؛

ر- روابط تأمین‌کنندگان (به بند ۱۵ مراجعه شود).

توصیه می‌شود این خط‌مشی‌ها به‌عنوان‌مثال در قالب «برنامه آگاه‌سازی، آموزش و تمرین امنیت اطلاعات» (به بند ۷-۲-۲)، به‌گونه‌ای برای کلیه کارکنان و طرف‌های بیرونی مرتبط ابلاغ شود که خط‌مشی‌ها برای خوانندگان موردنظر مرتبط، قابل‌درک و در دسترس باشد.

اطلاعات دیگر

نیاز به خط‌مشی‌های داخلی امنیت اطلاعات با توجه به سازمان‌ها متفاوت است. خط‌مشی‌های داخلی به‌طور خاص در سازمان‌های بزرگ‌تر و پیچیده‌تر مفید هستند؛ مثلاً درجایی که تعریف و تأیید سطح مورد انتظار کنترل‌ها از پیاده‌سازی کنترل‌ها مجزا است یا درجایی که خط‌مشی‌ها برای افراد و وظایف مختلف سازمان بکار گرفته می‌شود، خط‌مشی‌های امنیت اطلاعات می‌تواند به‌صورت یک سند «خط‌مشی امنیت» یا به‌صورت مجموعه‌ای از مستندات مستقل اما مرتبط صادر شود.

توصیه می‌شود اگر خط‌مشی امنیت اطلاعات به خارج از سازمان انتشار یابد، مراقبت شود که اطلاعات محرمانه سازمان فاش نشود.

برخی سازمان‌ها، از اصطلاحات دیگری مانند «استانداردها»، «راهنمایی‌ها[1]» و «قواعد[2]» برای اسناد خط‌مشی استفاده می‌کنند.

1 - Directives
2 - Rules

۵-۱-۲ بازنگری خط‌مشی‌های امنیت اطلاعات

کنترل

توصیه می‌شود، خط‌مشی‌های امنیت اطلاعات در فواصل زمانی طرح‌ریزی‌شده یا درصورتی‌که تغییرات بارزی رخ دهد، به‌منظور حصول اطمینان از تداوم تناسب، کفایت و اثربخشی آن‌ها، بازنگری شود.

راهنمای پیاده‌سازی

توصیه می‌شود، خط‌مشی دارای یک مالک باشد که مسئولیت مدیریتی تأییدشده برای توسعه، بازنگری و ارزشیابی خط‌مشی امنیت را برعهده‌گرفته باشد. توصیه می‌شود بازنگری، شامل برآورد فرصت‌هایی برای بهبود در خط‌مشی امنیتی سازمان و رویکرد مدیریت امنیت اطلاعات در واکنش به تغییرات محیط سازمانی، رویدادهای کسب‌وکار، شرایط قانونی، یا محیط فنی باشد.

توصیه می‌شود بازنگری خط‌مشی امنیت اطلاعات، نتایج بازنگری مدیریت را مدنظر قرار دهد. توصیه می‌شود، تائید مدیریت برای خط‌مشی بازنگری شده اخذ شود.

۶ سازمان امنیت اطلاعات

۶-۱ سازمان داخلی

قصد: ایجاد یک چارچوب مدیریتی جهت راه‌اندازی و کنترل پیاده‌سازی و عملیات امنیت اطلاعـات در درون سازمان.

۶-۱-۱ نقش‌ها و مسئولیت‌های امنیت اطلاعات

کنترل

توصیه می‌شود، تمامی مسئولیت‌های امنیت اطلاعات تعریف و تخصیص داده شود.

راهنمای پیاده‌سازی

توصیه می‌شود تخصیص مسئولیت‌های امنیت اطلاعات مطابق با خط‌مشی‌های امنیت اطلاعات (به بند ۵-۱-۱) صورت پذیرد. توصیه می‌شود برای محافظت از تک‌تک دارایی‌ها و انجام فرایندهای امنیت اطلاعات خاص، مسئولیت‌ها تعریف شوند. توصیه می‌شود که مسئولیت‌ها برای فعالیت‌های مدیریت مخاطرات امنیت اطلاعات و به‌طور خاص پذیرش مخاطرات باقیمانده[1] تعریف شود. توصیه می‌شود این مسئولیت‌ها در صورت لزوم برای سایت‌های خاص و تسهیلات پردازش اطلاعات باراهنمای جزئی‌تری تکمیل شود. توصیه می‌شود مسئولیت-های محلی برای محافظت از دارایی‌ها و انجام فرایندهای خاص امنیتی تعریف شوند.

1- residual

افراد با مسئولیت‌های امنیت اطلاعات تخصیص داده‌شده ممکن است وظیفه‌های امنیتی را به دیگران محـول کنند. بااین‌حال، آن‌ها همچنان مسئول بوده و توصیه می‌شود تعیین کنند که وظایف محول شده بـه‌درسـتی انجام می‌شوند.

توصیه می‌شود محدوده مسئولیت افراد به‌گونه‌ای شفاف بیان شود؛ به‌صورت خاص، توصیه می‌شود موارد زیر انجام شوند:

الف- توصیه می‌شود دارایی‌ها و فرایندهای امنیت اطلاعات، شناسایی و تعریف شود؛

ب- توصیه می‌شود مسئولی در قبال هر دارایی یا فرایند امنیت اطلاعات تخصیص داده شود و جزئیات این مسئولیت مستند شود (به بند ۸-۱-۲ مراجعه شود)؛

پ- توصیه می‌شود سطوح اختیارات، تعریف و مستند شود؛

ت- به‌منظور فراهم کردن امکان انجام مسئولیت‌های حوزه‌ی امنیت اطلاعات، توصیه می‌شود که افراد منتصب شده در آن حوزه دارای صلاحیت بوده و به آن‌ها فرصت‌هایی برای به‌روز شدن بر مبنای توسعه‌ها داده شود؛

ث- توصیه می‌شود، هماهنگی و نظارت بر جنبه‌های امنیت اطلاعات ارتباطات با تأمین‌کنندگان تعریف و مستند شود.

اطلاعات دیگر

بسیاری از سازمان‌ها یک مدیر امنیت اطلاعات جهت به عهده گرفتن مسئولیت کلان توسعه و پیاده‌سازی امنیت و پشتیبانی از شناسایی کنترل‌ها منصوب می‌کنند.

بااین‌وجود، مسئولیت تأمین منابع و پیاده‌سازی کنترل‌ها اغلب بر عهده هر یک از مدیران باقی خواهد ماند. یک نمونه[1] متداول این است که برای هر دارایی یک مالک مشخص شود که از آن به بعد مسئول محافظت روزانه از آن دارایی باشد.

۶-۱-۲ تفکیک وظایف

کنترل

توصیه می‌شود، به‌منظور کاهش فرصت‌های دست‌کاری غیر عمد یا غیرمجاز، یا سوءاستفاده از دارائی‌های سازمان، وظایف متداخل[2] و حدود مسئولیت‌ها، تفکیک شوند.

راهنمای پیاده‌سازی

1- practice
2- conflicting

توصیه می‌شود مراقبت‌های لازم صورت گیرد که هیچ فردی نتواند بدون اصالت‌سنجی یا شناسایی به دارایی ها دسترسی پیداکرده، آن‌ها را تغییر داده یا از آن‌ها استفاده کند. توصیه می‌شود شروع یک رویداد از اصالت‌سنجی آن مجزا باشد. توصیه می‌شود در طراحی کنترل‌ها، احتمال تبانی[1] در نظر گرفته شود.

سازمان‌های کوچک ممکن است انجام تفکیک وظایف را دشوار بدانند اما توصیه می‌شود این اصل تا حد امکان و به هر میزان که ممکن است رعایت شود. هر زمان که تفکیک وظایف دشوار باشد، توصیه می‌شود کنترل‌های دیگر نظیر پایش فعالیت‌ها، روند ممیزی و نظارت‌های مدیریتی بکار برده شود.

اطلاعات دیگر

تفکیک وظایف یک روش برای کاهش مخاطرات سوءاستفاده اتفاقی و یا عمدی از دارایی‌های سازمان است.

۶-۱-۳ برقراری ارتباط با مراجع دارای اختیار[2]

کنترل

توصیه می‌شود، ارتباطات مناسبی با مراجع دارای اختیار مرتبط، حفظ شود.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان‌ها رویه‌هایی در اختیار داشته باشند که مشخص می‌کند در چه زمانی و با کدام‌یک از مراجع دارای اختیار (به‌عنوان‌مثال مجریان قانون[3]، هیئت‌های تنظیم مقررات[4]، مراجع دارای اختیار نظارتی[5]) ارتباط داشته باشند و چگونه رخدادهای امنیت اطلاعات شناسایی‌شده در زمان مناسب گزارش دهی شوند، (برای مثال، اگر این تردید وجود دارد که قوانین نقض شده‌اند.)

اطلاعات دیگر

سازمان‌های تحت حمله از طریق اینترنت ممکن است برای اقدام در برابر منبع حمله نیاز به مراجع دارای اختیار داشته باشند.

حفظ چنین ارتباطاتی ممکن است از الزامی برای پشتیبانی از مدیریت رخدادهای امنیت اطلاعات (به بند ۱۶ مراجعه شود) یا فرایند طرح‌ریزی تداوم کسب‌وکار و اقدامات احتیاطی[6] (به بند ۱۷ مراجعه شود) باشد. همچنین تماس با نهادهای تنظیم مقررات، می‌تواند برای پیش‌بینی و آمادگی برای تغییرات آتی در قوانین یا مقرراتی که توسط سازمان باید رعایت شوند، مفید باشد. تماس با دیگر مراجع دارای اختیار، شامل تأسیسات زیرساختی، خدمات اضطراری، تأمین‌کنندگان برق و خدمات ایمنی و بهداشت مانند آتش‌نشانی (در رابطه با

1 - Collusion
2- Contact with authorities
2- Law enforcement
4- Regulatory bodies
5- Supervisory authorities
6 - contingency planning process

تـداوم کسـب‌وکـار)، تـأمین‌کننـدگان ارتباطـاتی (در ارتبـاط بـا مسـیریابی و دسـترس‌پـذیری خطـوط) و تأمین‌کنندگان آب (در ارتباط با تسهیلات خنک‌کننده برای تجهیزات) می‌شود.

۶-۱-۴ برقراری ارتباط با گروه‌های دارای علاقه‌مندی‌های خاص[1]

کنترل

توصیه می‌شود، ارتباطات مناسبی با گروه‌های دارای علاقه‌مندی‌های خاص یـا سـایر انجمـن‌هـای تخصصـی امنیت، حفظ شود.

راهنمای پیاده‌سازی

توصیه می‌شود، عضویت در گروه‌ها یا انجمن‌های دارای علاقه‌مندی‌های خاص به‌عنوان ابزاری برای موارد زیر در نظر گرفته شود:

الف- ارتقای دانش درباره بهروش‌ها[2] و به‌روز ماندن در خصوص اطلاعات مرتبط با امنیت اطلاعات؛

ب- اطمینان از اینکه درک از محیط امنیت اطلاعات به‌روز و کامل است؛

پ- دریافت سریع هشدارها، توصیه‌ها و وصله‌های[3] مربوط به حملات و آسیب‌پذیری‌ها؛

ت- دسترسی به توصیه‌های تخصصی امنیت اطلاعات؛

ث- به اشتراک‌گذاری و تبادل اطلاعات درباره فناوری‌ها، محصولات، تهدیدات یا آسیب‌پذیری‌های جدید؛

ج- ایجاد نقاط ارتباطی مناسب برای زمان برخورد با رخدادهای امنیت اطلاعات (به بند ۱۶ مراجعه شود).

اطلاعات دیگر

به‌منظور بهبود همکاری و هماهنگی در موضوعات امنیتی، توافقاتی برای به اشتراک‌گذاری اطلاعات می‌توانـد تدوین شود. توصیه می‌شود این توافقات، الزامات مربوط به حفاظت از اطلاعات محرمانه را شناسایی کند.

۶-۱-۵ امنیت اطلاعات در مدیریت پروژه

کنترل

توصیه می‌شود، صرف‌نظر از نوع پروژه، در مدیریت پروژه، به امنیت اطلاعات پرداخته شود.

راهنمای پیاده‌سازی

توصیه می‌شود، امنیت اطلاعات در روش (های) مدیریت پروژه سازمان یکپارچه شود تا اطمینان حاصل شود که مخاطرات امنیت اطلاعات به‌عنوان بخشی از پروژه، شناسایی‌شده و به آن‌ها پرداخته می‌شود. این کنترل

1- special interest groups
2 best practices

عموماً برای هر نوع پروژه‌ای صرف‌نظر از ویژگی آن کاربرد دارد، به‌عنوان‌مثال، پروژه‌ای در مورد فرآیند اصلی کسب‌وکار، فناوری اطلاعات، مدیریت تسهیلات و سایر فرآیندهای پشتیبان. توصیه می‌شود روش‌های مدیریت پروژه‌ی مورداستفاده، موارد زیر را الزام کنند:

الف- اهداف امنیت اطلاعات را در اهداف پروژه لحاظ کنند؛

ب- ارزیابی مخاطرات امنیت اطلاعات در مراحل اولیه پروژه انجام شود تا کنترل‌های ضروری شناسایی شود؛

پ- امنیت اطلاعات، بخشی از همه فازهای روشگان[1] پروژه به کار گرفته باشد.

توصیه می‌شود، پیامدهای امنیت اطلاعات به‌صورت دوره‌ای در تمامی پروژه‌ها مورد بازنگری قرارگرفته و به آن‌ها پرداخته شود. توصیه می‌شود، مسئولیت‌های امنیت اطلاعات در روش‌های مدیریت پروژه تعریف‌شده و به نقش‌های خاص واگذار شوند.

۶-۲ افزاره‌های سیار[2] و دورکاری

قصد: اطمینان از امنیت دورکاری و استفاده از افزاره‌های سیار.

۶-۲-۱ خط‌مشی افزاره سیار

کنترل

توصیه می‌شود، به‌منظور مدیریت مخاطرات ناشی از استفاده از افزاره‌های سیار، یک خط‌مشی و اقدامات امنیتی پشتیبان، به کار گرفته شود.

راهنمای پیاده‌سازی

توصیه می‌شود در زمان استفاده از افزاره‌های سیار، برای اطمینان از اینکه اطلاعات کسب‌وکار به خطر نمی‌افتد مراقبت‌های ویژه‌ای صورت گیرد. توصیه می‌شود خط‌مشی افزاره‌های سیار، مخاطرات کار با افزاره-های سیار در محیط‌های محافظت نشده را مدنظر قرار دهند.

توصیه می‌شود، خط‌مشی افزاره‌های سیار شامل موارد زیر باشد:

الف- ثبت افزاره‌های سیار؛

ب- الزامات حفاظت فیزیکی؛

پ- محدودیت نصب نرم‌افزار؛

ت- الزامات برای نسخه‌های نرم‌افزارهای افزاره‌های سیار و برای به‌کارگیری وصله‌ها؛

ث- محدودیت اتصال به خدمات اطلاعات؛

1- Metodology
2- Mobile devices

ج- کنترل‌های دسترسی؛

چ- فنون رمزنگاری؛

ح- محافظت در برابر بدافزار؛

خ- غیرفعال، پاک و یا قفل‌کردن از دور؛

د- نسخه‌های پشتیبان؛

ذ- استفاده از خدمات وب و برنامه‌های وب.

توصیه می‌شود در زمان استفاده از افزاره‌های سیار در مکان‌های عمومی، اتاق‌های جلسات و مناطق محافظت نشده دیگر سازمان، مراقبت شود. توصیه می‌شود برای اجتناب از دسترسی غیرمجاز یا افشای اطلاعات ذخیره‌شده و پردازش‌شده توسط این افزاره‌ها محافظت شود؛ برای مثال از فنون رمزنگاری استفاده شود (به بند ۳-۱۲ مراجعه شود) و استفاده از اطلاعات مخفی اصالت‌سنجی اجباری شود (به بند ۹-۲-۴ مراجعه شود).

همچنین توصیه می‌شود افزاره‌های سیار، ازنظر فیزیکی در برابر سرقت به‌خصوص درزمانی که مثلاً در خودرو و سایر وسایل انتقال، اتاق‌های هتل‌ها، مراکز جلسه‌ها و مکان‌های ملاقات جاگذاشته می‌شوند، محافظت شوند. توصیه می‌شود یک روش اجرایی خاص که الزامات امنیتی قانونی، بیمه‌ای و غیره سازمان را مدنظر قرار می‌دهد، برای موارد سرقت و گم‌شدن افزاره‌های سیار مستقر شود. توصیه می‌شود افزاره‌هایی که اطلاعات حساس، مهم و یا حیاتی را منتقل می‌کنند بی‌توجه رها نشوند و توصیه می‌شود در صورت امکان به‌صورت فیزیکی قفل شوند و یا از قفل‌های خاص برای امنیت افزاره‌ها استفاده شود

توصیه می‌شود برای کارکنانی که از افزاره‌های سیار استفاده می‌کنند، آموزش برای افزایش آگاهی آن‌ها درباره مخاطرات اضافی ناشی از این روش کار و کنترل‌هایی که برای اجرا توصیه می‌شود، انجام شود.

درجایی که خط‌مشی افزاره‌های سیار اجازه استفاده از افزاره‌های سیار شخصی را می‌دهند، توصیه می‌شود که خط‌مشی و اقدامات امنیتی مربوطه، موارد زیر را نیز مدنظر قرار دهند:

الف- تفکیک استفاده شخصی و کسب‌وکاری از افزاره‌ها، شامل استفاده از نرم‌افزار برای پشتیبانی از چنین تفکیکی و حفاظت از اطلاعات کسب‌وکار روی یک افزاره‌ی شخصی؛

ب- دادن دسترسی به اطلاعات کسب‌وکار صرفاً پس‌ازاینکه کاربران، توافق‌نامه کاربر نهایی را امضا کنند که به معنای پذیرفتن مسئولیت‌هایشان (حفاظت فیزیکی، به‌روزرسانی نرم‌افزارها و غیره)، چشم‌پوشی از مالکیت داده‌های کسب‌وکار، موافقت با پاک شدن از راه دور این داده‌ها توسط سازمان در صورت سرقت یا گم‌شدن افزاره و یا دیگر مجاز به استفاده از سرویس نباشد به آن است. نیاز است که این خط‌مشی، قوانین حفظ حریم خصوصی را مدنظر قرار دهد.

اطلاعات دیگر

ارتباطات بی‌سیم افزاره‌های سیار، شبیه به انواع دیگر ارتباطات شبکه است، اما تفاوت‌های مهمی وجـود دارد که توصیه می‌شود در زمان شناسایی کنترل‌ها در نظر گرفته شوند. تفاوت‌های معمول عبارت‌اند از:

الف- بعضی از پروتکل‌های امنیتی بی‌سیم، رشدنیافته[1] هستند و ضعف‌های شناخته‌شده‌ای دارند؛

ب- ممکن است به دلیل پهنای باند محدود شبکه و یا به این دلیل که افزاره‌های سیار ممکن است در زمان-های برنامه‌ریزی‌شده برای پشتیبان‌گیری به شبکه متصل نباشند، نتوان از اطلاعات ذخیره‌شده در افزاره‌هـای سیار نسخه پشتیبان گرفت.

افزاره‌های سیار عموماً کارکردهایی نظیر شبکه، دسترسی به اینترنت، رایانامه و مدیریت فایل را با افزاره‌هـای ثابت به اشتراک می‌گذارند. کنترل‌های امنیت اطلاعات برای افـزاره‌هـای سـیار معمـولاً شـامل کنتـرل‌هـای تعیین‌شده برای افزاره‌های ثابت و کنترل مرتبط با تهدیدهای ناشی از استفاده از آن‌هـا در خـارج از سـازمان است.

۶-۲-۲ دورکاری

کنترل

توصیه می‌شود، به‌منظور حفاظت از اطلاعاتی که در محل‌های دورکاری، در دسترس بوده، پردازش یا ذخیره می‌شود، یک خط‌مشی و اقدامات امنیتی پشتیبان، پیاده‌سازی شود.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان‌هایی که فعالیت‌های دورکاری را مجاز می‌سازند خط‌مشی‌ای تهیه کنند که شـرایط و محدودیت‌هایی برای استفاده از دورکاری را تعریف کند. درصورتی‌که این امر قابل انجام و ازنظر قانونی مجـاز به نظر می‌رسد، توصیه می‌شود که موارد زیر در نظر گرفته شود:

الف- امنیت فیزیکی فعلی محل دورکاری با در نظر گرفتن امنیت فیزیکی ساختمان و محیط محلی؛

ب- محیط فیزیکی پیشنهادی دورکاری؛

پ- الزامات امنیت ارتباطات با در نظر گرفتن نیاز به دسترسی از دور به سامانه‌های داخلی سازمان، حساسیت اطلاعاتی که در دسترس قرار خواهد گرفت و از پیونده‌های ارتباطی عبور می‌کند و حساسیت سامانه داخلی؛

ت- ایجاد دسترسی صفحه مجازی[2] که از پردازش و ذخیـره‌سـازی اطلاعـات بـر روی تجهیـزات بـا مالکیـت شخصی جلوگیری کند؛

ث- تهدید دسترسی غیرمجاز به اطلاعات یا منابع از سوی سایر اشخاص استفاده‌کننده از محل، مثلاً دوستان و خانواده؛

1- immature
2 - Virtual Desktop

ج- استفاده از شبکه‌های خانگی و الزامات یا محدودیت‌هایی در پیکربندی خدمات شبکه بی‌سیم؛

چ- خط‌مشی‌ها و روش‌های اجرایی برای جلوگیری از اختلافات در خصوص حقوق مالکیت معنوی که قبلاً بر روی تجهیزات تحت مالکیت شخصی ایجادشده است؛

ح- دسترسی به تجهیزات تحت مالکیت شخصی (برای تصدیق امنیت ماشین یا حین یک بررسی) که ممکن است ازنظر قانونی ممنوع باشد؛

خ- توافقنامه‌های مجوز دهی نرم‌افزاری که به‌گونه‌ای هستند که سازمان ممکن است مسئول صدور مجوز نرم‌افزارها یا ایستگاه‌های کاری کارخواه[1] باشد که تحت مالکیت شخصی آن با کارکنان، پیمانکاران یا کاربران بیرونی است؛

د- محافظت در برابر بدافزار و الزامات دیوار آتش.

توصیه می‌شود در راهنمایی‌ها و چینش‌ها[2] موارد زیر در نظر گرفته شوند:

الف- تأمین تجهیزات و وسایل ذخیره‌ی مناسب برای فعالیت‌های دورکاری، درجایی که استفاده از تجهیزات شخصی که تحت کنترل سازمان نیست مجاز نیست؛

ب- تعریفی از کار مجاز، ساعات کار، طبقه‌بندی اطلاعاتی که ممکن است در سامانه‌های داخلی نگهداری شود و سامانه‌ها و سرویس‌های داخلی که کاربر از دور مجاز به دسترسی به آن‌ها است؛

پ- تأمین تجهیزات ارتباطی مناسب، ازجمله روش‌هایی برای امن سازی دسترسی از دور؛

ت- امنیت فیزیکی؛

ث- قواعد و راهنمایی برای دسترسی خانواده و مراجعه‌کنندگان به تجهیزات و اطلاعات؛

ج- تأمین، پشتیبانی و نگهداری سخت‌افزار و نرم‌افزار؛

چ- تأمین بیمه؛

ح- رویه‌های اجرایی برای پشتیبان‌گیری و تداوم کسب‌وکار؛

خ- ممیزی و پایش امنیت؛

د- حذف اختیارات و حقوق دسترسی و بازگرداندن تجهیزات درزمانی که فعالیت‌های دورکاری خاتمه می‌یابند.

اطلاعات دیگر

دورکاری به همه‌ی شکل‌های کار خارج از سازمان ازجمله به محیط‌های کاری غیر سنتی مانند محیط‌های

1- client
2 - Arrangements

«ارتباط از دور»، «فضای کار قابل‌انعطاف[1]»، «کار از دور» و «کار مجازی» اشاره دارد.

۷ امنیت منابع انسانی

۷-۱ پیش از اشتغال[2]

قصد: حصول اطمینان از اینکه کارکنان و پیمانکاران، مسئولیت‌هایشان را درک کرده و برای نقش‌هایی که برای آن‌ها در نظر گرفته‌شده، مناسب هستند.

۷-۱-۱ گزینش

کنترل

توصیه می‌شود، بررسی‌های درستی‌سنجی سوابق تمامی داوطلبین اشتغال با توجه به قوانین، آئین‌نامه‌ها و اصول اخلاقی مرتبط انجام شود و با الزامات کسب‌وکار، طبقه‌بندی اطلاعاتی که در دسترس قرار می‌گیرد و مخاطرات درک شده، متناسب باشد.

راهنمای پیاده‌سازی

توصیه می‌شود که درستی‌سنجی با رعایت همه جنبه‌های حریم خصوصی، محافظت از اطلاعات شخصی قابل‌شناسایی و قوانین مرتبط با اشتغال انجام شود و توصیه می‌شود درصورتی‌که مجاز باشد، شامل موارد زیر باشد:

الف- در دسترس بودن معرف معتبر به‌عنوان‌مثال یک نفر با ارتباط کاری و یک نفر با ارتباط شخصی؛

ب- درستی سنجی (ازنظر کامل بودن و دقت) سوابق کاری فرد متقاضی؛

پ- تأیید صلاحیت‌های حرفه‌ای و دانشگاهی ادعاشده؛

ت- درستی سنجی مستقل هویت (گذرنامه یا سند مشابه)؛

ث- درستی‌سنجی‌های جزئی‌تر نظیر بازبینی‌های اعتبار یا بازبینی‌های سوابق کیفری.

زمانی که فردی برای یک نقش امنیت اطلاعاتی خاص به خدمت گرفته می‌شود توصیه می‌شود که سازمان اطمینان حاصل کند که داوطلب:

الف- شایستگی لازم جهت انجام نقش امنیتی را دارد؛

ب- برای بر عهده گرفتن نقش بتواند مورد اعتماد قرار گیرد، به‌ویژه اگر نقش برای سازمان حیاتی باشد.

توصیه می‌شود که سازمان، تصدیق‌هایی با جزئیات بیشتر درزمانی که یک شغل در زمان انتصاب اولیه یا در زمان ترفیع، شامل فردی می‌شود که به تسهیلات[1] پردازش اطلاعات دسترسی دارد، و به‌خصوص اگر این تسهیلات، اطلاعات حساس را اداره می‌کنند، مانند اطلاعات مالی یا اطلاعات خیلی محرمانه، در نظر بگیرد.

1- Flexible work Place
2- employment

توصیه می‌شود که رویه‌های اجرایی، معیارها و محدودیت‌هایی برای بررسی‌های درستی‌سنجی تعریف کنند، مثلاً این‌که چه کسی برای گزینش افراد، واجد شرایط است و چگونه، چه موقع و چرا بررسی‌های درستی سنجی انجام می‌شود.

توصیه می‌شود اطمینان حاصل شود که پیمانکاران هم از فرآیند گزینش استفاده کنند. در این موارد توصیه می‌شود، قرارداد بین سازمان و پیمانکار، مسئولیت‌ها برای برگزاری گزینش و روش‌های اجرایی اطلاع‌رسانی که در صورت کامل نشدن گزینش یا درصورتی‌که نتایج سبب شک و نگرانی شوند، لازم است از آن‌ها پیروی شود را مشخص کند.

توصیه می‌شود که اطلاعات درباره تمام داوطلب‌هایی که برای پست‌ها در سازمان در نظر گرفته می‌شوند، مطابق با هر یک از قوانین مناسب موجود در حوزه قضایی[2] مرتبط، جمع‌آوری‌شده و ساماندهی شود. توصیه می‌شود که برحسب قوانین مورد کاربرد، داوطلبین از قبل درباره فعالیت‌های گزینشی آگاه شوند.

۷-۱-۲ ضوابط و شرایط اشتغال

کنترل

توصیه می‌شود، توافق‌نامه‌های قراردادی با کارکنان و پیمانکاران، بیانگر مسئولیت‌های ایشان و سازمان در قبال امنیت اطلاعات باشد.

راهنمای پیاده‌سازی

توصیه می‌شود تعهدات قراردادی برای کارکنان و پیمانکاران علاوه بر روشن کردن و بیان موارد زیر، منعکس‌کننده خط‌مشی‌های سازمان برای امنیت اطلاعات باشد:

الف- توصیه می‌شود تمام کارکنان و پیمانکاران که به اطلاعات حساس دسترسی دارند، یک توافق‌نامه محرمانگی یا عدم افشا را قبل از دسترسی به تسهیلات پردازش اطلاعات، امضا کنند (به بند ۱۳-۲-۴ مراجعه شود)؛

ب- مسئولیت‌ها و حقوق قانونی کارکنان، پیمانکاران، برای مثال در موضوع قوانین حق نشر یا قوانین حفاظت از داده (به بندهای ۱۸-۱-۲ و ۱۸-۱-۴ مراجعه شود)؛

پ- مسئولیت‌ها برای طبقه‌بندی اطلاعات و مدیریت دارایی‌های سازمانی، دیگر دارایی‌های مرتبط با اطلاعات، تسهیلات پردازش اطلاعات و خدمات اطلاعاتی که توسط کارمند یا پیمانکار ساماندهی می‌شود (به بند ۸)؛

ت- مسئولیت‌های کارمند یا پیمانکار برای ساماندهی اطلاعات دریافتی از سایر شرکت‌ها یا طرف‌های بیرونی؛

1- Facilities
2- Jurisdication

ث- اقداماتی که در هنگام نادیده گرفتن الزامات امنیتی سازمان توسط کارکنان یا پیمانکاران انجام خواهند شد (به بند ۷-۲-۳ مراجعه شود).

توصیه می‌شود، نقش‌ها و مسئولیت‌های امنیتی داوطلب در طی فرآیند پیش از اشتغال به ایشان ابلاغ شود.

توصیه می‌شود که سازمان از موافقت کارکنان و پیمانکاران با ضوابط و شرایطی که در ارتباط با امنیت اطلاعات است و متناسب با ماهیت و گستره دسترسی آن‌ها به دارایی‌های سازمانی مرتبط با سامانه‌ها و خدمات اطلاعاتی تعیین‌شده است، اطمینان حاصل کند.

توصیه می‌شود که درصورتی‌که مناسب باشد مسئولیت‌های موجود در مفاد و شرایط اشتغال برای یک دوره مشخص پس از پایان اشتغال، ادامه یابند (به بند ۷-۳ مراجعه شود).

اطلاعات دیگر

می‌توان از یک روش کار برای بیان مسئولیت‌های امنیت اطلاعات کارمند، پیمانکار در رابطه با محرمانگی، حفاظت از داده، اخلاقیات، استفاده مناسب از تجهیزات و تسهیلات سازمان و نیز عملکردهای معتبر مورد انتظار سازمان استفاده کرد. ممکن است که به نمایندگی از فرد طرف قرارداد، طرف بیرونی که پیمانکار با آن در ارتباط است به چینش‌های قرارداد ورود کند.

۷-۲ در حین خدمت

قصد: حصول اطمینان از اینکه کارکنان و پیمانکاران از مسئولیت‌هایشان در مورد امنیت اطلاعات آگاه بوده و آن را انجام می‌دهند.

۷-۲-۱ مسئولیت‌های مدیریت

کنترل

توصیه می‌شود مدیریت، همه کارکنان و پیمانکاران را ملزم به به‌کارگیری امنیت اطلاعات با توجه به خط-مشی‌ها و روش‌های اجرایی استقراریافته سازمان کند.

راهنمای پیاده‌سازی

توصیه می‌شود که مسئولیت‌های مدیریت شامل حصول اطمینان از موارد زیر درباره کارکنان و پیمانکاران باشد:

الف- درباره نقش‌ها و مسئولیت‌های امنیت اطلاعات خود پیش از اعطای مجوز دسترسی به اطلاعات محرمانه یا سامانه‌های اطلاعاتی به‌صورت مناسب توجیه شده‌اند؛

ب- راهنمایی‌هایی که تبیین‌کننده‌ی انتظارات امنیتی از نقش آن‌ها در سازمان است، دریافت کرده‌اند؛

پ- برای رعایت خط‌مشی‌های امنیتی سازمان، انگیزه لازم را کسب کرده‌اند؛

ت- به سطحی از آگاهی درباره امنیت اطلاعات مرتبط با نقش‌ها و مسئولیت‌های خود در سازمان رسیده‌اند (به بند ۷-۲-۲ مراجعه شود)؛

ث- از ضوابط و شرایط اشتغال که شامل خط‌مشی امنیت اطلاعات سازمان و روش‌های مناسب کار است، پیروی کنند؛

ج- همچنان به کسب مهارت‌ها و صلاحیت مناسب ادامه می‌دهند و به‌صورت منظم آموزش می‌بینند؛

چ- یک کانال گزارش دهی مخفی در اختیار آن‌ها گذارده شده تا انحرافات از خط‌مشی یا روش اجرایی امنیت اطلاعات را گزارش دهند («دمیدن در سوت»).

توصیه می‌شود مدیریت، نشان‌دهنده پشتیبانی از خط‌مشی‌های امنیت اطلاعات، رویه‌ها و کنترل‌ها بوده و به‌عنوان یک الگو عمل کنند.

اطلاعات دیگر

اگر کارکنان و پیمانکاران از مسئولیت‌های امنیت اطلاعات خود مطلع نباشند، می‌توانند آسیب‌های جدی به سازمان وارد کنند. کارکنان باانگیزه، احتمالاً قابل‌اطمینان‌تر هستند و منشأ رخدادهای امنیت اطلاعات کمتری می‌شوند.

مدیریت ضعیف می‌تواند سبب شود کارکنان احساس کنند که کم‌اهمیت پنداشته می‌شوند که این امر منجر به تأثیرات منفی بر سازمان می‌شود. به‌عنوان‌مثال مدیریت ضعیف، ممکن است منجر به‌غفلت از امنیت اطلاعات شده یا منجر به سوءاستفاده بالقوه از دارایی‌ها شود.

۷-۲-۲ آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات

کنترل

توصیه می‌شود، تمامی کارکنان سازمان و در صورت لزوم پیمانکاران تا جایی که به کارکرد شغلی ایشان مرتبط است، در خصوص خط‌مشی‌ها و روش‌های اجرایی سازمان، تحصیل، آموزش و آگاهی و به‌روزرسانی منظم را دریافت کنند.

راهنمای پیاده‌سازی

توصیه می‌شود برنامهٔ آگاه‌سازی امنیت اطلاعات، به آگاه کردن کارکنان و درجایی که مرتبط است پیمانکاران، نسبت به مسئولیت‌های امنیت اطلاعات خود و ابزارهای اجرای آن مسئولیت یاری رساند.

توصیه می‌شود یک برنامهٔ آگاه‌سازی امنیت اطلاعات در راستای خط‌مشی‌های امنیت اطلاعات و روش‌های اجرایی مرتبط استقرار یابد که اطلاعاتی از سازمان که باید محافظت شوند و کنترل‌هایی که در این خصوص پیاده‌سازی می‌شوند را در نظر بگیرد. توصیه می‌شود برنامه آگاه‌سازی شامل تعدادی از فعالیت‌های افزایش آگاهی مانند کمپین[1]هایی (مثل روز امنیت اطلاعات) و انتشار کتابچه یا خبرنامه باشد.

1- Campaign

توصیه می‌شود برنامه آگاه‌سازی با در نظر گرفتن نقش کارکنان در سازمان و درجایی که کاربرد دارد، انتظارات سازمان از آگاهی پیمانکاران طرح‌ریزی شود. توصیه می‌شود برنامه آگاه‌سازی در طول زمان و ترجیحاً به‌صورت منظم، برنامه‌ریزی شود به‌نحوی‌که این فعالیت‌ها تکرار شده و کارکنان و پیمانکاران جدید را تحت پوشش قرار دهد. توصیه می‌شود برنامه آگاه‌سازی به‌گونه‌ای که با خط‌مشی‌ها و رویه‌های سازمان هم‌راستا باشد به‌طور منظم به‌روزرسانی شود و همچنین توصیه می‌شود بر اساس درس‌های آموخته‌شده از رخدادهای امنیت اطلاعات باشد.

توصیه می‌شود آموزش آگاه‌سازی در صورت نیاز توسط برنامه آگاه‌سازی امنیت اطلاعات سازمان اجرا شود. آموزش‌های آگاه‌سازی می‌تواند از رسانه‌های مختلفی مانند مبتنی بر کلاس، یادگیری از دور، مبتنی بر وب، خودآموز[1] یا غیره برای ارائه استفاده کند.

توصیه می‌شود تحصیل و آموزش امنیت اطلاعات، جنبه‌های عمومی ازجمله موارد زیر را لحاظ کند:

الف- بیانگر تعهد مدیریت به امنیت اطلاعات در کل سازمان باشد؛

ب- نیاز به آشنایی و انطباق با قواعد و تعهدات قابل کاربرد امنیت اطلاعات، همان‌طور که در خط‌مشی‌ها، استانداردها، قوانین، مقررات، قراردادها و توافق‌نامه‌ها تعریف‌شده است؛

پ - پاسخگویی فردی در خصوص کارهای انجام‌شده و انجام‌نشده خود و مسئولیت کلی آن‌ها نسبت به امن سازی یا محافظت اطلاعات متعلق به سازمان یا طرف‌های بیرونی؛

ت- رویه‌های امنیت اطلاعات‌پایه (مانند گزارش دهی رخداد امنیت اطلاعات) و کنترل‌های پایه مانند امنیت (کلیدواژه، کنترل بدافزار، میز پاک)؛

ث- نقاط تماس و منابع برای اطلاعات و توصیه‌های بیشتر در مورد موضوعات امنیت اطلاعات شامل مواد آموزشی بیشتر مرتبط با تحصیل و آموزش امنیت اطلاعات.

توصیه می‌شود تحصیل و آموزش امنیت اطلاعات به‌صورت دوره‌ای انجام شود. تحصیل و آموزش اولیه نه‌تنها برای کارکنان جدید بلکه برای کسانی که به سمت‌ها و نقش‌های جدید با الزامات امنیتی متفاوت منتقل می شوند کاربرد دارد و توصیه می‌شود که قبل از شروع فعالیت آن‌ها انجام شود.

توصیه می‌شود سازمان، برنامه تحصیل و آموزش را به‌منظور اجرای اثربخش آموزش‌ها و تحصیلات توسعه دهد. توصیه می‌شود که این برنامه در راستای خط‌مشی‌ها و روش‌های اجرایی مرتبط امنیت اطلاعات سازمان بوده و اطلاعاتی از سازمان که باید محافظت شوند و کنترل‌هایی که در این رابطه اجراشده‌اند تا از اطلاعات حفاظت کننده را در نظر بگیرد. توصیه می‌شود که این برنامه شکل‌های مختلف تحصیل و آموزش ازجمله سخنرانی و خودآموزی[2] را مدنظر قرار دهد.

1- Self-paced
2 - Self study

اطلاعات دیگر

توصیه می‌شود، در زمان شکل گرفتن برنامه آگاه‌سازی نه‌تنها تمرکز بر «چه چیزی» و «چگونگی» آگاه‌سازی مهم است، بلکه بر «چرایی» آن نیز تمرکز شود. مهم است که کارکنان، هدف از امنیت اطلاعات و تأثیر بالقوه، مثبت و منفی رفتار خود بر سازمان را درک کنند.

آگاه‌سازی، تحصیل و آموزش می‌تواند بخشی از یا همراه با دیگر فعالیت‌های آموزشی، به‌عنوان‌مثال آموزش-های عمومی فناوری اطلاعات یا آموزش عمومی امنیت باشند. توصیه می‌شود فعالیت‌های آگاه‌سازی، آموزش و تمرین مناسب بوده و مرتبط با نقش‌ها، مسئولیت‌ها و مهارت‌های فرد باشد.

به‌منظور آزمایش انتقال دانش، در پایان دوره‌ی آگاه‌سازی، تحصیل و آموزش، می‌توان ارزیابی از درک کارکنان انجام داد.

۷-۲-۳ فرآیند انضباطی

کنترل

توصیه می‌شود، یک فرآیند انضباطی رسمی و ابلاغ‌شده برای اقدام در مقابل کارکنانی که مرتکب یک نقض امنیت اطلاعاتی می‌شوند، وجود داشته باشد.

راهنمای پیاده‌سازی

توصیه می‌شود فرایند انضباطی بدون تصدیق اینکه نقض پیمان امنیتی صورت گرفته است، آغاز نشود (به بند ۱۶-۱-۷ مراجعه شود).

توصیه می‌شود فرایند انضباطی رسمی اطمینان دهد که با کارکنانی که مظنون به ارتکاب نقض پیمان امنیتی هستند، برخوردی صحیح و عادلانه انجام می‌شود. توصیه می‌شود فرایند انضباطی رسمی برای ارائه‌ی پاسخی متناسب با عواملی نظیر ماهیت و شدت نقض و تأثیر آن بر کسب‌وکار، اینکه این نقض برای اولین بار اتفاق می‌افتد یا تکراری است، اینکه نقض‌کننده به نحو مناسبی آموزش‌دیده بوده است یا خیر، قواعد مرتبط، قراردادهای کسب‌وکار و در صورت نیاز دیگر عوامل در نظر گرفته شود.

همچنین توصیه می‌شود که فرایند انضباطی به‌عنوان عامل بازدارنده کارکنان از نقض خط‌مشی‌ها و رویه‌های امنیت اطلاعات سازمانی و هر نقض پیمان امنیت اطلاعات دیگر، مورداستفاده قرار گیرد. افشا[1] ی عمدی ممکن است نیازمند اقدامات فوری باشد.

اطلاعات دیگر

اگر با توجه به امنیت اطلاعات برای رفتار قابل‌تقدیر، پاداش[1] تعریف شود، فرایند انضباطی همچنین می‌تواند به یک انگیزه دهنده یا مشوق تبدیل شود.

1- breach

۷-۳ خاتمه و تغییر اشتغال

قصد: حفاظت از منافع سازمان به‌عنوان بخشی از فرآیند تغییر یا خاتمه اشتغال.

۷-۳-۱ مسئولیت‌های خاتمه یا تغییر اشتغال

کنترل

توصیه می‌شود، مسئولیت‌ها و وظایف امنیت اطلاعات که بعد از خاتمه یا تغییر در شغل، معتبر باقی می‌مانند، تعریف‌شده و به کارکنان یا پیمانکاران، ابلاغ و اجبار شود.

راهنمای پیاده‌سازی

توصیه می‌شود ابلاغ مسئولیت‌های خاتمه خدمت دربرگیرنده‌ی الزامات امنیت اطلاعات جاری و مسئولیت‌های قانونی و در موارد متناسب، مسئولیت‌های موجود در هرگونه توافق‌نامه محرمانگی (به بند ۱۳-۲-۴ مراجعه شود) و مفاد و شرایط اشتغال (به بند ۷-۱-۲ مراجعه شود) که برای یک دوره تعیین‌شده پس از خاتمه اشتغال کارمندان یا پیمانکار ادامه خواهد داشت، باشد.

توصیه می‌شود مسئولیت‌ها و وظایفی که پس از خاتمه اشتغال همچنان معتبر هستند، در ضوابط و شرایط اشتغال کارکنان یا پیمانکاران (به بند ۷-۱-۲ مراجعه شود) گنجانده شوند.

توصیه می‌شود تغییرات مسئولیت یا اشتغال همانند خاتمه‌ی مسئولیت‌ها یا اشتغال جاری همراه با شروع یک مسئولیت جدید یا اشتغال، مدیریت شوند.

اطلاعات دیگر

بخش منابع انسانی عموماً مسئول کل فرایند خاتمه اشتغال است و با مدیر ناظر[2] شخصی که سازمان را ترک می‌کند، همکاری می‌کند تا جنبه‌های امنیت اطلاعات رویه‌های مرتبط را مدیریت کند. در مواردی که پیمانکار توسط یک‌طرف بیرونی برای سازمان آورده شده باشد، فرایند پایان خدمت توسط طرف بیرونی و بر اساس قرارداد بین سازمان و طرف بیرونی انجام خواهد شد.

ممکن است لازم باشد که کارکنان، مشتریان یا پیمانکاران از تغییرات در کارکنان و چینش‌های عملیاتی مطلع شوند.

۸ مدیریت دارایی

۸-۱ مسئولیت دارایی‌ها

قصد: شناسایی دارایی‌های سازمانی و تعریف مسئولیت‌های حفاظتی مناسب.

1- Positive sanction
2- supervising

۸-۱-۱ فهرست دارایی‌ها

کنترل

توصیه می‌شود دارایی‌های مرتبط با اطلاعات و تسهیلات پردازش اطلاعات شناسایی‌شده و فهرستی از این دارایی‌ها، تنظیم و نگهداری شود.

راهنمای پیاده‌سازی

توصیه می‌شود، سازمان دارایی‌های مرتبط با چرخه عمر اطلاعات را شناسایی و اهمیت آن را مستند کند. توصیه می‌شود، چرخه عمر اطلاعات شامل ایجاد، پردازش، ذخیره‌سازی، انتقال، حذف و تخریب باشد. توصیه می‌شود، در صورت نیاز مستندات در فهرست‌های دارایی موجود یا اختصاصی نگهداری شود.

توصیه می‌شود، فهرست موجودی دارایی، دقیق، به هنگام، سازگار و همسو با سایر فهرست‌های موجودی باشد.

توصیه می‌شود، برای هر یک از دارایی‌های شناسایی‌شده، مالک دارایی تعیین‌شده (به بند ۸-۱-۲ مراجعه شود) و طبقه‌بندی مشخص شود (به ۸-۲ مراجعه شود).

اطلاعات دیگر

فهرست دارایی‌ها کمک می‌کند تا این اطمینان ایجاد شود که از دارایی‌ها به نحو مؤثر محافظت می‌شود و همچنین ممکن است به دلیل دیگر اهداف مالی نظیر سلامت و ایمنی، دلایل بیمه‌ای یا مالی (مدیریت دارایی) لازم باشد.

ISO/IEC 27005 [۱۱] مثال‌هایی از دارایی‌هایی فراهم می‌کند که در زمان شناسایی دارایی‌های می‌تواند مدنظر قرار گیرد. فرایند تدوین فهرستی از دارایی‌ها، یک پیش‌نیاز مهم از مدیریت مخاطرات است (ISO/IEC 27000 و ISO/IEC 27005 [۱۱]).

۸-۱-۲ مالکیت دارایی‌ها

کنترل

توصیه می‌شود، دارایی‌های نگهداری شده در فهرست، دارای مالک باشد.

راهنمای پیاده‌سازی

افراد و موجودیت‌های دیگری که مسئولیت تأییدشده‌ی مدیریتی جهت چرخه عمر دارایی رادارند شایسته‌اند تا به‌عنوان صاحب آن دارایی قلمداد شوند.

معمولاً فرآیندی برای اطمینان از تخصیص به‌موقع مالکیت دارایی‌ها پیاده‌سازی می‌شود. توصیه می‌شود زمانی که دارایی‌ها ایجادشده و یا به سازمان منتقل می‌شوند مالکیت تخصیص یابد. توصیه می‌شود، مالک دارایی، مسئولیت مدیریت مناسب دارایی، در طول کل چرخه عمر دارایی را داشته باشد.

توصیه می‌شود که مالک دارایی مسئول موارد زیر باشد:

الف- اطمینان یابد که دارایی‌ها فهرست بندی شده‌اند؛

ب- تضمین کند که اطلاعات به‌طور مناسب طبقه‌بندی و محافظت‌شده‌اند؛

پ- محدودیت‌های دسترسی و طبقه‌بندی‌های دارایی‌های مهم را تعریف و به‌صورت دوره‌ای بازنگری کرده، خط‌مشی‌های کنترل دسترسی کاربردی را مدنظر قرار دهد؛

ث- اطمینان یابد در زمان حذف یا منهدم شدن دارایی، ساماندهی مناسب صورت گرفته است.

اطلاعات دیگر

مالک شناسایی‌شده می‌تواند فرد یا نهادی باشد که مسئولیت تأییدشده مدیریتی برای کنترل کل چرخه عمر یک دارایی را دارد. مالک شناسایی‌شده، لزوماً هرگونه حقوق مالکیت نسبت به دارایی ندارد.

وظایف روزمره می‌تواند مانند مراقبت روزانه از دارایی‌ها به یک متولی واگذار شود، ولی مسئولیت به عهده مالک دارایی باقی می‌ماند.

در سامانه‌های اطلاعاتی پیچیده، معین کردن گروه‌هایی از دارایی‌ها که با یکدیگر عمل می‌کنند تا یک خدمت مشخص را ارائه کنند، ممکن است مفید باشد. در این حالت، مالک خدمت برای ارائه سرویس که شامل عملکرد آن دارایی‌ها است پاسخگو است.

۸-۱-۳ استفاده قابل‌قبول[1] از دارایی‌ها

کنترل

توصیه می‌شود، قواعدی برای استفاده قابل‌قبول از اطلاعات و دارایی‌های مرتبط با اطلاعات و تسهیلات پردازش اطلاعات، شناسایی، مستند و پیاده‌سازی شود.

راهنمای پیاده‌سازی

توصیه می‌شود که کارکنان و کاربران طرف‌های بیرونی که از دارایی‌های سازمان استفاده می‌کنند یا به آن دسترسی دارند، از الزامات امنیت اطلاعات دارایی‌های سازمان که مرتبط با اطلاعات، منابع و تسهیلات پردازش اطلاعات هستند آگاه باشند. توصیه می‌شود که این اشخاص برای استفاده خود از منابع پردازش اطلاعات و هرگونه استفاده با مسئولیت آن‌ها، مسئول باشند.

۸-۱-۴ بازگرداندن دارایی‌ها

کنترل

توصیه می‌شود، تمامی کارکنان و کاربران طرف بیرونی، تمامی دارایی‌های سازمان را که در اختیارشان است، به‌محض خاتمه اشتغال، قرارداد یا توافقنامه‌شان، به سازمان بازگردانند.

1- acceptable

راهنمای پیاده‌سازی

توصیه می‌شود، فرایند خاتمه رسمی شود تا بازگرداندن تمام دارایی‌های فیزیکی و الکترونیکی در اختیار گذاشته‌شده قبلی که سازمان مالک یا عهده‌دار آن‌ها است را پوشش دهد.

در مواردی که کارمندی یا کاربر طرف‌های بیرونی، تجهیزات سازمان را خریداری کرده یا از تجهیزات شخصی خود استفاده کند، توصیه می‌شود، روش‌های اجرایی دنبال شود تا اطمینان حاصل شود که تمام اطلاعات مرتبط به سازمان منتقل‌شده و به‌طور امن از تجهیزات پاک‌شده است (به ۱۱-۲-۷ مراجعه شود).

در مواردی که کارمندی یا کاربر طرف بیرونی، دانشی دارد که برای انجام عملیات جاری مهم است، توصیه می‌شود آن اطلاعات، مستند شده و به سازمان منتقل شود.

در طول دوره اعلان خاتمه، توصیه می‌شود، سازمان ایجاد رونوشت غیرمجاز از اطلاعات مرتبط را (به‌عنوان‌مثال مالکیت معنوی) توسط کارکنان و پیمانکارانی که کار آن‌ها خاتمه یافته است، کنترل کند.

۸-۲ طبقه‌بندی اطلاعات

قصد: حصول اطمینان از اینکه اطلاعات، با توجه به اهمیتشان برای سازمان از سطح حفاظت مناسبی برخوردارند.

۸-۲-۱ طبقه‌بندی اطلاعات

کنترل

توصیه می‌شود، اطلاعات با توجه به الزامات قانونی، ارزش، بحرانی بودن و حساسیت در برابر افشای غیرمجاز یا تغییرات غیرمجاز، طبقه‌بندی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود، در طبقه‌بندی و کنترل‌های محافظتی مرتبط با اطلاعات، نیازهای کسب‌وکار برای به اشتراک‌گذاری و یا محدود کردن اطلاعات و همچنین الزامات قانونی مدنظر قرار گیرد. دارایی‌هایی به‌جز اطلاعات می‌تواند مطابق با طبقه‌بندی اطلاعاتی که در آن‌ها ذخیره‌شده، به‌وسیله آن‌ها پردازش می‌شود یا توسط آن‌ها مدیریت یا محافظت می‌شود طبقه‌بندی شود.

توصیه می‌شود مالکین دارایی‌های اطلاعاتی پاسخگوی طبقه‌بندی آن‌ها باشند.

توصیه می‌شود، طرح طبقه‌بندی شامل قواعدی برای طبقه‌بندی و معیارهایی جهت بازنگری طبقه‌بندی در طول زمان باشد. توصیه می‌شود، سطح حفاظت در طرح، توسط تحلیل محرمانگی، یکپارچگی و دسترس-پذیری و هرگونه الزامی که برای اطلاعات در نظر گرفته می‌شود ارزیابی می‌شود. توصیه می‌شود طرح با خط-مشی کنترل دسترسی هم‌راستا باشد (به بند ۹-۱-۱ مراجعه شود).

توصیه می‌شود به هر سطح، یک نام نسبت داده شود که در چارچوب به‌کارگیری طرح طبقه‌بندی، معقول باشد.

توصیه می‌شود، طرح در کل سازمان سازگار باشد به‌گونه‌ای که هر فرد، اطلاعات و دارایی‌های مرتبط با آن را به شیوه یکسان طبقه‌بندی کرده، یک درک مشترک از الزامات حفاظت داشته باشد و حفاظت مناسب را اعمال کند.

توصیه می‌شود، طبقه‌بندی اطلاعات در فرآیندهای سازمان لحاظ شده و سازگار و منسجم در سازمان باشد. توصیه می‌شود، نتایج طبقه‌بندی نشان‌دهنده ارزش دارایی متناسب با حساسیت و بحرانی بودن آن‌ها برای سازمان باشد، به‌عنوان‌مثال، ازلحاظ محرمانگی، یکپارچگی و دسترس‌پذیری مدنظر قرار بگیرد. توصیه می شود، نتایج طبقه‌بندی مطابق با تغییر ارزش آن‌ها، حساسیت و بحرانی بودن آن‌ها در طی چرخه حیات به‌روز شود.

اطلاعات دیگر

طبقه‌بندی برای افرادی که با اطلاعات سروکار دارند، نشانه مختصری از چگونگی ساماندهی و محافظت از آن فراهم می‌کند. ایجاد گروه‌هایی از اطلاعات با نیازهای حفاظتی مشابه و تعیین روش‌های اجرایی امنیت اطلاعات که به تمام اطلاعات در هر گروه اعمال می‌شود، این کار را تسهیل می‌کند. این رویکرد نیاز به ارزیابی مخاطرات مورد به مورد و طراحی سفارشی‌شده کنترل‌ها را کاهش می‌دهد.

اطلاعات می‌تواند پس از یک دوره زمانی معین، دیگر حساس و حیاتی نباشند، مثلاً هنگامی‌که اطلاعات در معرض دید عموم قرار داده می‌شود. توصیه می‌شود که این جنبه‌ها به‌حساب آورده شوند، چون طبقه‌بندی بیش‌ازحد، ممکن است منجر به پیاده‌سازی کنترل‌های غیرضروری و هزینه‌های اضافی و بالعکس طبقه‌بندی کمتر از میزان موردنیاز، منجر به به‌خطر افتادن دستیابی به اهداف کسب‌وکار شود.

مثالی از یک طرح طبقه‌بندی محرمانگی اطلاعات می‌تواند بر اساس چهار سطح به شرح زیر باشد:

الف- افشا باعث هیچ صدمه‌ای نمی‌شود؛

ب- افشا باعث آبروریزی[1] جزئی یا نامناسب بودن عملیاتی جزئی می‌شود؛

پ- افشا تأثیر کوتاه‌مدت قابل‌توجهی در عملیات و یا اهداف تاکتیکی دارد؛

ت- افشا تأثیری جدی بر اهداف راهبردی بلندمدت داشته یا بقای سازمان را در معرض مخاطره قرار می‌دهد.

۸-۲-۲ علامت‌گذاری اطلاعات

کنترل

توصیه می‌شود، برای علامت‌گذاری اطلاعات، مجموعهٔ مناسبی از روش‌های اجرایی با توجه به طرح طبقه-بندی مصوب سازمان، ایجاد و مستقر شود.

راهنمای پیاده‌سازی

1- Embarrassment

نیاز است، روش‌های اجرایی برچسب‌زنی اطلاعات و دارایی‌های مرتبط با آن‌ها در قالب‌های فیزیکی و الکترونیکی پوشش دهند. توصیه می‌شود که برچسب‌زنی، انعکاس‌دهنده طرح طبقه‌بندی بیان‌شده دربند ۸-۲-۱ باشد. توصیه می‌شود برچسب‌ها به‌راحتی قابل‌تشخیص باشد. توصیه می‌شود، روش‌های اجرایی، راهنمایی‌هایی در ارتباط با مکان و چگونگی برچسب‌گذاری با در نظر گرفتن نحوه در دسترس قرار گرفتن اطلاعات و اداره شدن تجهیزات با توجه به نوع رسانه ارائه کند. روش‌های اجرایی می‌تواند مواردی که در آن‌ها برچسب‌گذاری را می‌توان حذف کرد، تعریف کند، به‌عنوان‌مثال برچسب‌گذاری برای اطلاعات غیر محرمانه برای کاهش حجم کار. توصیه می‌شود، کارکنان و پیمانکاران از روش‌های اجرایی برچسب‌گذاری آگاه باشند.

توصیه می‌شود که خروجی سامانه‌هایی که حاوی اطلاعاتی است که حساس یا حیاتی قلمداد می‌شوند، دارای یک برچسب مناسب طبقه‌بندی باشند.

اطلاعات دیگر

برچسب زدن اطلاعات طبقه‌بندی‌شده، یک الزام کلیدی برای هماهنگی‌های اشتراک اطلاعات است. برچسب‌های فیزیکی و فراداده[1] انواع متداولی از برچسب‌زنی هستند.

گاهی اوقات، برچسب‌زنی اطلاعات و دارایی‌های مرتبط با آن می‌تواند اثرات منفی داشته باشد. دارایی‌های طبقه‌بندی‌شده برای شناسایی و سرقت توسط مهاجمان خارجی یا داخلی مناسب‌تر هستند.

۸-۲-۳ اداره کردن دارایی‌ها

کنترل

توصیه می‌شود، روش‌های اجرایی برای ساماندهی دارایی‌ها با توجه به طرح طبقه‌بندی اطلاعات مصوب سازمان، ایجاد و پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود روش‌های اجرایی برای ساماندهی، پردازش، ذخیره و مخابره اطلاعات سازگار با طبقه‌بندی آن‌ها در نظر گرفته شود (به بند ۸-۲-۱ مراجعه شود). توصیه می‌شود موارد زیر موردتوجه قرار گیرد:

الف- محدودیت‌های دسترسی برای حمایت از الزامات حفاظت برای هر سطح از طبقه‌بندی؛

ب- نگهداری از سوابق رسمی از دریافت‌کنندگان مجاز دارایی؛

پ- حفاظت از رونوشت‌های موقت یا دائم از اطلاعات با یک سطح سازگار با حفاظت از اطلاعات اصلی؛

ت- ذخیره‌سازی دارایی‌های فناوری اطلاعات مطابق با مشخصات تولیدکنندگان؛

1- Meta data

ث- علامت‌گذاری واضح تمام رونوشت‌های رسانه برای جلب‌توجه گیرنده مجاز.

طرح طبقه‌بندی مورداستفاده در سازمان ممکن است معادل با طرح‌های استفاده‌شده توسط سازمان‌های دیگر نباشد، حتی اگر نام سطوح مشابه باشند؛ علاوه بر این، اطلاعات در حال مبادله شده بین سازمان‌ها می‌تواند بسته به زمینه آن سازمان در طبقه‌بندی متفاوت باشد، حتی اگر طرح‌های طبقه‌بندی یکسان باشند.

توصیه می‌شود در توافق‌نامه‌ها با سازمان‌های دیگر که شامل اشتراک‌گذاری اطلاعات هستند، دربرگیرنده روش اجرایی برای شناسایی، طبقه‌بندی آن اطلاعات و تفسیر برچسب طبقه‌بندی از دیگر سازمان‌ها باشد.

۸-۳ ساماندهی رسانه‌ها

قصد: پیشگیری از افشاء، دست‌کاری، حذف یا تخریب غیرمجاز اطلاعات ذخیره‌شده در رسانه.

۸-۳-۱ مدیریت رسانه‌های قابل جابه‌جایی[1]

کنترل

توصیه می‌شود، برای مدیریت رسانه‌های قابل جابه‌جایی با توجه به طرح طبقه‌بندی اتخاذشده توسط سازمان، روش‌های اجرایی پیاده‌سازی شود.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر برای مدیریت رسانه‌های قابل جابه‌جایی در نظر گرفته شود:

الف- توصیه می‌شود محتوای هر یک از رسانه‌های چند بار مصرف که موردنیاز نیستند و باید از سازمان دور ریخته شوند به‌گونه‌ای پاک شوند که قابل بازیابی نباشد؛

ب- هر زمان که لازم و امکان‌پذیر باشد، توصیه می‌شود جابه‌جایی رسانه‌ها از سازمان و محیط‌های ذخیره اطلاعات با اخذ مجوز انجام پذیرد و یک نسخه از آن مجوز به‌منظور انجام حسابرسی حفظ شود؛

پ- توصیه می‌شود تمام رسانه‌ها و محیط‌های ذخیره اطلاعات در یک محیط ایمن و امن مطابق با مشخصات تولیدکننده ذخیره‌سازی شوند؛

ت- توصیه می‌شود درصورتی‌که محرمانگی یا یکپارچگی داده‌ها حائز اهمیت هستند از فنون رمزنگاری برای حفاظت از داده‌های ذخیره‌شده در رسانه‌های قابل جابه‌جایی استفاده شود؛

ث- توصیه می‌شود جهت کاهش مخاطرات پایین آمدن کیفیت رسانه، درزمانی که اطلاعات ذخیره‌سازی شده هنوز نیاز است، داده‌ها به رسانه جدید منتقل شود، قبل از اینکه اطلاعات غیرقابل‌خواندن شوند؛

ج- توصیه می‌شود نسخه‌های متعدد از داده‌های باارزش در رسانه‌های جداگانه ذخیره شود تا مخاطرات ناشی از آسیب یا از دست رفتن داده به‌صورت تصادفی کاهش یابد؛

1- removable

چ- توصیه می‌شود ثبت رسانه‌های قابل جابه‌جایی مدنظر قرار گیرد تا فرصت‌های از دست دادن داده را محدود کند؛

ح- توصیه می‌شود رانه[1] های مربوط به رسانه‌های قابل جابه‌جایی فقط زمانی فعال باشند که توجیهی در کسب‌وکار برای آن وجود داشته باشد؛

خ- درجایی که نیاز به استفاده از رسانه‌های قابل جابه‌جایی برای انتقال اطلاعات است، توصیه می‌شود چنین رسانه‌ای پایش شود.

توصیه می‌شود روش‌های اجرایی و سطوح اختیارت، مستند شود.

۸-۳-۲ امحای رسانه‌ها

کنترل

توصیه می‌شود، رسانه‌هایی که دیگر موردنیاز نیستند، با به‌کارگیری روش‌های اجرایی رسمی، به صورتی امن، امحاء شوند.

راهنمای پیاده‌سازی

توصیه می‌شود با به‌کارگیری روش‌های اجرایی رسمی برای امحاء امن رسانه‌ها، مخاطرات نشت اطلاعات محرمانه به افراد غیرمجاز کاهش داده شود. توصیه می‌شود روش‌های اجرایی برای امحاء امن رسانه‌هایی که حاوی اطلاعات محرمانه هستند با میزان حساسیت این اطلاعات همخوانی داشته باشد. توصیه می‌شود موارد زیر در نظر گرفته شود:

الف- توصیه می‌شود رسانه‌هایی که حاوی اطلاعات حساس هستند، به‌گونه‌ای امن نگهداری و یا امحاء شوند؛ برای مثال به‌وسیله سوزاندن یا تکه‌تکه کردن، یا پاک کردن داده‌ها برای استفاده توسط برنامه کاربردی دیگری در داخل سازمان؛

ب- توصیه می‌شود روش‌های اجرایی برای شناسایی مواردی که ممکن است به دورریز امن نیاز داشته باشند در نظر گرفته شود؛

پ- ممکن است برنامه‌ریزی برای تمام اقلام رسانه‌هایی که باید به‌طور امن جمع‌آوری و امحاء شوند از تلاش برای جدا کردن اقلام حساس راحت‌تر باشد؛

ت- بسیاری از سازمان‌ها، خدمات جمع‌آوری و امحاء رسانه‌های کاغذی خود را به پیمانکاران خارج از سازمان ارائه می‌کنند؛ توصیه می‌شود در انتخاب پیمانکار مناسب و باتجربه کافی، دقت لازم به عمل آید؛

1 - drives

ث- توصیه می‌شود، امحاء موارد حساس برای حسابرسی ثبت شود. در زمان انباشته کردن رسانه‌ها برای امحاء، توصیه می‌شود ملاحظات کافی در مورد تأثیر تجمیعی آن به عمل آید تا حجم زیاد اطلاعات غیر حساس به اطلاعات حساس تبدیل نشوند.

اطلاعات دیگر

افزاره‌های آسیب‌دیده که حاوی داده‌های حساس هستند ممکن است نیاز به ارزیابی مخاطرات داشته باشند تا مواردی که توصیه می‌شود به‌طور فیزیکی امحاء شوند، به‌جای اینکه برای تعمیر فرستاده‌شده یا دور ریخته شوند، شناسایی شوند (به بند ۱۱-۲-۷ مراجعه شود).

۸-۳-۳ انتقال فیزیکی رسانه‌ها

کنترل

توصیه می‌شود، رسانه‌های حاوی اطلاعات در هنگام انتقال در برابر دسترسی غیرمجاز، استفادهٔ نابجا یا صدمه، محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رهنمودهای زیر برای محافظت از رسانه‌هایی که حاوی اطلاعاتی هستند که می‌خواهند منتقل شوند رعایت شود:

الف- توصیه می‌شود از حمل‌ونقل مطمئن یا پیک استفاده شود؛

ب- توصیه می‌شود فهرستی از پیک‌های مجاز با توافق مدیریت تهیه شود؛

پ- توصیه می‌شود روش‌های اجرایی برای تائید هویت پیک‌ها تدوین شود؛

ت- توصیه می‌شود از بسته‌بندی مناسب برای محافظت از محتویات بسته‌ها در برابر هرگونه آسیب فیزیکی احتمالی در طول انتقال و مطابق با تمام مشخصات تولیدکننده استفاده شود، مثلاً محافظت در برابر هر عامل محیطی که ممکن است منجر به کاهش اثربخشی بازیابی رسانه‌ها شود، نظیر قرار گرفتن در معرض گرما، رطوبت یا میدان‌های الکترومغناطیسی؛

ث- توصیه می‌شود، ثبت وقایع شناسایی محتوای رسانه، محافظت صورت گرفته برای آن و همچنین ثبت زمان‌های انتقال بین افراد گیرنده و دریافت‌کننده در مقصد نگهداری شود.

اطلاعات دیگر

اطلاعات ممکن است در برابر دسترسی غیرمجاز، سوءاستفاده، یا اختلال در طول انتقال فیزیکی مثلاً در زمان ارسال رسانه‌ها از طریق خدمات پست یا پیک، آسیب‌پذیر باشد. در این کنترل، رسانه شامل مستندات کاغذی است.

هنگامی‌که اطلاعات محرمانه در رسانه، رمزگذاری نشده است، توصیه می‌شود، حفاظت فیزیکی بیشتری برای رسانه‌ها در نظر گرفته شود.

۹ کنترل دسترسی

۹-۱ الزامات کسب‌وکار کنترل دسترسی

قصد: محدودسازی دسترسی به اطلاعات و تسهیلات پردازش اطلاعات.

۹-۱-۱ خط‌مشی کنترل دسترسی

کنترل

توصیه می‌شود، یک خط‌مشی کنترل دسترسی بر مبنای الزامات کسب‌وکار و الزامات امنیت اطلاعات ایجاد، مستند و بازنگری شود.

راهنمای پیاده‌سازی

توصیه می‌شود، مالکان دارایی از طریق درجه‌ای از جزئیات و سخت‌گیری کنترل‌هایی که منعکس‌کننده مخاطرات امنیت اطلاعات باشد، قواعد کنترل دسترسی، حقوق دسترسی و محدودیت‌های مناسب را برای نقش‌های کاربری خاص در مورد دارایی‌های خود تعیین کنند.

کنترل‌های دسترسی، هم منطقی و هم فیزیکی هستند (به بند ۱۱ مراجعه شود) و توصیه می‌شود این‌ها باهم در نظر گرفته شوند. توصیه می‌شود کاربران و ارائه‌کنندگان خدمات، عبارت روشنی از الزامات کسب‌وکار که قراراست توسط کنترل دسترسی محقق گردد دریافت کنند.

توصیه می‌شود در این خط‌مشی موارد زیر لحاظ شود:

الف- الزامات امنیتی برنامه‌های کاربردی کسب‌وکاری؛

ب- خط‌مشی‌هایی برای انتشار[1] و مجوز دهی اطلاعات مانند اصل نیاز- به -دانستن و سطوح امنیت اطلاعات و طبقه‌بندی اطلاعات (به بند ۸-۲ مراجعه شود)؛

پ- سازگاری بین حقوق دسترسی و خط‌مشی‌های طبقه‌بندی اطلاعات سامانه‌ها و شبکه‌های مختلف؛

ت- قوانین مرتبط و هر یک از تعهدات قراردادی درباره محدود کردن دسترسی به داده‌ها یا خدمات (به بند ۱۸-۱ مراجعه شود)؛

ث- مدیریت حقوق دسترسی در یک محیط توزیع‌شده و شبکه‌ای که تمام انواع اتصالات موجود را شناسایی می‌کند؛

ج- تفکیک نقش‌های کنترل دسترسی مانند تقاضای دسترسی، مجوز دهی دسترسی، سرپرستی دسترسی؛

چ- الزامات مجوز دهی رسمی تقاضاهای دسترسی (به بندهای ۹-۲-۱ و ۹-۲-۲ مراجعه شود)؛

ح- الزامات بررسی دوره‌ای حقوق دسترسی (به بند ۹-۲-۵ مراجعه شود)؛

1- dissemination

خ- حذف حقوق دسترسی (به بند ۹-۲-۶ مراجعه شود)؛

د- بایگانی سوابق همه رویدادهای مهم مرتبط با در نظر گرفتن به‌کارگیری و مدیریت شناسه کاربران و اطلاعات محرمانه اصالت‌سنجی؛

ذ- نقش‌ها با دسترسی ویژه (به بند ۹-۲-۳ مراجعه شود).

اطلاعات دیگر

درزمانی که قواعد کنترل دسترسی تعریف می‌شوند، توصیه می‌شود موارد زیر دقیقاً در نظر گرفته شود:

الف- ایجاد قواعد بر اساس این قاعده که «هر چیزی به‌طورکلی ممنوع است مگر این‌که صریحاً اجازه داده شود» به‌جای این قاعده ضعیف‌تر که «هر چیزی عموماً مجاز است مگر این‌که صریحاً ممنوع شود»؛

ب- تغییرات در برچسب‌های اطلاعات (به بند ۸-۲-۲ مراجعه شود) که به‌طور خودکار توسط تجهیزات پردازش اطلاعات ایجاد می‌شوند و آن‌هایی که به صلاحدید کاربر ایجاد می‌شوند؛

پ- تغییرات مجوزهای کاربر که به‌طور خودکار توسط سامانه اطلاعاتی ایجاد می‌شود و آن‌هایی که به‌وسیله سرپرست سامانه ایجاد می‌شود؛

ت- قواعدی که نیازمند تأیید خاص قبل از اعمال هستند و قواعدی که نیازمند تأیید خاص قبل از اعمال نیستند؛

توصیه می‌شود قواعد کنترل دسترسی توسط روش‌های اجرایی رسمی (به بندهای ۹-۲، ۹-۳، ۹-۴ مراجعه شود) و مسئولیت‌های تعیین‌شده، پشتیبانی شوند (۶-۱-۱، ۹-۳).

کنترل دسترسی بر اساس نقش[1]، رویکردی است که به‌صورت موفق توسط سازمان‌های زیادی جهت مرتبط کردن حقوق دسترسی و نقش‌های کسب‌وکاری به کار گرفته‌شده است.

دو اصل رایجی که خط‌مشی‌های کنترل دسترسی را جهت‌دهی می‌کنند موارد زیر هستند:

الف- نیاز- به -دانستن[2]: به افراد، فقط دسترسی به اطلاعاتی داده می‌شود که برای انجام وظایفشان به آن نیاز دارند (وظایف/نقش‌های متفاوت به معنی نیاز-به-دانستن‌های متفاوت و درنتیجه رخ‌نماهای[3] دسترسی متفاوت است)

ب- نیاز –به- استفاده[1]: به افراد، فقط دسترسی به تسهیلات پردازش اطلاعاتی (تجهیز فناوری اطلاعات، برنامه‌های کاربردی، روش‌های اجرایی، اتاق‌ها) داده می‌شود که برای انجام وظایف/ کار/ نقش به آن نیاز دارند.

1 - Role based
2- Need-to-know
3 - profiles

۹-۱-۲ دسترسی به شبکه و خدمات شبکه

کنترل

توصیه می‌شود، کاربران تنها به شبکه و خدمات شبکه که مشخصاً استفاده از آن‌ها برایشان مجاز شده، دسترسی داشته باشند.

راهنمای پیاده‌سازی

توصیه می‌شود یک خط‌مشی درباره استفاده از شبکه‌ها و خدمات شبکه‌ای تدوین شود. توصیه می‌شود این خط‌مشی دربرگیرنده موارد زیر باشد:

الف- شبکه‌ها و خدمات شبکه‌ای که دسترسی به آن‌ها مجاز است؛

ب- روش‌های اجرایی مجوز دهی برای تعیین این‌که چه کسی مجاز است به کدام شبکه‌ها و خدمات شبکه-ای دسترسی پیدا کند؛

پ- کنترل‌ها و روش‌های اجرایی مدیریتی برای محافظت از دسترسی به اتصالات شبکه و خدمات شبکه؛

ت- ابزارهای به‌کاررفته برای دسترسی به شبکه‌ها و خدمات شبکه‌ای (برای مثال، استفاده از شبکه خصوصی مجازی یا شبکه بی‌سیم)؛

ث- الزامات اصالت‌سنجی کاربر برای دسترسی به خدمات شبکه‌های مختلف؛

ج- پایش استفاده از خدمات شبکه.

توصیه می‌شود خط‌مشی استفاده از خدمات شبکه‌ای با خط‌مشی کنترل دسترسی سازمان سازگار باشد (به بند ۹-۱-۱ مراجعه شود).

اطلاعات دیگر

اتصالات غیرمجاز و ناامن به خدمات شبکه می‌تواند بر کل سازمان تأثیر بگذارد. این کنترل به‌خصوص برای اتصالات شبکه‌ها به نرم‌افزارهای کاربردی کسب‌وکار حساس و حیاتی یا برای کاربران در مکان‌هایی با مخاطرات بالا مانند نواحی عمومی یا بیرونی که خارج از کنترل و مدیریت امنیت اطلاعات سازمان است، اهمیت ویژه‌ای دارد.

۹-۲ مدیریت دسترسی کاربر

قصد: حصول اطمینان از دسترسی کاربر مجاز و پیشگیری از دسترسی غیرمجاز به سامانه‌ها و خدمات.

۹-۲-۱ ثبت و حذف[2] کاربر

کنترل

1- Need-to-use
2- De-registration

توصیه می‌شود، جهت فراهم کردن امکان تخصیص حقوق دسترسی‌ها، یک فرآیند رسمی ثبت و حذف کاربر پیاده‌سازی شود.

راهنمای پیاده‌سازی

توصیه می‌شود روش‌های اجرایی کنترل دسترسی برای مدیریت شناسه کاربران شامل موارد زیر باشد:

الف- استفاده از شناسه‌های منحصربه‌فرد کاربر برای ایجاد امکان ارتباط دادن کاربران به فعالیت‌هایشان و پذیرش مسئولیت فعالیت‌هایشان؛ توصیه می‌شود استفاده از شناسه‌های مشترک فقط در صورتی مجاز شود که به دلایل کاری یا عملیاتی لازم باشد و توصیه می‌شود که تأیید و مستند شوند؛

ب- غیرفعال کردن یا حذف فوری شناسه کاربرانی که سازمان را ترک کرده‌اند (به بند ۹-۲-۶ مراجعه شود)؛

پ- شناسایی و حذف یا غیرفعال کردن دوره‌ای شناسه‌های تکراری کاربران؛

ت- اطمینان از اینکه شناسه تکراری کاربر برای کاربر دیگری صادر نشود.

اطلاعات دیگر

اعطا یا لغو دسترسی به اطلاعات و تجهیزات پردازش اطلاعات معمولاً در یک‌رویه دومرحله‌ای انجام می‌شود:

الف- انتساب و فعال‌سازی یا لغو شناسه کاربر؛

ب- فراهم کردن یا لغو کردن حق دسترسی به چنین شناسه کاربری (به بند ۹-۲-۲ مراجعه شود).

۹-۲-۲ تأمین دسترسی کاربر

کنترل

توصیه می‌شود، برای انتساب یا لغو حقوق دسترسی برای تمام انواع کاربران به همه سامانه‌ها و خدمات، یک فرآیند رسمی تأمین دسترسی کاربر پیاده‌سازی شود.

راهنمای پیاده‌سازی

توصیه می‌شود فرایند تأمین برای تخصیص یا لغو حقوق دسترسی به شناسه‌های کاربری شامل موارد زیر باشد:

الف- اخذ مجوز از مالک سامانه اطلاعاتی یا خدمت برای استفاده از سامانه اطلاعات یا خدمت (به کنترل بند ۸-۱-۲ مراجعه شود). تأیید جداگانه برای حقوق دسترسی از مدیریت نیز ممکن است مناسب باشد؛

ب- تأیید اینکه سطح دسترسی اعطاء شده متناسب با خط‌مشی دسترسی است (به بند ۹-۱ مراجعه شود) و با الزامات دیگر مانند جداسازی وظایف، سازگار است (به بند ۶-۱-۲ مراجعه شود)؛

پ- حصول اطمینان از اینکه حقوق دسترسی (به‌عنوان‌مثال توسط تأمین‌کنندگان خدمات) قبل از تکمیل روال مجوز دهی فعال نشود؛

ت- نگهداری سوابق متمرکز حقوق دسترسی داده‌شده به شناسه کاربری برای دسترسی به سامانه‌های اطلاعاتی و خدمات؛

ث- تطبیق حقوق دسترسی کاربرانی که نقش و یا شغل خود را تغییر داده‌اند و از بین بردن و یا مسدود کردن فوری حقوق دسترسی کاربرانی که سازمان را ترک کرده‌اند؛

ج- بازنگری دوره‌ای حقوق دسترسی با کمک مالکان سامانه‌های اطلاعاتی و یا خدمات (به بند ۹-۲-۵ مراجعه شود)؛

اطلاعات دیگر

توصیه می‌شود ایجاد نقش‌های دسترسی کاربری بر اساس الزامات کسب‌وکار که چندین حق دسترسی را در یک رخ‌نمای[1] دسترسی کاربری ویژه خلاصه می‌کنند در نظر گرفته شود. درخواست‌های دسترسی و بازبینی-ها (به بند ۹-۲-۴ مراجعه شود) در سطح چنین نقش‌هایی نسبت به سطح حقوق ویژه، راحت‌تر مدیریت می‌شود.

توصیه می‌شود در قراردادهای کارکنان و قراردادهای خدمات، بندهایی برای مشخص کردن مجازات تلاش-های دسترسی غیرمجاز توسط افراد و پیمانکاران در نظر گرفته شود (به بندهای ۷-۱-۲، ۷-۲-۳،۱۳-۲-۴، ۱۵-۱-۲ مراجعه شود).

۹-۲-۳ مدیریت حقوق ویژه[2] دسترسی

کنترل

توصیه می‌شود، تخصیص و به‌کارگیری حقوق ویژه دسترسی، محدود و کنترل شود.

راهنمای پیاده‌سازی

توصیه می‌شود تخصیص حقوق ویژه دسترسی، طی یک فرآیند رسمی مجوز دهی، هم‌راستا با خط‌مشی کنترل دسترسی مرتبط (به بند ۹-۱-۱ مراجعه شود)، کنترل شود. توصیه می‌شود مراحل زیر در نظر گرفته شود:

الف- توصیه می‌شود حقوق دسترسی ویژه در رابطه با هر یک از سامانه‌ها یا فرآیندها، مانند سیستم‌عامل، سامانه مدیریت بانک داده و هر یک از برنامه‌های کاربردی و کاربرانی که سامانه‌ها و فرآیندها باید به آن‌ها اختصاص داده شود، شناسایی شوند.

1- profile
2 - Privileged

ب- توصیه می‌شود دسترسی ویژه به کاربران بر مبنای نیاز- به- استفاده و بر مبنای رویداد-به-رویداد در راستای خط‌مشی کنترل دسترسی صورت گیرد (به بند ۹-۱-۱ مراجعه شود)، برای مثال بر مبنای کمینه الزامات نقش‌های عملکردی آن‌ها، انجام شود.

پ- توصیه می‌شود یک فرایند مجوز دهی و سوابق تمام دسترسی‌های ویژه اختصاص‌یافته، نگهداری شود. توصیه می‌شود حقوق ویژه دسترسی تا زمانی که فرایند صدور مجوز به‌طور کامل به انجام برسد، ارائه نشود؛

ت- توصیه می‌شود الزامات انقضای حقوق ویژه دسترسی تعریف شود؛

ث- توصیه می‌شود حقوق ویژه دسترسی به شناسه کاربری متفاوت از شناسه‌ای که برای انجام امور معمول کسب‌وکار استفاده می‌شود، اختصاص یابد. توصیه می‌شود اجرای امور معمول کسب‌وکار با شناسه دارای حقوق ویژه دسترسی انجام نشود؛

ج- توصیه می‌شود صلاحیت کاربران با حق ویژه دسترسی به‌طور منظم جهت هم‌راستا بودن با وظایف آن‌ها بررسی شود؛

چ- توصیه می‌شود روش اجرایی خاص به‌منظور جلوگیری از استفاده غیرمجاز از شناسه‌های عمومی راهبری[1]، با توجه به قابلیت‌های پیکربندی سامانه‌ها، پیاده‌سازی و نگهداری شود؛

ح- توصیه می‌شود در هنگام به اشتراک‌گذاری اطلاعات محرمانه اصالت‌سنجی مربوط به شناسه‌های عمومی راهبری، محرمانگی این اطلاعات حفظ شود. (به‌عنوان‌مثال تغییر متناوب رمز عبور و همچنین تغییر آن در اسرع وقت و اطلاع‌رسانی با سازوکار مناسب به کاربران دارای حق ویژه دسترسی، هنگامی‌که یک کاربر با دسترسی ویژه، سازمان را ترک کند و یا شغل خود را تغییر دهد).

اطلاعات دیگر

استفاده نامناسب از امتیازات سرپرستی سامانه‌ها (هر ویژگی یا امکانی از یک سامانه اطلاعاتی که امکان دور زدن کنترل‌های سامانه یا برنامه کاربردی را بدهد) عامل مؤثری برای خرابی یا رخنه[2] در سامانه‌ها است.

۹-۲-۴ مدیریت اطلاعات محرمانه اصالت‌سنجی[3] کاربران

کنترل

توصیه می‌شود، تخصیص اطلاعات محرمانه اصالت‌سنجی، از طریق یک فرآیند مدیریتی رسمی، کنترل شود.

راهنمای پیاده‌سازی

توصیه می‌شود این فرایند شامل الزامات زیر باشد:

1 - Administration
2 - Breach
3 -Authentication

الف- توصیه می‌شود کاربران ملزم شوند تعهدنامه‌ای را برای محرمانه نگه‌داشتن اطلاعات محرمانه اصالت‌سنجی شخصی و حفظ اطلاعات محرمانه اصالت‌سنجی گروهی فقط در میان اعضای گروه، امضا کنند؛ این تعهدنامه امضاشده را می‌توان در مفاد و شرایط اشتغال گنجاند (به بند ۷-۱-۲ مراجعه شود)؛

ب- زمانی که کاربران ملزم می‌شوند اطلاعات محرمانه اصالت‌سنجی خود را حفظ کنند، توصیه می‌شود ابتدا اطلاعات محرمانه اصالت‌سنجی موقت امن به آن‌ها داده شود که مجبور شوند در اولین بار استفاده، آن را تغییر دهند؛

پ- توصیه می‌شود رویه‌هایی برای احراز هویت کاربر، پیش از تأمین اطلاعات محرمانه جدید، اصالت‌سنجی تغییریافته یا موقت، ایجاد شود.

ت- توصیه می‌شود اطلاعات محرمانه اصالت‌سنجی موقت، به صورتی امن به کاربران داده شود؛ توصیه می‌شود از به کار بردن طرف‌های بیرونی یا رایانامه محافظت نشده (متن رمز نشده[1]) یا متعلق به طرف‌های بیرونی، اجتناب شود؛

ث- توصیه می‌شود اطلاعات محرمانه اصالت‌سنجی موقت برای هر شخص، منحصربه‌فرد باشد و توصیه می‌شود قابل حدس زدن نباشد؛

ج- توصیه می‌شود کاربران دریافت اطلاعات اصالت‌سنجی محرمانه خود را اعلام وصول کنند؛

چ- توصیه می‌شود اطلاعات محرمانه اصالت‌سنجی پیش‌فرض فروشندگان پس از نصب سامانه‌ها یا نرم‌افزار تغییر یابد.

اطلاعات دیگر

کلمات عبور از انواع متداول اطلاعات محرمانه اصالت‌سنجی و ابزاری متداول برای تصدیق هویت کاربران است. انواع دیگر اطلاعات محرمانه اصالت‌سنجی، کلیدهای رمزنگاری و داده‌های دیگری هستند که روی نمودافزار[2]های سخت‌افزاری (مثل کارت‌های هوشمند) ذخیره می‌شوند و کدهای اصالت‌سنجی تولید می کنند.

۹-۲-۵ بازنگری حقوق دسترسی کاربر

کنترل

توصیه می‌شود، مالکان دارایی حقوق دسترسی کاربران را در فواصل زمانی منظم بازنگری کنند.

راهنمای پیاده‌سازی

توصیه می‌شود در بازنگری حقوق دسترسی موارد زیر مدنظر قرار گیرد:

1 - clear text
2 - Token

الف- توصیه می‌شود حقوق دسترسی کاربران در فواصل زمانی منظم و پس از هر تغییر نظیر ارتقاء، تنزل رتبه، یا خاتمه اشتغال بررسی شوند (به بند ۷ مراجعه شود)؛

ب- توصیه می‌شود حقوق دسترسی کاربران در زمان جابجایی از یک نقش به نقش دیگر در همان سازمان بازنگری شود و مجدداً تخصیص یابد؛

پ- توصیه می‌شود مجوز دهی حقوق ویژه دسترسی مکرراً بازنگری شوند؛

ت- توصیه می‌شود تخصیص حقوق ویژه در فواصل منظم بررسی شود تا اطمینان حاصل شود که حقوق ویژه غیرمجازی کسب نشده است؛

ث- توصیه می‌شود تغییر در حساب‌های دارای حقوق ویژه برای بازنگری‌های دوره‌ای ثبت شود.

اطلاعات دیگر

این کنترل نقاط ضعف احتمالی در اجرای کنترل‌های بندهای ۹-۲-۱، ۹-۲-۲ و ۹-۲-۶ را جبران می‌کند.

۹-۲-۶ حذف یا تنظیم حقوق دسترسی

کنترل

توصیه می‌شود، حقوق دسترسی تمامی کارکنان و طرف‌های بیرونی به اطلاعات و تسهیلات پردازش اطلاعات، به‌محض خاتمه شغل، قرارداد یا توافقنامه آن‌ها، حذف‌شده یا به‌محض تغییر شغل، تنظیم شود.

راهنمای پیاده‌سازی

به‌محض خاتمه اشتغال، توصیه می‌شود حقوق دسترسی یک فرد به اطلاعات و دارایی‌های مربوط به تسهیلات پردازش اطلاعات و خدمات، حذف یا معلّق شود. این کار تعیین خواهد کرد که آیا لازم است تا حقوق دسترسی حذف شوند یا خیر. توصیه می‌شود تغییرات یک شغل در حذف تمام حقوق دسترسی که برای شغل جدید تأیید نشده‌اند، انعکاس یابد. توصیه می‌شود حقوق دسترسی که حذف یا تغییر داده شوند، شامل دسترسی فیزیکی و منطقی باشد. حذف یا تنظیم حقوق دسترسی می‌تواند با حذف، ابطال یا جایگزینی کلیدها، کارت‌های شناسایی، تسهیلات پردازش اطلاعات یا اشتراک‌ها[1] انجام شود. توصیه می‌شود حذف یا تنظیم حقوق دسترسی در تمامی مستنداتی که حقوق دسترسی کارکنان یا پیمانکاران را شناسایی می‌کند، منعکس شود. اگر کاربری از کارکنان یا طرف‌های بیرونی در حال ترک سازمان است و کلمه‌های عبور شناسه‌های کاربری که فعال باقی‌مانده‌اند را بداند، این کلمه‌های عبور توصیه می‌شود به‌محض خاتمه یا تغییر شغل، قرارداد یا موافقت‌نامه، تغییر داده شوند.

با توجه به ارزشیابی عوامل مخاطره، قبل از خاتمه یا تغییرات اشتغال، توصیه می‌شود حقوق دسترسی برای اطلاعات و دارایی‌های مرتبط با تسهیلات پردازش اطلاعات، کاهش‌یافته یا حذف شوند؛ مانند:

1 - Subscription

الف- این‌که آیا خاتمه خدمت یا تغییر توسط کارکنان یا کاربر طرف بیرونی یا توسط مدیریت انجام‌شده است و نیز دلیل خاتمه خدمت؛

ب- مسئولیت‌های فعلی کارکنان، طرف بیرونی یا هر کاربر دیگر؛

پ- ارزش دارایی‌هایی که در حال حاضر در دسترس هستند.

اطلاعات دیگر

در شرایط خاص، ممکن است حقوق دسترسی بر مبنایی اختصاص داده‌شده باشد که افراد بیشتری علاوه بر کارمند سازمان یا طرف بیرونی ترک‌کننده، به آن دسترسی داشته باشند، مثلاً شناسه‌های گروهی تعریف‌شده باشد. توصیه می‌شود در چنین شرایطی، افراد ترک‌کننده از همه فهرست‌های دسترسی گروهی حذف شوند و توصیه می‌شود تمهیداتی انجام شوند تا به تمام کارکنان، کاربران پیمانکاران مربوط توصیه شود که این اطلاعات را بعدازاین با شخصی که در حال ترک سازمان است، به اشتراک نگذارند.

درصورتی‌که خاتمه قرارداد توسط مدیریت آغاز شود، کارکنان و کاربران طرف‌های بیرونی ناراضی، ممکن است عمداً اطلاعات را خراب کنند یا تجهیزات پردازش اطلاعات را منهدم کنند. در صورت استعفا یا اخراج افراد، آن‌ها ممکن است وسوسه شوند تا اطلاعات را برای استفاده در آینده جمع‌آوری کنند.

۹-۳ مسئولیت‌های کاربر

قصد: مسئول ساختن کاربران برای حفاظت از اطلاعات اصالت‌سنجی‌شان.

۹-۳-۱ استفاده از اطلاعات اصالت‌سنجی مخفی

کنترل

توصیه می‌شود کاربران به تبعیت از شیوه‌های سازمان در استفاده از اطلاعات مخفی اصالت‌سنجی ملزم شوند.

راهنمای پیاده‌سازی

توصیه می‌شود تمام کاربران راهنمایی شوند که:

الف- اطلاعات مخفی اصالت‌سنجی را به‌صورت محرمانه نگهداری کنند و اطمینان حاصل کنند که این اطلاعات برای سایر طرف‌ها ازجمله افراد و مسئولین فاش نمی‌شود؛

ب- از نگهداری سابقه‌ای (مثلاً بر روی کاغذ، فایل نرم‌افزاری، یا وسیله دستی) از اطلاعات اصالت‌سنجی مخفی اجتناب کنند، مگر زمانی که بتوان آن را به‌طور ایمن ذخیره کرد و روش ذخیره‌سازی مورد تأیید باشد (مانند انباره رمز عبور)؛

پ- اطلاعات اصالت‌سنجی را هر زمان که نشانه‌ای از سوءاستفاده احتمالی از آن باشد، تغییر دهند؛

ت- هنگامی‌که کلمه عبور به‌عنوان اطلاعات مخفی اصالت‌سنجی مورداستفاده قرار می‌گیرد، کلمات عبور باکیفیت را با کمینه طول کافی انتخاب کنند که:

۱- به خاطر آوردنشان ساده باشد؛

۲- بر مبنای چیزی نباشد که شخص دیگری بتواند به‌سادگی آن را حدس بزند یا با استفاده از اطلاعات شخصی فرد به آن دست یابد. مثلاً: نام، شماره تلفن، تاریخ تولد و مانند آن؛
۳- نسبت به حملات واژه‌نامه‌ای آسیب‌پذیر نباشد؛ (برای مثال، متشکل از واژگانی که در واژه‌نامه‌ها آمده است، نباشد)؛
۴- حروف مشابه متوالی باشد، یعنی همگی عددی یا همگی الفبایی نباشد؛
۵- چنانچه موقتی است، در اولین ورود تغییر داده شود؛

ث- اطلاعات محرمانه اصالت‌سنجی فردی را به اشتراک نگذارند؛

ج- از محافظت مناسب از کلمات عبور هنگامی‌که در روال‌های ورود خودکار به‌عنوان اطلاعات محرمانه اصالت‌سنجی مورداستفاده قرار می‌گیرند و ذخیره می‌شوند اطمینان حاصل کنند؛
چ- از اطلاعات محرمانه اصالت‌سنجی یکسان برای اهداف کاری و غیر کاری استفاده نکنند.

اطلاعات دیگر

فراهم آوری ورود واحد به سامانه[1] (SSO) و یا دیگر ابزارهای مدیریت اطلاعات رمز شده اصالت‌سنجی مخفی، مقدار اطلاعات مخفی اصالت‌سنجی که کاربران ملزم به محافظت از آن هستند را کاهش می‌دهد و درنتیجه توانند اثربخشی این کنترل را افزایش دهد. بااین‌حال، این ابزارها همچنین می‌توانند تأثیر افشای اطلاعات اصالت‌سنجی مخفی را افزایش دهند.

۹-۴ کنترل دسترسی به سامانه‌ها و برنامه‌های کاربردی

قصد: پیشگیری از دسترسی غیرمجاز به سامانه‌ها و برنامه‌های کاربردی.

۹-۴-۱ محدودسازی دسترسی به اطلاعات

کنترل

توصیه می‌شود مطابق با خط‌مشی کنترل دسترسی، دسترسی به اطلاعات و کارکردهای سامانه برنامه کاربردی، محدود شود.

راهنمای پیاده‌سازی

توصیه می‌شود محدودیت در دسترسی بر اساس الزامات هریک از برنامه‌های کاربردی کسب‌وکار و هم‌راستا با خط‌مشی تعریف‌شده کنترل دسترسی باشد.

توصیه می‌شود به‌کارگیری موارد زیر به‌منظور پشتیبانی الزامات محدودیت دسترسی در نظر گرفته شود:

الف- ارائه گزینگانی[2] برای کنترل دسترسی به عملکردهای سامانه برنامه کاربردی؛

ب- کنترل اینکه چه داده‌ای در دسترس یک کاربر خاص قرار گیرد؛

1 - Single Sign On
2 - menu

پ- کنترل حقوق دسترسی کاربران، مانند خواندن، نوشتن، حذف کردن و اجرا کردن؛

ت- کنترل حقوق دسترسی نرم‌افزارهای کاربردی دیگر؛

ث- محدود کردن اطلاعات موجود در خروجی؛

ج- فراهم کردن کنترل‌های دسترسی منطقی و فیزیکی برای جداسازی برنامه‌های کاربردی، داده برنامه کاربردی یا سامانه‌های حساس.

۹-۴-۲ روش‌های اجرایی ورود امن

کنترل

توصیه می‌شود در مواردی که خط‌مشی کنترل دسترسی الزام کرده است، دسترسی به سامانه‌ها و برنامه‌های کاربردی از طریق یک روش اجرایی ورود امن، کنترل شود.

راهنمای پیاده‌سازی

توصیه می‌شود روش اصالت‌سنجی مناسب برای اثبات هویت ادعاشده یک کاربر انتخاب شود.

زمانی که اصالت‌سنجی و تأیید هویت مستحکمی موردنیاز است، توصیه می‌شود روش‌های اصالت‌سنجی جایگزین کلمات عبور، مانند ابزارهای رمزنگاری، کارت‌های هوشمند، نشانه و یا افزارهای زیست‌سنجی، مورداستفاده قرار گیرد.

توصیه می‌شود روش اجرایی ورود به یک سامانه یا برنامه کاربردی برای کاهش فرصت دسترسی غیرمجاز طراحی شود؛ بنابراین توصیه می‌شود این روش اجرایی ورود به سامانه، کمینه اطلاعات را درباره سامانه یا برنامه کاربردی افشا کند تا از ارائه کمک غیر لازم به یک کاربرد غیرمجاز اجتناب شود. توصیه می‌شود یک روش اجرایی خوب ورود به سامانه موارد زیر را لحاظ کند:

الف- شناسه‌های سامانه یا برنامه کاربردی را تا زمانی که فرایند ورود به سامانه با موفقیت کامل نشده است نشان ندهد؛

ب- یک هشدار عمومی را نمایش دهد مبنی بر اینکه رایانه فقط توسط کاربران مجاز مورد دسترسی قرار گیرد؛

پ- پیام‌های کمک را که می‌تواند به کاربر غیرمجاز کمک کند، در طول روش اجرایی ورود به سامانه ارائه نکند؛

ت- اطلاعات ورود به سامانه را تنها پس از تکمیل تمام داده‌های ورودی اعتبارسنجی کند. اگر شرایط خطایی پیش بیاید، توصیه می‌شود سامانه نشان ندهد که کدام بخش از داده‌ها صحیح است و کدام بخش صحیح نیست؛

ث- در مقابل تلاش‌های ورود به‌صورت جستجوی فراگیر محافظت کند؛

ج- تلاش‌های موفق و ناموفق ورود به سامانه را ثبت کند؛

چ- اعلان یک رویداد امنیتی، اگر تلاش‌های بالقوه و یا نقض موفق کنترل‌های ورود تشخیص داده شد؛

ح- اطلاعات زیر را هنگام تکمیل ورود موفق نمایش دهد:

۱- تاریخ و زمان ورود موفق قبلی؛
۲- جزئیات هر تلاش ناموفق برای ورود از زمان آخرین ورود موفق؛

خ- کلمه عبوری را که وارد می‌شود نمایش ندهد؛

د- کلمات عبور را به‌صورت متن آشکار، در شبکه منتقل نکند؛

ذ- نشست‌های غیرفعال پس از طی دوره تعریف‌شده‌ای غیرفعال بشود، مخصوصاً در محل‌های با مخاطرات بالا مانند مکان‌های عمومی یا فضاهای خارج از مدیریت امنیت سازمان یا بر روی تجهیزات سیار؛

ر- محدود کردن زمان‌های اتصال برای افزایش امنیت مضاعف در برنامه‌های کاربردی پرمخاطره و کاهش پنجره فرصت دسترسی‌های غیرمجاز.

اطلاعات دیگر

کلمات عبور، یک‌راه عمومی برای شناسایی و اصالت‌سنجی بر اساس رمزی است که تنها کاربر می‌داند. این موضوع همچنین می‌تواند با استفاده از ابزارهای رمزنگاری و پروتکل‌های اصالت‌سنجی به دست آید.

قدرت اصالت‌سنجی کاربر باید مناسب با طبقه‌بندی اطلاعات در نظر گرفته شود.

اگر کلمات عبور به‌صورت رمز شده در طول نشست ورود به سامانه بر روی شبکه انتقال یابد، ممکن است توسط برنامه‌های شنودگر[1] به دست آید.

۹-۴-۳ سیستم مدیریت کلمات عبور

کنترل

توصیه می‌شود، سامانه‌های مدیریت کلمات عبور، تعاملی بوده و کیفیت کلمات عبور را تضمین کنند.

راهنمای پیاده‌سازی

توصیه می‌شود یک سیستم مدیریت کلمه عبور، موارد زیر را پوشش دهد:

الف- جهت حفظ جوابگویی، استفاده از شناسه‌های کاربری و کلمات عبور شخصی را اجبار کند؛

ب- به کاربران اجازه دهد کلمه عبور خود را انتخاب کنند و تغییر دهند و شامل روش اجرایی تأییدی برای خطاهای ورود اطلاعات باشد؛

پ- انتخاب کلمات عبور باکیفیت را اجبار کند؛

1- sniffer

ث- کاربران را وادار کند کلمات عبور را در اولین ورود به سامانه تغییر دهند؛

ت- تغییرات کلمات عبور به‌طور منظم و در صورت نیاز را اجبار کند؛

ج- سابقه‌ای از کلمات عبور پیشین را نگهداری کند و از استفاده مجدد آن‌ها جلوگیری کند؛

چ- کلمات عبور را در زمان وارد شدن روی صفحه نشان ندهد؛

ح- فایل‌های کلمات عبور را جدا از داده‌های سامانه نرم‌افزار کاربردی ذخیره کند؛

خ- کلمات عبور را به شکل محافظت‌شده، ذخیره و منتقل کند.

اطلاعات دیگر

برخی از برنامه‌های کاربردی نیازمند کلمات عبور کاربری هستند که توسط مراجع مستقل تخصیص می‌یابند؛ در چنین مواردی نکات ب، ت و ث از راهنمای فوق به کار نمی‌روند. در اکثر موارد کلمات عبور توسط کاربران انتخاب و حفظ می‌شوند.

۹-۴-۴ استفاده از برنامه‌های کمکی ویژه

کنترل

توصیه می‌شود، استفاده از برنامه‌های کمکی ویژه که امکان دور زدن کنترل‌های سامانه و برنامه کاربردی را فراهم می‌کنند، محدود و به‌شدت کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر برای استفاده از برنامه‌های کمکی ویژه که توانایی دور زدن کنترل‌های سامانه و برنامه کاربردی رادارند در نظر گرفته شود:

الف- استفاده از روش‌های اجرایی شناسایی، اصالت‌سنجی و مجوز دهی برای برنامه‌های کمکی سامانه؛

ب- تفکیک برنامه‌های کمکی ویژه از نرم‌افزارهای کاربردی؛

پ- محدود کردن استفاده از برنامه‌های کمکی ویژه به کمینه تعداد عملی کاربران مجاز و مورداطمینان (به بند ۹-۲-۳ مراجعه شود)؛

ت- مجوز دهی برای استفاده اقتضایی[1] از برنامه‌های کمکی ویژه؛

ث- محدود کردن در دسترس بودن برنامه کمکی ویژه به‌عنوان‌مثال برای بازه زمانی یک تغییر مجاز؛

ج- واقعه‌نگاری همه استفاده‌ها از برنامه‌های کمکی ویژه؛

چ- تعریف و مستندسازی سطوح اختیارات مربوط به برنامه‌های کمکی ویژه؛

1- Ad-hoc

ح- از بین بردن یا غیرفعال کردن نرم‌افزارهای کمکی غیرضروری؛

خ- در دسترس قرار ندادن برنامه کمکی برای کاربرانی که دسترسی به برنامه‌های کاربردی روی سامانه‌هایی دارند که نیازمند تفکیک وظایف است.

اطلاعات دیگر

اکثر نصب‌های رایانه‌ای، یک یا چند برنامه کمکی دارند که ممکن است قادر به ابطال کنترل‌های سامانه و برنامه کاربردی باشند.

۹-۴-۵ کنترل دسترسی به کد منبع برنامه

کنترل

توصیه می‌شود، دسترسی به کد منبع برنامه، محدود شود.

راهنمای پیاده‌سازی

توصیه می‌شود دسترسی به کد منبع برنامه و موارد مربوط (مانند طراحی‌ها، مشخصات، طرح‌های درستی-سنجی و طرح‌های اعتبارسنجی) شدیداً کنترل شود تا از افزودن کارکرد غیرمجاز [1] و تغییرات غیرعمدی اجتناب شود و درعین‌حال از محرمانگی اطلاعات مالکیت معنوی ارزشمند نیز محافظت شود. برای کد منبع برنامه، این موضوع می‌تواند از طریق ذخیره مرکزی کنترل‌شده این کد، ترجیحاً در کتابخانه‌های منبع برنامه به دست آید. توصیه می‌شود راهنمایی‌های زیر، برای کنترل دسترسی به این کتابخانه‌های منبع برنامه، به‌منظور کاهش امکان اختلال برنامه‌های رایانه‌ی در نظر گرفته شوند:

الف- توصیه می‌شود در هرجایی که ممکن باشد کتابخانه‌های منبع برنامه، در سامانه‌های عملیاتی نگهداری نشود؛

ب- توصیه می‌شود کد منبع برنامه و کتابخانه‌های منبع برنامه مطابق با رویه‌های ایجادشده، مدیریت شود؛

پ- توصیه می‌شود کارکنان پشتیبانی، دسترسی نامحدود به کتابخانه‌های منبع برنامه نداشته باشد؛

ت- توصیه می‌شود روزآمدسازی کتابخانه‌های منبع برنامه و موارد مرتبط و توزیع منابع برنامه برای برنامه‌نویس‌ها فقط پس از دریافت مجوز مناسب اجرا شود؛

ث- توصیه می‌شود فهرست‌های برنامه در یک محیط امن نگهداری شود؛

ج- توصیه می‌شود ثبت وقایع ممیزی از تمام دسترسی‌ها به کتابخانه‌های منبع برنامه نگهداری شود؛

چ- توصیه می‌شود نگهداری و کپی کتابخانه‌های منبع برنامه وابسته به رویه‌های شدید کنترل تغییر باشد (به بند ۱۴-۲-۲ مراجعه شود)؛

1- introduction of unauthorized functionality

توصیه می‌شود اگر قصد انتشار کد منبع برنامه وجود دارد، کنترل‌های اضافی برای کمک به تضمین یکپارچگی آن (به‌عنوان‌مثال امضای دیجیتال) در نظر گرفته شود.

۱۰ رمزنگاری

۱-۱۰ کنترل‌های رمزنگاری

قصد: حصول اطمینان از استفاده مناسب و مؤثر رمزنگاری برای حفاظت از محرمانگی، اصالت و یا یکپارچگی اطلاعات.

۱-۱-۱۰ خط‌مشی استفاده از کنترل‌های رمزنگاری

کنترل

توصیه می‌شود، برای حفاظت از اطلاعات، یک خط‌مشی استفاده از کنترل‌های رمزنگاری، ایجاد و پیاده‌سازی شود.

راهنمای پیاده‌سازی

توصیه می‌شود در زمان ایجاد یک خط‌مشی رمزنگاری موارد زیر در نظر گرفته شود:

الف- رویکرد مدیریت در قبال استفاده از کنترل‌های رمزنگاری در سازمان، ازجمله اصول کلی که توصیه می‌شود اطلاعات کسب‌وکار تحت آن محافظت شود؛

ب- بر اساس ارزیابی مخاطرات، توصیه می‌شود سطح موردنیاز محافظت با احتساب نوع، قدرت و کیفیت الگوریتم رمزگذاری موردنیاز شناسایی شود؛

پ- استفاده از رمزگذاری برای محافظت از اطلاعاتی که توسط افزاره‌های سیار، رسانه‌های قابل‌حمل یا خطوط ارتباطی منتقل می‌شود؛

ت- رویکرد در قبال مدیریت کلید، ازجمله روش‌هایی برای پرداختن به محافظت از کلیدهای رمزنگاری و بازیابی اطلاعات رمزگذاری‌شده در صورت مفقود شدن، به خطر افتادن یا صدمه به کلید؛

ث- نقش‌ها و مسئولیت‌ها، مثلاً این‌که چه کسی مسئول موارد زیر است:

۱- اجرای خط‌مشی؛
۲- مدیریت کلید ازجمله تولید کلید (همچنین به بند ۱۰-۱-۲ مراجعه شود)؛

ج- استانداردهایی که باید برای اجرای مؤثر در تمام سازمان مورداستفاده قرار گیرد (که چه راه‌حلی برای چه فرایندهای کسب‌وکاری استفاده می‌شود)؛

چ- پیامد استفاده از اطلاعات رمزگذاری‌شده در کنترل‌هایی که بر بررسی محتوا تکیه‌دارند. (برای مثال، آشکارسازی بدافزار).

توصیه می‌شود در زمان اجرای خط‌مشی رمزنگاری سازمان، به مقررات و محدودیت‌های ملی که ممکن است در مورداستفاده از روش‌های رمزنگاری در بخش‌های مختلف جهان اعمال شود و نیز به مسائل جریان فرامرزی اطلاعات رمزنگاری‌شده توجه شود (همچنین به بند ۱۸-۱-۵ مراجعه شود).

کنترل‌های رمزنگاری را می‌توان برای دستیابی به اهداف مختلف امنیت اطلاعات مورداستفاده قرارداد، مثلاً:

الف- محرمانگی: استفاده از رمزگذاری اطلاعات برای محافظت از اطلاعات حساس و حیاتی، به‌صورت ذخیره‌شده یا منتقل‌شده؛

ب- یکپارچگی/اصالت: استفاده از امضاهای دیجیتال یا کد اصالت‌سنجی پیام برای تأیید اصالت یا یکپارچگی اطلاعات حساس یا حیاتی ذخیره‌شده یا منتقل‌شده؛

پ- عدم انکار: استفاده از روش‌های رمزنگاری برای به دست آوردن شواهد بر وقوع یا عدم وقوع یک رویداد یا فعالیت؛

ت- اصالت‌سنجی: استفاده از روش‌های رمزنگاری برای اصالت‌سنجی کاربران و سایر هستارهای سامانه‌هایی که درخواست دسترسی یا تراکنش با کاربران، هستارها یا منابع سامانه رادارند.

اطلاعات دیگر

توصیه می‌شود تصمیم‌گیری درباره این‌که آیا راه‌حل رمزنگاری مناسب است، به‌عنوان بخشی از فرایند گسترده‌تر ارزیابی مخاطرات و انتخاب کنترل‌ها در نظر گرفته شوند. این ارزیابی را سپس می‌توان برای تعیین این‌که آیا کنترل رمزنگاری مناسب است یا نه چه نوع کنترلی توصیه می‌شود که به کار گرفته شود و برای کدام هدف و فرایندهای کسب‌وکار مورداستفاده قرارداد.

وجود یک خط‌مشی درباره استفاده از کنترل‌های رمزنگاری برای بیشینه کردن منافع و کاهش مخاطرات استفاده از روش‌های رمزنگاری و اجتناب از استفاده نامناسب یا غیر صحیح لازم است.

توصیه می‌شود مشاوره تخصصی برای انتخاب کنترل‌های مناسب رمزنگاری جهت حصول اهداف خط‌مشی امنیت اطلاعات انجام شود.

۱۰-۱-۲ مدیریت کلید

کنترل

توصیه می‌شود، خط‌مشی برای استفاده، محافظت و طول عمر کلیدهای رمزنگاری در سراسر چرخه عمر آن ایجاد و پیاده‌سازی شود.

راهنمای پیاده‌سازی

خط‌مشی باید الزامات برای مدیریت کلیدهای رمزنگاری در کل چرخه عمر خود شامل تولید، ذخیره‌سازی، بایگانی، بازیابی، توزیع، انقضا و از بین بردن کلید را در برداشته باشد.

الگوریتم‌های رمزنگاری، طول کلید و شیوه‌های استفاده باید با توجه به بهروش انتخاب شود. مدیریت کلید مناسب نیاز به فرآیندهای امن برای تولید، ذخیره‌سازی، بایگانی، بازیابی، توزیع، انقضا و از بین بردن کلید رمزنگاری دارد.
توصیه می‌شود تمام کلیدهای رمزنگاری در مقابل دست‌کاری (تغییر) و مفقود شدن محافظت شوند. به‌علاوه، کلیدهای مخفی و خصوصی، نیازمند محافظت در برابر استفاده غیرمجاز و افشا هستند. توصیه می‌شود تجهیزات به‌کاررفته برای تولید، ذخیره و بایگانی کلیدها ازنظر فیزیکی محافظت شود.

توصیه می‌شود یک سیستم مدیریت کلید بر اساس مجموعه موردتوافق استانداردها، رویه‌ها و روش‌های امن برای موارد زیر ایجاد شود:

الف- تولید کلید برای سامانه‌های رمزنگاری مختلف و کاربردهای مختلف؛

ب- انتشار و به دست آوردن گواهینامه‌های کلید عمومی؛

پ- توزیع کلیدها بین هستارهای موردنظر ازجمله این‌که کلیدها چگونه در زمان دریافت فعال شوند؛

ت- ذخیره کلیدها ازجمله این‌که چگونه کاربران مجاز به کلیدها دسترسی پیدا می‌کنند؛

ث- تغییر یا روزآمد کردن کلیدها ازجمله قواعدی درباره این‌که چه زمانی کلیدها تغییر کنند و این کار چگونه انجام شود؛

ج- رسیدگی به کلیدهای در معرض خطر؛

چ- پس گرفتن کلیدها ازجمله این‌که چگونه کلیدها مسترد شوند یا غیرفعال شوند، مثلاً زمانی که کلیدها در معرض خطر قرارگرفته‌اند یا زمانی که یک کاربر از سازمان می‌رود. (در چه حالتی توصیه می‌شود که کلیدها بایگانی شوند)؛

ح- بازیابی کلیدهایی که گم می‌شوند یا خراب می‌شوند؛

خ- بایگانی و پشتیبان‌گیری از کلیدها؛

د- تخریب کلیدها؛

ذ- واقعه‌نگاری و ممیزی فعالیت‌های مرتبط با مدیریت کلید.

توصیه می‌شود به‌منظور کاهش احتمال استفاده نامناسب، تاریخ فعال‌سازی و غیر فعال‌سازی برای کلیدها تعریف شوند تا کلیدها را فقط بتوان برای دوره زمانی تعریف‌شده‌ای در خط‌مشی مدیریت کلید مرتبط، مورداستفاده قرارداد.

علاوه بر مدیریت مطمئن کلیدهای خصوصی و مخفی، توصیه می‌شود اصالت کلیدهای عمومی نیز در نظر گرفته شود. این فرایند اصالت‌سنجی می‌تواند با استفاده از گواهینامه‌های کلید عمومی که معمولاً توسط یک مرجع صدور گواهی صادر می‌شود انجام شود که توصیه می‌شود یک سازمان به رسمیت شناخته‌شده با کنترل‌ها و روش‌های اجرایی مناسب برای تأمین درجه اطمینان موردنیاز باشد.

توصیه می‌شود محتوای قراردادها یا توافق‌نامه‌های سطح خدمات با تأمین‌کنندگان بیرونی خدمات رمزنگاری (مثلاً با یک مسئول صدور گواهی)، موضوعات تعهد، اطمینان از خدمات و زمان‌های پاسخ برای فراهم کردن خدمات را پوشش دهد (به بند ۱۵-۲ مراجعه شود).

اطلاعات دیگر

مدیریت کلیدهای رمزنگاری برای استفاده مؤثر از فنون رمزنگاری لازم است. ISO/IEC 11770 [۲] [۳] [۴] اطلاعات بیشتری را درباره مدیریت کلید ارائه می‌کند.

فنون رمزنگاری نیز می‌تواند برای محافظت از کلیدهای رمزنگاری به کار گرفته شود. ممکن است نیاز باشد روش‌های اجرایی برای مدیریت درخواست‌های قانونی جهت دسترسی به کلیدهای رمزنگاری در نظر گرفته شود، به‌عنوان‌مثال ممکن است لازم باشد اطلاعات رمزگذاری شده به شکل رمزگشایی‌شده جهت ارائه به‌صورت شواهد در دادگاه در دسترس قرار گیرد.

۱۱ امنیت فیزیکی و محیطی

۱-۱۱ نواحی امن

قصد: پیشگیری از دسترسی غیر مجاز فیزیکی ، خسارت و تعارض به اطلاعات و تجهیزات پردازش اطلاعات سازمان.

۱-۱-۱۱ حصار[1] امنیت فیزیکی

کنترل

توصیه می‌شود، حصارهای امنیتی برای حفاظت نواحی حاوی اطلاعات حساس یا حیاتی و تسهیلات پردازش اطلاعات، تعریف و استفاده شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر در هنگام لزوم برای حصارهای امنیت فیزیکی در نظر گرفته‌شده و اجرا شوند:

الف- توصیه می‌شود حصارهای امنیتی تعریف شوند و محل قرارگیری و قدرت هر یک از حصارها متناسب با نیازهای امنیتی دارایی‌های آن حصار و نتایج ارزیابی مخاطرات باشد؛

ب- توصیه می‌شود محیط ساختمان یا سایت حاوی تجهیزات پردازش اطلاعات، ازنظر فیزیکی مناسب باشد (برای مثال، توصیه می‌شود هیچ شکافی در حصارها یا نواحی که شکستن حفاظ‌ها به‌راحتی می‌تواند اتفاق بی افتد، وجود نداشته باشد)؛ توصیه می‌شود سقف بیرونی، کف و دیوارهای بیرونی سایت سازه یکپارچه‌ای داشته باشد و توصیه می‌شود تمام درب‌ها به‌صورت مناسب در برابر دسترسی غیرمجاز با سازوکارهای کنترل

1- Perimeter

(ازجمله موانع، اخطارها، قفل‌ها) محافظت شوند؛ توصیه می‌شود درب‌ها و پنجره‌ها زمانی که مراقبت وجود ندارد، قفل شوند و محافظت بیرونی برای پنجره‌ها، به‌خصوص برای پنجره‌هایی که در طبقات همکف قرار دارند، در نظر گرفته شود؛

پ- توصیه می‌شود یک ناحیه پذیرش سرنشین دار یا هر ابزار دیگری برای کنترل دسترسی فیزیکی به سایت یا ساختمان‌ها وجود داشته باشد؛ توصیه می‌شود دسترسی به سایت‌ها و ساختمان‌ها فقط محدود به کارکنان مجاز شود؛

ت- توصیه می‌شود موانع فیزیکی در صورت امکان ایجاد شوند تا از دسترسی فیزیکی غیرمجاز و آلودگی‌های محیطی جلوگیری شود؛

ث- توصیه می‌شود تمام درب‌های خروجی اضطراری در حصار امنیتی، پایش شده و در ترکیب با دیوارها آزمون شوند تا سطح مقاومت موردنیاز را مطابق با استانداردهای مناسب منطقه‌ای، ملی و بین‌المللی فراهم کنند؛ توصیه می‌شود آن‌ها مطابق با استانداردهای محلی مقابله با حریق، به‌گونه‌ای ایمن عمل کنند؛

ج- توصیه می‌شود سامانه‌های کشف مزاحم مناسب مطابق با استانداردهای ملی، منطقه‌ای و بین‌المللی نصب شوند و به‌طور منظم مورد آزمون قرار گیرند تا تمام درب‌های بیرونی و پنجره‌های قابل‌دسترس را پوشش دهند. توصیه می‌شود فضاهای خالی همواره هشدار داده شوند؛ همچنین توصیه می‌شود این پوشش برای فضاهای دیگر مانند اتاق رایانه یا اتاق‌های ارتباطات تأمین شود؛

چ- توصیه می‌شود تجهیزات پردازش اطلاعات که توسط سازمان مدیریت می‌شوند ازنظر فیزیکی از تجهیزاتی که توسط طرف‌های بیرونی دیگر مدیریت می‌شوند تفکیک شوند.

اطلاعات دیگر

محافظت فیزیکی می‌تواند از طریق ایجاد یک یا چند مانع فیزیکی در اطراف محوطه سازمان و تجهیزات پردازش اطلاعات آن حاصل شود؛ استفاده از چندین مانع امنیت بیشتری را فراهم می‌کند، درحالی‌که عمل نکردن یک مانع به معنی مختل شدن سریع امنیت نیست.

یک ناحیه امن ممکن است یک دفتر کار قابل قفل‌شده یا چندین اتاق باشد که توسط یک مانع امنیت فیزیکی داخلی مستمر احاطه‌شده است؛ موانع و حفاظ‌های دیگری برای کنترل دسترسی فیزیکی ممکن است بین نواحی داخلی با نیازهای امنیتی متفاوت موردنیاز باشد. توصیه می‌شود ملاحظات خاصی در راستای امنیت دسترسی فیزیکی برای ساختمان‌هایی که دارایی‌های چندین سازمان مختلف در آن قرار دارند در نظر گرفته شود.

توصیه می‌شود به‌کارگیری کنترل‌های فیزیکی، به‌صورت خاص برای نواحی امن مطابق با شرایط اقتصادی و فنی سازمان، همان‌گونه که در ارزیابی مخاطره مشخص‌شده، باشد.

۱۱-۱-۲ کنترل‌های ورودی فیزیکی

کنترل

توصیه می‌شود، نواحی امن، به‌منظور حصول اطمینان از اینکه فقط کارکنان مجاز، اجازه دسترسی دارند، توسط کنترل‌های ورودی مناسب، حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر مدنظر قرار گیرند:

الف- توصیه می‌شود تاریخ و زمان ورود و خروج مراجعه‌کنندگان ثبت شود و توصیه می‌شود تمام مراجعه‌کنندگان تحت نظارت باشند مگر این‌که دسترسی آن‌ها قبلاً تأییدشده باشد؛ توصیه می‌شود آن‌ها فقط دسترسی برای اهداف خاص و مجاز را داشته باشند و دستورالعمل‌هایی درزمینهٔ الزامات امنیتی ناحیه و روش‌های اجرایی مربوط به شرایط اضطراری به آن‌ها اعلام شود. تعیین هویت مراجعه‌کنندگان به روش مناسبی انجام شود؛

ب- توصیه می‌شود دسترسی به نواحی که در آنجا، اطلاعات حساس مورد پردازش قرار می‌گیرد یا ذخیره می‌شود، صرفاً توسط کنترل‌های دسترسی مناسب ازجمله پیاده‌سازی سازوکار اصالت‌سنجی دوعاملی مانند کارت کنترل دسترسی یا شماره شناسایی شخصی (PIN)[1] مخفی محدود شود؛

پ- توصیه می‌شود دفتر فیزیکی ثبت وقایع یا رد[2] ممیزی الکترونیکی از تمام دسترسی‌ها به‌صورت امن نگهداری و پایش شود؛

ت- توصیه می‌شود از تمام کارکنان، پیمانکاران و طرف‌های بیرونی و تمام مراجعه‌کنندگان خواسته شود تا نوعی علامت شناسایی قابل‌رؤیت را به لباس خود نصب کنند و در صورت مواجهه با مراجعه‌کنندگان بدون همراه و یا بدون علامت شناسایی توصیه می‌شود بلافاصله کارکنان امنیتی را مطلع کنند؛

ث- توصیه می‌شود طرف‌های بیرونی که پشتیبانی خدمات کارکنان را انجام می‌دهند، امکان دسترسی محدود به نواحی امن یا تجهیزات پردازش اطلاعات حساس را فقط در صورت ضرورت داشته باشند؛ توصیه می‌شود این دسترسی مجاز و کنترل‌شده باشد؛

ج- توصیه می‌شود حقوق دسترسی به نواحی امن، به‌طور منظم بازنگری و به هنگام شوند و در زمان لازم باطل شوند (به بندهای ۹-۲-۵ و ۹-۲-۶ مراجعه شود)؛

۱۱-۱-۳ امن سازی دفاتر، اتاق‌ها و تسهیلات

کنترل

توصیه می‌شود، امنیت فیزیکی برای دفاتر، اتاق‌ها و تسهیلات، طراحی و به کار گرفته شود.

راهنمای پیاده‌سازی

1 - Personal Identification Number
2 - trail

توصیه می‌شود راهنمایی‌های زیر برای امنیت دفاتر، اتاق‌ها و تسهیلات در نظر گرفته شود:

الف- تسهیلات کلیدی در جایگاهی مستقر شوند تا از دسترس همگان دور نگه‌داشته شوند؛

ب- توصیه می‌شود در صورت امکان، ساختمان‌ها غیرقابل نفوذ باشند و کمینه نشانه‌ای از کاربردشان ارائه دهند و هیچ علائم واضحی خارج یا داخل ساختمان وجود نداشته باشد که وجود فعالیت‌های پردازش اطلاعات در آن را مشخص سازد؛

پ- توصیه می‌شود پیکربندی تجهیزات برای جلوگیری از قابل‌مشاهده و قابل‌شنود بودن اطلاعات و یا فعالیت‌های محرمانه از خارج انجام شود. توصیه می‌شود، محافظ الکترومغناطیسی نیز در صورت مناسب بودن در نظر گرفته شود؛

ت- راهنمای ساختمان و دفاتر تلفنی که محل قرارگیری تسهیلات پردازش اطلاعات حساس را نشان می‌دهند، توصیه می‌شود به‌سادگی در دسترس همگان قرار نداشته باشند.

۱۱-۱-۴ محافظت در برابر تهدیدهای محیطی و بیرونی

کنترل

توصیه می‌شود برای مقابله با فاجعه طبیعی، حملات مخرب یا سوانح، حفاظت فیزیکی طراحی و به کار گرفته شود.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های ویژه‌ای برای اجتناب از آسیب در برابر آتش‌سوزی، سیل، زلزله، انفجار، شورش، شکل‌های دیگر بلایای طبیعی یا انسانی به کار گرفته شود.

۱۱-۱-۵ کار در نواحی امن

کنترل

توصیه می‌شود، برای کار در نواحی امن، روش‌های اجرایی طراحی و به کار گرفته شود.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر مدنظر قرار گیرند:

الف- توصیه می‌شود کارکنان فقط در صورت لزوم، از وجود یا فعالیت‌های نواحی امن بر اساس اصل نیاز به دانستن مطلع شوند؛

ب- توصیه می‌شود از کار کردن بدون نظارت در نواحی امن به دلایل امنیتی و به‌منظور پیشگیری از فرصت انجام اقدامات خرابکارانه اجتناب شود؛

پ- توصیه می‌شود، مناطق امن خالی به‌صورت فیزیکی قفل‌شده و به‌صورت دوره‌ای بازنگری شود؛

ت- توصیه می‌شود تجهیزات عکس‌برداری، فیلم‌برداری، ضبط‌صوت یا دیگر تجهیزات ضبط کننده نظیر دوربین افزاره‌های سیار، اجازه ورود نداشته باشند، مگر این‌که برای آن‌ها مجوز ورود صادر شود؛

توصیه می‌شود، ملاحظات مربوط به کار در نواحی امن شامل کنترل‌هایی برای کار کارکنان و کاربران طرف‌های بیرونی در نواحی امن، تهیه‌شده و پوشش‌دهنده کلیه فعالیت‌های انجام‌شده در نواحی امن شود.

۱۱-۱-۶ نواحی تحویل و بارگیری

کنترل

توصیه می‌شود، نقاط دسترسی از قبیل نواحی تحویل و بارگیری و سایر نقاطی که افراد غیرمجاز امکان ورود به محوطه رادارند، تحت کنترل قرارگرفته و در صورت امکان، برای جلوگیری از دسترسی غیرمجاز، از تسهیلات پردازش اطلاعات، مجزا شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر لحاظ شوند:

الف- توصیه می‌شود دسترسی به نواحی تحویل و بارگیری از خارج از ساختمان، محدود به اشخاص شناخته‌شده و مجاز باشد؛

ب- توصیه می‌شود منطقه تحویل و بارگیری به‌گونه‌ای طراحی شود که بتوان بدون دسترسی کارکنان تحویل به بخش‌های دیگر ساختمان، بار را تخلیه کرد؛

پ- توصیه می‌شود درب‌های خارجی نواحی تحویل و بارگیری، درزمانی که درب‌های داخلی باز می‌شوند امن شوند؛

ت- توصیه می‌شود مواد ورودی قبل از این‌که از منطقه تحویل و بارگیری به منطقه مورداستفاده انتقال داده شوند برای مواد منفجره، مواد شیمیایی و یا دیگر مواد خطرناک بررسی و بازرسی شوند؛

ث- توصیه می‌شود مواد ورودی مطابق با روش‌های اجرایی مدیریت دارایی، در زمان ورود به محل، ثبت شوند (به بند ۸ مراجعه شود)؛

ج- توصیه می‌شود محموله‌های ورودی و خروجی تا جایی که ممکن است، به‌صورت فیزیکی تفکیک‌شده باشند؛

چ- توصیه می‌شود مواد ورودی برای شواهدی از دست‌کاری در طی مسیر بازرسی شود. اگر چنین دست‌کاری‌هایی کشف شد باید فوراً به کارکنان امنیتی گزارش داده شود.

۱۱-۲ تجهیزات

قصد: پیشگیری از زیان، خرابی، سرقت یا به خطر افتادن دارایی‌ها و ایجاد وقفه در عملیات سازمان.

۱۱-۲-۱ استقرار و حفاظت تجهیزات

کنترل

توصیه می‌شود، تجهیزات به‌گونه‌ای مستقر و محافظت شوند تا مخاطرات ناشی از تهدیدها و خطرات محیطی و فرصت‌های دسترسی غیرمجاز، کاهش یابند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر برای محافظت از تجهیزات موردتوجه قرار گیرند:

الف- توصیه می‌شود تجهیزات به نحوی مستقر شوند که دسترسی غیرضروری به نواحی کاری به کمینه کاهش یابد؛

ب- توصیه می‌شود تجهیزات پردازش اطلاعات که با داده‌های حساس سروکار دارند، با زاویه دید محدود قرار گیرند تا مخاطرات رؤیت اطلاعات توسط اشخاص غیرمجاز در زمان استفاده کاهش یابد؛

پ- توصیه می‌شود تجهیزات ذخیره‌سازی برای اجتناب از دسترسی غیرمجاز محافظت شوند؛

ت- توصیه می شود اجزایی که به محافظت خاص نیاز دارند جدا از سایر اقلام قرار گیرند تا سطح کلی محافظت موردنیاز کاهش یابد؛

ث- توصیه می‌شود کنترل‌هایی برای کاهش مخاطرات تهدیدهای فیزیکی بالقوه مانند سرقت، آتش‌سوزی، انفجار، دود، آب (خرابی منبع آب)، گردوغبار، لرزش، تأثیرات شیمیایی، تداخل منابع برق، تداخل ارتباطات، تابش الکترومغناطیسی و خراب‌کاری اتخاذ شود؛

ج- توصیه می‌شود رهنمود منع خوردن، آشامیدن و سیگار کشیدن در نزدیکی تسهیلات پردازش اطلاعات تهیه شود؛

چ- توصیه می‌شود شرایط محیطی نظیر دما و رطوبت برای شرایطی که ممکن است تأثیر منفی بر استفاده از تجهیزات اطلاعات بگذارند پایش شوند؛

ح- توصیه می‌شود محافظت در برابر رعدوبرق در تمام ساختمان به کار رود و توصیه می‌شود فیلترهای حفاظت در برابر رعدوبرق در تمامی خطوط ارتباطی و برق ورودی لحاظ شود ؛

خ- توصیه می‌شود استفاده از روش‌های محافظت خاص، نظیر روکش‌های صفحه‌کلید، برای تجهیزات مورداستفاده در محیط‌های صنعتی در نظر گرفته شوند؛

د- توصیه می‌شود تجهیزاتی که اطلاعات محرمانه را پردازش می‌کنند محافظت شوند تا مخاطره نشت اطلاعات در اثر تابش الکترومغناطیسی کمینه شود.

۱۱-۲-۲ ابزارهای پشتیبانی[1]

کنترل

1- Supporting Utilities

توصیه می‌شود، تجهیزات در برابر قطع برق و سایر اختلالات ناشی از نقص‌های ابزارهای پشتیبان، محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود تمام ابزارهای پشتیبان (نظیر برق، مخابرات، منبع آب، گاز، فاضلاب، تهویه و هواسازی):

الف- منطبق با مشخصات تولیدکننده تجهیزات و الزامات قانونی محلی باشد؛

ب- به‌صورت منظم برای ظرفیت‌هایش، جهت لحاظ کردن رشد کسب‌وکار و تعامل با سایر ابزارهای پشتیبانی، ارزیابی شود؛

پ- به‌طور منظم برای اطمینان از عملکرد مناسب بازرسی و آزمون شود؛

ت- در صورت لزوم، برای تشخیص اختلال در عملکرد، هشدار دهی شود؛

ث- در صورت لزوم، تغذیه متعدد با مسیریابی فیزیکی متنوع را داشته باشد.

توصیه می‌شود روشنایی و ارتباطات اضطراری فراهم شود. سوئیچ اضطراری و دریچه برای قطع برق، آب، گاز و یا دیگر تأسیسات باید در نزدیکی خروجی اضطراری و یا اتاق‌های تجهیزات واقع‌شده باشد.

اطلاعات دیگر

افزونگی اضافی برای اتصال به شبکه را می‌توان با استفاده از مسیرهای متعدد به کمک بیش از یک ارائه‌دهنده ابزارها به دست آورد.

۱۱-۲-۳ امنیت کابل‌کشی

کنترل

توصیه می‌شود، کابل‌کشی‌های برق و ارتباطات مورداستفاده برای انتقال داده یا پشتیبانی از خدمات اطلاعاتی، در برابر قطع شدن، تداخل یا وارد آمدن خسارت محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر برای امنیت کابل‌کشی مدنظر قرار گیرند:

الف- توصیه می‌شود خطوط برق و مخابرات متصل به امکانات پردازش اطلاعات در صورت امکان از زیرزمین انتقال یابد یا از روش‌های مناسب دیگر از آن‌ها محافظت به عمل آید؛

ب- توصیه می‌شود کابل‌کشی برق، برای جلوگیری از تداخل از کابل‌کشی شبکه مجزا شود؛

پ- برای سامانه‌های حساس و حیاتی کنترل‌های بیشتری لحاظ شود که عبارت‌اند از:

۱- نصب مسیرهای دارای حفاظ یا اتاق‌ها یا جعبه‌های قفل‌شده در نقاط بازرسی و نقاط انتهایی؛
۲- استفاده از محافظ‌های تداخل الکترومغناطیسی برای محافظت از کابل‌ها؛

۳- آغاز بررسی‌های فنی و بازرسی فیزیکی برای یافتن تجهیزاتی که به‌صورت غیرمجاز به کابل‌ها وصل شده‌اند؛

۴- دسترسی کنترل‌شده به پنل‌های اتصال و اتاق‌های اتصالات کابل‌ها.

۱۱-۲-۴ نگهداری تجهیزات

کنترل

توصیه می‌شود، تجهیزات به‌منظور حصول اطمینان از تداوم دسترس‌پذیری و یکپارچگی‌شان، به‌درستی نگهداری شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر برای نگهداری از تجهیزات در نظر گرفته شود:

الف- توصیه می‌شود تجهیزات مطابق با فواصل زمانی و مشخصات فنی پیشنهادی تأمین‌کننده نگهداری شوند؛

ب- تعمیر و نگهداری تجهیزات باید فقط توسط کارکنان مجاز بخش نگهداری انجام شود؛

پ- توصیه می‌شود گزارش‌هایی از سوابقی از تمام خطاهای واقعی یا مشکوک و تمامی اقدامات نگهداری اصلاحی و پیشگیرانه نگهداری شود؛

ت- توصیه می‌شود کنترل‌های مناسب در زمان برنامه‌ریزی‌شده برای تعمیر و نگهداری تجهیزات اجرا شود و به این مسئله توجه شود که آیا این تعمیر و نگهداری توسط کارکنان در داخل یا خارج از سازمان انجام می‌شود؛ همچنین در مواقع لازم، توصیه می‌شود اطلاعات محرمانه از تجهیزات پاک شود، یا کارکنان تعمیر و نگهداری تجهیزات بازرسی بدنی شوند؛

ث- توصیه می‌شود تمام تعهدات قیدشده در بیمه‌نامه‌ها رعایت شوند؛

ج- قبل از قرار دادن تجهیزات جهت بهره‌برداری و پس از تعمیر و نگهداری آن، برای حصول اطمینان از اینکه تجهیزات دست‌کاری نشده و دارای نقص نیست بازرسی شود.

۱۱-۲-۵ خروج دارایی

کنترل

توصیه می‌شود، تجهیزات، اطلاعات یا نرم‌افزار، بدون مجوز قبلی، از محوطه خارج نشوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر در نظر گرفته شوند:

الف- توصیه می‌شود کارکنان و کاربران طرف بیرونی که مجاز هستند اجازه خروج اموال را صادر کنند، مشخص شوند؛

ب- توصیه می‌شود محدودیت‌های زمانی برای بازگرداندن دارایی‌ها تعیین و تاریخ بازگشت جهت انطباق بررسی شود؛

پ- توصیه می‌شود در صورت امکان و لزوم، دارایی‌ها در زمان خروج و بازگشت ثبت شوند؛

ت- توصیه می‌شود، هویت، نقش و وابستگی هر فردی که دارایی را اداره یا از آن استفاده می‌کند مستند شود و این مستندات با تجهیزات، اطلاعات و یا نرم‌افزار برگشت داده شود؛

اطلاعات دیگر

بازدیدهای سریع محلی که عهده‌دار آشکار کردن خروج غیرمجاز اموال است، ممکن است برای آشکار کردن تجهیزات ضبط غیرمجاز، سلاح و غیره نیز به عمل آید و از ورود آن‌ها به سایت جلوگیری شود. چنین بازدیدهای سریع محلی توصیه می‌شود منطبق با ضوابط و قوانین باشد. توصیه می‌شود افراد از وجود چنین بازدیدهای سریع محلی آگاه بوده و توصیه می‌شود درستی‌سنجی با مجوز دهی متناسب با نیازهای قانونی و حقوقی منطبق صورت پذیرد.

۱۱-۲-۶ امنیت تجهیزات خارج از محوطه[1]

کنترل

توصیه می‌شود، برای دارایی‌های خارج از محوطه، با توجه به مخاطرات مختلف ناشی از انجام کار در خارج از مرز فیزیکی سازمان، امنیت برقرار شود.

راهنمای پیاده‌سازی

توصیه می‌شود مجوز استفاده از تجهیزات ذخیره و پردازش اطلاعات در خارج از محوطه سازمان توسط مدیریت صادر شود. این موضوع در مورد تجهیزات متعلق به سازمان و تجهیزات با مالکیت شخصی که مورداستفاده سازمان است، انجام شود.

توصیه می‌شود راهنمایی‌های زیر برای محافظت از تجهیزات خارج از سازمان رعایت شوند:

الف- توصیه می‌شود تجهیزات و رسانه‌هایی که به خارج از محوطه سازمان برده می‌شوند بدون حضور مراقب در محل‌های عمومی رها نشوند؛

ب- توصیه می‌شود دستورالعمل‌های تولیدکننده همواره برای محافظت از تجهیزات موردتوجه قرار گیرد؛ مثلاً محافظت در برابر قرار گرفتن در معرض میدان‌های الکترومغناطیسی قوی؛

پ- توصیه می‌شود کنترل‌های مربوط به مکان‌های خارج از محوطه به‌عنوان‌مثال کار در خانه، دورکاری و سایت‌های موقت توسط ارزیابی مخاطرات مرتبط تهیه و در زمان مناسب اعمال شوند؛ مثلاً قفسه‌ها بایگانی

1- Premises

قابل قفل شدن، خط‌مشی میز پاک، کنترل دسترسی به رایانه‌ها و ارتباط امن با شبکه سازمان (به استاندارد ISO/IEC 27033 [۱۵]، [۱۶]، [۱۷]، [۱۸]، [۱۹] مراجعه شود)؛

ت- هنگامی‌که تجهیزات در میان افراد مختلف و/یا طرف‌های بیرونی منتقل می‌شود، توصیه می‌شود سوابقی نگهداری شود که در آن زنجیره‌ای از مسئولیت‌ها تعریف شود به‌گونه‌ای که کمینه، نام‌ها و سازمان‌هایی که مسئول تجهیزات می‌باشند را شامل شود.

مخاطرات مانند خرابی، سرقت یا شنود ممکن است بین محل‌های مختلف متفاوت باشد و بنابراین توصیه می‌شود مناسب‌ترین کنترل‌ها مورداستفاده قرار گیرد.

اطلاعات دیگر

تجهیزات ذخیره‌سازی و پردازش اطلاعات شامل انواع رایانه‌های شخصی، سازمان دهنده‌ها، تلفن‌های همراه، کارت‌های هوشمند، کاغذ یا سایر شکل‌هایی که برای کار در خانه یا انتقال به سایر نقاط دور از محل کار استفاده می‌شوند، است.

اطلاعات بیشتر درباره جنبه‌های دیگر محافظت از تجهیزات سیّار را می‌توانید دربند ۶-۲ پیدا کنید.

ممکن است برای اجتناب از مخاطره، کارکنان خاص را از کار کردن بیرون سایت بر حذر داشت یا استفاده از تجهیزات قابل‌حمل فناوری اطلاعات را محدود کرد.

۱۱-۲-۷ امحاء یا استفاده مجدد امن از تجهیزات

کنترل

توصیه می‌شود، تمام اجزای تجهیزاتی که دارای رسانهٔ ذخیره‌سازی می‌باشند، به‌منظور حصول اطمینان از اینکه هر داده حساس و نرم‌افزار مجاز، پیش از امحاء یا استفاده مجدد، حذف یا به شیوه امنی بازنویسی شده، بررسی شود.

راهنمای پیاده‌سازی

توصیه می‌شود، تجهیزات برای اطمینان از اینکه آیا دارای رسانه‌های ذخیره‌سازی هست یا خیر، قبل از امحاء یا استفاده مجدد بررسی شوند.

پیش از امحا دستگاه‌هایی که حاوی اطلاعات محرمانه یا دارای حق نشر هستند، توصیه می‌شود به‌جای استفاده از عملکرد استاندارد «حذف کردن» یا «قالب‌بندی»، آن‌ها ازنظر فیزیکی تخریب شوند یا اطلاعات روی آن‌ها توسط روش‌هایی خراب، پاک یا حذف شود تا اطلاعات اصلی غیرقابل‌بازیابی باشد.

اطلاعات دیگر

تجهیز آسیب‌دیده که حاوی رسانه ذخیره‌سازی است نیازمند ارزیابی مخاطرات است تا عناصری که توصیه می‌شود به‌جای اینکه جهت تعمیر یا دور انداختن ارسال شود به‌صورت فیزیکی امحاء شوند، تعیین شود. اطلاعات ممکن است به‌واسطه امحاء با دقت ناکافی یا استفاده مجدد از تجهیز به خطر بیافتند. علاوه بر این

برای پاک کردن امن دیسک، زمانی که تجهیز، امحا یا مجدداً مستقر شود، رمزگذاری کامل دیسک، مخاطرات افشای اطلاعات محرمانه را کاهش می‌دهد مشروط بر اینکه:

الف- فرآیند رمزگذاری به‌اندازه کافی قوی و پوشش‌دهنده تمام دیسک باشد (ازجمله فضای باقیمانده استفاده‌نشده[1]، فایل‌های مبادله و مانند آن)؛

ب- کلیدهای رمزگذاری به‌اندازه کافی طولانی باشد که در برابر حملات جستجوی فراگیر[2] مقاومت کند؛

پ- از خود کلیدهای رمزگذاری به‌صورت محرمانه نگهداری شود (به‌عنوان‌مثال هرگز بر روی همان دیسک ذخیره نشود).

برای توصیه‌های بیشتر در مورد رمزگذاری، به بند ۱۰ مراجعه شود.

فنون رونویسی[3] امن رسانه‌های ذخیره‌سازی با توجه به فناوری رسانه‌های ذخیره‌سازی متفاوت است. توصیه می‌شود، ابزار رونویسی برای حصول اطمینان از اینکه قابل به‌کارگیری در فناوری رسانه است، بازنگری شود.

۱۱-۲-۸ تجهیزات بدون مراقبت کاربر

کنترل

توصیه می‌شود، کاربران اطمینان داشته باشند که تجهیزات بدون مراقبت، حفاظت مناسبی دارند.

راهنمای پیاده‌سازی

توصیه می‌شود تمام کاربران از الزامات امنیتی و روش‌های اجرایی محافظت از تجهیزات بدون مراقبت و نیز مسئولیتشان برای اجرای این محافظت آگاه شوند. توصیه می‌شود به کاربران توصیه شود که:

الف- نشست‌های فعال پس از پایان یافتن، به خاتمه برسانند مگر این‌که بتوان آن‌ها را از طریق یک سازوکار قفل مناسب مانند یک برنامه محافظ صفحه‌نمایش رمزدار محافظت کرد؛

ب- از برنامه‌های کاربردی و خدمات شبکه درزمانی که نیاز نیستند، خارج شوند؛

پ- رایانه‌ها یا افزارهای قابل‌حمل توسط قفل کلیددار یا کنترل معادل، مانند دسترسی توسط کلمه عبور درزمانی که در حال استفاده نیست، از استفاده غیرمجاز محافظت شوند.

۱۱-۲-۹ خط‌مشی میز پاک و صفحه پاک

کنترل

توصیه می‌شود، یک خط‌مشی میز پاک برای کاغذها و محیط‌های ذخیره‌سازی قابل‌جابه‌جایی و یک خط-مشی صفحه پاک برای تسهیلات پردازش اطلاعات، به کار گرفته شود.

---

1 - Slack
2 - Brute Force
3 - Overwrite

راهنمای پیاده‌سازی

توصیه می‌شود در خط‌مشی میز پاک و صفحه پاک، طبقه‌بندی اطلاعات (به بند ۸-۲ مراجعه شود)، الزامات قانونی و قراردادی (به بند ۱۸-۱ مراجعه شود) و مخاطرات مشابه و جنبه‌های فرهنگی سازمان در نظر گرفته شود. توصیه می‌شود راهنمایی‌های زیر مدنظر قرار گیرد:

الف- توصیه می‌شود اطلاعات کسب‌وکار حیاتی یا حساس، برای مثال روی کاغذ یا رسانه ذخیره‌سازی الکترونیکی، وقتی‌که به آن‌ها نیاز نیست در جای امن گذاشته‌شده و در اتاق قفل شود (به‌طور آرمانی در یک گاوصندوق یا قفسه یا سایر شکل‌های وسایل حفاظتی)، مخصوصاً وقتی‌که اداره تخلیه‌شده است؛

ب- توصیه می‌شود رایانه‌ها و پایانه‌ها زمانی که بدون بهره‌بردار هستند، در حالت خروج از سامانه[1]، باقی‌مانده یا با یک سازوکار قفل صفحه‌کلید و صفحه‌نمایش که با کلمه عبور، کلمه رمز یا سازوکار مشابهی برای احراز اصالت کاربر، کنترل می‌شود، حفاظت شوند و توصیه می‌شود با قفل رمزی، کلمه عبور یا سایر کنترل‌ها وقتی‌که مورداستفاده نیستند، محافظت شوند؛

پ- توصیه می‌شود از استفاده غیرمجاز از تجهیزات نسخه‌برداری و سایر فناوری‌های تکثیر (مثلاً اسکنرها، دوربین‌های عکاسی) جلوگیری شود؛

ت- توصیه می‌شود مدارک حاوی اطلاعات طبقه‌بندی‌شده و حساس سریعاً از چاپگرها برداشته شوند.

اطلاعات دیگر

یک خط‌مشی میز پاک/صفحه پاک مخاطرات دسترسی غیرمجاز، از دست دادن، یا آسیب به اطلاعات در حین و خارج از ساعات کاری عادی را کاهش می‌دهد. همچنین گاوصندوق‌ها یا سایر انواع تسهیلات نگهداری امن ممکن است از اطلاعات نگهداری شده در آن‌ها در برابر بلاهایی مانند آتش، زمین‌لرزه، سیل یا انفجار حفاظت کنند.

در نظر بگیرید استفاده از چاپگر با پین کد شخصی عمل کند، بنابراین درخواست دهنده چاپ، تنها کسی است که می‌تواند چاپ را دریافت کند و تنها درزمانی که در کنار چاپگر ایستاده است.

۱۲ امنیت عملیات

۱-۱۲ مسئولیت‌ها و روش‌های اجرایی عملیاتی

قصد: حصول اطمینان از کارکرد صحیح و امن تسهیلات پردازش اطلاعات.

۱-۱-۱۲ روش‌های اجرایی عملیاتی مستند

کنترل

1 - Logged of

توصیه می‌شود، روش‌های اجرایی عملیاتی، مستند شده و در دسترس تمام کاربرانی که به آن‌ها نیاز دارند قرار بگیرد.

راهنمای پیاده‌سازی

توصیه می‌شود روش‌های اجرایی مستند برای فعالیت‌های عملیاتی مرتبط با تسهیلات پردازش اطلاعات و ارتباطات مانند روش‌های اجرایی روشن و خاموش کردن رایانه‌ها، تهیه فایل پشتیبان، نگهداری از تجهیزات، اداره کردن رسانه، اتاق رایانه و مدیریت رسیدگی به نامه و ایمنی تهیه شود.

توصیه می‌شود روش‌های اجرایی، دستورالعمل‌های عملیاتی را مشخص کنند ازجمله:

الف- نصب و پیکربندی سامانه‌ها؛

ب- پردازش و ساماندهی اطلاعات به دو صورت خودکار و دستی؛

پ- تهیه فایل‌های پشتیبان (به بند ۱۲-۳ مراجعه شود)؛

ت- الزامات زمان‌بندی ازجمله وابستگی‌های متقابل با سامانه‌های دیگر، اولین زمان شروع و آخرین زمان تکمیل کار؛

ث- دستورالعمل‌هایی برای رسیدگی به خطاها یا دیگر شرایط استثنایی که ممکن است در طول اجرای کار رخ دهد ازجمله محدودیت‌های استفاده از ابزارهای سامانه‌ها (به بند ۹-۴-۴ مراجعه شود)؛

ج- راه‌های ارتباطی با کارکنان پشتیانی و سرپرستان شامل شماره تماس‌های پشتیبانی‌کنندگان بیرونی در صورت بروز مشکلات پیش‌بینی‌نشده فنی و عملیاتی؛

چ- دستورالعمل‌های ویژه خروج و اداره کردن رسانه‌ها نظیر استفاده از محل خاص یا مدیریت خروجی‌های محرمانه شامل روش‌های اجرایی برای امحای امن خروجی کارهای ناموفق (به بندهای ۸-۳ و ۱۱-۲-۷ مراجعه شود)؛

ح- آغاز مجدد[1] سامانه و روش‌های اجرایی بازیابی برای استفاده در صورت ناموفق بودن سیستم؛

خ- مدیریت رد ممیزی سامانه و اطلاعات ثبت‌شده وقایع (به بند ۱۲-۴ مراجعه شود)؛

د- روش‌های اجرایی پایش.

توصیه می‌شود روش‌های اجرایی عملیاتی و روش‌های اجرایی مستند برای فعالیت‌های سامانه به‌عنوان اسناد رسمی در نظر گرفته شوند و تغییرات آن‌ها فقط با مجوز مدیریت انجام شود. هر زمان که ازنظر فنی امکان-پذیر باشد، توصیه می‌شود سامانه‌های اطلاعات با استفاده از روش‌های اجرایی، ابزارها و برنامه‌های کمکی، یکسان و به‌صورت سازگار مدیریت شوند.

1- restart

۱۲-۱-۲ مدیریت تغییر

کنترل

توصیه می‌شود، تغییرات در سازمان، فرآیند کسب‌وکار، تسهیلات و سامانه‌های پردازش اطلاعات که بر امنیت اطلاعات تأثیر دارد تحت کنترل باشد.

راهنمای پیاده‌سازی

توصیه می‌شود موارد زیر به‌صورت خاص، مدنظر قرار گیرد:

الف- شناسایی و ثبت تغییرات قابل‌توجه؛

ب- طرح‌ریزی و آزمون تغییرات؛

پ- ارزیابی تأثیرات بالقوه، شامل تأثیرات امنیت اطلاعات این تغییرات؛

ت- روش‌های اجرایی تأیید رسمی برای تغییرات پیشنهادی؛

ث- درستی‌سنجی اینکه الزامات امنیت اطلاعات محقق شده‌اند؛

ج- برقراری ارتباط در مورد جزییات تغییر با همه افراد مرتبط؛

چ- روش‌های اجرایی بازگشتی شامل روش‌های اجرایی و مسئولیت‌های توقف و بازیابی سامانه به دلیل تغییرات ناموفق و رویدادهای پیش‌بینی‌نشده؛

ح- تأمین فرایند تغییر اضطراری جهت فعال کردن سریع و کنترل‌شده پیاده‌سازی تغییرات موردنیاز برای رفع کردن یک رخداد (به بند ۱۶-۱ مراجعه شود).

توصیه می‌شود مسئولیت‌ها و روش‌های اجرایی مدیریتی رسمی برای تضمین کنترل رضایت‌بخش تمام تغییرات ایجاد شود. زمانی که تغییرات انجام شد، توصیه می‌شود اطلاعات ثبت‌شده ممیزی حاوی تمامی اطلاعات مرتبط، حفظ شود.

اطلاعات دیگر

کنترل ناکافی تغییرات در تسهیلات و سامانه‌های پردازش اطلاعات، یکی از دلایل متداول عدم موفقیت سیستم یا امنیت است. تغییرات محیط عملیاتی، به‌خصوص در زمان انتقال یک سامانه از مرحله توسعه به مرحله عملیاتی، می‌تواند بر قابلیت اطمینان برنامه‌های کاربردی تأثیر بگذارد (همچنین به بند ۱۴-۲-۲ مراجعه شود).

۱۲-۱-۳ مدیریت ظرفیت

کنترل

توصیه می‌شود استفاده از منابع پایش، تنظیم‌شده و پیش‌بینی نیازمندی‌های ظرفیت آینده انجام شود تا از عملکرد موردنیاز سیستم اطمینان حاصل شود.

راهنمای پیاده‌سازی

توصیه می‌شود الزامات ظرفیت با توجه به حساسیت کسب‌وکاری سامانه موردنظر، شناسایی شود. توصیه می‌شود سامانه‌ها تنظیم و پایش شوند تا از تداوم عملکرد و مطلوبیت کارایی آن‌ها در هنگام نیاز، اطمینان حاصل شود و در صورت لزوم بهبود یابد. توصیه می‌شود از کنترل‌های تشخیصی استفاده شود تا مشکلات در زمان مقرر نمایان شوند. توصیه می‌شود پیش‌بینی الزامات ظرفیتی آینده، الزامات کسب‌وکار و سامانه‌ای جدید و روندهای جاری و پیش‌بینی‌شده را در قابلیت‌های پردازش اطلاعات سازمان در نظر بگیرند.

توصیه می‌شود، توجه خاصی به منابعی که زمان طولانی یا هزینه بالایی جهت تهیه دارند، شود؛ بنابراین توصیه می‌شود مدیران نحوه استفاده از منابع کلیدی سامانه‌ها را پایش کنند. توصیه می‌شود آن‌ها روند استفاده را به‌خصوص در رابطه با نرم‌افزارهای کاربردی کسب‌وکار یا ابزارهای مدیریت سامانه‌های اطلاعاتی، شناسایی کنند.

توصیه می‌شود مدیران از این اطلاعات برای شناسایی و اجتناب از تنگناهای احتمالی و وابستگی به کارکنان کلیدی که ممکن است برای امنیت سامانه‌ها یا خدمات تهدید به‌حساب آیند استفاده کرده و اقدامات مناسب را برنامه‌ریزی کنند.

تأمین ظرفیت کافی را می‌توان با افزایش ظرفیت و یا با کاهش تقاضا به دست آورد. نمونه‌هایی از مدیریت تقاضای ظرفیت عبارت‌اند از:

الف- حذف داده‌های منسوخ (فضای دیسک)؛

ب- کنار گذاشتن برنامه‌های کاربردی، سامانه‌ها، پایگاه‌های داده یا محیط‌ها؛

پ- بهینه‌سازی فرآیندهای دسته‌ای و زمان‌بندی‌ها؛

ت- بهینه‌سازی منطق برنامه و یا پرس و جوی‌های پایگاه داده؛

ث- نپذیرفتن و یا محدود کردن پهنای باند برای خدماتی که به منابع زیادی نیاز دارند، اگر برای کسب‌وکار بحرانی نیست (به‌عنوان‌مثال جریان تصویر[1]).

توصیه می‌شود، طرح مدیریت ظرفیت مستند برای سامانه‌هایی که برای مأموریت سازمان حساس هستند در نظر گرفته شود.

اطلاعات دیگر

این کنترل همچنین ظرفیت منابع انسانی، دفاتر و تسهیلات را نیز پوشش می‌دهد.

1 - video

۱۲-۱-۴ جداسازی محیط توسعه، آزمون و عملیاتی

کنترل

توصیه می‌شود، محیط‌های توسعه، آزمون و عملیاتی، به‌منظور کاهش مخاطرات ناشی از دسترسی غیرمجاز یا تغییرات در محیط‌های عملیاتی، تفکیک شوند.

راهنمای پیاده‌سازی

توصیه می‌شود سطح تفکیک بین محیط‌های عملیاتی، آزمون و درحال‌توسعه که برای پیشگیری از مشکلات عملیاتی لازم است، شناسایی و مستقر شود.

توصیه می‌شود موارد زیر مدنظر قرار گیرد:

الف- توصیه می‌شود قواعد انتقال نرم‌افزار از حالت توسعه به حالت عملیاتی، تعریف و مستند شود؛

ب- توصیه می‌شود نرم‌افزارهای در حال توسعه و عملیاتی، بر روی سامانه‌ها و پردازشگرهای رایانه‌ای مختلف و در دامنه‌ها و پوشه‌های مختلف اجرا شوند؛

پ- توصیه می‌شود تغییرات در سامانه‌های عملیاتی و برنامه‌های کاربردی در یک محیط آزمایشی یا تمرینی، قبل از اینکه به سامانه‌های عملیاتی اعمال شود، آزمون شود؛

ت- توصیه می‌شود آزمون در سامانه‌های عملیاتی انجام نشود، مگر در موارد استثناء؛

ث- توصیه می‌شود مترجم‌ها، ویرایشگرها و دیگر ابزارهای توسعه یا برنامه‌های کمکی سامانه‌ای، از سامانه‌های عملیاتی، در مواقع غیرضروری قابل‌دسترسی نباشند؛

ج- توصیه می‌شود کاربران از رخ‌نماهای کاربری متفاوتی برای کار در سامانه‌های تحت آزمون و عملیاتی استفاده کنند و توصیه می‌شود که گزینگانی، پیغام‌های شناسایی مناسب برای کاهش مخاطرات خطا، نمایش دهند؛

چ- توصیه می‌شود داده‌های حساس، به محیط سیستم آزمون منتقل نشوند، مگر اینکه کنترل‌های معادلی برای سیستم آزمون تهیه‌شده باشد (به بند ۱۴-۳ مراجعه شود).

اطلاعات دیگر

فعالیت‌های آزمون و توسعه می‌توانند باعث بروز مشکلات جدی، مانند اصلاح ناخواسته‌ی فایل‌ها یا محیط سامانه و یا خرابی سامانه شوند. نیاز است که محیط شناخته‌شده و پایداری حفظ شود که در آن، آزمون معنادار انجام شود و مانع از دسترسی نامناسب توسعه‌دهندگان به سامانه‌های عملیاتی شود.

درجایی که کارکنان توسعه و آزمون، به سامانه‌های عملیاتی و اطلاعات آن دسترسی دارند، ممکن است آن‌ها قادر به واردکردن کد غیرمجاز و آزمون نشده باشند یا داده‌های عملیاتی را تغییر دهند. در بعضی از سامانه‌ها، به‌واسطه سوءاستفاده از این قابلیت ممکن است، تقلب شود، یا کد غیرمجاز یا مخرب وارد شود که ممکن است باعث مشکلات عملیاتی مهمی شود.

کارکنان توسعه و آزمون سامانه‌ها، یک تهدید برای محرمانگی اطلاعات سامانه‌های عملیاتی به‌حساب می‌آیند. اگر فعالیت‌های توسعه و آزمون سامانه‌ها در محیط محاسباتی مشترکی انجام شود، ممکن است باعث تغییرات ناخواسته‌ای برای نرم‌افزار یا اطلاعات بشود؛ بنابراین تفکیک محیط‌های عملیاتی، توسعه و آزمون، برای کاهش مخاطرات تغییرات تصادفی یا دسترسی غیرمجاز به نرم‌افزار عملیاتی و داده‌های کسب‌وکار، مطلوب است (برای حفاظت از داده‌های آزمون، به بند ۱۴-۳ مراجعه شود).

۱۲-۲ حفاظت در برابر بدافزار

قصد: حصول اطمینان از محافظت از اطلاعات و تسهیلات پردازش اطلاعات در برابر بدافزار.

۱۲-۲-۱ کنترل‌هایی در برابر بدافزار

کنترل

توصیه می‌شود، کنترل‌های لازم برای تشخیص، پیشگیری و ترمیم به‌منظور محافظت در برابر بدافزار، همراه با آگاه‌سازی مناسب کاربر پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود حفاظت در مقابل بدافزار بر اساس نرم‌افزار تشخیص بدافزار و نرم‌افزار ترمیم گر، آگاهی‌های امنیت اطلاعات و کنترل‌های مناسب دسترسی و مدیریت تغییر سامانه، انجام شود. توصیه می‌شود راهنمایی-های زیر در نظر گرفته شود:

الف- استقرار یک خط‌مشی رسمی جهت منع استفاده از نرم‌افزارهای غیرمجاز (به بندهای ۱۲-۶-۲ و ۱۴-۲ مراجعه شود)؛

ب- پیاده‌سازی کنترل‌هایی که استفاده از نرم‌افزارهای غیرمجاز را پیشگیری کرده یا تشخیص می‌دهد (به‌عنوان‌مثال فهرست سفید برنامه‌های کاربردی)؛

پ- پیاده‌سازی کنترل‌هایی که استفاده از وب‌سایت‌های مخرب شناخته‌شده و یا مشکوک را پیشگیری کرده یا تشخیص می‌دهد (به‌عنوان‌مثال فهرست سیاه)؛

ت- استقرار یک خط‌مشی رسمی برای محافظت در برابر مخاطرات مرتبط با به دست آوردن فایل‌ها و نرم-افزار از طریق یا به‌واسطه شبکه‌های خارجی یا از هر رسانه دیگر که مشخص‌کننده اقدامات حفاظتی موردنیاز باشد؛

ث- کاهش آسیب‌پذیری که می‌تواند توسط بدافزار مورد سوءاستفاده قرار گیرد، به‌عنوان‌مثال از طریق مدیریت آسیب‌پذیری‌های فنی (به بند ۱۲-۶ مراجعه شود)؛

ج- انجام منظم بازنگری نرم‌افزار و محتوای داده‌های سامانه‌های پشتیبانی‌کننده فرایندهای بحرانی کسب‌وکار؛ وجود هرگونه فایل تأیید نشده و یا اصلاحیه‌های غیرمجاز باید به‌صورت رسمی بررسی شود؛

چ- نصب و به‌روزآوری منظم نرم‌افزار تشخیص و ترمیم بدافزار برای پویش رایانه‌ها و رسانه به‌عنوان یک کنترل احتیاطی یا بر اساس یک‌روال منظم. توصیه می‌شود پایش انجام‌شده، شامل موارد زیر باشد:

۱- پویش هر فایل دریافت شده از شبکه‌ها یا از طریق هر نوع رسانه ذخیره‌سازی، جهت بدافزار قبل از استفاده؛

۲- پویش فایل‌های پیوست رایانامه‌ها و دانلودها جهت بدافزار قبل از استفاده. توصیه می‌شود این پویش در مکان‌های مختلف انجام شود، به‌عنوان‌مثال در کارساز[1] های رایانامه، رایانه‌های رومیزی و در زمان ورود به شبکه سازمان؛

۳- پویش صفحات وب برای بدافزار؛

ح- تعریف روش‌های اجرایی و مسئولیت‌ها جهت برخورد با بدافزار بر روی سامانه‌ها، آموزش استفاده از آن‌ها، گزارش دهی و ترمیم بعد از حملات بدافزار؛

خ- تهیه طرح‌های تداوم کسب‌وکار مناسب برای ترمیم بعد از حملات بدافزار، شامل تمام اطلاعات لازم و تمهیدات پشتیبان‌گیری و بازیابی نرم‌افزار (به بند ۱۲-۳ مراجعه شود)؛

د- پیاده‌سازی روش‌های اجرایی برای جمع‌آوری منظم اطلاعات، ازجمله عضویت در فهرست‌های پستی و یا وب‌سایت‌های تأییدکننده‌ی اطلاعات ارائه‌شده در مورد بدافزار جدید؛

ذ- پیاده‌سازی روش‌های اجرایی برای بررسی اینکه اطلاعات مربوط به بدافزارها بوده و خبرنامه‌های هشدار-دهنده دقیق و آموزنده هستند. توصیه می‌شود مدیران اطمینان حاصل کنند که منابع واجد شرایط، به‌عنوان‌مثال مجلات مشهور، سایت‌های اینترنتی قابل‌اطمینان، یا تأمین‌کنندگان نرم‌افزارهای حفاظت کننده در مقابل بدافزار، جهت متمایز کردن بدافزار غیرواقعی و واقعی مورداستفاده قرار می‌گیرند. توصیه می‌شود تمام کاربران از مشکل بدافزار غیرواقعی و آنچه در زمان دریافت آن‌ها انجام دهند، آگاه باشند.

ر- جدا کردن محیط‌ها درزمانی که ممکن است منجر به اثرات فاجعه‌بار شود.

اطلاعات دیگر

استفاده از دو یا چند محصول نرم‌افزاری محافظت در برابر بدافزار در محیط‌های پردازش اطلاعات، از شرکت-های متفاوت، ممکن است اثربخشی محافظت در مقابل بدافزار را بهبود دهد.

توصیه می‌شود مراقبت لازم برای محافظت در برابر ورود بدافزار در طی انجام روش‌های اجرایی نگهداری و برخورد با شرایط اضطراری انجام شود که ممکن است کنترل‌های معمول حفاظت در برابر بدافزار، کنار گذاشته شود.

تحت شرایط خاصی، حفاظت در مقابل بدافزار ممکن است باعث اختلال در عملیات شود.

1 - servers

استفاده از نرم‌افزارهای تشخیص و ترمیم بدافزار، معمولاً به‌تنهایی به‌عنوان یک کنترل برای بدافزار کافی نیستند و معمولاً نیاز است که با روش‌های اجرایی عملیاتی برای جلوگیری از ورود بدافزارها همراه شوند.

۱۲-۳ نسخه‌های پشتیبان

قصد: محافظت در برابر از دست دادن داده‌ها.

۱۲-۳-۱ ایجاد پشتیبان از اطلاعات

کنترل

توصیه می‌شود، نسخه‌های پشتیبان از اطلاعات، نرم‌افزارها و رونوشت‌های سامانه‌ها، با توجه به یک خط‌مشی توافق شدهٔ نسخه‌های پشتیبان، به‌صورت منظم تهیه و آزمایش شوند.

راهنمای پیاده‌سازی

توصیه می‌شود، خط‌مشی پشتیبان‌گیری به‌منظور تعریف الزامات سازمان برای تهیه پشتیبان از اطلاعات، نرم‌افزار و سامانه‌ها مستقر شود.

خط‌مشی پشتیبان‌گیری باید الزامات نگهداری و حفاظت را تعریف کند.

توصیه می‌شود تسهیلات کافی پشتیبان‌گیری فراهم شود تا اطمینان حاصل شود که تمام اطلاعات ضروری و نرم‌افزار را می‌توان پس از یک حادثه یا خرابی رسانه‌ها، بازیابی کرد.

توصیه می‌شود در زمان تهیه طرح پشتیبان از اطلاعات، موارد زیر در نظر گرفته شود:

الف- توصیه می‌شود سوابق دقیق و کامل از رونوشت‌های پشتیبان و روش‌های اجرایی مستند برای بازیابی آن‌ها تهیه شود؛

ب- توصیه می‌شود گستره (به‌عنوان‌مثال پشتیبان‌گیری کامل یا تفاضلی) و بسامد پشتیبان‌گیری، منعکس‌کننده الزامات کسب‌وکار سازمان، الزامات امنیت اطلاعات درگیر و حیاتی بودن اطلاعات برای تداوم عملیات سازمان باشد؛

پ- توصیه می‌شود پشتیبان‌ها در یک محل دور، بافاصله کافی، برای اجتناب از هرگونه آسیب ناشی از وقوع حادثه در سایت اصلی ذخیره شوند؛

ت- توصیه می‌شود اطلاعات پشتیبان دارای سطح مناسبی از محافظت فیزیکی و محیطی باشند که سازگار با استانداردهای به‌کاررفته در سایت اصلی باشد (به بند ۱۱ مراجعه شود)؛

ث- توصیه می‌شود رسانه‌های ذخیره‌سازی پشتیبان‌ها به‌طور منظم آزمایش شوند تا اطمینان حاصل شود که می‌توان برای استفاده اضطراری در زمان لازم به آن‌ها تکیه کرد. این آزمون باید با آزمون روش‌های اجرایی بازیابی ترکیب شود تا زمان موردنیاز برای بازیابی تعیین شود. توصیه می‌شود آزمودن توانایی بازگرداندن اطلاعات بر روی رسانه‌های آزمون اختصاص داده‌شده انجام شود و روی رسانه اصلی بازنویسی نشود که در

صورت شکست فرآیند پشتیبان‌گیری یا بازیابی، باعث ایجاد آسیب جبران‌ناپذیر به داده یا از دست دادن داده شود؛

ج- توصیه می‌شود در شرایطی که محرمانگی اهمیت دارد، فایل‌های پشتیبان با رمزگذاری محافظت شوند.

توصیه می‌شود، روش‌های اجرایی عملیاتی، پشتیبان‌گیری را پایش کرده و عدم موفقیت در پشتیبان‌گیری برنامه‌ریزی‌شده را پوشش دهد تا از کامل بودن پشتیبان‌گیری با توجه به خط‌مشی پشتیبان‌گیری اطمینان حاصل کند.

توصیه می‌شود تمهیدات پشتیبان‌گیری برای تک‌تک سامانه‌ها و خدمات به‌صورت منظم آزمایش شود تا تضمین شود که آن‌ها الزامات برنامه‌های استمرار کسب‌وکار را برآورده می‌سازند. توصیه می‌شود برای سامانه‌ها و خدمات حیاتی، تمهیدات پشتیبان‌گیری همه اطلاعات، برنامه‌های کاربردی و داده‌های موردنیاز که برای بازیابی کامل سیستم در صورت بروز حادثه به آن‌ها نیاز است را پوشش دهد.

توصیه می‌شود زمان نگهداری اطلاعات ضروری کسب‌وکار، با در نظر گرفتن هر الزامی که رونوشت‌های آرشیو برای همیشه نگهداری شود، تعیین شود.

۱۲-۴ واقعه‌نگاری و پایش

قصد: ثبت رویدادها و تولید شواهد.

۱۲-۴-۱ واقعه‌نگاری رویداد

کنترل

توصیه می‌شود، سوابق واقعه‌نگاری رویدادها شامل فعالیت‌های کاربر، استثناها، خطاها و رویدادهای امنیت اطلاعات، ایجاد، نگهداری و به‌طور منظم بازنگری شوند.

راهنمای پیاده‌سازی

توصیه می‌شود گزارش‌های واقعه‌نگاری در صورت مرتبط بودن، شامل موارد زیر باشند:

الف- شناسه کاربر؛

ب- فعالیت‌های سامانه؛

پ- تاریخ، زمان و جزییات وقایع کلیدی، مانند ورود و خروج از سامانه؛

پ- شناسه تجهیز یا محل آن در صورت امکان و شناسه سامانه؛

ت- سوابق مربوط به تلاش‌های موفق و غیر موفق برای دسترسی به داده‌ها و سایر منابع؛

ج- تغییرات در پیکربندی سامانه؛

چ- استفاده از حقوق دسترسی؛

ح- استفاده از برنامه‌های کاربردی و برنامه‌های کمکی سامانه؛

خ- فایل‌های مورد دسترسی و نوع دسترسی؛

د- آدرس‌های شبکه و پروتکل‌ها؛

ذ- هشدارهای ایجادشده توسط سامانه کنترل دسترسی؛

ر- فعال‌سازی و غیر فعال‌سازی سامانه‌های مراقبت نظیر سامانه‌های ضدبدافزار و سامانه‌های تشخیص نفوذ؛

ز - سوابق تراکنش‌های اجراشده توسط کاربران در برنامه‌های کاربردی.

واقعه‌نگاری رویداد، مبنایی برای پایش خودکاری که توانایی تولید هشدارها و گزارش‌های تلفیقی برای امنیت سامانه دارد، فراهم می‌کند.

اطلاعات دیگر

واقعه‌نگاری رویدادها می‌تواند حاوی داده‌های حساس و اطلاعات قابل‌شناسایی شخصی افراد باشد. توصیه می‌شود اقدامات مناسب برای محافظت از حریم شخصی به کار گرفته شود (به بند ۱۸-۱-۴ مراجعه شود). توصیه می‌شود در صورت امکان، سرپرستان سامانه، مجوز پاک کردن یا غیرفعال کردن وقایع فعالیت‌های خودشان را نداشته باشند (به بند ۱۲-۴-۳ مراجعه شود).

۱۲-۴-۲ حفاظت از اطلاعات ثبت‌شده وقایع

کنترل

توصیه می‌شود، تسهیلات واقعه‌نگاری و اطلاعات ثبت‌شدهٔ وقایع، در برابر دست‌کاری و دسترسی غیرمجاز، حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود هدف‌گذاری کنترل‌ها، برای محافظت در برابر تغییرات غیرمجاز اطلاعات واقعه‌نگاری و مشکلات عملیاتی تسهیلات واقعه‌نگاری شامل موارد زیر باشد:

الف- تغییرات در انواع پیام‌هایی که ثبت می‌شوند؛

ب- فایل‌های ثبت وقایع که ویرایش یا حذف شوند؛

پ- محدودیت در ظرفیت رسانه‌های ثبت وقایع که تکمیل آن، منجر به ناکامی در ثبت وقایع یا رونویسی وقایع ثبت‌شده درگذشته شود؛

بعضی از وقایع ممیزی ممکن است بر اساس خط‌مشی نگهداری سوابق یا به دلیل نیاز به جمع‌آوری و نگهداری شواهد، لازم باشد که نگهداری شود (به بند ۱۶-۱-۷ مراجعه شود).

اطلاعات دیگر

وقایع ثبت‌شده سامانه‌ها، اغلب حاوی حجم وسیعی از اطلاعات است که بسیاری از آن‌ها برای پایش امنیت اطلاعات، کاربردی ندارد. توصیه می‌شود برای کمک به شناسایی رویدادهای مهم برای اهداف پایش امنیت

اطلاعات، رونویسی خودکار پیام‌های مناسب به یک ثبت واقعه دوم، یا استفاده از ابزارهای مناسب کمکی سامانه یا ابزارهای ممیزی برای فایل، در نظر گرفته شود.

توصیه می‌شود وقایع سامانه، محافظت شود، زیرا اگر داده‌ها را بتوان تغییر داده یا حذف کرد، وجود آن‌ها ممکن است احساس نادرستی از امنیت ایجاد کند. رونویسی همزمان وقایع روی سامانه‌ای بیرون از کنترل سرپرست یا بهره‌بردار سامانه، می‌تواند برای حفاظت از وقایع استفاده شود.

۱۲-۴-۳ ثبت وقایع سرپرست و بهره‌بردار سیستم

کنترل

توصیه می‌شود، وقایع فعالیت‌های سرپرست و بهره‌بردار سیستم ثبت شود و این وقایع محافظت و به‌طور منظم بازنگری شود.

راهنمای پیاده‌سازی

دارندگان حساب‌های کاربری ویژه ممکن است قادر به دست‌کاری اطلاعات وقایع روی تسهیلات پردازش اطلاعات تحت کنترل مستقیم خود باشند، بنابراین لازم است حفاظت و بازنگری وقایع جهت حفظ پاسخگویی کاربران ویژه انجام شود.

اطلاعات دیگر

سامانه‌های تشخیص نفوذ که در خارج از کنترل مدیران شبکه و سامانه مدیریت می‌شوند، می‌توانند برای پایش سامانه و فعالیت‌های مدیر شبکه جهت انطباق استفاده شود.

۱۲-۴-۴ هم‌زمان‌سازی ساعت‌ها

کنترل

توصیه می‌شود، ساعت‌های تمامی سامانه‌های پردازش اطلاعات مرتبط در درون یک سازمان یا دامنه امنیتی، با یک منبع زمانی مرجع واحد، هم‌زمان شوند.

راهنمای پیاده‌سازی

توصیه می‌شود الزامات خارجی و داخلی برای نمایش زمان، هم‌زمان‌سازی و دقیق بودن، مستند شود. چنین الزاماتی می‌تواند قانونی، نظارتی، نیازمندی‌های قراردادی، انطباق با استاندارد یا الزامات موردنیاز برای پایش داخلی باشد. توصیه می‌شود زمان مرجع استاندارد برای استفاده درون سازمان تعریف شود.

توصیه می‌شود رویکرد سازمان برای به دست آوردن یک‌زمان مرجع از منبع (های) خارجی و چگونگی همگام‌سازی مطمئن ساعت داخلی، مستند و پیاده‌سازی شود.

اطلاعات دیگر

تنظیم صحیح ساعت رایانه‌ها برای تضمین دقت وقایع ممیزی مهم است و ممکن است برای تحقیقات یا به‌عنوان شواهد در دادگاه یا فرایند انضباطی لازم باشد. وقایع ممیزی غیردقیق، ممکن است مانع از این

بررسی‌ها شود و به اعتبار این شواهد خدشه وارد کند. ساعتی که با ساعت ارسال‌کننده رادیویی ساعت اتمی ملی، همزمان است، می‌تواند به‌عنوان ساعت اصلی برای سامانه‌های ثبت‌کننده استفاده شود. یک پروتکل زمان شبکه را می‌توان برای حفظ تمام کارسازها[1] به‌صورت همزمان با ساعت اصلی مورداستفاده قرارداد.

۱۲-۵ کنترل نرم‌افزارهای عملیاتی

قصد: حصول اطمینان از یکپارچگی سامانه‌های عملیاتی.

۱۲-۵-۱ نصب نرم‌افزار بر سامانه‌های عملیاتی

کنترل

توصیه می‌شود، به‌منظور کنترل نصب نرم‌افزار بر سامانه‌های عملیاتی، روش‌های اجرایی پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر برای کنترل تغییرات نرم‌افزار روی سامانه‌های عملیاتی در نظر گرفته شود:

الف- توصیه می‌شود روزآمدسازی نرم‌افزار عملیاتی، برنامه‌های کاربردی و کتابخانه‌های برنامه فقط توسط سرپرستان آموزش‌دیده پس از تأیید مدیریتی مناسب انجام شود (به بند ۹-۴-۵ مراجعه شود)؛

ب- توصیه می‌شود سامانه‌های عملیاتی فقط کد قابل‌اجرای تأییدشده را داشته باشند و نه کد توسعه‌یافته یا هم گردان‌ها را؛

پ- توصیه می‌شود برنامه‌های کاربردی و نرم‌افزار سامانه عامل فقط پس از آزمون گسترده و موفقیت‌آمیز مستقر شود؛ توصیه می‌شود آزمون‌ها شامل قابل‌استفاده بودن، امنیت، تأثیرات بر دیگر سامانه‌ها و مناسب بودن برای کاربر باشند و توصیه می‌شود روی سامانه‌های جداگانه انجام شوند (به بند ۱۲-۱-۴ مراجعه شود)؛ توصیه می‌شود تضمین شود که تمام کتابخانه‌های منبع برنامه متناظر روزآمد شده‌اند؛

ت- توصیه می‌شود از سیستم کنترل پیکربندی برای حفظ کنترل تمام نرم‌افزارهای مستقرشده و نیز مستندات سامانه استفاده شود؛

ث- توصیه می‌شود یک راهبرد برگشت به حالت اولیه[2]، قبل از پیاده‌سازی تغییرات وجود داشته باشد؛

ج- توصیه می‌شود وقایع ممیزی‌ها از تمام روزآمدسازی‌های کتابخانه‌های برنامه عملیاتی نگهداری شود؛

چ- توصیه می‌شود نسخه‌های قبلی نرم‌افزار کاربردی، به‌عنوان یک اقدام احتیاطی حفظ شود؛

ح- توصیه می‌شود نسخه‌های قدیمی نرم‌افزار، به همراه اطلاعات موردنیاز و پارامترها، روش‌های اجرایی، جزئیات پیکربندی و نرم‌افزار پشتیبانی برای مدت‌زمانی که داده‌ها در آرشیو نگهداری می‌شوند ذخیره شوند.

---

[1] Servers

2- rollback

توصیه می‌شود نرم‌افزارهای تأمین‌شده توسط فروشندگان که در سامانه‌های عملیاتی مورداستفاده قرارگرفته‌اند، در سطح پشتیبانی شده توسط تأمین‌کننده نگهداری شوند. باگذشت زمان، فروشندگان نرم‌افزار نسخه‌های قدیمی‌تر نرم‌افزار را پشتیبانی نمی‌کنند. توصیه می‌شود سازمان مخاطرات تکیه‌بر نرم‌افزار پشتیبانی نشده را در نظر بگیرد.

توصیه می‌شود هر تصمیمی برای روزآمدسازی به یک نسخه جدید، الزامات کسب‌وکار را برای تغییر و امنیت نسخه جدید به‌حساب آورد، به‌عنوان‌مثال، ورود یک کارایی جدید امنیتی یا تعداد و شدت مشکلات امنیتی که بر این نسخه تأثیر می‌گذارند. توصیه می‌شود وصله‌های نرم‌افزاری درزمانی که می‌توانند به از بین بردن یا کاهش ضعف‌های امنیتی اطلاعات کمک کنند به کار گرفته شوند (به بند ۱۲-۶ مراجعه شود).

توصیه می‌شود دسترسی فیزیکی یا منطقی فقط به تأمین‌کنندگان برای اهداف پشتیبانی در زمان لازم و با تأیید مدیریت داده شود. توصیه می‌شود فعالیت‌های تأمین‌کننده پایش شوند (به بند ۱۵-۲-۱ مراجعه شود).

نرم‌افزار رایانه‌ای ممکن است بر نرم‌افزار و پیمانه‌های تأمین‌شده از خارج تکیه داشته باشند که توصیه می‌شود برای اجتناب از تغییرات غیرمجاز که ممکن است ضعف‌های امنیتی ایجاد کند، پایش و کنترل شوند.

۱۲-۶ مدیریت آسیب‌پذیری فنی

قصد: جلوگیری از سوءاستفاده از آسیب‌پذیری‌های فنی.

۱۲-۶-۱ مدیریت آسیب‌پذیری‌های فنی

کنترل

توصیه می‌شود، اطلاعات در خصوص آسیب‌پذیری‌های فنی سامانه‌های اطلاعاتی مورداستفاده، به‌موقع کسب شود، قرار گرفتن سازمان در معرض چنین آسیب‌پذیری‌هایی ارزشیابی شود و اقدامات مناسبی برای مخاطرات مرتبط، اجرا شوند.

راهنمای پیاده‌سازی

یک فهرست موجودی به‌روز و کامل از دارایی‌ها (به بند ۸ مراجعه شود)، پیش‌نیاز مدیریت مؤثر آسیب‌پذیری فنی است. اطلاعات خاص موردنیاز برای پشتیبانی مدیریت آسیب‌پذیری فنی شامل فروشنده نرم‌افزار، شماره نسخه‌ها، وضعیت فعلی استقرار (برای مثال چه نرم‌افزاری روی چه سامانه‌ای نصب‌شده) و شخص (اشخاص) درگیر در سازمان که مسئول نرم‌افزار هستند، است.

توصیه می‌شود فعالیت مناسب و به‌موقع در پاسخ به شناسایی آسیب‌پذیری‌های فنی بالقوه صورت گیرد. توصیه می‌شود راهنمایی‌های زیر برای استقرار یک فرایند مدیریت مؤثر برای آسیب‌پذیری‌های فنی دنبال شوند:

الف- توصیه می‌شود سازمان نقش‌ها و مسئولیت‌های مربوط به مدیریت آسیب‌پذیری فنی ازجمله پایش آسیب‌پذیری، ارزیابی مخاطره آسیب‌پذیری، وصله کردن، ردیابی دارایی و هر هماهنگی موردنیاز را تعریف و ایجاد کند؛

ب- توصیه می‌شود منابع اطلاعات که برای شناسایی آسیب‌پذیری‌های فنی مرتبط و حفظ آگاهی درباره آن‌ها استفاده خواهد شد، برای نرم‌افزار و فن‌آوری دیگر شناسایی شود. (بر اساس فهرست موجودی دارایی‌ها، به بند ۸-۱-۱ مراجعه شود)؛ توصیه می‌شود این منابع اطلاعات بر اساس تغییرات در فهرست موجودی یا درزمانی که منابع جدید یا مفیدی پیدا می‌شوند، روزآمد شوند؛

پ- توصیه می‌شود برای واکنش به اعلان آسیب‌پذیری‌های فنی مرتبط، یک‌زمان بندی تعریف شود؛

ت- توصیه می‌شود به‌محض این‌که یک آسیب‌پذیری فنی بالقوه شناسایی شد، سازمان مخاطرات مرتبط و فعالیت‌های موردنیاز را شناسایی کند. این فعالیت‌ها می‌تواند شامل وصله کردن سیستم آسیب‌پذیر یا به‌کارگیری کنترل‌های دیگر باشد؛

ث- توصیه می‌شود برحسب این‌که یک آسیب‌پذیری فنی با چه فوریتی نیاز به رسیدگی دارد، فعالیت‌هایی مطابق با کنترل‌های مربوط به مدیریت تغییر (به بند ۱۲-۱-۲ مراجعه شود) یا با پیروی از روش‌های اجرایی واکنش به رخدادهای امنیتی اطلاعات انجام شوند (به بند ۱۶-۱-۵ مراجعه شود)؛

ج- توصیه می‌شود درصورتی‌که یک وصله از یک منبع مورداطمینان در دسترس قرارگرفته، مخاطرات مربوط به نصب وصله ارزیابی شود (توصیه می‌شود مخاطرات تحمیل‌شده به‌وسیله آسیب‌پذیری با مخاطرات نصب وصله مقایسه شود)؛

چ- توصیه می‌شود وصله‌ها قبل از این‌که نصب شوند، آزموده و ارزیابی شوند تا تضمین شود که آن‌ها مؤثر هستند و منجر به عوارض جانبی غیرقابل‌تحمل نمی‌شوند. توصیه می‌شود اگر هیچ وصله‌ای در دسترس نیست، کنترل‌های دیگر در نظر گرفته شود نظیر:

۱- متوقف کردن خدمات یا قابلیت‌های مربوط به آسیب‌پذیری؛
۲- منطبق کردن یا اضافه کردن کنترل‌های دسترسی مانند دیوارهای آتش، در مرزهای شبکه (به بند ۱۳-۱ مراجعه شود)؛
۳- افزایش پایش برای کشف حملات واقعی؛
۴- افزایش آگاهی از آسیب‌پذیری؛

ح- توصیه می‌شود وقایع ممیزی برای همه روش‌های اجرایی تحت مسئولیت، نگهداری شود؛

خ- توصیه می‌شود فرایند مدیریت آسیب‌پذیری فنی به‌صورت منظم پایش شود و به‌منظور اطمینان از کارایی و اثربخشی ارزشیابی شود؛

د- توصیه می‌شود سامانه‌هایی که مخاطرات بالایی دارند ابتدا مورد رسیدگی قرار گیرند؛

ذ- توصیه می‌شود فرایند مدیریت آسیب‌پذیری فنی مؤثر و هم‌راستا با فعالیت‌های مدیریت رخداد انجام شود تا تعامل داده‌های آسیب‌پذیری‌ها در اختیار واحد واکنش به رخداد داده‌شده و روش‌های اجرایی فنی که توصیه می‌شود در موقع رخداد انجام شود را فراهم کند؛

ر- روش اجرایی برای رسیدگی به وضعیتی که در آن‌یک آسیب‌پذیری شناسایی‌شده است اما هیچ راه تقابل مناسب وجود ندارد، تعریف شود. در این وضعیت توصیه می‌شود سازمان، مخاطرات مربوط به آسیب‌پذیری شناخته‌شده را ارزشیابی کرده و اقدام تشخیصی و اصلاحی مناسب را تعریف کند.

اطلاعات دیگر

مدیریت آسیب‌پذیری فنی را می‌توان به‌عنوان یک عملکرد فرعی مدیریت تغییر دانست و بدین ترتیب می‌تواند از مزیت فرایندها و روش‌های اجرایی مدیریت تغییر استفاده کند (به بندهای ۱۲-۱-۲ و ۱۴-۲-۲ مراجعه شود).

فروشندگان اغلب زیر فشار زیادی برای انتشار بسته‌ها در سریع‌ترین زمان ممکن قرار دارند. بنابراین، امکان دارد که یک وصله به‌صورت کافی یک مشکل را پوشش ندهد و تأثیرات جانبی منفی داشته باشد. همچنین در بعضی موارد، از نصب خارج کردن یک وصله ممکن است پس از نصب شدن وصله، به‌سادگی امکان‌پذیر نباشد.

اگر آزمون کافی از وصله‌ها ممکن نباشد، مثلاً به دلیل هزینه یا کمبود منابع، تأخیر در نصب وصله را می‌توان برای ارزشیابی مخاطرات مرتبط بر اساس تجربه گزارش‌شده توسط کاربران دیگر در نظر گرفت. استفاده از ISO/IEC 27031 [۱۴] می‌تواند مفید باشد.

۱۲-۶-۲ محدودسازی در نصب نرم‌افزار

کنترل

توصیه می‌شود، قواعدی حاکم بر نصب نرم‌افزار توسط کاربر، ایجاد و پیاده‌سازی شود.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان، خط‌مشی سخت‌گیرانه در مورد انواع نرم‌افزارهایی که توسط کاربران نصب می‌شوند، تعریف و اجبار کند.

توصیه می‌شود اصل کمینه سطح دسترسی اعمال شود. اگر دسترسی‌های خاصی اعطا شود، کاربران ممکن است توانایی نصب نرم‌افزار را داشته باشند. توصیه می‌شود، سازمان مشخص کند چه نوع نصب‌هایی از نرم-افزار دارای مجوز است (به‌عنوان‌مثال به‌روزآوری و وصله‌های امنیتی برای نرم‌افزارهای موجود) و چه نوع نصب‌هایی ممنوع است (به‌عنوان‌مثال نرم‌افزارهایی که تنها برای استفاده شخصی و نرم‌افزارهایی که بالقوه مخرب بودن اشتقاق آن‌ها ناشناخته یا مشکوک است). توصیه می‌شود این سطوح دسترسی با توجه به نقش کاربران مرتبط اعطا شود.

اطلاعات دیگر

نصب کنترل نشده نرم‌افزار بر روی دستگاه‌های محاسباتی می‌تواند منجر به ورود آسیب‌پذیری و درنتیجه نشت اطلاعات، از دست دادن جامعیت و یا دیگر رخدادهای امنیت اطلاعات و یا نقض حقوق مالکیت معنوی شود.

۱۲-۷ ملاحظات ممیزی سامانه‌های اطلاعاتی

قصد: کمینه کردن اثر فعالیت‌های ممیزی بر روی سامانه‌های عملیاتی.

۱۲-۷-۱ کنترل‌های ممیزی سامانه‌های اطلاعاتی

کنترل

توصیه می‌شود، الزامات و فعالیت‌های ممیزی شامل بررسی‌های سامانه‌های عملیاتی، به‌دقت طرح‌ریزی و موردتوافق قرار گیرند تا اختلال در فرآیندهای کسب‌وکار، کمینه شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر رعایت شوند:

الف- توصیه می‌شود الزامات ممیزی برای دسترسی به سامانه‌ها و داده‌ها با مدیریت مناسب، موردتوافق قرار گیرند؛

ب- توصیه می‌شود محدوده آزمون‌های ممیزی فنی موردتوافق قرارگرفته و کنترل شوند؛

پ- توصیه می‌شود آزمون‌های ممیزی، محدود به دسترسی فقط خواندنی به نرم‌افزار و داده باشد؛

ت- توصیه می‌شود دسترسی غیر از فقط خواندنی فقط برای رونوشت‌های ایزوله فایل‌های سامانه، مجاز شوند که توصیه می‌شود درزمانی که ممیزی تکمیل می‌شود پاک شوند، یا درصورتی‌که اجباری به حفظ این فایل-ها برای الزامات مستندسازی ممیزی وجود دارد، محافظت مناسب از آن‌ها به عمل آید؛

ث- توصیه می‌شود الزامات پردازش اضافه یا ویژه، شناسایی‌شده و موردتوافق قرار گیرد؛

ج- توصیه می‌شود آزمون‌های ممیزی که می‌تواند در دسترس بودن سیستم را تحت تأثیر قرار دهند، در خارج از ساعات کسب‌وکار اجرا شود؛

چ- توصیه می‌شود همه دسترسی برای تولید یک رد مرجع[1]، تحت پایش و واقعه‌نگاری شود.

۱۳ امنیت ارتباطات

۱۳-۱ مدیریت امنیت شبکه

قصد: حصول اطمینان از حفاظت اطلاعات در شبکه‌ها و تسهیلات پردازش اطلاعات پشتیبان.

۱۳-۱-۱ کنترل‌های شبکه

کنترل

توصیه می‌شود، شبکه‌ها به‌منظور محافظت اطلاعات در سامانه‌ها و برنامه‌های کاربردی مدیریت و کنترل شود.

1 - Reference trail

راهنمای پیاده‌سازی

توصیه می‌شود کنترل‌هایی پیاده‌سازی شوند تا امنیت اطلاعات در شبکه‌ها تضمین‌شده و خدمات شبکه در برابر دسترسی غیرمجاز حفظ شوند. به‌خصوص، توصیه می‌شود موارد زیر در نظر گرفته شود:

الف- توصیه می‌شود مسئولیت‌ها و روش‌های اجرایی برای مدیریت تجهیزات شبکه مستقر شود؛

ب- توصیه می‌شود درجایی که تناسب دارد، مسئول عملیاتی شبکه‌ها از مسئول عملیاتی رایانه‌ها تفکیک شود (به بند ۶-۱-۲ مراجعه شود)؛

پ- توصیه می‌شود کنترل‌های خاص برای محافظت از محرمانگی و یکپارچگی داده‌هایی که از شبکه‌های همگانی یا شبکه‌های بی‌سیم عبور می‌کند مستقر شود و از سامانه‌ها و برنامه‌های کاربردی متصل محافظت شود (به بندهای ۱۰ و ۱۳-۲ مراجعه شود)؛ کنترل‌های خاصی نیز ممکن است برای حفظ دسترسی به خدمات شبکه و رایانه‌های متصل لازم باشد؛

ت- توصیه می‌شود پایش و واقعه‌نگاری مناسب استفاده شود تا ثبت سوابق و تشخیص اقداماتی که روی وقایع امنیتی اثر می‌گذارد یا به آن مرتبط است، امکان‌پذیر شود؛

ث- توصیه می‌شود فعالیت‌های مدیریتی به‌دقت هماهنگ شود تا خدمات مربوط به سازمان بهینه‌شده و همچنین از به‌کارگیری مناسب کنترل‌ها در زیر ساختار پردازش اطلاعات اطمینان حاصل شود؛

ج- توصیه می‌شود سامانه‌ها روی شبکه، تعیین هویت شوند؛

چ- توصیه می‌شود اتصال سامانه‌ها به شبکه محدود باشد.

اطلاعات دیگر

اطلاعات تکمیلی درباره امنیت شبکه را می‌توانید در استاندارد ISO/IEC 27033 [۱۵]، [۱۶]، [۱۷]، [۱۸]، [۱۹]، بیابید.

۱۳-۱-۲ امنیت خدمات شبکه

کنترل

توصیه می‌شود، سازوکارهای امنیتی، سطوح خدمت و الزامات مدیریتی تمامی خدمات شبکه، شناسایی‌شده و در هر توافقنامهٔ خدمات شبکه، اعم از اینکه این خدمات در داخل تهیه‌شده یا برون‌سپاری شده‌اند، لحاظ شوند.

راهنمای پیاده‌سازی

توصیه می‌شود توانایی ارائه‌کننده خدمات شبکه جهت مدیریت خدمات توافق شده به‌صورت امن، تعیین شود و به‌صورت منظم مورد پایش قرار گیرد و توصیه می‌شود حق ممیزی کارفرما موردتوافق قرار گیرد.

توصیه می‌شود تمهیدات امنیتی موردنیاز برای خدمات خاص مانند ویژگی‌های امنیتی، سطوح خدمات و الزامات مدیریت شناسایی شوند. توصیه می‌شود سازمان اطمینان حاصل کند که ارائه‌کنندگان خدمات شبکه این سنجه‌ها را پیاده‌سازی می‌کنند.

اطلاعات دیگر

خدمات شبکه می‌تواند شامل تأمین ارتباطات، خدمات شبکه خصوصی، شبکه‌های ارزش‌افزوده و راه‌حل‌های امنیت شبکه مدیریت‌شده مانند دیوارهای آتش و سامانه‌های کشف ورود غیرمجاز باشد. این خدمات ممکن است از طیف ارائه پهنای باند مدیریت نشده ساده تا ارائه خدمات ارزش‌افزوده پیچیده، متغیر باشد.

ویژگی‌های امنیتی خدمات شبکه می‌تواند شامل موارد زیر باشد:

الف- فن‌آوری به‌کاررفته برای امنیت خدمات شبکه نظیر اصالت‌سنجی، رمزگذاری و کنترل‌های اتصال به شبکه؛

ب- پارامترهای فنی موردنیاز برای ارتباط امن با خدمات شبکه مطابق با قواعد اتصال شبکه و امنیت؛

پ- روش‌های اجرایی برای استفاده از خدمت شبکه جهت محدود کردن دسترسی به خدمات شبکه یا برنامه های کاربردی در صورت لزوم؛

۱۳-۱-۳ تفکیک در شبکه‌ها

کنترل

توصیه می‌شود، گروه‌های خدمات اطلاعاتی، کاربران و سامانه‌های اطلاعاتی، در شبکه‌ها تفکیک شوند.

راهنمای پیاده‌سازی

یکی از روش‌های مدیریت امنیت شبکه‌های بزرگ تقسیم آن‌ها به حوزه‌های شبکه جداگانه است.

حوزه را می‌توان بر اساس سطوح اعتماد (به‌عنوان‌مثال دامنه دسترسی عمومی، دامنه رایانه رومیزی، دامنه کارساز)، به همراه واحدهای سازمانی (به‌عنوان‌مثال منابع انسانی، مالی، بازاریابی) و یا ترکیبی (به‌عنوان‌مثال دامنه کارساز اتصال به واحدهای سازمانی متعدد) انتخاب کرد. جداسازی را می‌توان با استفاده از شبکه‌های مختلف فیزیکی یا با استفاده از شبکه‌های مختلف منطقی (به‌عنوان‌مثال شبکه خصوصی مجازی) انجام داد.

توصیه می‌شود، مرزهای هر حوزه به‌خوبی تعریف‌شده باشد. دسترسی بین حوزه‌های شبکه مجاز است، اما توصیه می‌شود با استفاده از یک دروازه[1](به‌عنوان‌مثال دیواره آتش، مسیریاب فیلتر کننده) کنترل شود. توصیه می‌شود معیار تفکیک شبکه‌ها به حوزه‌ها و دسترسی مجاز از طریق دروازه، بر اساس یک ارزیابی از نیازمندی‌های امنیتی هر دامنه باشد. توصیه می‌شود این ارزیابی مطابق با خط‌مشی کنترل دسترسی (به بند

1- Gateway

۹-۱-۱ مراجعه شود)، الزامات دسترسی، ارزش و طبقه‌بندی اطلاعات پردازش‌شده و همچنین با در نظر گرفتن حساب هزینه و عملکرد نسبی ناشی از به‌کارگیری فن‌آوری دروازه باشد.

ازآنجایی‌که محیط شبکه در شبکه‌های بی‌سیم، ضعیف تعریف‌شده است، نیاز به برخورد خاص دارد. توصیه می‌شود برای محیط حساس، این ملاحظه مدنظر قرار گیرد که تمام دسترسی‌های بی‌سیم به‌عنوان اتصالات خارجی در نظر گرفته شود و این دسترسی از شبکه‌های داخلی جدا شود تا دسترسی از طریق یک دروازه مطابق با خط‌مشی کنترل‌های شبکه (به بند ۱۳-۱-۱ مراجعه شود) قبل از صدور دسترسی به سامانه‌های داخلی انجام شود.

اصالت‌سنجی، رمزگذاری و فناوری کنترل دسترسی سطح کاربر شبکه مبتنی بر شبکه‌های بی‌سیم مدرن و استاندارد، می‌تواند زمانی که به‌درستی پیاده‌سازی شده باشد، برای اتصال مستقیم به شبکه داخلی سازمان کافی باشد

اطلاعات دیگر

شبکه‌ها اغلب فراتر از مرزهای سازمانی، در جهت مشارکت کسب‌وکار گسترش می‌یابند به‌گونه‌ای که نیازمند اتصال و یا به اشتراک‌گذاری تسهیلات پردازش اطلاعات و شبکه است. چنین گسترشی می‌تواند مخاطرات دسترسی غیرمجاز به سامانه‌های اطلاعاتی سازمان که از شبکه استفاده می‌کنند را افزایش دهد و برخی از آن‌ها به حفاظت از دیگر کاربران شبکه به دلیل حساسیت و بحرانی بودن نیاز دارند.

۱۳-۲ انتقال اطلاعات

قصد: حفظ امنیت اطلاعات انتقال‌یافته در درون سازمان و با هر هستار بیرونی.

۱۳-۲-۱ خط‌مشی‌ها و روش‌های اجرایی انتقال اطلاعات

کنترل

توصیه می‌شود، برای حفاظت انتقال اطلاعات به‌واسطهٔ استفاده از تمام انواع تسهیلات ارتباطی، خط‌مشی‌ها، روش‌های اجرایی و کنترل‌های انتقال رسمی ایجاد شوند.

راهنمای پیاده‌سازی

توصیه می‌شود در روش‌های اجرایی و کنترل‌هایی که در زمان استفاده از تسهیلات ارتباطات برای تبادل اطلاعات، دنبال می‌شوند، موارد زیر در نظر گرفته شود:

الف- روش‌های اجرایی طراحی‌شده برای محافظت از اطلاعات انتقال داده‌شده در برابر دستبرد، نسخه‌برداری، تغییر، تغییر مسیر و تخریب؛

ب- روش‌های اجرایی برای کشف و محافظت در برابر بدافزار که ممکن است با استفاده از ارتباطات الکترونیکی منتقل شوند (به بند ۱۲-۲-۱ مراجعه شود)؛

پ- روش‌های اجرایی برای محافظت از اطلاعات الکترونیکی حساس مبادله شده که به شکل فایل پیوست هستند؛

ت- خط‌مشی یا راهنماهایی که استفاده قابل‌قبول از تسهیلات ارتباطی را ترسیم می‌کنند (به بند ۸-۱-۳ مراجعه شود)؛

ج- مسئولیت‌های کارکنان، طرف‌های بیرونی و هر کاربر دیگر برای این‌که به سازمان آسیب نرساند، مثلاً از طریق بدنام کردن، آزار رسانی، جعل هویت، رد کردن نامه زنجیره‌ای، خرید غیرمجاز و مانند آن؛

چ- استفاده از فنون رمزنگاری؛ برای مثال، برای حفاظت از محرمانگی، تمامیت و صحت اطلاعات (به بند ۱۰ مراجعه شود)؛

ح- راهنمایی‌های حفظ و امحا برای تمام مکاتبات کسب‌وکار ازجمله پیام‌ها، مطابق با قوانین و مقررات ملی و محلی؛

خ- کنترل‌ها و محدودیت‌های مربوط به استفاده از تسهیلات ارتباطی مانند انتقال خودکار رایانامه به نشانی-های پستی خارجی؛

د- توصیه به کارکنان جهت اقدامات احتیاطی مناسب برای فاش نکردن اطلاعات محرمانه؛

ذ- عدم گذاشتن پیام‌هایی که حاوی اطلاعات حساس هستند روی دستگاه‌های پاسخگو، زیرا این اطلاعات ممکن است توسط اشخاص غیرمجاز مورد دسترسی قرار گیرند و یا در سامانه‌های اشتراکی ذخیره شوند یا در اثر شماره‌گیری اشتباه در جای دیگری ذخیره شوند؛

ر- یادآوری به کارکنان درباره مشکلات استفاده از خدمات یا دستگاه‌های نمابر مخصوصاً در موارد زیر:

۱- دسترسی غیرمجاز به رسانه ذخیره‌سازی داخلی پیام برای بازیابی پیام‌ها؛
۲- برنامه‌ریزی عمدی یا تصادفی ماشین‌ها برای ارسال پیام‌ها به شماره‌های خاص؛
۳- ارسال اسناد و پیام‌ها به شماره اشتباه از طریق شماره‌گیری اشتباه یا شماره‌ای که به‌اشتباه ذخیره‌شده است.

به‌علاوه، توصیه می‌شود به کارکنان یادآوری شود که مکالمات محرمانه خود را در مکان‌های عمومی یا کانال‌های ارتباطی ناامن، اماکن بدون دیوار و محل‌های ملاقات، انجام ندهند.

توصیه می‌شود خدمات تبادل اطلاعات، الزامات قانونی مرتبط را رعایت کنند (به بند ۱۸-۱ مراجعه شود).

اطلاعات دیگر

تبادل اطلاعات ممکن است با استفاده از تعدادی از انواع مختلف تسهیلات تبادل اطلاعات ازجمله رایانامه، صوت، نمابر و تصویر انجام شود.

تبادل نرم‌افزارها ممکن است از طریق تعدادی از رسانه‌های مختلف ازجمله دریافت از اینترنت و خرید از فروشندگانی که این محصولات آماده را می‌فروشند انجام شود.

توصیه می‌شود موارد کسب‌وکاری، قانونی و ضمنی امنیتی که مرتبط با تبادل اطلاعات الکترونیکی، تجارت الکترونیکی و ارتباطات الکترونیکی و الزامات کنترل‌ها است، در نظر گرفته شوند.

۱۳-۲-۲ توافق‌نامه‌های انتقال اطلاعات

کنترل

توصیه می‌شود، توافق‌نامه‌ها به انتقال امن اطلاعات کسب‌وکار بین سازمان و طرف‌های بیرونی بپردازد.

راهنمای پیاده‌سازی

توصیه می‌شود در توافق‌نامه‌های تبادل اطلاعات موارد زیر لحاظ شوند:

الف- مسئولیت‌های مدیریت در مورد کنترل و اعلام انتقال، ارسال و دریافت؛

ب- روش‌های اجرایی برای تضمین قابلیت پیگیری و عدم انکار؛

ت- کمینه استانداردهای فنی برای بسته‌بندی و انتقال؛

ث- توافق‌نامه‌های وجه‌الضمان؛

ج- استانداردهای شناسایی حامل؛

چ- مسئولیت‌ها و تعهدات در صورت بروز رخدادهای امنیت اطلاعات نظیر آسیب به داده‌ها؛

ح- استفاده از یک سامانه برچسب‌زنی موردتوافق برای اطلاعات حساس یا حیاتی و اطمینان از این‌که معنای برچسب بلافاصله فهمیده می‌شود و این‌که اطلاعات به‌طور مناسب محافظت می‌شود (به ۸-۲ مراجعه شود)؛

خ- استانداردهای فنی برای ثبت و خواندن اطلاعات و نرم‌افزار؛

د- هر کنترل خاصی که برای حفاظت از موارد حساس نظیر رمزگشایی لازم است (به بند ۱۰ مراجعه شود)؛

ذ- حفظ زنجیره‌ای از حفاظت، برای اطلاعات در حال انتقال؛

ر- سطوح قابل‌قبول از کنترل دسترسی.

توصیه می‌شود خط‌مشی‌ها، روش‌های اجرایی و استانداردهایی برای محافظت از اطلاعات و رسانه‌های فیزیکی در انتقال، مستقر و اعمال شود (همچنین به بند ۸-۳-۳ مراجعه شود) و توصیه می‌شود در توافق‌نامه های تبادل به آن‌ها ارجاع داده شود.

توصیه می‌شود محتوای امنیت اطلاعات هر قرارداد، نشان‌دهنده حساسیت اطلاعات کسب‌وکار مرتبط باشد.

اطلاعات دیگر

توافق‌نامه‌ها می‌توانند الکترونیکی یا دستی و ممکن است به شکل قراردادهای رسمی باشند. توصیه می‌شود برای اطلاعات حساس، سازوکارهای خاص به کار گرفته‌شده برای تبادل، برای تمام سازمان‌ها و انواع قراردادها یکسان باشد.

۱۳-۲-۳ پیام‌رسانی الکترونیکی

کنترل

توصیه می‌شود، اطلاعات موجود در پیام‌رسانی الکترونیکی به‌صورت مناسبی حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیت اطلاعات برای پیام‌رسانی الکترونیکی شامل موارد زیر باشد:

الف- محافظت از پیام‌ها در برابر دسترسی غیرمجاز، تغییر، یا جلوگیری از ارائه خدمات متناسب با طرح طبقه بندی اطلاعات مصوب شده توسط سازمان؛

ب- اطمینان از نشانی‌دهی و انتقال صحیح پیام؛

پ- قابلیت اطمینان و دسترس‌پذیری خدمات؛

ت- ملاحظات قانونی مانند الزامات امضاهای دیجیتال؛

ث- کسب مجوز قبل از استفاده از خدمات همگانی خارجی نظیر پیام سریع، شبکه‌های اجتماعی، یا اشتراک‌گذاری فایل؛

ج- سطوح قوی‌تر اصالت‌سنجی جهت کنترل دسترسی از شبکه‌های عمومی دسترس‌پذیر.

اطلاعات دیگر

انواع مختلفی از پیام‌رسانی الکترونیکی مانند رایانامه، تبادل الکترونیکی داده و شبکه‌های اجتماعی وجود دارند که نقش مهمی در تبادلات کسب‌وکاری دارند.

۱۳-۲-۴ توافق‌نامه‌های محرمانگی یا عدم افشاء

کنترل

توصیه می‌شود، الزاماتی برای توافق‌نامه‌های محرمانگی یا عدم افشاء که منعکس‌کنندهٔ نیازهای سازمان به حفاظت از اطلاعات است، شناسایی و به‌طور منظم بازنگری و تدوین شود.

راهنمای پیاده‌سازی

توصیه می‌شود توافقنامه‌های محرمانگی یا عدم افشا به نیازمندی‌های محافظت از اطلاعات محرمانه از طریق به‌کارگیری واژه‌های لازم‌الاجرای قانونی، اشاره کند. توافقنامه‌های محرمانگی یا عدم افشا برای طرف‌های بیرونی یا کارمندان سازمان، کاربردپذیر هستند. عناصر باید با در نظر گرفتن نوع طرف‌های دیگر و دسترسی

مجاز آن‌ها برای اداره کردن اطلاعات، انتخاب و یا اضافه شوند. توصیه می‌شود برای شناسایی الزامات توافق‌نامه‌های محرمانگی یا عدم افشا عناصر زیر مدنظر قرار گیرند:

الف- تعریفی از اطلاعاتی که محافظت شوند (به‌عنوان‌مثال اطلاعات محرمانگی)؛

ب- طول مدت مورد انتظار برای یک توافق‌نامه، دربرگیرنده مواردی که محرمانگی باید به‌طور نامحدود رعایت شود؛

پ- اقدامات موردنیاز هنگامی‌که قرارداد خاتمه می‌پذیرد؛

ت- مسئولیت‌ها و اقدامات امضاکنندگان برای اجتناب از افشا اطلاعات غیرمجاز؛

ث- مالک اطلاعات، اطلاعات محرمانه تجاری و مالکیت معنوی و اینکه چگونه این با حفاظت از اطلاعات محرمانه مرتبط است؛

ج- اجازه استفاده از اطلاعات محرمانه و حقوق امضاکننده استفاده از اطلاعات؛

چ- حق فعالیت‌های ممیزی و پایش فعالیت‌هایی که شامل اطلاعات محرمانه می‌شوند؛

ح- فرایندی برای اخطار و گزارش دهی افشا غیرمجاز یا نشت اطلاعات محرمانه؛

خ- شرایط برای اطلاعاتی که باید در زمان خاتمه قرارداد، عودت داده شود یا از بین بروند؛

د- اقدامات مورد انتظاری که در صورت تخطی از این قرارداد انجام می‌گیرند.

بر اساس الزامات امنیت اطلاعات سازمان، موارد دیگری ممکن است درباره قرارداد محرمانگی یا عدم افشا موردنیاز باشد.

توصیه می‌شود توافق‌نامه‌های محرمانگی و عدم افشا، مطابق با همه قوانین و مقررات قابل کاربرد برای حوزه قضایی که در آن اجرا می‌شود، باشد (به بند ۱۸-۱ مراجعه شود).

توصیه می‌شود الزامات توافق‌نامه‌های محرمانگی و عدم افشا در بازه‌های زمانی منظم و هنگامی‌که تغییری روی‌داده که این الزامات را متأثر می‌کند، بازنگری شود.

اطلاعات دیگر

توافق‌نامه‌های محرمانگی و عدم افشا، اطلاعات سازمانی را محافظت کرده و مسئولیت امضاکنندگان را برای حفظ، به‌کارگیری و افشا اطلاعات به شیوه‌ای مسئولانه و تفویضی، بیان می‌کند.

ممکن است یک سازمان نیازمند نمونه‌های مختلفی از توافق‌نامه‌های محرمانگی و عدم افشا در شرایط مختلف باشد.

۱۴ اکتساب، توسعه و نگهداری سامانه

۱-۱۴ الزامات امنیتی سامانه‌های اطلاعاتی

قصد: حصول اطمینان از اینکه امنیت اطلاعات، یک جزء جدایی‌ناپذیر از سامانه‌های اطلاعاتی در تمام چرخه حیات است. همچنین شامل الزاماتی برای سامانه‌های اطلاعاتی که بر روی شبکه‌های عمومی ارائه خدمات می‌کنند، می‌شود.

۱-۱-۱۴ تحلیل و تعیین الزامات امنیت اطلاعات

کنترل

توصیه می‌شود، الزامات مرتبط با امنیت اطلاعات در الزامات سامانه‌های اطلاعاتی جدید یا ارتقا سامانه‌های اطلاعاتی فعلی، موجود باشد.

راهنمای پیاده‌سازی

توصیه می‌شود نیازمندی‌های امنیت اطلاعات با استفاده از روش‌های مختلف مانند استخراج الزامات انطباق از خط‌مشی‌ها و مقررات، مدل‌سازی تهدید، بازنگری رخداد، یا استفاده از آستانه‌های آسیب‌پذیری، شناسایی شود. توصیه می‌شود نتایج به‌دست‌آمده از شناسایی، مستند و توسط همه ذی‌نفعان بازنگری شود.

توصیه می‌شود نیازمندی‌های امنیت اطلاعات و کنترل‌ها، ارزش کسب‌وکار از اطلاعات مرتبط (به بند ۸- ۲ مراجعه شود) و امکان تأثیر منفی بر کسب‌وکار که ممکن است از کمبود امنیت ایجاد شود را منعکس کند.

توصیه می‌شود شناسایی و مدیریت الزامات امنیت اطلاعات و فرایندهای مرتبط، در مراحل اولیه پروژه‌های سامانه‌های اطلاعات یکپارچه شود. لحاظ کردن اولیه الزامات امنیت اطلاعات به‌عنوان‌مثال در مرحله طراحی، می‌تواند منجر به راه‌حل‌های اثربخش‌تر و ازلحاظ هزینه کاراتر شود.

الزامات امنیت اطلاعات همچنین باید موارد زیر را در نظر داشته باشد:

الف- سطح اعتماد موردنیاز نسبت به هویت ادعاشده کاربران، به‌منظور استخراج الزامات اصالت‌سنجی کاربر؛

ب- فرآیندهای تأمین دسترسی و مجوز، برای کاربران کسب‌وکار و نیز برای کاربران ممتاز یا فنی؛

پ- اطلاع‌رسانی به کاربران و بهره‌برداران در مورد وظایف و مسئولیت‌های خود؛

ت- الزامات حفاظتی موردنیاز از دارایی‌های درگیر، به‌ویژه با توجه به دسترس‌پذیری، محرمانگی، یکپارچگی؛

ث- الزامات استخراج‌شده از فرآیندهای کسب‌وکار، مانند واقعه‌نگاری و پایش و الزامات عدم انکار تراکنش؛

ج- الزامات اجباری توسط دیگر کنترل‌های امنیتی، به‌عنوان‌مثال رابط‌های واقعه‌نگاری و پایش یا سامانه‌های تشخیص نشت داده.

توصیه می‌شود برای برنامه‌های کاربردی که خدمات از طریق شبکه‌های عمومی ارائه می‌دهند یا تراکنش‌ها را پیاده‌سازی می‌کنند، کنترل‌های اختصاصی ۱۴-۱-۲ و ۱۴-۱-۳ در نظر گرفته شود.

توصیه می‌شود اگر محصولات خریداری می‌شوند، یک فرایند آزمون و اکتساب رسمی، دنبال شود. توصیه می‌شود قراردادها با تأمین‌کننده به الزامات امنیتی شناخته‌شده، اشاره داشته باشند. توصیه می‌شود درجایی که عملکرد در محصول پیشنهادی، الزامات مشخص‌شده را برآورده نمی‌کند، مخاطرات مطرح‌شده و کنترل-های مرتبط، مجدداً قبل از خرید محصول، مورد ملاحظه قرار گیرد.

توصیه می‌شود راهنمایی موجود برای پیکربندی امنیتی محصول که با پشته نهایی نرم‌افزار / خدمات سامانه هم‌راستا شده است، ارزشیابی و پیاده‌سازی شود.

توصیه می‌شود معیار برای پذیرش محصولات تعریف شود، به‌عنوان‌مثال، به‌صورت بیان عملکرد خودشان که اطمینان دهد که نیازمندی‌های امنیتی شناسایی‌شده برآورده شده‌اند. توصیه می‌شود محصولات در برابر این معیارها قبل از اکتساب، ارزشیابی شوند. توصیه می‌شود عملکردهای اضافی برای اطمینان از آن‌که مخاطرات اضافی غیرقابل‌قبول ایجاد نمی‌کنند، بازنگری شوند.

اطلاعات دیگر

استانداردهای ISO/IEC 27005 [۱۱] و ISO 31000 [۲۷]راهنمایی‌هایی را برای استفاده از فرآیندهای مدیریت مخاطرات جهت شناسایی کنترل‌ها جهت برآورده سازی الزامات امنیت اطلاعات، فراهم می‌کند.

۲-۱-۱۴ امن سازی خدمات برنامه‌های کاربردی در شبکه‌های عمومی

کنترل

توصیه می‌شود، اطلاعات مورداستفاده در خدمات برنامه‌های کاربردی که از شبکه‌های عمومی عبور می‌کنند، در برابر فعالیت‌های کلاه‌برداری، اختلاف‌نظر در قرارداد و افشاء و دست‌کاری غیرمجاز محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیت اطلاعات برای خدمات کاربردی که از طریق شبکه‌های عمومی ارائه می‌شوند، شامل موارد زیر باشد:

الف- سطح اطمینان موردنیاز هر یک از دو طرف نسبت به هویت مورد ادعای طرف دیگر، مثلاً از طریق اصالت‌سنجی؛

ب- فرایندهای مجوز دهی مرتبط با هرکسی که ممکن است محتوا را تأیید کند و اسناد مهم کسب‌وکار را صادر یا امضا کند؛

پ- حصول اطمینان از این‌که شرکای در ارتباط کسب‌وکار، کاملاً از اختیارات خود برای تأمین یا استفاده از خدمات، مطلع هستند؛

ت- تعیین و رعایت الزامات محرمانگی، یکپارچگی، اثبات ارسال و دریافت اسناد کلیدی و عدم انکار قراردادها مثلاً در رابطه با فرایندهای مناقصه یا قرارداد؛

ث- سطح اعتمادی که در یکپارچگی مستندات کلیدی لازم است؛

ج- الزامات محافظت از همه اطلاعات محرمانه؛

چ- محرمانگی و یکپارچگی هر یک از تراکنش‌ها، اطلاعات پرداخت، جزییات نشانی تحویل و تأیید رسیدها؛

ح- میزان درستی‌سنجی مناسب جهت بررسی درستی اطلاعات پرداختی که توسط مشتری ارائه‌شده است؛

خ- انتخاب مناسب‌ترین نحوه تسویه‌ی پرداخت برای محافظت در برابر تقلب؛

د- سطح محافظت موردنیاز برای حفظ محرمانگی و یکپارچگی اطلاعات سفارش؛

ذ- اجتناب از تکرار یا از دست دادن در اطلاعات تراکنش‌ها؛

ر- مسئولیت مرتبط با تراکنش‌های جعلی؛

ز- الزامات بیمه.

بسیاری از ملاحظات فوق را می‌توان با به‌کارگیری کنترل‌های رمزنگاری (به بند ۱۰ مراجعه شود)، با احتساب انطباق با الزامات قانونی پوشش داد (به بند ۱۸، مخصوصاً بند ۱۸-۱-۵ برای قواعد رمزنگاری مراجعه شود).

توصیه می‌شود تمهیدات خدمات کاربردی بین شرکا، توسط یک توافق‌نامه‌ی مستند که هر دو طرف را به رعایت مفاد موردتوافق خدمات، ازجمله جزییات اختیارات، متعهد می‌کند، پشتیبانی شود (به مورد ب در بالا مراجعه شود).

توصیه می‌شود الزامات برگشت‌پذیری[1] در برابر حملات در نظر گرفته شود که می‌تواند شامل الزامات برای حفاظت از سرویس‌دهنده‌های برنامه‌های کاربردی و یا حصول اطمینان از دسترس‌پذیری ارتباطات شبکه موردنیاز برای ارائه خدمت باشد.

اطلاعات دیگر

برنامه‌های کاربردی که از طریق شبکه‌های عمومی در دسترس هستند، در معرض تعدادی از تهدیدهای مرتبط با شبکه مانند فعالیت‌های کلاه‌برداری، اختلاف در قرارداد و افشا اطلاعات برای عموم قرار دارند؛ بنابراین، ارزیابی‌های مخاطرات با جزئیات و انتخاب مناسب کنترل‌ها ضروری است. کنترل‌های موردنیاز اغلب شامل روش‌های رمزنگاری برای اصالت‌سنجی و امن سازی انتقال داده، است.

خدمات کاربردی، می‌تواند از روش‌های امن اصالت‌سنجی استفاده کند، برای مثال می‌تواند از رمزنگاری کلید عمومی و امضاهای دیجیتال (به بند ۱۰ مراجعه شود) برای کاهش مخاطرات استفاده کند. همچنین از اشخاص ثالث مورد اعتماد می‌توان درزمانی که به این خدمات نیاز است، استفاده کرد.

۱۴-۱-۳ محافظت از تراکنش‌های خدمات کاربردی

کنترل

1 - resilience

توصیه می‌شود، اطلاعات مورداستفاده در خدمات کاربردی، به‌منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه، تغییر یافتن غیرمجاز پیغام، افشای غیرمجاز، بازخوانی یا رونوشت شدن غیرمجاز پیغام، حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیت اطلاعات برای تراکنش‌های خدمات کاربردی، شامل موارد زیر باشد:

الف- استفاده از امضاهای الکترونیکی توسط هر یک از دو طرف درگیر در تراکنش؛

ب- رعایت تمام جنبه‌های تراکنش به این معنی که اطمینان از موارد زیر حاصل شود:

۱-اطلاعات مخفی اصالت‌سنجی کاربران همه طرف‌ها، معتبر و تأییدشده است؛

۲-تراکنش محرمانه باقی می‌ماند؛ و

۳-حریم خصوصی همه طرف‌ها، حفظ می‌شود؛

پ- مسیر ارتباطی بین همه طرف‌های درگیر، رمزگذاری‌شده است؛

ت- پروتکل‌های به‌کاررفته برای ارتباط بین همه طرف‌های درگیر، امن شده است؛

ث- اطمینان از اینکه رسانه ذخیره‌سازی جزییات تراکنش، در مکانی خارج از دسترسی عموم مثلاً در یک سکوی ذخیره‌سازی موجود روی اینترانت سازمان قرار دارد و نه بر روی رسانه ذخیره‌سازی که مستقیماً از اینترنت قابل‌دسترسی است؛

ج- درجایی که از یک مرجع مورد اعتماد استفاده می‌شود (مثلاً، برای صدور و حفظ امضاهای دیجیتال یا گواهینامه دیجیتال)، امنیت در سراسر فرایند مدیریت انتها به انتهای امضا/گواهینامه، یکپارچه‌سازی و تعبیه شود.

اطلاعات دیگر

توصیه می‌شود میزان کنترل‌های به‌کاررفته با سطح مخاطرات مربوط به هر شکل از تراکنش خدمات کاربردی، تناسب داشته باشد.

تراکنش‌ها ممکن است نیاز به تطابق با قوانین، الزامات مقرراتی در حوزه قضایی که در آن تراکنش، ایجاد، پردازش، تکمیل یا نگهداری می‌شوند، داشته باشند.

۱۴-۲ امنیت در فرآیندهای توسعه و پشتیبانی

قصد: حصول اطمینان از اینکه امنیت درون چرخه حیات توسعه سامانه‌های اطلاعاتی، طراحی و پیاده‌سازی شده است.

۱۴-۲-۱ خط‌مشی توسعه امن

کنترل

توصیه می‌شود، قوانینی برای توسعه نرم‌افزار و سامانه‌ها ایجادشده و برای توسعه‌های درون سازمان به‌کارگیری شود.

راهنمای پیاده‌سازی

توسعه امن، الزامی برای ایجاد خدمت، معماری، نرم‌افزار و سامانه امن است. توصیه می‌شود در خط‌مشی توسعه امن، جنبه‌های زیر موردتوجه قرار داده شود:

الف- امنیت محیط توسعه؛

ب- راهنمایی در مورد امنیت در چرخه حیات توسعه نرم‌افزار شامل:

۱- امنیت در روشگان توسعه نرم‌افزار؛

۲- راهنمایی برنامه‌نویسی امن برای هر زبان برنامه‌نویسی مورداستفاده؛

پ- الزامات امنیتی در مرحله طراحی؛

ت- نقاط بازرسی امنیتی در نقاط مهم[1] پروژه؛

ث- انباره‌های[2] امن؛

ج- امنیت در کنترل نسخه؛

چ- دانش امنیتی برنامه کاربردی موردنیاز؛

ح- قابلیت توسعه‌دهندگان در اجتناب، یافتن و اصلاح آسیب‌پذیری.

توصیه می‌شود فنون برنامه‌نویسی امن درجایی که استانداردهای به کار گرفته‌شده جهت توسعه، شناخته‌شده و یا سازگار با بهروش نیستند؛ در هر دو سناریوی توسعه جدید و استفاده مجدد از کد، مورداستفاده قرار گیرد. توصیه می‌شود استانداردهای کد نویسی امن در نظر گرفته شود و در جای مناسب، استفاده از آن اجباری شود. توصیه می‌شود توسعه‌دهندگان در استفاده و آزمون آن‌ها آموزش‌دیده و با بازنگری کد، استفاده از آن‌ها تأیید شود.

توصیه می‌شود که اگر توسعه برون‌سپاری شده است، سازمان اطمینان یابد که طرف بیرونی مطابق با این قواعد برای توسعه امن عمل می‌کند (به بند ۱۴-۲-۷ مراجعه شود).

اطلاعات دیگر

توسعه ممکن است همچنین در داخل برنامه‌های کاربردی، مانند برنامه‌های کاربردی اداری، اسکریپت نویسی، مرورگرها و پایگاه‌های داده صورت گیرد.

1- Milestones
2-Storages

۱۴-۲-۲ روش‌های اجرایی کنترل تغییر سامانه

کنترل

توصیه می‌شود، تغییرات در سامانه‌های درون چرخه توسعه، با استفاده از روش‌های اجرایی رسمی کنترل تغییر، کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود روش‌های اجرایی کنترل تغییرات رسمی به‌منظور حصول اطمینان از یکپارچگی سامانه، برنامه‌های کاربردی و محصولات، از اولین مراحل طراحی تا فعالیت‌های نگهداری آتی، مستندسازی و اجباری شود.

توصیه می‌شود ورود سامانه‌های جدید و تغییرات عمده در سامانه‌های فعلی، یک فرایند رسمی مستندسازی، مشخص‌سازی، آزمون، کنترل کیفیت و پیاده‌سازی مدیریت‌شده را دنبال کند.

توصیه می‌شود این فرایند شامل ارزیابی مخاطرات، تحلیل پیامدهای تغییرات و مشخصات کنترل‌های امنیتی موردنیاز باشد. توصیه می‌شود این فرایند همچنین تضمین کند که روش‌های اجرایی فعلی امنیت و کنترل، مسامحه نمی‌شوند و برنامه‌نویس‌ها، دسترسی را فقط به بخش‌هایی از سامانه دارند که برای وظایفشان لازم است و قرارداد و تأیید رسمی برای هر تغییر کسب می‌شود.

توصیه می‌شود در صورت امکان، روش‌های اجرایی کنترل تغییر عملیاتی و برنامه‌های کاربردی، یکپارچه باشند (همچنین به بند ۱۲-۱-۲ مراجعه شود). توصیه می‌شود روش‌های اجرایی کنترل تغییر شامل و نه محدود به موارد زیر باشند:

الف- حفظ سوابق سطوح مجوز دهی موردتوافق؛

ب- تضمین اینکه تغییرات توسط کاربران مجاز ارائه می‌شوند؛

پ- بازنگری کنترل‌ها و روش‌های اجرایی یکپارچگی برای تضمین این‌که آن‌ها به‌واسطه تغییرات مختل نخواهند شد؛

ت- شناسایی همه نرم‌افزارها، اطلاعات، هستارهای بانک داده و سخت‌افزار که اصلاحاتی را نیاز دارند؛

ث- شناسایی و بازرسی کدهای بحرانی امنیتی برای کمینه‌سازی امکان وجود ضعف‌های امنیتی شناخته‌شده؛

ج- به دست آوردن تأیید رسمی برای پیشنهادهای تفصیلی قبل از آغاز کار؛

چ- تضمین این‌که کاربران مجاز، تغییرات را قبل از پیاده‌سازی آن‌ها می‌پذیرند؛

ح- تضمین این‌که مجموعه مستندات سیستم، پس از تکمیل هر تغییر روزآمد می‌شود و این‌که مستندات قدیمی بایگانی یا امحا می‌شود؛

خ- حفظ یک کنترل نسخه برای تمام روزآمدسازی‌های نرم‌افزار؛

د- حفظ یک رد ممیزی از تمام درخواست‌های تغییرات؛

ذ- تضمین این‌که مستندات عملیاتی (به بند ۱۲-۱-۱ مراجعه شود) و روش‌های اجرایی کاربر در زمان لازم تغییر می‌کنند تا متناسب باقی بمانند؛

ر- تضمین این‌که پیاده‌سازی تغییرات در زمان صحیح انجام می‌شود و فرایندهای کسب‌وکار مرتبط را مختل نمی‌کند.

اطلاعات دیگر

تغییر نرم‌افزار می‌تواند بر محیط عملیاتی تأثیر بگذارد و برعکس.

تجربه خوب شامل آزمون نرم‌افزار جدید در محیطی است که هم از محیط تولید و هم از محیط توسعه جداشده باشد (به بند ۱۲-۱-۴ مراجعه شود). این، ابزاری برای کنترل بر نرم‌افزار جدید و ایجاد محافظت بیشتر اطلاعات عملیاتی که برای اهداف آزمون مورداستفاده قرار می‌گیرد، فراهم می‌آورد. توصیه می‌شود این، شامل وصله‌ها، بسته‌های خدمات و دیگر روزآمدسازی‌ها باشد.

توصیه می‌شود درجایی که روزآمدسازی‌های خودکار موردنظر است، مخاطرات جامعیت و دسترس‌پذیری در مقابل مزایای استقرار سریع روزآمدسازی‌ها وزن دهی شود. توصیه می‌شود روزآمدسازی خودکار روی سامانه‌های حیاتی انجام نشود، زیرا بعضی روزآمدسازی‌ها ممکن است باعث ایجاد نقص در برنامه‌های کاربردهای حیاتی شوند.

۱۴-۲-۳ بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات بسترهای نرم‌افزاری

کنترل

توصیه می‌شود، در هنگام تغییر بسترهای نرم‌افزاری، به‌منظور حصول اطمینان از عدم وجود تأثیر سوء بر عملیات یا امنیت سازمانی، نرم‌افزارهای کاربردی حیاتی کسب‌وکار، بازنگری و آزمایش شوند.

راهنمای پیاده‌سازی

توصیه می‌شود این فرایند، موارد زیر را پوشش دهد:

الف- بازنگری کنترل برنامه کاربردی و روش‌های اجرایی یکپارچگی برای تضمین این‌که آن‌ها از طریق تغییرات بستر عامل، مختل نشده‌اند؛

ب- تضمین این‌که اخطار تغییرات بستر عامل به‌موقع انجام می‌شود تا آزمون‌ها و بازنگری‌های مناسب قبل از پیاده‌سازی انجام شوند؛

پ- تضمین این‌که تغییرات مناسب در برنامه‌های استمرار کسب‌وکار انجام می‌شوند (به بند ۱۷ مراجعه شود).

اطلاعات دیگر

بسترهای عامل شامل سامانه‌های عامل، پایگاه‌های داده، میان‌افزارها می‌باشند. توصیه می‌شود این کنترل برای تغییرات برنامه‌های کاربردی نیز مورداستفاده قرار گیرد.

۱۴-۲-۴ محدودسازی در اعمال تغییرات دربسته‌های نرم‌افزاری

کنترل

توصیه می‌شود، از دست‌کاری دربسته‌های نرم‌افزاری، اجتناب شده، محدود به تغییرات ضروری باشد و تمامی تغییرات به‌شدت کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود تا حد امکان و قابل‌اجرا، بسته‌های نرم‌افزاری پشتیبانی شده توسط فروشندگان بدون تغییر مورداستفاده قرار گیرد. توصیه می‌شود درجایی که بسته نرم‌افزاری نیاز به تغییر داشته باشد، نکات زیر رعایت شود:

الف- مخاطره کنترل‌های درونی و فرایندهای یکپارچه‌ای که به خطر می‌افتند؛

ب- آیا توصیه می‌شود رضایت فروشنده کسب شود یا نه؛

پ- امکان دریافت تغییرات لازم از فروشنده هنگامی‌که برنامه‌های استاندارد به‌روز می‌شوند؛

ت- پیامد این‌که سازمان، در آینده مسئول نگهداری نرم‌افزار درنتیجه تغییر بشود.

توصیه می‌شود اگر تغییرات لازم باشد، نرم‌افزار اصلی حفظ شود و تغییرات به یک نسخه‌ی معین‌شده، اعمال شود. توصیه می‌شود فرایند مدیریت روزآمدسازی نرم‌افزار، برای تضمین این‌که روزآمدترین وصله‌ها و روزآمدسازی‌های برنامه‌های کاربردی تأییدشده برای تمام نرم‌افزارهای مجاز نصب‌شده، پیاده‌سازی شود (به بند ۱۲-۶-۱ مراجعه شود). توصیه می‌شود تمام تغییرات به‌صورت کامل آزموده و مستند شود به‌گونه‌ای که آن‌ها را بتوان در صورت لزوم در ارتقاهای آتی نرم‌افزار، مجدداً به کاربرد. توصیه می‌شود در صورت لزوم، تغییرات توسط یک‌نهاد ارزشیابی مستقل، آزموده و ارزیابی شود.

۱۴-۲-۵ اصول مهندسی نرم‌افزار امن

کنترل

توصیه می‌شود، اصولی برای مهندسی سامانه‌های امن استقرار یابد، مستند، نگهداری شده و برای هرگونه تلاش‌های پیاده‌سازی سیستم اطلاعاتی به‌کارگیری شود.

راهنمای پیاده‌سازی

توصیه می‌شود روش‌های اجرایی مهندسی امن سامانه اطلاعاتی، مبتنی بر اصول مهندسی امنیت، برای فعالیت‌های مهندسی سامانه اطلاعاتی درون‌سازمانی، مستقر، مستند و به‌کارگیری شود. توصیه می‌شود امنیت در تمام لایه‌های معماری (کسب‌وکار، داده، برنامه‌های کاربردی و فناوری)، به‌گونه‌ای که نیاز به امنیت

با نیاز به دسترسی متوازن شود، طراحی شود. توصیه می‌شود فناوری‌های جدید برای مخاطرات امنیتی تحلیل شوند و توصیه می‌شود طراحی از دیدگاه الگوهای حمله‌های شناخته‌شده، بازنگری شود.

توصیه می‌شود این اصول و روش‌های اجرایی مهندسی استقراریافته به‌صورت منظم بازنگری شوند تا اطمینان حاصل شود که آن‌ها به‌صورت مؤثری در جهت بالا بردن استانداردهای امنیت در فرایند مهندسی، بررسی می‌شوند. همچنین توصیه می‌شود، آن‌ها به‌صورت منظم بازنگری شوند تا اطمینان حاصل شود که ازلحاظ مقابله با هر تهدید بالقوه‌ای، روزآمد باقی‌مانده و همچنان کاربردپذیر برای پیشرفت‌های فناوری و راه‌حل‌های به‌کاررفته هستند.

توصیه می‌شود درجایی که کاربردپذیر است، اصول مهندسی امن برای سامانه‌های اطلاعاتی برون‌سپاری شده از طریق قرارداد و دیگر توافقنامه‌های دوطرفه بین سازمان و تأمین‌کنندگانی که به آن‌ها برون‌سپاری شده است، به کار گرفته شود. توصیه می‌شود سازمان تأیید کند که سخت‌گیری اصول مهندسی امنیت تأمین‌کننده قابل‌مقایسه با خود سازمان است.

اطلاعات دیگر

توصیه می‌شود روش‌های اجرایی توسعه برنامه‌های کاربردی، از فناوری‌های مهندسی امن برای توسعه برنامه های کاربردی که دارای واسط ورودی و خروجی هستند، استفاده کنند. فناوری‌های مهندسی امن، راهنمایی‌هایی برای فناوری‌های احراز اصالت کاربر، کنترل امن نشست و اعتبارسنجی داده، بهسازی و مرتفع سازی و اشکال‌زدایی کدها فراهم می‌آورد.

۱۴-۲-۶ محیط توسعه امن

کنترل

توصیه می‌شود، سازمان‌ها محیط‌های توسعه امن را جهت توسعه و یکپارچه‌سازی سیستم که کل چرخه توسعه سیستم را در برمی‌گیرد، مستقر و به‌طور مناسب حفاظت کنند.

راهنمای پیاده‌سازی

محیط توسعه امن شامل افراد، فرآیندها و فن‌آوری مرتبط با توسعه سامانه و یکپارچه‌سازی است.

توصیه می‌شود سازمان‌ها، مخاطرات مرتبط با تلاش‌های توسعه سامانه‌های فردی را ارزیابی و محیط‌های توسعه امن برای تلاش‌های خاص توسعه سامانه را، با لحاظ کردن موارد زیر مستقر کنند:

الف- حساسیت داده‌هایی که توسط سامانه باید پردازش، ذخیره و منتقل شود؛

ب- الزامات داخلی و خارجی قابل‌اجرا، به‌عنوان‌مثال مقررات یا خط‌مشی‌ها؛

پ- کنترل‌های امنیتی که در حال حاضر توسط سازمان جهت حمایت از توسعه سامانه پیاده‌سازی شده است؛

ت- قابل‌اعتماد بودن کارکنان مشغول به کار در محیط (به بند ۷-۱-۱ مراجعه شود)؛

ث- میزان برون‌سپاری مرتبط با توسعه سیستم؛

ج- نیاز به جداسازی بین محیط‌های توسعه مختلف؛

چ- کنترل دسترسی به محیط توسعه؛

ح- پایش تغییر در محیط و کدهای ذخیره‌شده در آن؛

خ- ذخیره شدن پشتیبان‌ها در مکان‌های امن دور؛

د- کنترل حرکت داده‌ها از و به محیط.

توصیه می‌شود هنگامی‌که سطح حفاظت برای یک محیط توسعه خاص تعیین شد، سازمان فرآیندهای مرتبط با روش‌های اجرایی توسعه امن را مستند و آن را به تمام افرادی که به آن‌ها نیاز دارند ارائه کند.

۱۴-۲-۷ توسعهٔ برون‌سپاری شده

کنترل

توصیه می‌شود، سازمان فعالیت توسعه سامانه به‌صورت برون‌سپاری شده را، نظارت و پایش کند.

راهنمای پیاده‌سازی

توصیه می‌شود درزمانی که توسعه سامانه‌ها برون‌سپاری شده است، نکات زیر در کل زنجیره تأمین خارجی سازمان در نظر گرفته شود:

الف- تمهیدات صدور پروانه، مالکیت کد و حقوق مالکیت معنوی مربوط به محتوای برون‌سپاری شده (به بند ۱۸-۱-۲ مراجعه شود)؛

ب- الزامات قراردادی برای شیوه‌های امن طراحی، برنامه‌نویسی و آزمون (به بند ۱۴-۲-۱ مراجعه شود)؛

پ- ارائه مدل تهدید تأییدشده به توسعه‌دهنده بیرونی؛

ت- آزمون پذیرش برای کیفیت و دقت تحویل دادنی‌ها؛

ث- ارائه شواهدی که نشان‌دهنده‌ی استفاده از آستانه‌های امنیتی برای استقرار کمینه سطوح قابل‌قبول کیفیت امنیت و حریم خصوصی باشد؛

ج- ارائه شواهدی که نشان‌دهنده‌ی انجام آزمون کافی جهت محافظت در برابر عدم وجود محتوای مخرب عمدی و غیرعمدی در زمان تحویل باشد؛

چ- ارائه شواهدی که نشان‌دهنده‌ی انجام آزمون کافی جهت محافظت در برابر وجود آسیب‌پذیری‌های شناخته‌شده باشد؛

ح- تمهیدات واگذاری، به‌عنوان‌مثال اگر کد منبع دیگر در دسترس نیست؛

خ- حق معنوی مربوط به ممیزی فرایندهای توسعه و کنترل‌ها؛

د- مستندات مؤثر از محیط ساخت مورداستفاده برای ایجاد تحویل دادنی‌ها؛

ذ- سازمان مسئول انطباق با قوانین کاربردپذیر و تأیید کارایی کنترل باقی می‌ماند.

اطلاعات دیگر

اطلاعات بیشتر در ارتباط با تأمین‌کنندگان را می‌توان در ISO/IEC 27036 [۲۱] [۲۲] [۲۳] یافت.

۱۴-۲-۸ آزمون امنیت سامانه

کنترل

توصیه می‌شود، آزمون کارکرد امنیتی، در طول توسعه انجام شود.

راهنمای پیاده‌سازی

سامانه جدید و به‌روزرسانی شده، نیازمند آزمایش کامل و درستی سنجی در طی فرایندهای توسعه است که شامل آماده کردن برنامه‌ریزی تفصیلی از فعالیت‌ها و ورودی‌های آزمون و خروجی مورد انتظار در طیف وسیعی از شرایط است. توصیه می‌شود برای توسعه درون‌سازمانی، این‌گونه آزمون‌ها در ابتدا، توسط گروه‌های توسعه‌دهنده انجام شود. توصیه می‌شود پس‌ازآن، آزمون پذیرش مستقل (برای هردو نوع، توسعه درون‌سازمانی و توسعه برون‌سپاری) انجام شود تا اطمینان حاصل شود که سامانه طبق انتظار و فقط طبق انتظار کار می‌کند (به بندهای ۱۴-۱-۱ و ۱۴-۱-۹ مراجعه شود). توصیه می‌شود، گستره آزمون نسبت به اهمیت و ماهیت سامانه باشد.

۱۴-۲-۹ آزمون پذیرش سامانه

کنترل

توصیه می‌شود، آزمون پذیرش برنامه‌ها و معیارهای مرتبط برای سامانه‌های اطلاعاتی جدید، ارتقاها و ویرایش‌های جدید، ایجاد شود.

راهنمای پیاده‌سازی

توصیه می‌شود، آزمون پذیرش سامانه شامل آزمودن الزامات امنیت اطلاعات (به بندهای ۱۴-۱-۱ و ۱۴-۱-۲ مراجعه شود) و پایبندی به شیوه‌های امن توسعه سامانه (به بند ۱۴-۲-۱ مراجعه شود) باشد. همچنین توصیه می‌شود آزمون روی مؤلفه‌های دریافت شده و سامانه‌های یکپارچه‌شده انجام شود. سازمان می‌تواند ابزار خودکار، مانند ابزارهای تحلیل کد یا پویش‌گر آسیب‌پذیری را بکار گیرد و توصیه می‌شود درستی‌سنجی کند که نقایص امنیتی مرتفع شده‌اند.

توصیه می‌شود آزمون در یک محیط آزمون واقعی انجام شود تا اطمینان حاصل شود که سامانه، آسیب‌پذیری را به محیط سازمان ارائه نمی‌کند و آن آزمون‌ها قابل‌اطمینان هستند.

۱۴-۳ داده آزمون

قصد: حصول اطمینان از محافظت داده مورداستفاده برای آزمایش.

۱۴-۳-۱ حفاظت از داده‌های آزمون

کنترل

توصیه می‌شود، داده‌های آزمایشی، به‌دقت انتخاب‌شده، محافظت و کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود از به کار بردن داده‌های عملیاتی که حاوی اطلاعات قابل‌شناسایی شخصی یا هر اطلاعات محرمانه دیگری است، برای اهداف آزمون، اجتناب شود. توصیه می‌شود اگر اطلاعات قابل‌شناسایی شخصی یا اطلاعات محرمانه برای اهداف آزمون مورداستفاده قرار گیرد، تمام جزئیات و محتوای حساس قبل از استفاده حذف شوند یا تغییر کنند (به ISO/IEC 29101 [۲۶] مراجعه شود).

توصیه می‌شود راهنمایی‌های زیر برای محافظت از داده‌های عملیاتی زمانی که برای اهداف آزمونی استفاده می‌شود به کار گرفته شود:

الف- توصیه می‌شود روش‌های اجرایی کنترل دسترسی که در سامانه‌های کاربردی عملیاتی به کار می‌روند، در سامانه‌های کاربردی تحت آزمون به کار روند؛

ب- توصیه می‌شود هر زمان که اطلاعات عملیاتی به محیط آزمون رونویسی می‌شود مجوز جداگانه‌ای لازم باشد؛

پ- توصیه می‌شود اطلاعات عملیاتی بلافاصله پس از کامل شدن آزمون، از محیط آزمون، حذف شوند؛

ت- توصیه می‌شود رونویسی کردن و استفاده از اطلاعات عملیاتی، برای فراهم کردن رد ممیزی، واقعه‌نگاری شود.

اطلاعات دیگر

آزمون پذیرش و سامانه معمولاً نیازمند حجم‌های مهمی از داده‌های آزمون هستند که تا حد امکان به داده-های عملیاتی نزدیک است.

۱۵ ارتباط با تأمین‌کنندگان

۱۵-۱ امنیت اطلاعات در ارتباط با تأمین‌کنندگان

قصد: حصول اطمینان از حفاظت دارایی‌های سازمان که در دسترس تأمین‌کنندگان است.

۱۵-۱-۱ خط‌مشی امنیت اطلاعات برای ارتباط با تأمین‌کنندگان

کنترل

توصیه می‌شود، الزامات امنیت اطلاعات برای کاهش مخاطرات مربوط به دسترسی تأمین‌کنندگان به دارایی-های سازمان توافق شده و مستند شود.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان، کنترل‌های امنیت اطلاعات جهت دسترسی تأمین‌کنندگان به اطلاعات سازمان را در خط‌مشی به‌طور خاص شناسایی و ابلاغ کند. توصیه می‌شود این کنترل‌ها، فرآیندها و روش‌های اجرایی که توسط سازمان باید پیاده‌سازی شوند را پوشش دهد و همچنین فرآیندها و روش‌های اجرایی که سازمان خواهان الزام شدن برای تأمین‌کنندگان است شامل:

الف- شناسایی و مستندسازی انواع تأمین‌کنندگان، به‌عنوان‌مثال خدمات فناوری اطلاعات، تدارکات خدمات شهری، خدمات مالی، اجزای زیرساخت فناوری اطلاعات، کسانی که این سازمان برای دسترسی به اطلاعات خود، به آن‌ها اجازه می‌دهد؛

ب- یک فرآیند استانداردشده و چرخه عمر برای مدیریت روابط با تأمین‌کنندگان؛

پ- تعریف انواع دسترسی به اطلاعات که انواع مختلف تأمین‌کنندگان مجاز به آن دسترسی خواهند شد و پایش و کنترل دسترسی؛

ت- کمینه الزامات امنیت اطلاعات برای هر نوع اطلاعات و هر نوع دسترسی برای به‌کارگیری به‌عنوان پایه‌ای برای توافقنامه‌های هر یک از تأمین‌کنندگان بر اساس الزامات و نیازهای کسب‌وکار سازمان و مشخصات مخاطرات آن؛

ث- فرآیندها و روش های اجرایی برای پایش پایبندی به استقرار الزامات امنیت اطلاعات برای هر نوع تأمین‌کننده و هر نوع دسترسی، ازجمله بازنگری شخص ثالث و اعتبارسنجی محصول؛

ج- کنترل‌های مرتبط با دقت و کامل بودن برای اطمینان از یکپارچگی اطلاعات و یا پردازش اطلاعات انجام‌شده توسط هریک از دو طرف؛

چ- انواع تعهدات قابل‌اجرا توسط تأمین‌کنندگان جهت محافظت از اطلاعات سازمان؛

ح- رسیدگی به رخدادها و شرایط احتیاطی مرتبط با دسترسی تأمین‌کنندگان شامل مسئولیت‌های سازمان و تأمین‌کنندگان؛

خ- انعطاف‌پذیری و در صورت لزوم، بازیابی و تمهیدات احتمالی برای اطمینان از دسترس‌پذیری اطلاعات یا پردازش اطلاعات انجام‌شده توسط هریک از دو طرف؛

د- آموزش آگاه‌سازی برای کارکنان درگیر در سازمان برای جمع‌آوری با توجه به خط‌مشی‌ها، فرآیندها و روش‌های اجرایی کاربردپذیر؛

ذ- آموزش آگاه‌سازی برای کارکنان سازمان که در تعامل با کارکنان تأمین‌کننده هستند، در مورد قواعد مناسب اشتغال و رفتار بر اساس نوع تأمین‌کننده و سطح دسترسی تأمین‌کننده به سامانه‌های سازمان و اطلاعات؛

ر- شرایطی که بر اساس آن، الزامات امنیت اطلاعات و کنترل‌ها در توافق امضاشده توسط هر دو طرف، مستند خواهد شد؛

ز- مدیریت انتقال‌های موردنیاز اطلاعات، تسهیلات پردازش اطلاعات و هر چیزی دیگری که نیاز به انتقال دارد و حصول اطمینان از حفظ امنیت اطلاعات در طی انتقال.

اطلاعات دیگر

اطلاعات را می‌توان با مدیریت ناکافی امنیت اطلاعات، در معرض مخاطرات توسط تأمین‌کنندگان قرارداد. توصیه می‌شود کنترل‌ها، برای اداره کردن دسترسی تأمین‌کنندگان به تسهیلات پردازش اطلاعات شناسایی و بکار گرفته شود. به‌عنوان‌مثال، اگر نیاز خاصی برای محرمانه بودن اطلاعات وجود دارد، توافقنامه عدم افشا می‌تواند مورداستفاده قرار گیرد. مثال دیگر مخاطرات حفاظت از داده‌ها زمانی است که توافق‌نامه تأمین‌کننده شامل انتقال یا دسترسی به اطلاعات فراتر از مرزهای سازمان است. سازمان باید آگاه باشد مسئولیت قانونی یا قراردادی حفاظت از اطلاعات، با سازمان باقی می‌ماند.

۱۵-۱-۲ پرداختن به امنیت درون توافقنامه‌های تأمین‌کننده

کنترل

توصیه می‌شود، تمامی الزامات امنیت اطلاعات، با هر تأمین‌کننده که امکان دسترسی، پردازش، ذخیره، مبادله یا تهیه اجزاء زیرساخت فن‌آوری اطلاعات برای اطلاعات سازمان را دارد، ایجاد و توافق شود.

راهنمای پیاده‌سازی

توصیه می‌شود، توافق‌نامه‌هایی با تأمین‌کنندگان، استقراریافته و مستند شود تا اطمینان حاصل شود که سوءتفاهمی بین سازمان و تأمین‌کنندگان در مورد تعهدات دو طرف برای انجام الزامات امنیت اطلاعات، وجود ندارد.

توصیه می‌شود مفاد زیر، برای برآورده سازی الزامات شناسایی‌شده امنیت اطلاعات، در توافق‌نامه‌ها قرار گیرد:

الف- توصیفی از اطلاعاتی که توصیه می‌شود فراهم آید یا مورد دسترسی واقع شود و روش‌هایی برای دسترسی یا فراهم آوری اطلاعات؛

ب- طبقه‌بندی اطلاعات بر اساس طرح طبقه‌بندی سازمان (به بند ۸-۲ مراجعه شود)؛ اگر لازم است همچنین یک نگاشت بین طرح طبقه‌بندی سازمان و طرح طبقه‌بندی تأمین‌کننده؛

پ- الزامات قانونی و قراردادی شامل محافظت از داده‌ها، حقوق مالکیت معنوی و حق نشر و توصیفی از چگونگی حصول اطمینان از انجام شدن آن؛

ت- تعهدات هر یک از دو طرف قرارداد برای استقرار مجموعه کنترل‌های موردتوافق شامل کنترل دسترسی، بازنگری عملکرد، پایش، گزارش‌گیری و ممیزی؛

ث- قواعد استفاده پسندیده از اطلاعات، شامل استفاده‌های ناپسند در صورت لزوم؛

ج- فهرست تصریح‌شده از افراد تأمین‌کننده که مجاز به دسترسی هستند یا دریافت اطلاعات یا روش‌های اجرایی یا شرایط سازمان برای مجوز دهی و سلب مجوز، برای دسترسی یا تحویل اطلاعات سازمان توسط کارکنان تأمین‌کننده؛

چ- خط‌مشی‌های امنیت اطلاعات مرتبط با قرارداد خاص؛

ح- الزامات و روش‌های اجرایی مدیریت رخداد (مخصوصاً اخطار و همکاری در مدت ترمیم رخداد)؛

خ- الزامات آموزش و آگاه‌سازی برای الزامات و روش‌های اجرایی خاص امنیت اطلاعات، به‌عنوان‌مثال برای پاسخ به رخداد، روش‌های اجرایی مجوز دهی؛

د- قوانین مرتبط برای پیمانکاران فرعی، شامل کنترل‌هایی که لازم است پیاده‌سازی شود؛

ذ- طرفین توافقنامه مرتبط، شامل اطلاعات تماس فرد مرتبط برای موارد امنیت اطلاعات؛

ر- اگر الزامات غربالگری برای کارکنان تأمین‌کننده وجود دارد، شامل مسئولیت‌هایی برای هدایت غربالگری و روش‌های اجرایی اخطار برای مواقعی که غربالگری تکمیل‌نشده است و یا نتایج مشکوک یا مورد دغدغه داشته است؛

ز- حق ممیزی فرایندهای تأمین‌کننده و کنترل‌های مرتبط با توافق‌نامه؛

ژ- فرایندهای رفع نقص و رفع تضاد؛

س- تعهدات تأمین‌کننده برای ارائه منظم گزارش‌های مستقل در مورد کارایی کنترل‌ها و توافق برای اصلاح موارد مشخص‌شده مرتبط در گزارش‌ها در زمان مناسب؛

ش- تعهدات تأمین‌کننده برای انطباق با الزامات امنیتی سازمان.

سایر اطلاعات

توافق‌نامه‌ها ممکن است برای سازمان‌های مختلف و در میان انواع مختلف تأمین‌کنندگان، متفاوت باشند. بنابراین، توصیه می‌شود که مراقبت شود که تمام مخاطرات و الزامات مرتبط امنیت اطلاعات وجود داشته باشد. توافق‌نامه‌های تأمین‌کننده، ممکن است دیگران (مانند تأمین‌کنندگان فرعی) را نیز درگیر کند. روش های اجرایی برای استمرار پردازش درصورتی‌که پیمانکار از تأمین محصولات یا خدماتش ناتوان باشد، لازم است در توافق‌نامه در نظر گرفته شود تا از هرگونه تأخیر در هماهنگ کردن محصولات یا خدمات جایگزینی اجتناب شود.

۱۵-۱-۳ زنجیره تأمین فناوری اطلاعات و ارتباطات

کنترل

توصیه می‌شود، توافق‌نامه‌ها با تأمین‌کنندگان شامل الزاماتی برای پرداختن به مخاطرات امنیت اطلاعات مربوط به زنجیره تأمین خدمات و محصولات فناوری اطلاعات و ارتباطات باشد.

راهنمای پیاده‌سازی

توصیه می‌شود موضوعات زیر برای گنجاندن در توافق‌نامه‌های تأمین‌کنندگان در ارتباط با امنیت در زنجیره تأمین در نظر گرفته شود:

الف- تعریف الزامات امنیت اطلاعات جهت به‌کارگیری در تهیه محصول یا خدمات فناوری اطلاعات و ارتباطات علاوه بر الزامات امنیت اطلاعات عمومی برای ارتباط با تأمین‌کننده؛

ب- برای خدمات فناوری اطلاعات و ارتباطات، نیازاست که تأمین‌کنندگان نیازمندی‌های امنیتی سازمان را در سراسر زنجیره عرضه انتشار دهند؛ درصورتی‌که تأمین‌کنندگان دارای قرارداد فرعی برای بخشی از خدمات فناوری اطلاعات و ارتباطات ارائه‌شده به سازمان باشند؛

پ- برای محصولات فناوری اطلاعات و ارتباطات، نیاز است که تأمین‌کنندگان شیوه‌های امنیتی مناسبی در سراسر زنجیره عرضه انتشار دهند؛ اگر این محصولات شامل اجزای خریداری‌شده از سایر تأمین‌کنندگان باشد؛

ت- پیاده‌سازی یک فرایند پایش و روش‌های قابل‌قبول برای اعتبارسنجی این‌که محصولات و خدمات فناوری اطلاعات و ارتباطات تحویل داده‌شده، به‌وضوح پایبند به الزامات امنیت هستند؛

ث- پیاده‌سازی یک فرایند برای شناسایی اجزای محصول یا خدمات که برای حفظ عملکرد، حیاتی هستند و درنتیجه به توجه و بررسی بیشتری، زمانی که در خارج ساخته‌شده‌اند، نیاز دارند به‌خصوص اگر تأمین‌کننده سطح بالا[1]، برخی از اجزای محصول و یا خدمات را به دیگر تأمین‌کنندگان برون‌سپاری کرده باشد؛

ج- حصول اطمینان از اینکه اجزای مهم و منشأ آن‌ها را در سراسر زنجیره تأمین می‌توان ردیابی کرد؛

چ- حصول اطمینان از اینکه محصولات فناوری اطلاعات و ارتباطات ارائه‌شده، عملکرد لازم را بدون هیچ ویژگی غیرمنتظره و یا ناخواسته، طبق انتظار انجام می‌دهند؛

ح- تعریف قواعدی برای به اشتراک‌گذاری اطلاعات در مورد زنجیره تأمین و همه موارد بالقوه‌ای که بین سازمان و تأمین‌کنندگان به مصالحه افتاده است؛

خ- پیاده‌سازی فرآیندهای خاص برای مدیریت چرخه عمر اجزاء فناوری اطلاعات و ارتباطات و دسترس‌پذیری و مخاطرات امنیتی مرتبط. این، شامل مدیریت مخاطرات اجزای دیگر که در حال حاضر در دسترس نیست؛ به این دلیل که تأمین‌کنندگان، دیگر در کسب‌وکار نیستند و یا تأمین‌کنندگان هیچ‌یک از این اجزاء را با توجه به پیشرفت فناوری ارائه نمی‌کنند؛ نیز هست.

اطلاعات دیگر

1 - Top tier

شیوه‌های خاص مدیریت مخاطرات زنجیره تـأمین فنـاوری اطلاعـات و ارتباطـات بـر روی امنیـت اطلاعـات عمومی، کیفیت، مدیریت پروژه و شیوه مهندسی سامانه قرار دارد، اما جایگزین آن‌ها نیست.

به سازمان‌ها توصیه می‌شود با تأمین‌کنندگانی کار کنند که زنجیره تأمین فناوری اطلاعات و ارتباطـات و یـا موضوعاتی که تأثیر مهمی در محصولات و خدمات ارائه‌شده دارد را درک کرده‌اند. سازمان می‌تواند بر شیوه-های امنیت اطلاعات زنجیره تأمین فناوری اطلاعات و ارتباطات، با شفاف‌سازی توافق‌نامه‌ها با تأمین‌کنندگان خود که توصیه می‌شود در زنجیره تأمین فناوری اطلاعات و ارتباطات سایر تأمین‌کنندگان بیان شـود، تـأثیر بگذارد.

زنجیره تأمین فناوری اطلاعات و ارتباطات اشاره‌شده در اینجا شامل خدمات پردازش ابری نیز می‌شود.

۱۵-۲ مدیریت تحویل خدمت تأمین‌کننده

قصد: نگهداری یک سطح موردتوافق امنیت اطلاعات و تحویل خدمت، در راستای توافق‌نامه‌های تأمین‌کننده.

۱۵-۲-۱ پایش و بازنگری خدمات تأمین‌کننده

کنترل

توصیه می‌شود، سازمان‌ها تحویل خدمت تأمین‌کننده را به‌صورت منظم پایش، بازنگری و ممیزی کنند.

راهنمای پیاده‌سازی

توصیه می‌شود پایش و بازنگری خدمات تأمین‌کننده، تضمینی بر رعایت مفاد و شرایط توافق‌نامه مربوط به امنیت اطلاعات و نیز مدیریت رخدادها و مشکلات امنیت اطلاعات به‌صورت مطلوب باشد.

توصیه می‌شود این موضوع دربرگیرنده فرایند ارتباط مدیریت خدمت بین سازمان و تأمین‌کننده باشد تا:

الف- سطوح عملکرد خدمت را جهت اعتبارسنجی پایبندی به توافق‌نامه پایش کند؛

ب- بازنگری گزارش‌های ارائه‌شده خدمت توسط تأمین‌کننده و ترتیب دادن جلسات منظم برای بررسی تطابق روند پیشرفت با مفاد توافق‌نامه؛

پ- ممیزی تأمین‌کنندگان را اجرا کند و در صورت امکان، این ممیزی به همراه بازنگری گزارش‌های ممیز مستقل صورت گرفته و موارد مشخص‌شده را پیگیری کند؛

ت- اطلاعاتی در رابطه با رخدادهای امنیت اطلاعات ارائه دهد و این اطلاعات را همان‌گونه که در توافق‌نامه‌ها و هر راهنمایی و روش اجرایی پشتیبان، الزام شده است، بازنگری کند؛

ث- دنباله‌های ممیزی تأمین‌کننده و سوابق رویدادهای امنیت اطلاعات، مشکلات عملیاتی، خرابی و ردیابی نقایص و اختلالات در رابطه با خدمات ارائه‌شده را بازنگری کند؛

ج- هر مشکل شناسایی‌شده‌ای را حل و مدیریت کند؛

چ- جنبه‌های امنیت اطلاعات روابط تأمین‌کننده با تأمین‌کنندگانش را بازنگری کند؛

ح- اطمینان حاصل کند که تأمین‌کننده، ظرفیت کافی خدمت را به همراه طرح‌های قابل‌اجرا، حفظ کرده تا اطمینان حاصل کند که سطوح تداوم خدمت توافق شده باوجود خرابی عمده یا حوادث در خدمت، حفظ می‌شود (به بند ۱۷ مراجعه شود).

توصیه می‌شود مسئولیت مدیریت روابط با تأمین‌کننده، به یک فرد منصوب‌شده یا به گروه مدیریت خدمت سپرده شود. به‌علاوه، توصیه می‌شود سازمان اطمینان حاصل کند که تأمین‌کنندگان، مسئولیت‌های بازنگری تطابق و اجبار الزامات توافق‌نامه را منتصب کرده‌اند. توصیه می‌شود منابع و مهارت‌های فنی کافی در دسترس قرار گیرد تا پایش الزامات توافق‌نامه به‌خصوص الزامات امنیت اطلاعات انجام شود. توصیه می‌شود اقدام مناسب، زمانی که عدم‌کفایت در ارائه خدمات مشاهده می‌شود، انجام شود.

توصیه می‌شود سازمان در تمام جنبه‌های امنیتی مربوط به اطلاعات حساس یا حیاتی یا تسهیلات پردازش اطلاعات که مورد دسترسی یا پردازش یا مدیریت تأمین‌کننده قرار دارند، میدان دید و کنترل جامع و کافی خود را حفظ کند. توصیه می‌شود سازمان، میدان دید مربوط به فعالیت‌های امنیتی نظیر مدیریت تغییرات، شناسایی آسیب‌پذیری‌ها و رخدادهای امنیت اطلاعات که از طریق فرایند گزارش دهی تعریف‌شده، دریافت و پاسخ‌دهی می‌شود را حفظ کند.

۱۵-۲-۲ مدیریت تغییرات در خدمات تأمین‌کننده

کنترل

توصیه می‌شود، تغییرات در ارائه خدمات توسط تأمین‌کننده، شامل نگهداری و بهبود خط‌مشی‌های امنیت اطلاعات، روش‌های اجرایی و کنترل‌های موجود، با توجه به میزان بحرانی بودن اطلاعات کسب‌وکار، سامانه‌ها و فرآیندهای مرتبط و برآورد مجدد مخاطرات، مدیریت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود جنبه‌های زیر در نظر گرفته شود:

الف- تغییرات در توافق‌نامه‌های تأمین‌کنندگان؛

ب- تغییرات ایجادشده توسط سازمان برای پیاده‌سازی:

۱- بهبود پیشنهادشده برای هر یک از خدمات جاری؛
۲- توسعه هر یک از برنامه‌های کاربردی و سامانه‌های جدید؛
۳- اصلاحات یا به‌روزآوری خط‌مشی‌ها و روش‌های اجرایی سازمان؛
۴- کنترل‌های جدید یا تغییریافته برای حل رخدادهای امنیت اطلاعات و بهبود امنیت؛

پ- تغییرات در خدمات تأمین‌کننده برای پیاده‌سازی:

۱- تغییرات و بهبود شبکه‌ها؛
۲- استفاده از فناوری‌های جدید؛

۳- استفاده از محصولات جدید یا نشرها یا نسخه‌های جدیدتر محصول؛
۴- ابزارها و محیط‌های جدید توسعه؛
۵- تغییرات در محل فیزیکی تجهیزات خدمات؛
۶- تغییر تأمین‌کنندگان؛
۷- قرارداد فرعی با تأمین‌کننده دیگر.

۱۶ مدیریت رخداد امنیت اطلاعات

۱-۱۶ مدیریت رخدادهای امنیت اطلاعات و بهبودها

قصد: حصول اطمینان از رویکردی استوار و مؤثر برای مدیریت رخدادهای امنیت اطلاعات، شامل ارتباط در مورد رویدادهای امنیتی و ضعف‌ها.

۱-۱-۱۶ مسئولیت‌ها و روش‌های اجرایی

کنترل

توصیه می‌شود، به‌منظور حصول اطمینان از یک پاسخ سریع، مؤثر و منظم به رخدادهای امنیت اطلاعات، مسئولیت‌های مدیریتی و روش‌های اجرایی ایجاد شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر برای مسئولیت‌های مدیریت و روش‌های اجرایی با توجه به مدیریت رخداد امنیت اطلاعات، در نظر گرفته شود:

الف- توصیه می‌شود مسئولیت‌های مدیریت استقرار یابد تا اطمینان حاصل شود که روش‌های اجرایی زیر به‌اندازه کافی توسعه و در درون سازمان ابلاغ‌شده‌اند:

۱- روش‌های اجرایی برای طرح‌ریزی و آماده‌سازی پاسخ‌دهی به رخداد؛

۲- روش‌های اجرایی برای پایش، تشخیص، تحلیل و گزارش از رویدادها و رخدادهای امنیت اطلاعات؛

۳- روش‌های اجرایی برای واقعه‌نگاری فعالیت‌های مدیریت رخداد؛

۴- روش‌های اجرایی برای اداره کردن شواهد[1]؛

۵- روش‌های اجرایی برای ارزیابی و تصمیم‌گیری در مورد رویدادهای امنیت اطلاعات و ارزیابی نقاط ضعف امنیت اطلاعات؛

۶- روش‌های اجرایی جهت پاسخ‌دهی به‌خصوص در موارد ارجاع به مقامات بالاتر، بازیابی کنترل‌شده از یک رخداد و اطلاع‌رسانی به افراد داخل و خارج سازمان؛

1 - forensic

ب- توصیه می‌شود روش‌های اجرایی استقراریافته اطمینان دهند که:

۱- کارکنان شایسته، به مسائل مربوط به رخدادهای امنیت اطلاعات در سازمان رسیدگی می‌کنند؛

۲- نقطه تماس برای تشخیص و گزارش رخدادهای امنیتی، پیاده‌سازی شده است؛

۳- اطلاعات تماس مناسب با مقامات، گروه‌های ذینفع بیرونی و یا انجمن‌هایی که مسئولیت رسیدگی به مسائل مربوط به رخدادهای امنیت اطلاعات رادارند، حفظ‌شده است؛

پ- توصیه می‌شود روش‌های اجرایی گزارش دهی، شامل موارد زیر باشند:

۱- آماده‌سازی فرم‌های گزارش دهی رویداد امنیت اطلاعات برای حمایت از گزارش دهی و برای کمک به فرد گزارش دهنده جهت یادآوری تمام اقدامات لازم در مورد یک رویداد امنیت اطلاعات؛

۲- روش اجرایی بکار گرفته‌شده در رویداد امنیت اطلاعات، به‌عنوان‌مثال اعلام بی‌درنگ تمام جزئیات، مانند نوع عدم انطباق یا نقض، بدعمل کردن، پیام در صفحه‌نمایش و بلافاصله گزارش دهی به نقطه تماس و فقط انجام اقدامات هماهنگ شده؛

۳- ارجاع به فرایند رسمی انضباطی مستقرشده برای برخورد با کارکنان که مرتکب نقض امنیتی شده‌اند؛

۴- فرآیندهای بازخورد مناسب تا اطمینان حاصل شود که افراد گزارش دهنده‌ی رویدادهای امنیت اطلاعات، پس از برخورد با آن رویداد و بسته شدن آن، از نتایج مطلع شده‌اند.

توصیه می‌شود اهداف برای مدیریت رخداد امنیت اطلاعات، با توافق مدیریت بوده و توصیه می‌شود اطمینان حاصل شود که کسانی که مسئول مدیریت رخداد امنیت اطلاعات هستند، اولویت‌های سازمان را برای رسیدگی به رخدادهای امنیت اطلاعات درک کرده‌اند.

اطلاعات دیگر

رخدادهای امنیت اطلاعات ممکن است از مرزهای سازمانی و ملی فراتر رود. برای پاسخ به این رخدادها، نیاز روزافزون به هماهنگ کردن واکنش‌ها و به اشتراک‌گذاری اطلاعات در مورد این رخدادها با سازمان‌های بیرونی به شکل مناسب وجود دارد.
راهنمایی تفصیلی در مدیریت رخداد امنیت اطلاعات در ISO/IEC 27035 [۲۰] ارائه‌شده است.

۲-۱-۱۶ گزارش‌دهی رویدادهای امنیت اطلاعات

کنترل

توصیه می‌شود، رویدادهای امنیت اطلاعات در کوتاه‌ترین زمان ممکن، از طریق مجاری مدیریتی مناسب، گزارش شوند.
راهنمای پیاده‌سازی

توصیه می‌شود تمام کارکنان و پیمانکاران از مسئولیتشان در گزارش دهی رویدادهای امنیت اطلاعات در اسرع وقت، آگاه شوند. توصیه می‌شود آن‌ها همچنین از روش اجرایی گزارش دهی رویدادهای امنیت اطلاعات و محل تماس که توصیه می‌شود رویدادها به آنجا گزارش شود، آگاه باشند.

توصیه می‌شود شرایطی که باید برای گزارش رویداد امنیت اطلاعات در نظر گرفته شود عبارت‌اند از:

الف- کنترل امنیتی بی‌اثر؛

ب- نقض انتظارات از یکپارچگی، محرمانگی یا دسترس‌پذیری اطلاعات؛

پ- خطاهای انسانی؛

ت- عدم انطباق با خط‌مشی‌ها و یا راهنمایی‌ها؛

ث- نقض تمهیدات امنیت فیزیکی؛

ج- تغییرات کنترل نشده سامانه؛

چ- بدعمل کردن نرم‌افزار یا سخت‌افزار؛

ح- نقض در دسترسی.

اطلاعات دیگر

عملکرد نامناسب یا دیگر رفتارهای نامناسب سامانه، ممکن است نشان‌دهنده یک حمله امنیتی یا رخنه واقعی امنیت باشد و بنابراین توصیه می‌شود همیشه به‌عنوان رویداد امنیت اطلاعات گزارش شود.

۳-۱-۱۶ گزارش دهی ضعف‌های امنیتی

کنترل

توصیه می‌شود، کارکنان و پیمانکارانی که از سامانه‌ها و خدمات اطلاعاتی سازمان استفاده می‌کنند، نسبت به توجه و گزارش دهی هر ضعف امنیتی مشاهده‌شده یا مورد سوءظن در سامانه‌ها یا خدمات، ملزم شوند.

راهنمای پیاده‌سازی

توصیه می‌شود تمام کارمندان، پیمانکاران این موضوعات را در اولین فرصت ممکن به محل تماس، گزارش کنند تا از رخدادهای امنیت اطلاعات جلوگیری شود. توصیه می‌شود سازوکار گزارش دهی تا حد امکان ساده، موجود و در دسترس باشد.

اطلاعات دیگر

توصیه می‌شود به کارکنان و پیمانکاران اطلاع داده شود که سعی نکنند ضعف‌های امنیتی مشکوک را اثبات کنند. آزمون ضعف ممکن است به‌عنوان سوءاستفاده احتمالی از سامانه تلقی شود و همچنین ممکن است

باعث آسیب به سامانه اطلاعات یا خدمات شود و منجر به ایجاد مسئولیت قانونی برای شخصی شود که آزمون را انجام می‌دهد.

۱۶-۱-۴ ارزیابی و تصمیم برای رویدادهای امنیت اطلاعات

کنترل

توصیه می‌شود، رویدادهای امنیت اطلاعات ارزیابی شود و تصمیم‌گیری شود که در صورت نیاز، به‌عنوان رخدادهای امنیت اطلاعات طبقه‌بندی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود نقطه تماس، هر رویداد امنیت اطلاعات را با استفاده از اطلاعات رویداد امنیت اطلاعات و مقیاس توافق شده طبقه‌بندی رخداد، ارزیابی کرده و تصمیم بگیرد که آیا این رویداد باید به‌عنوان یک رخداد امنیت اطلاعات طبقه‌بندی شود. طبقه‌بندی و اولویت‌بندی رخدادها می‌تواند به شناسایی تأثیر و گستره‌ی رخداد کمک کند.

در مواردی که این سازمان دارای یک گروه پاسخ رخداد امنیت اطلاعات (ISIRT)[1] است ارزیابی و تصمیم-گیری را می‌توان به ISIRT برای تأیید یا ارزیابی ارسال کرد.
توصیه می‌شود نتایج ارزیابی و تصمیم‌گیری با جزئیات، به‌منظور مراجعه در آینده و درستی سنجی ثبت شود.

۱۶-۱-۵ پاسخ به رخدادهای امنیت اطلاعات

کنترل

توصیه می‌شود، به رخدادهای امنیت اطلاعات مطابق با روش‌های اجرایی مستند، پاسخ داده شود.

راهنمای پیاده‌سازی

توصیه می‌شود رخدادهای امنیت اطلاعات از طریق یک نقطه تماس تعیین‌شده و سایر افراد سازمان و یا طرف‌های بیرونی مرتبط، پاسخ داده شود (به بند ۱۶-۱-۱ مراجعه شود).

توصیه می‌شود پاسخ شامل موارد زیر باشد:

الف- جمع‌آوری شواهد در اسرع وقت پس از وقوع؛

ب- انجام تحلیل قانونی امنیت اطلاعات، به‌عنوان شواهد موردنیاز (به بند ۱۶-۱-۷ مراجعه شود)؛

پ- ارجاع به مقامات بالاتر، در صورت نیاز؛

ت- اطمینان حاصل شود که تمام فعالیت‌های درگیر پاسخ به‌درستی برای تحلیل‌های بعدی ثبت‌شده است؛

1 - Information Security Incident Response Team

ث- برقراری ارتباط با افراد داخل و خارج سازمان، برای مواردی که نیاز است بدانند، در مورد وجـود رخـداد امنیت اطلاعات یا هرگونه اطلاعات مربوط به آن؛

ج- برخورد با ضعف (های) امنیت اطلاعات که علت یک رخداد است یا در بروز آن، مشارکت دارد؛

چ- زمانی که با موفقیت با رخداد برخورد شد، به‌طور رسمی بسته‌شده و سوابق آن نگهداری شود.

توصیه می‌شود تحلیل پس از رخداد، در صورت لزوم، برای شناسایی منبع رخداد انجام شود.

اطلاعات دیگر

هدف اول در پاسخ به رخداد، ازسرگیری «سطح امنیتی عادی» است و سپس احیای موردنیاز شروع شود.

۱۶-۱-۶ یادگیری از رخدادهای امنیت اطلاعات

کنترل

توصیه می‌شود، دانش به‌دست‌آمده از تحلیل رخـدادهای امنیـت اطلاعـات بـرای کـاهش احتمـال یـا تـأثیر رخدادهای آینده، استفاده شود.

راهنمای پیاده‌سازی

توصیه می‌شود سازوکارهایی جهت ایجاد توانمندی در عددی سازی و پایش برای انواع، حجم‌ها و هزینه‌های رخدادهای امنیت اطلاعات، وجود داشته باشد. توصیه می‌شود اطلاعات به‌دست‌آمده از ارزشـیابی رخـدادهای امنیت اطلاعات، برای شناسایی رخدادهای پر تأثیر یا با تکرار بالا مورداستفاده قرار گیرد.

اطلاعات دیگر

ارزشیابی رخدادهای امنیت اطلاعات ممکن است نشان‌دهنده نیاز به بهبود یا افـزایش کنتـرل بـرای محـدود کردن تواتر، ضرر و هزینه وقایع آینده یا در نظر گرفته شدن در فرایند بازنگری خط‌مشی امنیت باشد (به بند ۵-۱-۲ مراجعه شود).

با رعایت جنبه‌های محرمانگی، بازگویی رخدادهای امنیت اطلاعات واقعی، می‌تواند در آموزش آگـاهی‌رسـانی کاربر (به بند ۷-۲-۲ مراجعه شود) به‌عنوان نمونه‌هایی ازآنچه می‌تواند رخ دهـد، چگونـه بـه ایـن رخـدادها، پاسخ داده می‌شود و چگونه در آینده از آن‌ها اجتناب شود، مورداستفاده قرار گیرد.

۱۶-۱-۷ گردآوری شواهد

کنترل

توصیه می‌شود، سازمان روش‌های اجرایی برای شناسایی، جمع‌آوری، اکتساب و حفاظت از اطلاعات که می‌تواند به‌عنوان شواهد استفاده شود را، تعریف کرده و به کاربرد.

راهنمای پیاده‌سازی

توصیه می‌شود روش‌های اجرایی داخلی توسعه یابند و هنگامی‌که به‌عنوان شواهدی برای اهداف انضباطی و قانونی مطرح هستند، دنبال شود.

به‌صورت کلی، توصیه می‌شود این روش‌های اجرایی برای شواهد، فرآیندهای شناسایی، جمع‌آوری، اکتساب و حفظ شواهد مطابق با انواع مختلف رسانه‌ها، دستگاه‌ها و وضعیت دستگاه‌ها، به‌عنوان‌مثال روشن یا خاموش را فراهم آورد. توصیه می‌شود روش‌های اجرایی موارد زیر را در نظر بگیرد:

الف- زنجیره‌ای از توقیف؛

ب- امنیت شاهد؛

پ- امنیت کارکنان؛

ت- نقش‌ها و مسئولیت‌های کارکنان درگیر؛

ث- صلاحیت کارکنان؛

ج- مستندسازی؛

چ- توجیه.

درجایی که مقدور است، توصیه می‌شود تائیدیه‌ها یا سایر موارد مربوط به صلاحیت کارکنان و ابزارها در جهت تقویت ارزش شواهد جمع‌آوری‌شده، فراهم شود.

شواهد قانونی ممکن است از مرزهای سازمان یا حوزه قضایی فراتر روند. در این موارد، توصیه می‌شود تضمین شود که سازمان حق دارد اطلاعات لازم را به‌عنوان شواهد قانونی جمع‌آوری کند. توصیه می‌شود الزامات حوزه‌های قضایی مختلف نیز برای بیشینه‌سازی شانس پذیرش، فراسوی مرزهای قضایی مرتبط در نظر گرفته شود.

اطلاعات دیگر

شناسایی، فرایندی است که دربرگیرنده جستجو، تشخیص و مستند کردن شواهد بالقوه است. جمع‌آوری، فرایند جمع‌آوری اقلام فیزیکی است که می‌تواند شامل شاهد بالقوه باشد. اکتساب، فرایند ایجاد یک رونوشت از داده‌ها در یک مجموعه تعریف‌شده است. حفظ، فرایندی برای حفظ و امن نگه‌داشتن یکپارچگی و شرایط اصلی شاهد بالقوه است.

هنگامی‌که یک رویداد امنیت اطلاعات برای اولین بار تشخیص داده می‌شود، ممکن است واضح نباشد که آیا این رویداد منجر به یک اقدام دادگاهی می‌شود یا خیر؛ بنابراین این خطر وجود دارد که شواهد لازم عمداً یا به‌طور تصادفی قبل از اینکه میزان جدی بودن این رخداد مشخص شود، نابود شوند. بهتر است با یک وکیل یا پلیس در اوایل هرگونه اقدام قانونی در مورد شواهد موردنیاز، همفکری صورت گیرد.

ISO/IEC 27037 [۲۴] راهنمایی‌هایی برای شناسایی، جمع‌آوری، اکتساب و حفظ شواهد دیجیتال (رقمی) فراهم می‌کند.

۱۷ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار

۱-۱۷ تداوم امنیت اطلاعات

قصد: تداوم امنیت اطلاعات باید به سامانه‌های مدیریت تداوم کسب‌وکار سازمان اعمال شود.

۱-۱-۱۷ طرح‌ریزی تداوم امنیت اطلاعات

کنترل

توصیه می‌شود، سازمان نیازهای خود را برای امنیت اطلاعات و تداوم مدیریت امنیت اطلاعات در موقعیت-های ناسازگار، به‌طور مثال در طول یک بحران یا فاجعه تعیین کند.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان تعیین کند که آیا تداوم امنیت اطلاعات درون فرآیند مدیریت تداوم کسب‌وکار و یا در فرآیند مدیریت بحران قرارگرفته است. توصیه می‌شود نیازمندی‌های امنیت اطلاعات، هنگام برنامه‌ریزی برای تداوم کسب‌وکار و مدیریت بحران تعیین شود.
توصیه می‌شود در صورت عدم وجود طرح‌ریزی رسمی تداوم کسب‌وکار و مدیریت بحران، مدیریت امنیت اطلاعات فرض کند که الزامات امنیت اطلاعات در شرایط نامطلوب در مقایسه با شرایط عملیاتی عادی، یکسان در نظر گرفته می‌شود. درروش دیگر، سازمان می‌تواند تحلیل تأثیر کسب‌وکار را برای جنبه‌های امنیت اطلاعات انجام دهد تا الزامات امنیت اطلاعات قابل‌اعمال به شرایط نامطلوب را تعیین کند.

اطلاعات دیگر

به‌منظور کاهش زمان و تلاش «اضافه» جهت تحلیل تأثیر کسب‌وکار برای امنیت اطلاعات، توصیه می‌شود، جنبه‌های امنیت اطلاعات در مدیریت تداوم کسب‌وکار در شرایط عادی یا در تحلیل تأثیر مدیریت بحران در کسب‌وکار لحاظ شود. به‌صورت ضمنی به این معنی است که الزامات تداوم امنیت اطلاعات به‌صراحت در فرایندهای مدیریت تداوم کسب‌وکار یا مدیریت بحران ضابطه‌مند شده باشد.

اطلاعات در مورد مدیریت تداوم کسب‌وکار را می‌توان در استانداردهای ISO/IEC 27031 [۱۴]، ISO 22313 [۹] و ISO 22301[۸] یافت.

۲-۱-۱۷ پیاده‌سازی تداوم امنیت اطلاعات

کنترل

توصیه می‌شود، برای حصول اطمینان از سطح موردنیاز تداوم امنیت اطلاعات در حین یک موقعیت منفی، سازمان، فرآیندها، روش‌های اجرایی و کنترل‌هایی ایجاد، مستندسازی، پیاده‌سازی و نگهداری کند.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان اطمینان حاصل کند که:

الف- ساختار مدیریتی کافی در محل برای آماده شدن، کاهش و پاسخ به رویدادهای مخرب با استفاده از کارکنان با اختیار، باتجربه و با شایستگی فراهم کند؛

ب- فرد مسئول پاسخگویی به رخداد با مسئولیت، اختیار و شایستگی موردنیاز، جهت مدیریت رخداد امنیتی و نگهداری امنیت اطلاعات انتخاب شود؛

پ- طرح‌های مستند، روش‌های اجرایی پاسخ و احیا، توسعه داده‌شده و مورد تأیید قرار گیرد، با شرح اینکه چگونه سازمان یک رویداد مخرب را مدیریت می‌کند و امنیت اطلاعات خود را در یک سطح از پیش تعیین‌شده بر اساس اهداف، تداوم امنیت اطلاعات مورد تأیید مدیریت، حفظ می‌کند (به بند ۱۷-۱-۱ مراجعه شود).

توصیه می‌شود با توجه به الزامات تداوم امنیت اطلاعات، سازمان موارد زیر را ایجاد، مستند، پیاده‌سازی و حفظ کند:

الف- کنترل‌های امنیت اطلاعات در فرآیندها، روش‌های اجرایی و سامانه‌ها و ابزارهای حمایت تداوم کسب‌وکار یا مدیریت بحران؛

ب- فرآیندها، روش‌های اجرایی و تغییرات پیاده‌سازی برای حفظ کنترل‌های موجود امنیت اطلاعات در طول یک وضعیت نامطلوب؛

پ- کنترل‌های جبرانی برای کنترل‌های امنیت اطلاعات که در طول وضعیت نامطلوب نمی‌توان حفظ کرد.

اطلاعات دیگر

درزمینهٔ تداوم کسب‌وکار یا مدیریت بحران، فرآیندها و روش‌های اجرایی خاص، ممکن است تعریف‌شده باشد. توصیه می‌شود اطلاعاتی که در این فرآیندها و مراحل یا در درون سامانه‌های اطلاعات اختصاصی برای حمایت از آن‌ها، به کار گرفته‌شده است، محافظت شود؛ بنابراین توصیه می‌شود سازمان متخصصان امنیت اطلاعات را در زمان استقرار، پیاده‌سازی و نگهداری فرآیندها و روش‌های اجرایی تداوم کسب‌وکار و مدیریت بحران، درگیر کند.

توصیه می‌شود کنترل‌های امنیت اطلاعات که پیاده‌سازی شده‌اند، در طول شرایط نامطلوب به کار خود ادامه دهند. توصیه می‌شود اگر کنترل‌های امنیتی قادر به حفظ امنیت اطلاعات نیستد، کنترل‌های دیگری برای حفظ سطح قابل قبولی از امنیت اطلاعات مستقر، پیاده‌سازی و نگهداری شوند.

۱۷-۱-۳ درستی‌سنجی، بازنگری و ارزشیابی تداوم امنیت اطلاعات

کنترل

توصیه می‌شود، سازمان کنترل‌های تداوم امنیت اطلاعات، ایجاد و پیاده‌سازی شده را به‌منظور حصول اطمینان از معتبر و مؤثر بودنشان در حین موقعیت‌ها، در بازه‌های زمانی منظم بررسی کند.

راهنمای پیاده‌سازی

تغییرات فرآیندها، روش‌های اجرایی، فنی و سازمانی، چه در زمینهٔ عملیاتی، چه درزمینهٔ تداوم، ممکن است به تغییرات در الزامات تداوم امنیت اطلاعات منجر شود. در چنین مواردی، توصیه می‌شود تداوم فرآیندها، روش‌های اجرایی و کنترل‌ها برای امنیت اطلاعات، در برابر این الزامات تغییریافته، بازنگری شوند.

توصیه می‌شود سازمان‌ها تداوم مدیریت امنیت اطلاعات خود را از طریق موارد زیر بررسی کنند:

الف- تمرین و آزمون عملکرد فرآیندها، روش‌های اجرایی و کنترل‌های تداوم امنیت اطلاعات تا اطمینان حاصل شود که آن‌ها سازگار با اهداف تداوم امنیت اطلاعات هستند؛

ب- تمرین کردن و آزمون، دانش و روال اجرای فرآیندها، روش‌های اجرایی و کنترل‌های تداوم امنیت اطلاعات تا اطمینان حاصل شود که عملکرد آن‌ها مطابق با اهداف تداوم امنیت اطلاعات است؛

پ- بازنگری اعتبار و اثربخشی سنجه‌های تداوم امنیت اطلاعات، زمانی که سامانه‌های اطلاعات، فرآیندهای امنیت اطلاعات، روش‌های اجرایی و کنترل‌ها یا فرآیندها و راه‌حل‌های مدیریت تداوم کسب‌وکار یا مدیریت بازیابی بحران تغییر کند.

اطلاعات دیگر

درستی سنجی کنترل‌های تداوم امنیت اطلاعات، از آزمون و درستی سنجی امنیت اطلاعات عمومی جدا بوده و توصیه می‌شود خارج از حیطه آزمون تغییرات انجام شود. در صورت امکان، ترجیح داده می‌شود که کنترل‌های تداوم امنیت اطلاعات سازمان با آزمون تداوم کسب‌وکار یا مدیریت بحران سازمان یکپارچه شود.

۱۷-۲ افزونگی‌ها

قصد: حصول اطمینان از دسترس‌پذیری تسهیلات پردازش اطلاعات.

۱۷-۲-۱ دسترس‌پذیری تسهیلات پردازش اطلاعات

کنترل

توصیه می‌شود، تسهیلات پردازش اطلاعات، برای برآورده ساختن الزامات دسترس‌پذیری، با افزونگی کافی پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان‌ها الزامات کسب‌وکار برای دسترس‌پذیری سامانه‌های اطلاعات را شناسایی کنند. توصیه می‌شود جایی که دسترس‌پذیری با استفاده از معماری موجود سامانه‌ها تضمین نمی‌شود، مؤلفه‌ها یا معماری افزونه در نظر گرفته شود.

توصیه می‌شود درجایی که کاربردپذیر است، سامانه‌های اطلاعاتی دارای افزونگی، آزموده شوند تا اطمینان حاصل شود که غلبه بر خرابی[1] یک مؤلفه به یک مؤلفه دیگر، طبق انتظار عمل می‌کند.

1 - failover

اطلاعات دیگر

پیاده‌سازی افزونگی‌ها می‌تواند منجر به مخاطرات مربوط به یکپارچگی و یا محرمانگی اطلاعات و سامانه‌های اطلاعاتی شود که نیازاست در هنگام طراحی سامانه‌های اطلاعات، در نظر گرفته شود.

۱۸ انطباق

۱-۱۸ انطباق با الزامات قانونی و قراردادی

قصد: پرهیز از نقض هر نوع قانون، مقررات، تعهدات آئین‌نامه‌ای یا قراردادی مرتبط با امنیت اطلاعات و هر الزام امنیتی.

۱-۱-۱۸ شناسایی الزامات قانونی و قراردادی قابل‌اجرا

کنترل

توصیه می‌شود، تمامی مقررات قانون گزاری، الزامات آئین‌نامه‌ای، قراردادی مرتبط و رویکرد سازمان نسبت به برآورده سازی این الزامات، برای هر سیستم اطلاعاتی و سازمان، به‌وضوح شناسایی‌شده، تدوین‌شده و به‌روز نگه‌داشته شوند.

راهنمای پیاده‌سازی

توصیه می‌شود کنترل‌های خاص و مسئولیت فردی برای پاسخگویی به این نیاز نیز تعریف و مستند شود.
توصیه می‌شود مدیران تمام قوانین قابل‌اجرا در سازمان خود را به‌منظور برآورده سازی الزامات برای نوع کسب‌وکار خود شناسایی کنند. اگر این سازمان کسب‌وکار را در کشورهای دیگر انجام می‌دهد، توصیه می شود مدیران انطباق در همه کشورهای مرتبط را در نظر بگیرند.

۲-۱-۱۸ حقوق دارایی فکری

کنترل

توصیه می‌شود، به‌منظور حصول اطمینان از انطباق با الزامات قانون گزار، الزامات آئین‌نامه‌ای و قراردادی و استفاده از محصولات نرم‌افزاری دارای حقوق تجاری، روش‌های اجرایی مناسب، پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود راهنمایی‌های زیر برای محافظت از هر کالایی که ممکن است به‌عنوان مالکیت فکری در نظر گرفته شود رعایت شود:

الف- انتشار خط‌مشی انطباق با حقوق مالکیت فکری که استفاده قانونی از محصولات نرم‌افزاری و اطلاعاتی را تعریف می‌کند؛

ب- دستیابی به نرم‌افزار فقط از طریق منابع شناخته‌شده و معتبر برای تضمین این‌که حق تکثیر نقض نمی-شود؛

پ- حفظ و آگاهی از خط‌مشی‌ها به‌منظور محافظت از حقوق مالکیت فکری و اطلاع‌رسانی درباره برخورد انضباطی در برابر افراد نقض‌کننده آن‌ها؛

ت- نگهداری گزارش‌های مناسب از دارایی‌ها و شناسایی تمام آن‌ها با الزامات مرتبط به‌منظور محافظت از حقوق مالکیت فکری؛

ث- حفظ شواهد و مدارک مالکیت گواهی‌ها و پروانه‌ها، دیسک‌های اصلی، راهنماها و غیره؛

ج- اجرای کنترل‌هایی برای تضمین این‌که حداکثر استفاده‌کنندگان مجاز از حد خاصی فراتر نمی‌رود؛

چ- انجام بازنگری‌هایی که فقط نرم‌افزارهای مجاز و محصولات دارای مجوز نصب می‌شوند؛

ح- ارائه خط‌مشی برای حفظ شرایط مناسب گواهی؛

خ- ارائه خط‌مشی برای دورریز یا انتقال نرم‌افزار به دیگران؛

د- مطابقت مفاد و شرایط نرم‌افزار و اطلاعات به‌دست‌آمده از شبکه‌های همگانی؛

ذ- عدم تکثیر، تبدیل به قالب دیگر یا استخراج کردن محتوای ضبط‌شده تجاری (تصویر، صوت) غیر از مواردی که در قانون حق تکثیر مجاز دانسته شده‌اند؛

ر- عدم رونوشت برداری کامل یا جزئی از کتاب‌ها، مقالات، گزارش‌ها و دیگر مستندات، غیر از مواردی که در قانون حق تکثیر مجاز دانسته شده‌اند.

اطلاعات دیگر

حقوق مالکیت فکری شامل حق تکثیر نرم‌افزار یا مستندات، حقوق طراحی، علائم تجاری، حق انحصاری و گواهی‌های کد منبع است.

محصولات نرم‌افزاری اختصاصی معمولاً در قالب یک قرارداد دارای مجوز، تهیه می‌شوند که مفاد و شرایط گواهی را مثلاً برای محدود کردن استفاده از محصولات در ماشین‌های خاص یا محدود کردن رونوشت برداری برای ایجاد نسخه‌های پشتیبان مشخص می‌کند. توصیه می‌شود شرایط حقوق مالکیت معنوی یک نرم‌افزار که توسط سازمان توسعه‌یافته است، برای کارکنان روشن شود.

الزامات قانونی، مقرراتی و قراردادی ممکن است محدودیت‌هایی در تکثیر مطالب اختصاصی ایجاد کند. به‌خصوص، ممکن است آن‌ها این‌گونه الزام کنند که فقط مطالبی که توسط سازمان توسعه‌یافته است یا توسط سازنده برای سازمان تهیه یا گواهی‌شده است می‌تواند مورداستفاده قرار گیرد. نقض حق تکثیر ممکن است منجر به اقدام حقوقی شود که دربرگیرنده جریمه و محاکمه کیفری است.

۱۸-۱-۳ حفاظت از سوابق

کنترل

توصیه می‌شود، سوابق، با توجه به الزامات قانونی، آئین‌نامه‌ای، قراردادی و کسب‌وکار، در برابر گم‌شدن، تخریب، تحریف، دسترسی غیرمجاز و پخش غیرمجاز محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود، هنگامی‌که تصمیم بر حفاظت از سوابق خاص سازمانی گرفته می‌شود، طبقه‌بندی مرتبط بر اساس طرح طبقه‌بندی سازمان، در نظر گرفته شود. توصیه می‌شود سوابق در بخش‌های مختلف گروه‌بندی شوند به‌عنوان‌مثال سوابق حسابداری، سوابق پایگاه داده‌ها، وقایع تراکنش، وقایع ثبت‌شده ممیزی و روش های اجرایی عملیاتی، هر یک با جزئیاتی از دوره نگهداری و نوع رسانه ذخیره‌سازی مجاز مثلاً، کاغذ، ریز فیش، مغناطیسی یا نوری. توصیه می‌شود، هرگونه کلید و برنامه‌های مرتبط با بایگانی‌های رمزگذاری‌شده یا امضاهای دیجیتال نیز ذخیره شود (به بند ۱۰ مراجعه شود) تا امکان رمزگشایی سوابق در طول بازه زمانی که سوابق نگهداری می‌شوند، فراهم شود.

توصیه می‌شود درباره احتمال خرابی رسانه‌های به‌کاررفته به‌منظور ذخیره سوابق تمهیداتی اندیشیده شود. توصیه می‌شود رویه‌های ذخیره‌سازی و اداره کردن، مطابق با پیشنهادهای تولیدکننده اجرا شوند.

درجایی که رسانه‌های ذخیره‌سازی الکترونیکی انتخاب می‌شوند، توصیه می‌شود روش‌های اجرایی برای تضمین توانایی دسترسی به داده‌ها در سراسر دوره نگهداری گنجانده شود تا در برابر آسیب ناشی از تغییر فناوری در آینده، محافظت شود.

توصیه می‌شود سامانه‌های ذخیره‌سازی داده‌ها به‌گونه‌ای انتخاب شود که داده‌های موردنیاز را بتوان در یک‌شکل و بازه زمانی قابل‌قبول با توجه به الزاماتی که باید برآورده شود، بازیابی کرد.

توصیه می‌شود سامانه ذخیره کننده و اداره‌کننده، در صورت امکان، شناسایی سوابق و دوره‌های حفظ آن‌ها را به‌گونه‌ای که در مقررات یا قوانین ملی و منطقه‌ای تعریف‌شده است تضمین کند. این سامانه باید امحاء مناسب سوابق را پس‌ازآن دوره، درصورتی‌که سازمان به آن‌ها نیاز ندارد، مجاز شمارد.

به‌منظور رعایت این اهداف حفاظتی سوابق، توصیه می‌شود مراحل زیر در سازمان انجام شوند:

الف- توصیه می‌شود راهنمایی‌هایی درباره حفظ، ذخیره و کار و دورریز سوابق و اطلاعات صادر شود؛

ب- توصیه می‌شود یک جدول زمانی نگهداری برای شناسایی سوابق و دوره زمانی که برای آن نگهداری شده‌اند، تهیه شود؛

پ- توصیه می‌شود فهرستی از منابع اطلاعات کلیدی نگهداری شود.

اطلاعات دیگر

بعضی سوابق ممکن است نیازمند این باشند که به‌گونه‌ای امن حفظ شوند تا الزامات آئین‌نامه‌ای، مقرراتی یا قراردادی رعایت شوند و نیز فعالیت‌های ضروری کسب‌وکار را پشتیبانی کنند. به‌عنوان نمونه، سوابقی وجود دارند که ممکن است به‌عنوان شواهدی که یک سازمان در چارچوب قوانین عمل می‌کند، موردنیاز باشند تا

دفاع کافی در برابر اقدامات غیرحقوقی یا حقوقی یا تأیید وضعیت مالی یک سازمان در قبال سهام‌داران، اشخاص بیرونی و حسابرسان تضمین شود. دوره زمانی و محتوای داده‌ها برای حفظ اطلاعات ممکن است توسط قوانین و مقررات ملی تعیین شوند.

اطلاعات بیشتر درباره مدیریت گزارش‌های سازمانی را می‌توانید در استاندارد ISO 15489-1 [۵] بیابید.

۱۸-۱-۴ حریم خصوصی و حفاظت از اطلاعات شخصی قابل‌شناسایی

کنترل

توصیه می‌شود، حریم خصوصی و حفاظت از اطلاعات شخصی قابل‌شناسایی در صورت امکان آن‌گونه که در قوانین و آئین‌نامه‌های مرتبط الزام شده، تضمین شود.

راهنمای پیاده‌سازی

توصیه می‌شود یک خط‌مشی سازمانی محافظت از داده‌ها و حریم خصوصی، توسعه داده‌شده و اجرا شود. توصیه می‌شود این خط‌مشی به تمام اشخاصی که در پردازش اطلاعات شخصی نقش دارند، اطلاع داده شود.

انطباق با این خط‌مشی و تمام قوانین و مقررات محافظت از حریم خصوصی یا اطلاعات شخصی، نیازمند ساختار و کنترل مدیریتی مناسب است. اغلب این امر به بهترین نحو توسط انتصاب یک شخص مسئول مانند یک مأمور حریم خصوصی انجام می‌شود که توصیه می‌شود این شخص راهنمایی را برای مدیران، کاربران و ارائه‌کنندگان خدمات درباره مسئولیت فردی و رویه‌های خاصی که توصیه می‌شود دنبال شود، ارائه کند. توصیه می‌شود مسئولیت کار با اطلاعات شخصی و تضمین آگاهی از اصول حریم خصوصی مطابق با قوانین و مقررات مرتبط موردتوجه قرار گیرد. توصیه می‌شود سنجه‌های فنی و سازمانی مناسب برای محافظت از اطلاعات شخصی اجرا شود.

اطلاعات دیگر

استاندارد ISO/IEC 29100 [۲۵] یک چارچوب سطح بالا برای حفاظت از اطلاعات شخصی در سامانه‌های فناوری اطلاعات و ارتباطات فراهم می‌کند. تعدادی از کشورها مقرراتی دارند که کنترل‌هایی را درباره جمع آوری، پردازش و انتقال داده‌های شخصی (به‌طورکلی اطلاعات زندگی افرادی که ممکن است از این اطلاعات شناسایی شوند) اعمال می‌کنند. با توجه به مقررات ملی مرتبط این کنترل‌ها ممکن است وظایفی را برای جمع‌آوری‌کننده، پردازش کننده و منتشرکننده اطلاعات شخصی ایجاد کند و ممکن است امکان انتقال داده‌ها را به کشورهای دیگر محدود کند.

۱۸-۱-۵ قواعد کنترل‌های رمزنگاری

کنترل

توصیه می‌شود، کنترل‌های رمزنگاری در انطباق با تمامی توافقنامه‌ها، قوانین و آئین‌نامه‌های مرتبط، به کار گرفته شوند.

راهنمای پیاده‌سازی

توصیه می‌شود موارد زیر برای انطباق با قراردادها، قوانین و مقررات مرتبط در نظر گرفته شود:

الف- محدودیت‌های ورود یا خروج سخت‌افزار و نرم‌افزار رایانه برای اجرای عملکردهای رمزنگاری؛

ب- محدودیت‌هایی درباره ورود یا خروج نرم‌افزار و سخت‌افزار رایانه‌ای که برای اضافه شدن عملکرد رمزنگاری طراحی‌شده است؛

پ- محدودیت‌هایی درباره استفاده از رمزگذاری؛

ت- روش‌های اجباری یا اختیاری دسترسی مراجع دارای اختیار کشورها به اطلاعات رمزگذاری‌شده توسط سخت‌افزار یا نرم‌افزار برای تضمین محرمانگی محتوا.

توصیه می‌شود مشاوره قانونی برای تضمین انطباق با قوانین و مقررات ملی انجام شود. قبل از این‌که اطلاعات رمزگذاری‌شده یا کنترل‌های رمزنگاری به حوزه قضایی دیگری منتقل شود توصیه می‌شود مشاوره قانونی انجام شود.

۱۸-۲ بازنگری‌های امنیت اطلاعات

قصد: حصول اطمینان از اینکه امنیت اطلاعات مطابق با خط‌مشی‌ها و روش‌های اجرایی سازمانی پیاده‌سازی و اجراشده است.

۱۸-۲-۱ بازنگری مستقل امنیت اطلاعات

کنترل

توصیه می‌شود، رویکرد سازمان به مدیریت امنیت اطلاعات و پیاده‌سازی آن (به‌عنوان‌مثال اهداف کنترلی، کنترل‌ها، خط‌مشی‌ها، فرآیندها و روش‌های اجرایی امنیت اطلاعات)، در فواصل زمانی طرح‌ریزی‌شده یا هنگامی‌که تغییرات عمده‌ای رخ دهد، به‌صورت مستقل بازنگری شود.

راهنمای پیاده‌سازی

توصیه می‌شود بازنگری مستقل توسط مدیریت آغاز شود. چنین بازنگری مستقلی برای اطمینان از تداوم مناسب بودن، کفایت و اثربخشی رویکرد سازمان به مدیریت امنیت اطلاعات ضروری است. توصیه می‌شود بازنگری شامل ارزیابی فرصت‌های بهبود و نیاز به تغییرات رویکردی در امنیت که شامل خط‌مشی و اهداف کنترلی می‌شود، باشد.

توصیه می‌شود بازنگری توسط افراد مستقل از حیطه بازنگری، به‌عنوان‌مثال فعالیت ممیزی داخلی، یک مدیر مستقل یا سازمان ثالث متخصص در چنین بازنگری‌هایی، انجام شود. توصیه می‌شود افرادی که این‌گونه بازنگری‌ها را انجام می‌دهند از مهارت و تجربه مناسب برخوردار باشند.

توصیه می‌شود نتایج بازنگری مستقل ثبت‌شده و به مدیریتی که آغازگر این بازنگری‌ها بوده است، گزارش شود. توصیه می‌شود این سوابق نگهداری شوند.

اگر بازنگری‌های مستقل نشان دهند که رویکرد سازمان و پیاده‌سازی مدیریت امنیت اطلاعات کافی نبوده است به‌عنوان‌مثال اهداف و الزامات مستند برآورده نشده است یا با جهت‌گیری بیان‌شده امنیت اطلاعات در خط‌مشی‌های امنیت اطلاعات منطبق نیست (به بند ۵-۱-۱ مراجعه شود)، توصیه می‌شود مدیریت اقدام‌های اصلاحی را در این موارد مدنظر قرار دهد.

اطلاعات دیگر

استاندارد ISO/IEC 27007 [۱۲] «راهنمایی‌هایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات» و استاندارد ISO/IEC TR 2008 [۱۳] «راهنمایی‌هایی برای ممیزی کنترل‌های مدیریت امنیت» راهنمایی هایی برای بازنگری مستقل ارائه می‌کند.

۱۸-۲-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی

کنترل

توصیه می‌شود، مدیران به‌طور منظم انطباق پردازش و روش‌های اجرایی اطلاعات در حیطهٔ مسئولیتشان را با خط‌مشی‌های امنیتی، استانداردها و الزامات امنیتی مناسب دیگر، بازنگری کنند.

راهنمای پیاده‌سازی

توصیه می‌شود مدیران شیوه‌های بازنگری که منجر به برآورده شدن الزامات امنیت اطلاعات تعریف‌شده در خط‌مشی‌ها، استانداردها و دیگر الزامات امنیتی می‌شود را شناسایی کنند. ابزارهای سنجش و گزارش دهی خودکار می‌تواند برای یک بازنگری کارایی مفید باشد.

اگر هرگونه عدم انطباق درنتیجه بازنگری مشاهده شود، توصیه می‌شود مدیران:

الف- علل عدم انطباق را تعیین کنند؛

ب- نیاز به اقداماتی برای اطمینان از عدم وقوع مجدد عدم انطباق را ارزشیابی کنند؛

پ- اقدام اصلاحی مناسب را تعیین و اجرا کنند؛

ت- اقدام اصلاحی انجام‌شده را جهت اطمینان از کارایی و شناسایی ناکارآمدی و نقاط ضعف بررسی کنند.

توصیه می‌شود نتایج بازنگری‌ها و اقدامات اصلاحی انجام‌شده توسط مدیران ثبت شود و توصیه می‌شود این گزارش‌ها نگهداری شوند. توصیه می‌شود مدیریان نتایج را به اشخاصی که بازنگری‌های مستقل (به بند ۱۸-۲-۱ مراجعه شود) را انجام می‌دهند، درزمانی که بازنگری‌های مستقل در حوزه مسئولیتشان انجام می‌شود، گزارش کنند.

اطلاعات دیگر

پایش عملیاتی استفاده از سامانه دربند ۱۲-۴ پوشش داده‌شده است.

۱۸-۲-۳ بازنگری انطباق فنی

کنترل

توصیه می‌شود، به‌منظور انطباق با خط‌مشی‌ها و استانداردهای امنیت اطلاعات سازمان، سامانه‌های اطلاعاتی را به‌طور منظم بازنگری کند.

راهنمای پیاده‌سازی

توصیه می‌شود انطباق فنی ترجیحاً به کمک ابزار خودکار بازنگری شود تا امکان تولید گزارش‌های فنی برای تفسیر بعدی آن توسط یک متخصص فنی فراهم شود. روش دیگر، بازنگری دستی است که توسط یک مهندس سامانه باتجربه (در صورت لزوم توسط ابزار نرم‌افزاری مناسب پشتیبانی می‌شود) می‌تواند انجام شود.

اگر آزمون نفوذ یا ارزیابی آسیب‌پذیری انجام می‌شود، احتیاط لازم صورت گیرد چراکه چنین فعالیتی می‌تواند سبب به خطر افتادن امنیت سامانه شود. چنین آزمون باید برنامه‌ریزی‌شده، مستند و تکرارپذیر باشد. هر بازنگری انطباق فنی تنها باید توسط افراد مجاز و باصلاحیت و یا تحت نظارت چنین افرادی انجام شود.

اطلاعات دیگر

بازنگری انطباق فنی شامل بازنگری سامانه‌های عملیاتی است تا اطمینان حاصل شود که کنترل‌های سخت‌افزاری و نرم‌افزار به‌درستی پیاده‌سازی شده‌اند. این نوع از بازنگری انطباق نیاز به تخصص فنی متخصص دارد.

بازنگری انطباق همچنین پوشش‌دهنده مواردی مانند آزمون نفوذ و ارزیابی آسیب‌پذیری است که ممکن است توسط کارشناسان مستقل که به‌طور خاص برای این منظور دارای قرارداد هستند، انجام شود. این بررسی می‌تواند در تشخیص آسیب‌پذیری و برای بازرسی چگونگی مؤثر بودن کنترل در جلوگیری از دسترسی غیرمجاز به علت این آسیب‌پذیری مفید باشد.

آزمون نفوذ و ارزیابی آسیب‌پذیری، یک تصویر کلی از یک سامانه در یک حالت خاص و در زمان خاص ارائه می‌کند. تصویر کلی محدود به بخش‌هایی از سامانه است که در زمان تلاش (های) نفوذ مورد آزمایش قرارگرفته‌اند. آزمون نفوذ و ارزیابی آسیب‌پذیری یک جایگزین برای ارزیابی مخاطرات نیست.

استاندارد ISO/IEC TR 27008 [۱۳] راهنمایی‌های خاص در موردبازنگری انطباق فنی را فراهم می‌کند.

کتاب‌نامه

[1] ISO/IEC Directives, Part 2

[2] ISO/IEC 11770-1, Information technology Security techniques — Key management — Part 1: Framework

[3] ISO/IEC 11770-2, Information technology — Security techniques — Key management — Part 2:Mechanisms using symmetric techniques

[4] ISO/IEC 11770-3, Information technology — Security techniques — Key management — Part 3:Mechanisms using asymmetric techniques

[5] ISO 15489-1, Information and documentation — Records management — Part 1: General

[6] ISO/IEC 20000-1, Information technology — Service management — Part 1: Service management system requirements

[7] ISO/IEC 20000-2,[1]Information technology — Service management — Part 2: Guidance on the application of service management systems

[8] ISO 22301, Societal security — Business continuity management systems — Requirements

[9] ISO 22313, Societal security — Business continuity management systems — Guidance

[10] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[11] ISO/IEC 27005,Information technology— Security techniques— Information security risk management

[12] ISO/IEC 27007, Information technology — Security techniques — Guidelines for information security management systems auditing

[13] ISO/IEC TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls

[14] ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[15] ISO/IEC 27033-1, Information technology — Security techniques — Network security — Part 1:Overview and concepts

[16] ISO/IEC 27033-2, Information technology — Security techniques — Network security — Part 2:Guidelines for the design and implementation of network security

[17] ISO/IEC 27033-3, Information technology — Security techniques — Network security — Part 3:Reference networking scenarios — Threats, design techniques and control issues

[18] ISO/IEC 27033-4, Information technology — Security techniques — Network security — Part 4:Securing communications between networks using security gateways

[19] ISO/IEC 27033-5, Information technology — Security techniques — Network security — Part 5:Securing communications across networks using Virtual Private Network (VPNs)

[20] ISO/IEC 27035, Information technology — Security techniques — Information security incident management

[21] ISO/IEC 27036-1, Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts

[1] ISO/IEC 20000-2:2005 has been cancelled and replaced by ISO/IEC 20000-2:2012, Information technology — Service management — Part 2: Guidance on the application of service management systems.

[22] ISO/IEC 27036-2, Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements

[23] ISO/IEC 27036-3, Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security

[24] ISO/IEC 27037, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

[25] ISO/IEC 29100, Information technology — Security techniques — Privacy framework

[26] ISO/IEC 29101, Information technology — Security techniques — Privacy architecture framework

[27] ISO 31000, Risk management — Principles and guidelines