استاندارد ایران -ایزو- آی ای سی

۲۷۰۰۲

چاپ اول

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

ISIRI-ISO/IEC

27002

1st. edition

فن‌آوری اطلاعات- فنون امنیتی- آیین‌کار مدیریت امنیت اطلاعات

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

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران
تهران - خیابان ولیعصر، ضلع جنوبی میدان ونک، پلاک ۱۲۹۴، صندوق پستی: ۶۱۳۹-۱۴۱۵۵
تلفن: ۵-۸۸۸۷۹۴۶۱
دورنگار: ۸۸۸۸۷۰۸۰ و۸۸۸۸۷۱۰۳
کرج - شهر صنعتی، صندوق پستی ۱۶۳-۳۱۵۸۵
تلفن: ۸- ۲۸۰۶۰۳۱(۰۲۶۱)
دورنگار: ۲۸۰۸۱۱۴ (۰۲۶۱)
پیام نگار: standard@isiri.org.ir
وب‌گاه: www.isiri.org
بخش فروش، تلفن: ۲۸۱۸۹۸۹ (۰۲۶۱)، دورنگار: ۲۸۱۸۷۸۷ (۰۲۶۱)
بها: ۱۵۶۲۵ ریال

Institute of Standards and Industrial Research of IRAN
Central Office: No.1294 Valiaser Ave. Vanak corner, Tehran, Iran
P. O. Box: 14155-6139, Tehran, Iran
Tel: +98 (21) 88879461-5
Fax: +98 (21) 88887080, 88887103
Headquarters: Standard Square, Karaj, Iran
P.O. Box: 31585-163
Tel: +98 (261) 2806031-8
Fax: +98 (261) 2808114
Email: standard @ isiri.org.ir
Website: www.isiri.org
Sales Dep.: Tel: +98(261) 2818989, Fax.: +98(261) 2818787
Price: 15625 Rls.

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی 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.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فن‌آوری 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 می‌شود .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 می‌شود.

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

مؤسسهٔ استاندارد و تحقیقات صنعتی 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 می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور، از آخرین پیشرفتهای علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می‌تواند 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 کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه می‌تواند 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 سا زمانها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، مؤسسهٔ استاندارد این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آنها نظارت می‌کند .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 مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1 - International organization for Standardization
2 - International Electro technical Commission
3 - International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فن‌آوری اطلاعات- فنون امنیتی- آیین‌کار مدیریت امنیت اطلاعات »

رئیس:	**سمت و/ یا نمایندگی**
حسینی خیاط، سعید	عضو هیات علمی دانشکده مهندسی
(دکترای مهندسی برق)	دانشگاه فردوسی مشهد
دبیر:	
خانیکی، رضا	اداره کل استاندارد و تحقیقات صنعتی
(لیسانس مهندسی برق - مخابرات)	خراسان رضوی
سهی زاده ابیانه، محمد رضا	شرکت صنایع الکترونیکی زعیم
(فوق لیسانس مهندسی مخابرات- رمز)	(سهامی خاص)
اعضاء: (اسامی به ترتیب حروف الفبا)	
اثنی عشری، امیر مهدی	موسسه تحقیقات و فن‌آوری پارس
(لیسانس مهندسی برق - کنترل)	
ایرانپور، نادر	گروه مخابراتی رهنما فردا
(فوق لیسانس مدیریت حرفه‌ای کسب وکار)	(سهامی خاص)
خانیکی، مریم	شرکت نفت ایران
(فوق لیسانس مدیریت)	(سهامی عام)
رضایی، امید	شرکت مهندسی ایمن رایانه شرق
(فوق لیسانس مهندسی مخابرات- رمز)	(سهامی خاص)
روشن روان، راما	بانک رفاه
(لیسانس مهندسی کامپیوتر – نرم‌افزار)	
صدری‌زاده، مریم	موسسه تحقیقات و فن‌آوری پارس
(فوق لیسانس مدیریت‌اجرایی)	

صمدی، جواد (لیسانس شیمی)	اداره کل استاندارد و تحقیقات صنعتی خراسان رضوی
صمدی، فرشید (لیسانس مهندسی صنایع)	موسسه تحقیقات و فن‌آوری پارس
ضیاء علی نسب‌پور، مسعود (فوق لیسانس مهندسی پزشکی)	شرکت صنایع الکترونیکی زعیم (سهامی خاص)
فاطمی نسب، امیر مسعود (فوق‌لیسانس مهندسی سیستم‌های مخابرات دیجیتال)	شرکت سیستم و خدمات اریکسون (سهامی خاص)
مهدوی اردستانی، سید علیرضا (فوق لیسانس مدیریت فن‌آوری اطلاعات)	کارشناس آزاد
نورا، علیرضا (فوق لیسانس مهندسی صنایع- مدیریت سیستم و بهره‌وری)	شرکت مرساکو (سهامی خاص)

فهرست مندرجات

عنوان	صفحه
آشنایی با مؤسسهٔ استاندارد	ج
کمیسیون فنی تدوین استاندارد	د
پیش گفتار	م
۰ مقدمه	ن
۰-۱ امنیت اطلاعات چیست ؟	ن
۰-۲ چرا امنیت اطلاعات لازم است ؟	ن
۰-۳ چگونه نیازهای امنیت شناسایی می‌شوند ؟	س
۰-۴ برآورد ریسک‌های امنیت	س
۰-۵ انتخاب کنترل‌ها	س
۰-۶ نقطه آغازین امنیت اطلاعات	ع
۰-۷ عوامل حیاتی موفقیت	ع
۰-۸ توسعه رهنمودهای مربوط به خود	ف
۱ هدف و دامنه کاربرد	۱
۲ اصطلاحات و تعاریف	۱
۳ ساختار این استاندارد	۵
۳-۱ بندها	۵
۳-۲ طبقه‌بندی‌های اصلی امنیت	۵
۴ ارزیابی و برطرف سازی ریسک	۶
۴-۱ ارزیابی ریسک‌های امنیت	۶
۴-۲ آموزش ریسک‌های امنیت	۶
۵ خط‌مشی امنیتی	۸
۵-۱ خط‌مشی امنیتی	۸
۵-۱- ۱ مدرک خط‌مشی امنیت اطلاعات	۸
۵-۱-۲ بازبینی خط‌مشی امنیت اطلاعات	۹
۶ سازمان امنیت اطلاعات	۱۰
۶-۱ سازمان داخلی	۱۰
۶-۱-۱ تعهد مدیریت به امنیت اطلاعات	۱۰
۶-۱-۲ هماهنگی امنیت اطلاعات	۱۱
۶-۱-۳ تخصیص مسوولیت‌های امنیت اطلاعات	۱۱
۶-۱-۴ فرایند مجوزدهی برای امکانات پردازش اطلاعات	۱۲

ادامه فهرست مندرجات

عنوان	صفحه
۶-۱-۵ توافق‌نامه‌های محرمانگی	۱۳
۶-۱-۶ برقراری ارتباط‌با مراجع‌دارای‌اختیار	۱۴
۶-۱-۷ برقراری ارتباط با گروههای بامنافع خاص	۱۴
۶-۱-۸ بازنگری مستقل امنیت اطلاعات	۱۵
۶-۲ اشخاص بیرونی	۱۶
۶-۲-۱ شناسایی ریسک‌های مرتبط با اشخاص بیرونی	۱۶
۶-۲-۲ نشانی دهی امنیت هنگام سرو کار داشتن با مشتریان	۱۸
۶-۲-۳ نشانی‌دهی امنیت در توافق‌های شخص‌سوم	۱۹
۷ مدیریت دارایی	۲۲
۷-۱ مسوولیت داراییها	۲۲
۷-۱-۱ لیست موجودی اموال	۲۲
۷-۱-۲ مالکیت داراییها	۲۳
۷-۱-۳ استفاده پسندیده از دارایی‌ها	۲۴
۷-۲ طبقه بندی اطلاعات	۲۴
۷-۲-۱ رهنمودهای طبقه بندی	۲۵
۷-۲-۲ برچسب‌گذاری و اداره‌کردن‌اطلاعات	۲۵
۸ امنیت منابع انسانی	۲۷
۸-۱ پیش از اشتغال	۲۷
۸-۱-۱ نقش‌ها و مسوولیت‌ها	۲۷
۸-۱-۲ گزینش	۲۸
۸-۱-۳ ضوابط و شرایط استخدام	۲۸
۸-۲ حین خدمت	۳۰
۸-۲-۱ مسوولیت‌های مدیریت	۳۰
۸-۲-۲ آگاهی رسانی، تحصیل و آموزش امنیت اطلاعات	۳۱
۸-۲-۳ فرآیند انضباطی	۳۱
۸-۳ خاتمه استخدام یا تغییر در شغل	۳۲
۸-۳-۱ مسوولیت‌های خاتمه خدمت	۳۲
۸-۳-۲ عودت دارایی‌ها	۳۲
۸-۳-۳ حذف حقوق دسترسی	۳۳
۹ امنیت فیزیکی و محیطی	۳۵

فهرست مندرجات

عنوان	صفحه
۹-۱ نواحی امن	۳۵
۹-۱-۱حصار امنیت فیزیکی	۳۵
۹-۱-۲ کنترل‌های مداخل فیزیکی ورودی	۳۶
۹-۱-۳ ایمن سازی دفاتر،اتاقها وامکانات	۳۷
۹-۱-۴ محافظت در برابر تهدید های بیرونی و محیطی	۳۷
۹-۱-۵ کار در نواحی امن	۳۸
۹-۱-۶ نواحی دسترسی عمومی، نواحی تحویل و بارگیری	۳۸
۹-۲ نگهداری تجهیزات	۳۹
۹-۲-۱ استقرار و حفاظت تجهیزات	۳۹
۹-۲-۲ امکانات پشتیبانی	۴۰
۹-۲-۳ امنیت کابل کشی	۴۰
۹-۲-۴ نگهداری تجهیزات	۴۱
۹-۲-۵ امنیت تجهیزات خارج از ابینه اماکن سازمان	۴۲
۹-۲-۶ امحاء یا استفاده مجدد از تجهیزات به صورت ایمن	۴۲
۹-۲-۷ خروج اموال	۴۳
۱۰ مدیریت ارتباطات و عملیات	۴۴
۱۰-۱ روش‌های‌اجرایی‌عملیاتی‌ومسوولیت‌ها	۴۴
۱۰-۱-۱روش‌های اجرایی عملیاتی مستندشده	۴۴
۱۰-۱-۲ مدیریت تغییر	۴۵
۱۰-۱-۳ تفکیک وظایف	۴۵
۱۰-۱-۴ جداسازی امکانات توسعه، آزمون و عملیاتی	۴۶
۱۰-۲ مدیریت تحویل خدمت شخص‌سوم	۴۷
۱۰-۲-۱ تحویل خدمت	۴۷
۱۰-۲-۲ پایش و بازنگری خدمات شخص‌سوم	۴۷
۱۰-۲-۳ مدیریت تغییرات در خدمات شخص‌سوم	۴۸
۱۰-۳ طرح‌ریزی و پذیرش سیستم	۴۹
۱۰-۳-۱ مدیریت ظرفیت	۴۹
۱۰-۳-۲ پذیرش سیستم	۴۹
۱۰-۴ حفاظت در برابر کدهای مخرب‌وسیار	۵۰
۱۰-۴-۱ کنترل‌هایی در برابر کدهای‌مخرب	۵۰

فهرست مندرجات

عنوان	صفحه
۱۰-۴-۲ کنترل‌هایی در برابر کدهای سیار	۵۲
۱۰-۵ نسخه‌های پشتیبان	۵۲
۱۰-۵-۱ ایجاد پشتیبان از اطلاعات	۵۲
۱۰-۶ مدیریت امنیت شبکه	۵۴
۱۰-۶-۱ کنترل های شبکه	۵۴
۱۰-۶-۲ امنیت خدمات شبکه	۵۴
۱۰-۷ اداره کرده محیط های ذخیره سازی	۵۵
۱۰-۷-۱ مدیریت محیط های ذخیره سازی قابل جابجایی	۵۵
۱۰-۷-۲ امحای محیط های ذخیره سازی	۵۶
۱۰-۷-۳ روش‌های‌اجرایی جابجایی‌اطلاعات	۵۷
۱۰-۷-۴ امنیت مستندات سیستم	۵۷
۱۰-۸ تبادل اطلاعات	۵۸
۱۰-۸-۱ خط‌مشی‌ها و روش‌های اجرایی تبادل اطلاعات	۵۸
۱۰-۸-۲ توافق‌نامه‌های تبادل	۶۰
۱۰-۸-۳ محیط های ذخیره سازی(رسانه) فیزیکی، حین حمل و نقل	۶۱
۱۰-۸-۴ پیام رسانی الکترونیکی	۶۱
۱۰-۸-۵ سیستم‌های اطلاعاتی کسب‌وکار	۶۲
۱۰-۹ خدمات تجارت الکترونیک	۶۳
۱۰-۹-۱ تجارت الکترونیک	۶۳
۱۰-۹-۲ تراکنش‌های برخط	۶۴
۱۰-۹-۳ اطلاعات قابل‌دسترس عموم	۶۵
۱۰-۱۰ پایش	۶۵
۱۰-۱۰-۱ واقعه نگاری ممیزی	۶۶
۱۰-۱۰-۲ پایش کاربرد سیستم	۶۶
۱۰-۱۰-۳ حفاظت‌از اطلاعات ثبت شده‌وقایع	۶۸
۱۰-۱۰-۴ اطلاعات ثبت‌شده وقایع مربوط به راهبر و اپراتور سیستم	۶۸
۱۰-۱۰-۵ واقعه نگاری خرابی	۶۹
۱۰-۱۰-۶ هم زمان سازی ساعتها	۶۹
۱۱ کنترل دسترسی	۷۰
۱۱-۱ الزامات کسب‌وکار برای کنترل دسترسی	۷۰

فهرست مندرجات

عنوان	صفحه
۱۱-۱-۱ خط‌مشی کنترل دسترسی	۷۰
۱۱-۲ مدیریت دسترسی کاربر	۷۱
۱۱-۲-۱ ثبت کاربر	۷۱
۱۱-۲-۲ مدیریت اختیارات ویژه	۷۲
۱۱-۲-۳ مدیریت کلمه عبور کاربر	۷۳
۱۱-۲-۴ بازنگری حقوق دسترسی کاربر	۷۴
۱۱-۳ مسوولیت‌های کاربر	۷۴
۱۱-۳-۱ استفاده از کلمه عبور	۷۴
۱۱-۳-۲ تجهیزات بدون مراقبت کاربر	۷۵
۱۱-۳-۳ خط‌مشی میز پاک و صفحه پاک	۷۶
۱۱-۴ کنترل دسترسی به شبکه	۷۷
۱۱-۴-۱ خط‌مشی استفاده از خدمات شبکه	۷۷
۱۱-۴-۲ احراز اصالت کاربر برای اتصالات بیرونی	۷۷
۱۱-۴-۳ شناسایی تجهیزات در شبکه ها	۷۸
۱۱-۴-۴ حفاظت از درگاه عیب یابی و پیکربندی راه‌دور	۷۹
۱۱-۴-۵ تفکیک در شبکه ها	۷۹
۱۱-۴-۶ کنترل اتصال به شبکه	۸۰
۱۱-۴-۷ کنترل مسیریابی در شبکه	۸۱
۱۱-۵ کنترل دسترسی به سیستم عامل	۸۲
۱۱-۵-۱روش‌های اجرایی برقراری ارتباط امن	۸۲
۱۱-۵-۲ شناسایی و احراز اصالت کاربر	۸۳
۱۱-۵-۳ سیستم مدیریت کلمه عبور	۸۴
۱۱-۵-۴ استفاده از برنامه‌های کمکی سیستم	۸۴
۱۱-۵-۵ خروج زمانی از لایه ارتباطی	۸۵
۱۱-۵-۶ محدود سازی زمان اتصال	۸۵
۱۱-۶ کنترل دسترسی به برنامه‌های کاربردی و اطلاعات	۸۶
۱۱-۶-۱ محدودیت دسترسی به اطلاعات	۸۶
۱۱-۶-۲ جداسازی سیستم‌های حساس	۸۷
۱۱-۷ محاسبه سیار و کار از راه‌دور	۸۷
۱۱-۷-۱ محاسبه و ارتباطات سیار	۸۷

فهرست مندرجات

عنوان	صفحه
۱۱-۷-۲ کار از راه‌دور	۸۹
۱۲ اکتساب، بهبود و نگهداری سیستم‌های اطلاعاتی	۹۱
۱۲-۱ الزامات امنیتی سیستم‌های اطلاعاتی	۹۱
۱۲-۱-۱ مشخصات و تحلیل الزامات امنیتی	۹۱
۱۲-۲ پردازش صحیح در برنامه‌های کاربردی	۹۲
۱۲-۲-۱ صحه‌گذاری داده ورودی	۹۲
۱۲-۲-۲ کنترل پردازش درونی	۹۳
۱۲-۲-۳ تمامیت پیغام	۹۴
۱۲-۲-۴ صحه‌گذاری داده خروجی	۹۴
۱۲-۳ کنترل‌های رمزنگاری	۹۵
۱۲-۳-۱خط‌مشی استفاده از کنترل‌های رمزنگاری	۹۵
۱۲-۳-۲ مدیریت کلید	۹۶
۱۲-۴ امنیت فایل‌های سیستم	۹۸
۱۲-۴-۱ کنترل نرم‌افزار عملیاتی	۹۸
۱۲-۴-۲حفاظت از داده‌های آزمون سیستم	۹۹
۱۲-۴-۳ کنترل دسترسی به کدمنبع برنامه	۱۰۰
۱۲-۵ امنیت در فرایندهای بهبود و پشتیبانی	۱۰۰
۱۲-۵-۱ روش‌های اجرایی کنترل تغییر	۱۰۱
۱۲-۵-۲ بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات سیستم عامل	۱۰۲
۱۲-۵-۳ محدود سازی در اعمال تغییرات در بسته های نرم‌افزاری	۱۰۲
۱۲-۵-۴ نشت اطلاعات	۱۰۳
۱۲-۵-۵ بهبود نرم‌افزار برون‌سپاری‌شده	۱۰۳
۱۲-۶ مدیریت آسیب پذیری فنی	۱۰۴
۱۲-۶-۱ کنترل آسیب پذیرهای فنی	۱۰۴
۱۳ مدیریت رخدادهای امنیت اطلاعات	۱۰۶
۱۳-۱ گزارش دهی وقایع و ضعفهای امنیت اطلاعات	۱۰۶
۱۳-۱-۱گزارش دهی وقایع امنیت اطلاعات	۱۰۶
۱۳-۱-۲ گزارش دهی ضعفهای امنیتی	۱۰۷
۱۳-۲ مدیریت رخدادها و بهبودهای امنیت اطلاعات	۱۰۸
۱۳-۲-۱ مسوولیت ها و روش‌های اجرایی	۱۰۸

فهرست مندرجات

عنوان	صفحه
۱۳-۲-۲یادگیری‌ازرخدادهای‌امنیت‌اطلاعات	۱۰۹
۱۳-۲-۳ گرد آوری شواهد	۱۰۹
۱۴ مدیریت استمرار کسب‌وکار	۱۱۱
۱۴-۱ جنبه های امنیت اطلاعات مدیریت استمرار کسب‌وکار	۱۱۱
۱۴-۱-۱ لحاظ کردن امنیت اطلاعات در فرایند مدیریت استمرار کسب‌وکار	۱۱۱
۱۴-۱-۲ استمرار کسب‌وکار و ارزیابی‌ریسک	۱۱۲
۱۴-۱-۳ ایجاد و پیاده سازی طرح‌های استمرار در برگیرنده امنیت اطلاعات	۱۱۲
۱۴-۱-۴ چارچوب طرح‌ریزی استمرار کسب‌وکار	۱۱۳
۱۴-۱-۵ حفظ‌ونگهداری آزمون و ارزیابی مجدد طرح های استمرار کسب‌وکار	۱۱۵
۱۵ انطباق	۱۱۷
۱۵-۱ انطباق با الزامات قانونی	۱۱۷
۱۵-۱-۱ شناسایی قوانین قابل اجرا	۱۱۷
۱۵-۱-۲ حقوق مالکیت فکری	۱۱۷
۱۵-۱-۳ حفاظت از سوابق سازمانی	۱۱۸
۱۵-۱-۴ حفاظت داده‌ها و حریم خصوصی اطلاعات شخصی	۱۱۹
۱۵-۱-۵ پیشگیری از استفاده نابجا از امکانات پردازش اطلاعات	۱۲۰
۱۵-۱-۶ مقررات کنترل‌های رمزنگاری	۱۲۱
۱۵-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی، و انطباق فنی	۱۲۱
۱۵-۲-۱ انطباق خط‌مشی ها واستانداردهای امنیتی	۱۲۱
۱۵-۲-۲ بررسی انطباق فنی	۱۲۲
۱۵-۳ ملاحظات ممیزی سیستم‌های اطلاعاتی	۱۲۳
۱۵-۳-۱ کنترل‌های ممیزی سیستم‌های اطلاعاتی	۱۲۳
۱۵-۳-۲ حفاظت از ابزارهای ممیزی سیستم‌های اطلاعاتی	۱۲۳
کتابنامه	۱۲۵

پیش گفتار

استاندارد "فن‌آوری اطلاعات - فنون امنیتی- آیین‌کار مدیریت امنیت اطلاعات" که پیش نویس آن در کمیسیون های مربوط توسط مؤسسهٔ استاندارد و تحقیقات صنعتی ایران تهیه و تدوین شده و در پنجاه و پنجمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۸۷/۸/۱۲ مورد تصویب قرارگرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

این استاندارد ملی بر مبنای استاندارد بین المللی زیر تدوین شده و معادل آن به زبان فارسی است:

1- ISO/IEC 27002:2005, 2nd Ed.: Information technology — Security techniques — Code of practice for information security management

۲ - کلیه واژگان مصوب فرهنگستان علوم, سایت اینترنتی فرهنگستان زبان و ادبیات پارسی
http://www.persianacademy.ir/

۰ مقدمه

۰-۱ امنیت اطلاعات چیست ؟

اطلاعات، دارایی است همانند سایر دارایی‌های مهم کسب وکار که برای کسب وکار سازمان دارای اهمیت است، و درنتیجه باید بگونه ای مناسب محافظت شود. این موضوع مخصوصاً در محیطی که تعاملات کسب وکار رو به رشد است، از اهمیت بیشتری برخوردار است. در نتیجه این افزایش تعامل، اطلاعات در معرض تعداد بیشتر و انواع گوناگون تری از تهدیدات و آسیب پذیریها قرار گرفته است.(همچنین رهنمودهای OECD[1] (سازمان همکاری و توسعه اقتصادی) برای امنیت اطلاعات سامانه ها و شبکه ها می باشد، ملاحظه نمایید).

اطلاعات می‌تواند به اشکال گوناگون وجود داشته باشد. می‌تواند چاپ شده یا نوشته شده بر روی کاغذ، ذخیره شده الکترونیکی باشد، با پست یا وسایل الکترونیکی ارسال شود، از طریق فیلم به نمایش درآید، یا در مکالمات بیان شود. توصیه می‌شود، همیشه هر شکلی که اطلاعات دارد، یا به هر وسیله ای که به اشتراک گذاشته می‌شود، بگونه ای مناسب محافظت شود.

امنیت اطلاعات، محافظت از اطلاعات در برابر طیف گسترده ای از تهدیدات است که به منظور اطمینان از استمرار کسب وکار، کمینه کردن ریسک کسب وکار، حداکثر کردن آورده و فرصتهای کسب وکار است.

دستیابی به امنیت اطلاعات، با پیاده سازی مجموعه ای از کنترل‌های مناسب از جمله خط مشی ها، فرایندها، رویه ها، ساختارهای سازمانی و فعالیتهای نرم‌افزاری و سخت افزاری میسر می‌شود. این کنترل‌ها در موارد لازم باید مستقر، پیاده سازی، پایش، بازبینی و اصلاح شده تا از برآورده شدن اهداف خاص امنیتی و کسب وکار در سازمان اطمینان حاصل شود. توصیه می‌شود این موارد در راستای سایر فرایندهای مدیریت کسب وکار انجام شود.

۰-۲ چرا امنیت اطلاعات لازم است ؟

اطلاعات، فرایندهای پشتیبانی، سیستم‌ها و شبکه ها دارایی‌های مهم کسب وکار هستند. تعریف، دستیابی، نگهداری و توسعه امنیت اطلاعات می‌تواند تاثیر بسزایی بر ماندگاری در عرصه رقابت، گردش مالی، سودآوری، انطباق با قانون و تصویر کسب وکار داشته باشد.

سازمانها و سیستم‌های اطلاعاتی و شبکه های با تهدیدات امنیتی از منابع گسترده و گوناگون مواجه می‌شوند، که شامل سوء استفاده رایانه ای، جاسوسی، خرابکاری، تخریب، آتش سوزی و سیل است. دلایل بروز ایراد از قبیل کد مخرب، دستیابی غیر مجاز رایانه ای، حملات ممانعت از ارایه خدمات متداول تر، زیاده خواهانه تر[2] و پیچیده تر شده اند.

امنیت اطلاعات برای کسب وکار بخشهای خصوصی و عمومی و همچنین محافظت از زیرساختارهای حیاتی اهمیت دارد. در این دو بخش، امنیت اطلاعات بعنوان توانمندساز عمل خواهد کرد، بعنوان مثال برای دستیابی به دولت الکترونیکی یا کسب وکار الکترونیکی و اجتناب یا کاهش ریسک‌های مرتبط است. تعامل شبکه های عمومی و خصوصی و به اشتراک گذاشتن منابع اطلاعاتی، موجب افزایش دشواری در کنترل دسترسی می‌شود.

1- Organisation for Economic Co-operation and Development (OECD)
2- Ambitious

بسیاری از سیستم‌های اطلاعاتی بگونه ای طراحی نشده اند که بتوان آنها را امن کرد.امنیتی که از طریق ابزار فنی بدست می‌آید، محدود بوده و توصیه می‌شود از طریق رویه ها و مدیریت مناسب پشتیبانی شود. شناسایی کنترل‌های مناسب، نیازمند برنامه ریزی دقیق و توجه به جزئیات است. مدیریت امنیت اطلاعات دست کم نیازمند مشارکت تمامی افراد سازمان است. همچنین ممکن است به مشارکت سهامداران، تامین کنندگان، اشخاص ثالث، مشتریان و سایر اشخاص بیرونی نیاز باشد. هچنین ممکن است به دریافت مشاوره از متخصصین در خارج سازمان نیاز باشد.

۰-۳ چگونه نیازهای امنیت شناسایی می‌شوند ؟

ضروری است سازمان نیازهای امنیتی خود را شناسایی نماید. سه منبع اصلی برای نیازمندیهای امنیت وجود دارد.

۱- یکی از منابع، از برآورد ریسک سازمان منتج می‌شود، که با در نظر گرفتن اهداف و راهبردهای کلان کسب وکار سازمان میسر می باشد. از طریق برآورد ریسک، تهدیدات داراییها شناسایی شده، آسیب‌پذیری و احتمال رخداد آن ارزیابی شده و میزان پیامد بالقوه حاصل از آن تخمین زده می‌شود.
۲- منبع دیگر، شامل قوانین، مقررات، حقوق مدنی و الزامات قراردادی بوده که سازمان با شرکای کسب‌وکار، پیمانکاران و خدمت دهندگان خود داشته و همچنین فضای فرهنگی جامعه آنها است.
۳- منبع دیگر، مجموعه ای خاص از اصول، اهداف و الزامات کسب وکار برای پردازش اطلاعات بوده که سازمان آنها را برای پشتیبانی از عملیات خود توسعه داده است.

۰-۴ برآورد ریسک‌های امنیت

نیازهای امنیتی از طریق برآورد روش‌مند ریسک‌های امنیت، شناسایی می‌شود. هزینه های صرف شده برای کنترل‌ها باید به گونه‌ای آسیب احتمالی رسیده به کسب وکار که ناشی از خطاهای امنیتی است را تعدیل نماید.
نتیجه برآورد ریسک به راهنمایی و تعیین اقدام مدیریتی مناسب و اولویت دهی برای مدیریت ریسک‌های امنیت اطلاعات و پیاده سازی کنترل‌های انتخاب شده برای مقابله با این ریسک‌ها، کمک خواهد کرد.
توصیه می‌شود، برآورد ریسک در بازه های زمانی تکرار شود تا هر تغییری که ممکن است بر نتایج برآورد ریسک تاثیر گذار باشد را لحاظ نماید.
اطلاعات بیشتر درباره برآورد ریسک‌های امنیت را می‌توان در بند ۴-۱ " برآورد ریسک‌های امنیت" یافت.

۰-۵ انتخاب کنترل‌ها

پس از اینکه نیازهای امنیتی و ریسک‌ها، شناسایی شدند و تصمیم برای برطرف سازی ریسک‌ها اتخاذ گردید، کنترل‌های مناسب باید به نحوی انتخاب و بکار گرفته شوند، تا از کاهش ریسک‌ها و رسیدن آنها به حدقابل قبول، اطمینان حاصل شود.کنترل‌ها را می‌توان از این استاندارد یا دیگر مجموعه های کنترلی، یا از کنترل‌های جدید که به منظور برآورده ساختن نیازهای خاص طراحی شده اند، به فرا خور حال، انتخاب نمود. انتخاب کنترل‌های امنیتی، بستگی به تصمیمات سازمان دارد که بر اساس، معیار پذیرش ریسک، گزینه های برطرف

سازی ریسک و رویکرد اتخاذ شده مدیریت ریسک در سازمان و همچنین کلیه قوانین و مقررات ملی و بین المللی که باید مدنظر قرار گیرد، اتخاذ می‌شود.
تعدادی از این کنترل‌ها در این استاندارد می‌تواند بعنوان اصول راهنما برای مدیریت امنیت اطلاعات، در نظر گرفته شود که در بیشتر سازمانها قابل بکارگیری هستند. جزئیات بیشتر در این باره در زیر و تحت عنوان "نقطه آغازین امنیت اطلاعات" تشریح شده است.
اطلاعات بیشتر درباره انتخاب کنترل‌ها و سایر گزینه‌های برطرف‌سازی ریسک را می‌توان در بند ۴-۲ "برطرف‌سازی ریسک‌های امنیت" پیدا کرد.

۶-۰ نقطه آغازین امنیت اطلاعات

تعدادی از کنترل‌ها را می‌توان به عنوان نقطه شروع مناسبی برای پیاده سازی امنیت اطلاعات در نظر گرفت. این کنترل‌ها یا بر اساس الزامات قانونی ضروری هستند و یا تجربیات مشترک[1] امنیت اطلاعات.
کنترل‌های در نظر گرفته شده که برای هر سازمان از منظر قانونی ضروری بوده بسته به قابل اجرا بودن قوانین، شامل :

الف- حفاظت از داده‌ها و حریم خصوصی افراد (رجوع کنید به بند ۱۵-۱-۴)
ب- حفاظت از سوابق سازمانی (رجوع کنید به بند ۱۵-۱-۳)
پ- حقوق مالکیت فکری (رجوع کنید به بند ۱۵-۱-۲)

کنترل‌های در نظر گرفته شده که حاصل تجربیات مشترک امنیت اطلاعات هستند، شامل:

الف- مستند خط مشی امنیت اطلاعات (رجوع کنید به بند ۵-۱-۱)
ب- تخصیص مسوولیت‌های امنیت اطلاعات (رجوع کنید به بند ۶-۱-۳)
پ- یادگیری، آموزش و آگاه سازی امنیت اطلاعات (رجوع کنید به بند ۸-۲-۲)
ت- اصلاح پردازش برنامه های کاربردی (رجوع کنید به بند ۱۲-۲)
ث- مدیریت آسیب پذیری فنی (رجوع کنید به بند ۱۲-۶)
ج- مدیریت استمرار کسب وکار (رجوع کنید به بند ۱۴)
چ- مدیریت رخدادهای[2] امنیت اطلاعات و بهبودها (رجوع کنید به بند ۱۳-۲)

این کنترل‌ها به اکثر سازمانها و محیط‌ها اعمال می‌شوند.
لازم به ذکر است که همه کنترل‌های این استاندارد مهم بوده و توصیه می‌شود در نظر گرفته شوند، ارتباط هر کنترل از لحاظ مواجهه با ریسک‌های مشخص سازمان باید در نظر گرفته شود. از اینرو، هر چند که رویکرد در نظر گرفته شده در بالا نقطه شروع مناسبی است، ولی نمی‌تواند جایگزین انتخاب کنترل‌ها بر اساس برآورد ریسک شود.

1- Common Paracticed
2- Incident

۰-۷ عوامل حیاتی موفقیت

تجربه نشان داده است، که عوامل زیر معمولاً نقش اساسی را در پیاده سازی موفق امنیت اطلاعات در سازمان بر عهده دارند :

الف - خط‌مشی امنیت اطلاعات، اهداف و فعالیتهایی که منعکس کننده اهداف کسب‌وکار هستند؛

ب – یک رویکرد و چارچوب برای پیاده سازی، پایش و اصلاح امنیت اطلاعات که با فرهنگ سازمانی سازگار است؛

پ - پشتیبانی صریح و تعهد کلیه سطوح مدیریتی؛

ت - درک مناسب از الزامات امنیت اطلاعات، برآورد ریسک و مدیریت ریسک؛

ث - بازاریابی اثربخش از امنیت اطلاعات به تمام مدیران، کارکنان و سایر افراد بمنظور آگاه‌سازی آنها؛

ج - انتشار راهنما برای خط‌مشی و استانداردهای امنیت اطلاعات برای کلیه مدیران، کارکنان و سایر افراد؛

چ - تامین منابع مالی برای فعالیتهای مدیریت امنیت اطلاعات؛

ح - آگاه‌سازی، تعلیم و آموزش مناسب؛

خ - تدوین فرایند اثربخش مدیریت رخدادهای امنیت اطلاعات؛

د - پیاده سازی سامانه ای قابل اندازه گیری[1] که برای ارزیابی عملکرد مدیریت امنیت اطلاعات و ارایه بازخورد برای بهبود بکار رود.

۰-۸ توسعه رهنمودهای مربوط به خود

این راهنمای پیاده سازی ممکن است به عنوان نقطه شروعی برای توسعه دستورالعمل‌های اختصاصی رهنمود برای سازمان بکار گرفته شود. ممکن است همه بخشهای این راهنمای پیاده سازی و کنترل‌ها قابل استفاده نباشند. از این گذشته ممکن است رهنمودها و کنترل‌های تکمیلی، که در این استاندارد نیامده است، مورد نیاز باشند. هنگامی که مستندات توسعه داده می‌شوند، این مستندات شامل کنترل‌ها و خطوط راهنمای تکمیلی هستند، که ممکن است شامل ارجاعات- متقاطع[2] به بندهای این استاندارد، در موارد مقتضی، جهت سهولت در بررسی انطباق بوسیله ممیزین و شرکا کسب وکار، باشد.

۱- توجه شود که اندازه گیری‌های مدیریت امنیت اطلاعات خارج از هدف و دامنه کاربرد این استاندارد می باشد.

2- Cross-Reference

فن‌آوری اطلاعات – فنون امنیتی – آیین کار مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، برقرار کردن خطوط راهنما و اصول کلی برای راه اندازی، پیاده سازی، نگهداری و توسعه مدیریت امنیت اطلاعات در یک سازمان است. اهداف آورده شده در این استاندارد ملی، راهنمایی عمومی برای اهداف عرفاً مورد قبول مدیریت امنیت اطلاعات است.

اهداف کنترلی و کنترل‌های این استاندارد ملی برای برآورده ساختن الزامات شناساییِ داده شده بوسیله ارزیابی ریسک، پیاده سازی می‌شوند. این استاندارد ملی ممکن است بعنوان رهنمود پیاده سازی برای توسعه استانداردهای امنیت سازمانی، تجارب مدیریت امنیت اثربخش و کمک به ایجاد اطمینان در فعالیتهای درون سازمانی بکار رود.

این استاندارد معادل استاندارد بین‌المللی ISO/IEC 27002:2005 می‌باشد؛ و ساختار، بندها، ارجاعات، مفاهیم و شماره این استاندارد ملی هماهنگ با استاندارد بین‌المللی معادل می‌باشد. این استاندارد ملیِ معادل به صورت زیر شناخته می‌شود:

استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۲: سال ۱۳۸۷

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر بکار می رود.

۱-۲

دارایی[1]

هر چیزی که برای سازمان دارای ارزش است.

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

۲-۲

کنترل[2]

ابزار مدیریت کردن ریسک، شامل خط‌مشی ها، رویه ها، رهنمودها، دستورالعمل‌ها یا ساختارهای سازمانی، که می‌تواند ماهیتی اجرایی، فنی، مدیریتی یا قانونی داشته باشند.

یادآوری : کنترل همچنین بعنوان مترادفی برای محافظ یا اقدام متقابل است.

۳-۲

خطوط راهنما[3]

توصیفی که روشن می‌کند، چه چیزی و چطور برای انجام توصیه می‌شود، تا اهداف تعیین شده در خط‌مشی بدست آید.

1- Asset
2- Control
3- Guideline : خطوط راهنما، رهنمود

۴-۲

تجهیزات پردازش اطلاعات[1]

هر سامانهٔ پردازش اطلاعات، خدمت[2] یا زیر ساخت یا مکانهای فیزیکی که در آن قرار دارند.

۵-۲

امنیت اطلاعات[3]

حفظ محرمانگی، یکپارچگی و در دسترس پذیری اطلاعات. همچنین ویژگیهایی از قبیل سندیت، پاسخگویی، انکارناپذیری و قابلیت اطمینان، را نیز می‌تواند شامل شود.

۶-۲

رویداد امنیت اطلاعات[4]

رویداد امنیت اطلاعات، رویداد شناسایی شده یک سیستم، خدمت یا شبکه است که دلالت بر نقض احتمالی خط‌مشی امنیت اطلاعات یا نقص حفاظتی، یا وضعیت ناشناخته قبلی که ممکن است با امنیت مرتبط باشد، دارد.
[ISO/IEC TR 18044:2004]

۷-۲

رخداد امنیت اطلاعات[5]

یک رخداد امنیت اطلاعات، با یک یا مجموعه ای از رویدادهای امنیت اطلاعات ناخواسته یا پیش بینی نشده که به احتمال زیاد، عملیات کسب‌وکار را به خطر انداخته و امنیت اطلاعات را تهدید می‌کند، معین می‌شوند.
[ISO/IEC TR 18044:2004]

۸-۲

خط‌مشی[6]

قصد و جهت‌گیری کلی که بطور رسمی‌توسط مدیریت بیان می‌شود.

1- Information processing facilities
2- Service
3- Information security
4- Information security event
5- Information security incident
6- Policy

۹-۲

ریسک[1]

ترکیب احتمال یک رویداد و میزان پیامدهای آن.
[ISO/IEC Guide 73:2002]

۱۰-۲

تحلیل ریسک[2]

استفاده نظام مند از اطلاعات به منظور شناسایی منابع و تخمین ریسک
[ISO/IEC Guide 73:2002]

۱۱-۲

برآورد ریسک[3]

فرایند کلی تحلیل و ارزیابی ریسک
[ISO/IEC Guide 73:2002]

۱۲-۲

ارزیابی ریسک[4]

فرایند مقایسه ریسک تخمین زده شده با معیار ریسک ارایه شده، به منظور تعیین اهمیت ریسک
[ISO/IEC Guide 73:2002]

۱۳-۲

مدیریت ریسک[5]

فعالیتهای هماهنگ شده برای هدایت و کنترل یک سازمان با توجه به ریسک.

یادآوری : مدیریت ریسک بطور معمول شامل ارزیابی ریسک، برطرف سازی ریسک، پذیرش ریسک و ارتباط با ریسک است.
[ISO/IEC Guide 73:2002]

۱۴-۲

برطرف سازی ریسک[6]

فرایند انتخاب و پیاده سازی تمهیداتی برای اصلاح ریسک
[ISO/IEC Guide 73:2002]

1- Risk
2- Risk analysis
3- Risk assessment
4- Risk evaluation
5- Risk management
6- Risk treatment

۱۵-۲

شخص سوم[1]

شخص یا نهادی که مستقل از اشخاص درگیر به موضوع مورد بحث، شناخته می‌شود.

۱۶-۲

تهدید[2]

دلیل بالقوه یک رخداد ناخواسته، که ممکن است نتیجه آن خسارت به سازمان یا سامانه باشد.
[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

۱۷-۲

آسیب پذیری[3]

یک ضعف در یک دارایی یا مجموعه ای از دارایی‌ها که می‌تواند بوسیله یک یا چند تهدید مورد بهره برداری قرار گیرد.
[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

1- Third party
2- Threat
3- Vulnerability

۳ ساختار این استاندارد

این استاندارد شامل ۱۱ بند کنترل امنیت، که در کل مشتمل بر ۳۹ طبقه اصلی امنیتی و یک بند مقدماتی از جمله برآورد و برطرف سازی ریسک، است.

۳-۱ بندها

هر بند شامل تعدادی طبقه امنیتی عمده است. این یازده بند (که با تعدادی از طبقات امنیتی عمده همراه است که در هر بند گنجانده شده اند) عبارتند از:

الف - خط مشی امنیت (۱)؛

ب - سازمان امنیت اطلاعات (۲)؛

پ - مدیریت دارایی (۲)؛

ت - امنیت منابع انسانی (۳)؛

ث - امنیت فیزیکی و محیطی (۲)؛

ج - مدیریت ارتباطات و عملیات (۱۰)؛

چ - کنترل دسترسی (۷)؛

ح - اکتساب، توسعه و نگهداری سیستم‌های عملیاتی (۶)؛

خ - مدیریت رخداد امنیت اطلاعات (۲)؛

د - مدیریت استمرارکسب وکار (۱)؛

ذ - انطباق (۳)؛

یادآوری: ترتیب بندها در این استاندارد به معنای اهمیت آنها نیست. بسته به شرایط، تمام بندها ممکن است مهم باشند. بنابراین توصیه می‌شود، هر سازمانی که این استاندارد را به کار می‌گیرد، بندهای قابل استفاده، اهمیت آنها و کاربردشان را برای فرایندهای کسب وکار خود شناسایی کند. همچنین، تمام این فهرست ها در این استاندارد به ترتیب اولویت نیستند مگر در مواردی که ذکر شده باشد.

۳-۲ طبقه های امنیتی عمده

هرطبقه امنیتی عمده شامل موارد زیر است:

الف - یک هدف کنترلی که نشان می دهد چه چیزی باید به دست آید؛ و

ب - یک یا چند کنترل که می‌توان آن برای دستیابی به هدف کنترل پیاده سازی کرد؛

شرح کنترل ها به قرار زیر است:

کنترل

بیانیه کنترل خاصی را برای برآورده سازی هدف کنترل، تعریف می‌کند.

راهنمای پیاده سازی

اطلاعات مفصل تری برای پشتیبانی از پیاده سازی کنترل و دستیابی به هدف کنترل، بدست می دهد. بعضی از این راهنمایی‌ها ممکن است در تمام موارد مناسب نباشند و بنابراین دیگر راههای پیاده سازی کنترل ممکن است مناسب تر باشند.

سایر اطلاعات

اطلاعات بیشتری ارایه می دهد که ممکن است لازم باشد در نظر گرفته شود، مثلا ملاحظات قانونی و اشاره به استانداردهای دیگر.

۴ برآورد و برطرف سازی ریسک

۴-۱ برآورد ریسک های امنیتی

برآورد ریسک باید ریسک‌ها را در مقایسه با معیارهای قابل قبول ریسک و اهداف مربوط به سازمان، شناسایی، مقدار دهی کمی و اولویت بندی نماید. توصیه می‌شود، نتایج اقدام مناسب مدیریت و اولویت های مدیریت ریسک‌ها امنیت اطلاعات برای پیاده سازی کنترل های انتخاب شده جهت محافظت در برابر این ریسک‌ها را، تعیین و راهنمایی کند. ممکن است نیاز باشد، فرایند برآورد ریسک‌ها و انتخاب کنترل ها چند بار انجام شود تا بخش های مختلف سازمان یا سامانه های اطلاعات فردی را پوشش دهد.

توصیه می‌شود برآورد ریسک شامل رویکرد نظام مند برای تخمین شدت ریسک و فرایند مقایسه ریسک تخمین زده شده در مقایسه با معیارهای ریسک باشد، تا اهمیت ریسک‌ها را تعیین نماید (ارزیابی ریسک)

توصیه می‌شود برآورد های ریسک همچنین به طور دوره ای انجام شود تا تغییرات در الزامات امنیتی و در شرایط ریسک، بعنوان مثال در دارایی‌ها، تهدیدها، آسیب پذیری ها، پیامدها، اریابی ریسک، و زمانی که تغییرات مهم رخ می دهد، را نیز لحاظ کند. توصیه می‌شود این ارزیابی های ریسک به گونه ای روش مند[1] به کار گرفته شوند تا نتایج تکرارپذیر و قابل قیاس ارایه دهد.

توصیه می‌شود، برآورد ریسک امنیت اطلاعات دارای یک هدف و دامنه کاربرد تعریف مشخص باشد، تا اثربخش باشد و همچنین توصیه می‌شود شامل روابط برآورد های ریسک در زمینه های دیگر، به شرط تناسب، نیز باشد.

هدف و دامنه کاربرد ریسک می‌تواند در کل سازمان، بخش هایی از سازمان، یک سامانه اطلاعات فردی، اجزا سیستم خاص، یا خدمات، در جاییکه که قابل اجرا است، واقع گرایانه و مفید باشد. مثال های روش شناسی های برآورد ریسک در ISO/IEC TR 13335-3 (رهنمودهای مدیریت امنیت فن‌آوری اطلاعات: روشهایی برای مدیریت امنیت فن‌آوری اطلاعات)

۴-۲ برطرف سازی ریسک‌های امنیتی

توصیه می‌شود قبل از در نظر گرفتن برطرف سازی ریسک، سازمان معیارهایی برای تعیین این که آیا ریسک را می‌توان پذیرفت یا نه تعیین کند. مثلا اگر برآورد شود که ریسک پایین است یا هزینه برطرف سازی آن برای سازمان مقرون به صرفه نیست ریسک‌ها مجاز است پذیرفته شوند. توصیه می‌شود این تصمیمات ثبت شوند.

برای هر یک از ریسک‌های که شناسایی شده پس از برآورد ریسک یک تصمیم برای برطرف سازی ریسک باید اتخاذ شود. گزینه های ممکن برای برطرف سازی ریسک عبارتند از:

الف - اعمال کنترل های مناسب برای کاهش ریسک‌ها

ب - پذیرش آگاهانه و هدفمند ریسک‌ها، به شرط آن که آنها به روشنی خط مشی و معیارهای سازمان را برای پذیرش ریسک رعایت کنند.

پ - اجتناب از ریسک با اجازه ندادن به فعالیت هایی که باعث رخ دادن ریسک می‌شوند.

ت - انتقال ریسک‌ها مربوطه به اشخاص دیگر، مثلا بیمه گران و تامین کنندگان.

1- Methodological

برای ریسک‌هایی که در برطرف سازی ریسک تصمیم به اعمال کنترل های مناسب گرفته شده است، توصیه می‌شود این کنترل ها انتخاب و برای برآورده ساختن الزامات شناسایی شده در برآورد ریسک، پیاده سازی شوند. توصیه می‌شود کنترل ها تضمین کنند که ریسک‌ها با احتساب موارد زیر تا حد قابل قبولی کاهش یافته است:

الف - الزامات و محدودیت های قوانین و مقررات ملی و بین المللی

ب - اهداف سازمانی

پ - الزامات و محدودیت های عملیاتی؛

ت - هزینه اجرا، و عملیات در رابطه با ریسک‌های که کاهش می یابند و نسبت ریسک باقیمانده با الزامات و محدودیت های سازمان؛

ث - نیاز به تعدیل سرمایه گذاری در پیاده سازی و عملیات کنترل ها در مقابل آسیبی که ممکن است از نارسایی های امنیتی حاصل شود؛

کنترل ها را می‌توان از این استاندارد یا از هر مجموعه کنترلی دیگر انتخاب کرد یا کنترل های جدید را می‌توان برای برآورده ساختن نیازهای خاص سازمان طراحی کرد. لازم به یادآوری است که بعضی از کنترل ها ممکن است در هر سامانه یا محیط اطلاعاتی قابل استفاده نبوده و ممکن است برای تمام سازمان ها قابل اجرا نباشد. مثلا، ۱۰-۱-۳ بیان می‌کند که وظایف چگونه برای جلوگیری از سوء استفاده و خطا تفکیک می‌شوند. ممکن است برای سازمان های کوچک تر امکانپذیر نباشد که تمام وظایف را تفکیک کنند و دیگر راه های دستیابی به یک هدف کنترلی ممکن است لازم باشند. در یک مثال دیگر، ۱۰-۱۰ بیان می‌کند که استفاده از سیستم را چگونه می‌توان پایش کرد و شواهد را جمع آوری کرد. کنترل های بیان شده مثلا ثبت وقایع، ممکن است با مقررات قابل قبول، نظیر محافظت از حریم خصوصی مشتریان یا محیط کار تناقض داشته باشند.

توصیه می‌شود کنترل های امنیت اطلاعات، در مرحله تعیین الزامات طراحی و خصوصیات پروژه ها و سیستم‌ها در نظر گرفته شود. قصور در انجام این کار ممکن است منجر به هزینه های اضافه و راه حلهایی با اثربخشی کمتر شود و شاید در بدترین شرایط منجر به ناتوانی در دستیابی به امنیت کافی شود.

توصیه می‌شود که به خاطر داشت؛ هیچ مجموعه ای از کنترل ها نمی‌توانند امنیت کامل را بدست دهند و توصیه می‌شود اقدام تکمیلی مدیریتی برای پایش، ارزیابی، و بهبود بازدهی و اثربخشی کنترل‌های امنیتی برای پشتیبانی از دستیابی به اهداف سازمان پیاده سازی شوند.

۵ خط‌مشی امنیتی

۵-۱ خط‌مشی امنیتی

هدف : فراهم آوری جهت‌گیری و حمایت مدیریت برای امنیت اطلاعات مطابق با الزامات کسب‌وکار و قوانین و مقررات مرتبط. توصیه می‌شود، مدیریت، خط مشی روشنی در ارتباط با اهداف کسب‌وکار اتخاذ نماید و حمایت و تعهد خود را به امنیت اطلاعات از این طریق صدور و نگهداری از خط‌مشی امنیت اطلاعات در سرتاسر سازمان به اثبات برساند.

۵-۱-۱ *مدرک خط‌مشی امنیت اطلاعات*

کنترل

توصیه می‌شود، یک سند خط‌مشی امنیت اطلاعات، توسط مدیریت تصویب و منتشر و به اطلاع همه کارکنان و اشخاص مرتبط بیرونی برسد.

راهنمای پیاده سازی

توصیه می‌شود، سند خط‌مشی امنیت اطلاعات تعهد مدیریت را بیان نماید و رویکرد سازمان به مدیریت امنیت اطلاعات را تعیین کند.

توصیه می‌شود، سند خط‌مشی محتوی بیانیه ای باشد که موارد زیر را شامل شود :

الف - تعریفی از امنیت اطلاعات، اهداف کلی آن، و دامنه کاربرد و اهمیت امنیت بعنوان ساز وکاری برای به اشتراک گذاشتن اطلاعات (رجوع کنید به مقدمه)؛

ب – بیانیه نیت مدیریت برای پشتیبانی از اهداف و اصول امنیت اطلاعات در راستای راهبرد و اهداف کسب‌وکار؛

پ - یک چارچوبی برای انتخاب کنترل‌ها و اهداف کنترلی، از جمله ساختار مدیریت و برآورد ریسک؛

ت - تشریح مختصری از خط مشی‌های امنیت، اصول، استانداردها و انطباق های قانونی مورد نظر سازمان از جمله :

۱- انطباق با قوانین و مقررات و الزامات قراردادی؛

۲- نیازمندیهای آگاه‌سازی، یادگیری و آموزش امنیت؛

۳- مدیریت استمرارکسب‌وکار؛

۴- پیامدهای حاصل از خطاهای خط‌مشی امنیت اطلاعات؛

ث - تعریفی از مسوولیت‌های عمومی و تخصصی مدیریت امنیت اطلاعات، از جمله گزارش رخدادهای امنیت اطلاعات؛

ج - ارجاع به مستنداتی که ممکن است خط‌مشی را پشتیبانی کند، از جمله برای یک سیستم اطلاعاتی خاص کدام یک از رویه ها و خط‌مشی‌های امنیتی مطابقت دارد یا توصیه می‌شود هر کاربری چه قواعدی را رعایت نماید.

توصیه می‌شود این خط مشی امنیت اطلاعات به نحوی که برای کلیه افراد قابل فهم باشد از طریق سازمان برای افراد تهیه شده و در دسترس افراد مربوطه قرار گیرد.

سایر اطلاعات

خط‌مشی امنیت اطلاعات ممکن است بعنوان بخشی از سند خط‌مشی عمومی باشد. اگر خط‌مشی امنیت اطلاعات به خارج از سازمان انتشار یابد، توصیه می‌شود مراقب بود اطلاعات حساس سازمان را فاش نکند. اطلاعات بیشتر را می‌توان در استاندارد ملی ایران به شماره ۱-۹۹۷۰ پیدا کرد.

۵-۱-۲ بازبینی خط‌مشی امنیت اطلاعات

کنترل

توصیه می‌شود خط‌مشی امنیت اطلاعات در بازه‌های زمانی برنامه ریزی شده بازبینی شود، یا اگر تغییرات معناداری رخ داد، تا همواره از مناسبت، کفایت و اثربخشی آن اطمینان حاصل شود.

راهنمای پیاده سازی

توصیه می‌شود، خط‌مشی دارای یک مالک باشد که از سوی مدیریت مسوولیت توسعه، بازبینی و ارزیابی خط‌مشی امنیت را برعهده گرفته است.توصیه می‌شود بازبینی شامل برآورد فرصت هایی برای بهبود در خط مشی امنیتی سازمان و رویکرد به مدیریت امنیت اطلاعات در واکنش به تغییرات در محیط سازمانی، رویدادهای کسب وکار، شرایط قانونی، یا محیط فنی، باشد.

توصیه می‌شود بازبینی خط مشی امنیت اطلاعات نتایج بررسی های مدیریت را مد نظر قرار دهد. توصیه می‌شود، رویه هایی تعریف شده برای بازبینی مدیریت، از جمله یک جدول زمان بندی یا دوره بازبینی وجود داشته باشند.

توصیه می‌شود ورودی بازبینی مدیریت شامل اطلاعاتی درباره موارد زیر باشد:

الف - بازخورد اشخاص ذینفع

ب - نتایج بازبینی های مستقل (رجوع کنید به ۶-۱-۸)

پ - وضعیت اقدام های اصلاحی و پیشگیرانه (رجوع کنید به ۶-۱-۸ و ۱۵-۲-۱)

ت - نتایج بازبینی های پیشین مدیریت

ث - انطباق با خط مشی امنیت اطلاعات و عملکرد فرایند

ج - تغییراتی که ممکن است بر رویکرد سازمان به مدیریت امنیت اطلاعات تاثیر بگذارد؛ از جمله تغییرات درمحیط سازمانی، شرایط کسب وکار، دسترسی به منابع، شرایط قراردادی، قانونی و حقوقی، یا محیط فنی؛

چ - روندهای مربوط به تهدیدها و آسیب پذیری ها؛

ح - رخدادهای گزارش شده امنیت اطلاعات (رجوع کنید به ۱۳-۱)؛

خ - پیشنهادات ارایه شده توسط مراجع مربوطه (رجوع کنید به ۶-۱-۶)؛

توصیه می‌شود خروجی بازبینی مدیریت شامل هر تصمیم و اقدامی درباره موارد زیر باشد:

الف - بهبود رویکرد سازمان در مدیریت امنیت اطلاعات و فرایندهای آن؛

ب - بهبود اهداف کنترلی و کنترل ها؛

پ - بهبود تخصیص منابع و/ یا مسوولیت ها.

توصیه می‌شود سابقه ای از بازبینی مدیریت نگهداری شود.

توصیه می‌شود تایید مدیریت برای خط مشی بازبینی شده اخذ شود.

۶ سازمان امنیت اطلاعات

۶-۱ سازمان داخلی

هدف : مدیریت امنیت اطلاعات در درون سازمان.
توصیه می‌شود یک چارچوب مدیریتی برای بنیان نهادن و کنترل نمودن پیاده سازی امنیت اطلاعات در درون سازمان تدوین شود.
توصیه می‌شود مدیریت خط‌مشی امنیت اطلاعات را تصویب و نقشهای امنیتی را تکلیف کند و پیاده سازی امنیت در سازمان را هماهنگ و بازبینی نماید.
توصیه می‌شود در صورت لزوم، یک منبع مشاوره تخصصی امنیت اطلاعات ایجاد و در دسترس سازمان قرار گیرد.
برقراری ارتباط با مشاوران خارج از سازمان برای آگاهی از وضعیت رویکردهای صنعتی، پایش استانداردها و روشهای ارزیابی و ارتباطات مناسب برای زمان وقوع رخدادهای امنیتی، گسترش داده می‌شود.
توصیه می‌شود رویکردی چند جانبه انظباطی برای امنیت اطلاعات ایجاد شود

۶-۱-۱ *تعهد مدیریت به امنیت اطلاعات*

کنترل

توصیه می‌شود مدیریت فعالانه، امنیت را در درون سازمان از طریق جهت‌گیری شفاف، تعهد اثبات شده، مکلف کردن به صورت صریح و اعلام مسوولیت‌های امنیت اطلاعات، حمایت نماید.

راهنمای پیاده سازی

توصیه می‌شود مدیریت:

الف - اطمینان حاصل کند که اهداف امنیت اطلاعات شناسایی می‌شوند، الزامات سازمان را برآورده می سازند و به صورت فرایندهای مرتبط یکپارچه شده اند؛

ب - خط‌مشی امنیت اطلاعات را قاعده سازی، بازبینی و تصویب کند؛

پ – اثربخشی اجرای خط‌مشی امنیت اطلاعات را بازبینی نماید؛

ت – جهت‌گیری مشخص و حمایت های مدیریتی مشهود برای طرحهای ابتکاری امنیت را فراهم آورد؛

ث - منابع لازم برای امنیت اطلاعات را تامین کند؛

ج – تخصیص نقش ها و مسوولیت های مشخص برای امنیت اطلاعات در سراسر سازمان را تایید نماید؛

چ - طرحها و برنامه هایی بمنظور آگاه سازی ازامنیت اطلاعات ایجاد نماید؛

ح - اطمینان حاصل کند که پیاده سازی کنترل‌های امنیت در سراسر سازمان هماهنگ شده اند؛

توصیه می‌شود مدیریت نیاز به مشاوره متخصصین داخلی و خارجی را شناسایی و نتایج مشورتی را در سراسر سازمان بازبینی نموده و هماهنگی های لازم را انجام دهد.

بر اساس اندازه سازمان، چنین مسوولیت‌هایی می‌توانست توسط یک مجمع مدیریتی اختصاصی یا بوسیله نهاد مدیریتی موجود، همچون هیات مدیره انجام شود.

سایر اطلاعات

اطلاعات بیشتر در استاندارد ملی ایران به شماره ۱-۹۹۷۰ وجود دارد.

۶-۱-۲ هماهنگی امنیت اطلاعات

کنترل

توصیه می‌شود فعالیتهای امنیت اطلاعات، توسط نمایندگانی از بخش‌های مختلف سازمان با نقش ها و کارکردهای شغلی مرتبط، هماهنگ شوند.

راهنمای پیاده سازی

به طور معمول، توصیه می‌شود هماهنگی امنیت اطلاعات شامل تعامل و همکاری مدیران، کاربران، راهبران[1]، طراحان برنامه های کاربردی، ممیزین، کارکنان امنیت و مهارت متخصصین این حوزه ها از جمله بیمه، موارد قانونی، منابع انسانی، فن‌آوری اطلاعات[2] یا مدیریت ریسک باشد.

توصیه می‌شود این فعالیت:

الف - تضمین نماید فعالیتهای امنیت، مطابق با خط‌مشی امنیت اطلاعات اجرا می‌شوند؛

ب - تعیین نماید چگونه با عدم انطباقها برخورد می‌شود؛

پ - روش شناسی و فرایندهایی برای امنیت اطلاعات، از جمله برآورد ریسک، طبقه‌بندی اطلاعات را تصویب کند؛

ت - تغییرات معنی دار در تهدید و در معرض تهدید قرار گرفتن اطلاعات و امکانات پردازش اطلاعات را شناسایی کند.

ث - کفایت هماهنگی در پیاده سازی کنترل‌های امنیت اطلاعات را ارزیابی کند.

ج - تحصیل، یادگیری و آگاه‌سازی امنیت اطلاعات در سراسر سازمان را بگونه ای اثربخش ارتقا دهد.

چ - اطلاعات حاصل از پایش و بازبینی رخدادهای امنیت اطلاعات را ارزیابی نموده و اقدامات مناسب را در پاسخ به رخدادهای شناسایی شدهٔ امنیت اطلاعات پیشنهاد نماید.

اگر سازمان از گروهی با عملکرد متقاطع[3] جداگانه استفاده نمی‌کند، برای مثال به این دلیل که این گروه برای اندازه سازمان مناسب نیست، توصیه می‌شود این اقدامات به نهاد مدیریتی مناسب و یا حتی مدیری مناسب سپرده شود.

۶-۱-۳ تخصیص مسوولیت‌های امنیت اطلاعات

کنترل

توصیه می‌شود تمامی مسوولیت‌های امنیت اطلاعات، به وضوح تعریف شوند.

راهنمای پیاده سازی

توصیه می‌شود تخصیص مسوولیت‌های امنیت اطلاعات مطابق با خط‌مشی امنیت اطلاعات (به بند ۴ رجوع شود) صورت پذیرد. توصیه می‌شود برای محافظت از تک تک داراییها و انجام فرایندهای امنیتی خاص، مسوولیت‌ها به

1- Administrators
2- Information Technology (IT)
3- Cross-Functional

گونه ای شفاف تعریف شوند. توصیه می‌شود این مسوولیت در صورت لزوم برای سایتهای خاص و امکانات پردازش اطلاعات با راهنمای جزیی‌تری تکمیل شود. توصیه می‌شود مسوولیت‌های محلی برای محافظت از داراییها و انجام فرایندهای خاص امنیتی، از قبیل طرح‌ریزی استمرار کسب‌وکار، بگونه ای شفاف تعریف شوند.
افراد با مسوولیت‌های امنیت تخصیص داده شده ممکن است وظیفه های امنیتی را به دیگران محول نمایند. با این حال، آنها همچنان مسوول بوده و توصیه می‌شود تعیین کنند وظایف محول شده به درستی انجام می‌شوند.
توصیه می‌شود محدودهٔ مسوولیت افراد بگونه ای شفاف بیان شود؛ بطور خاص موارد زیر باید رخ دهند :

الف – توصیه می‌شود دارایی‌ها و فرایندهای امنیتی مربوط به هر سیستم خاص شناسایی و به‌گونه ای شفاف تعریف شود؛

ب – توصیه می‌شود موجودیت مسوول در قبال هر دارایی یا فرایند امنیتی گماشته شده و جزئیات این مسوولیت مستند شود. (رجوع کنید به ۷-۱-۲)؛

پ – توصیه می‌شود سطوح اختیارات بطور شفاف تعریف گردیده و مستند شود؛

سایر اطلاعات

در بسیاری از سازمانها یک مدیر امنیت اطلاعات برای برعهده گیری مسوولیت کلان توسعه و پیاده سازی امنیت و پشتیبانی از کنترل‌های شناسایی شده منصوب خواهد شد.
با این وجود، مسوولیت تامین منابع و پیاده سازی کنترل‌ها اغلب بر عهده مدیران مختلف باقی خواهد ماند. یک تجربه مشترک این است که برای هر دارایی یک مالک مشخص شود که از آن به بعد مسوول محافظت روزانه از آن دارایی است.

۶-۱-۴ *فرایند مجوزدهی برای امکانات پردازش اطلاعات*

کنترل

توصیه می‌شود یک فرایند مجوزدهی مدیریتی برای امکانات جدید پردازش اطلاعات، تعریف و پیاده سازی شود.

راهنمای پیاده سازی

توصیه می‌شود خطوط راهنمای زیر برای فرایند مجوزدهی مد نظر قرار گیرند :

الف – توصیه می‌شود تجهیزات جدید دارای مجوزدهی مدیریت کاربری، مجوزدهی روش استفاده و دلیل استفاده، باشند. همچنین توصیه می‌شود، مجوز دهی از سوی مدیری که مسوول حفظ فضای امنیت سیستم اطلاعاتی محلی است، اخذ شود تا اطمینان حاصل شود کلیهٔ الزامات خط‌مشی های امنیت اطلاعات برآورده می‌شوند.

ب - هر جا که نیاز است، توصیه می‌شود نرم‌افزار و سخت افزار مورد بررسی قرار گیرد تا از سازگاری آنها با اجزا دیگر سیستم اطمینان حاصل شود.

پ - استفاده از امکانات پردازش اطلاعات شخصی یا خصوصی به عنوان مثال رایانه های قابل حمل، رایانه های خانگی یا وسایل قابل حمل، برای پردازش اطلاعات کسب وکار ممکن است خود باعث افزایش آسیب پذیری شود و بنابراین توصیه می‌شود کنترل‌های ضروری شناسایی و پیاده سازی شوند.

۶-۱-۵ توافق‌نامه‌های محرمانگی

کنترل

توصیه می‌شود الزاماتی برای قراردادهای محرمانگی یا عدم افشا که منعکس کننده نیازهای سازمان به حفاظت از اطلاعات است، شناسایی و بطور منظم بازبینی شوند.

راهنمای پیاده سازی

توصیه می‌شود قراردادهای محرمانگی یا عدم افشا به نیازمندیهای محافظت از اطلاعات محرمانه از طریق بکارگیری واژه های لازم الاجرای قانونی، اشاره کند. توصیه می‌شود برای شناسایی الزامات قراردادهای محرمانگی یا عدم افشا عناصر زیر مد نظر قرار گیرند :

الف – تعریفی از اطلاعاتی که باید محافظت شوند.(بعنوان مثال اطلاعات محرمانگی)؛

ب – طول مدت مورد انتظار برای یک قرارداد، دربرگیرنده مواردی که محرمانگی باید بطور نامحدود رعایت شود؛

پ - اقدامات مورد نیاز هنگامی که قرارداد خاتمه می پذیرد؛

ت - مسوولیت‌ها و اقدامات امضاکنندگان برای اجتناب از افشا اطلاعات غیر مجاز(مانند، "نیاز است که بداند")؛

ث - مالک اطلاعات، اطلاعات محرمانه تجاری و مالکیت معنوی و اینکه چگونه این با حفاظت از اطلاعات محرمانه مرتبط است؛

ج – اجازهٔ استفاده از اطلاعات محرمانه، و حق امضا استفاده از اطلاعات؛

چ - حق فعالیت‌های ممیزی و پایشی که شامل اطلاعات محرمانه می‌شوند.

ح - فرایندی برای اخطار و گزارش دهی افشا غیر مجاز یا رخنه در اطلاعات محرمانه؛

خ - مفادی[1] برای اطلاعاتی که باید در زمان خاتمه قرارداد عودت داده شوند یا از بین بروند، و

د - اقدامات مورد انتظاری که در صورت تخطی از این قرارداد انجام می‌گیرند.

بر اساس الزامات امنیت سازمان، موارد دیگری ممکن است در باره قرارداد محرمانگی یا عدم افشا مورد نیاز باشد.

توصیه می‌شود قرارداد محرمانگی و عدم افشا، مطابق با قوانین و مقررات قابل اجرا برای حوزهٔ قضایی که در آن اجرا می‌شود، باشد. (رجوع کنید به ۱۵-۱-۱).

توصیه می‌شود الزامات قراردادهای محرمانگی و عدم افشا در بازه‌های زمانی منظم و هنگامی که تغییری روی داده که این الزامات را متاثر می‌کند، بازبینی شوند.

سایر اطلاعات

قراردادهای محرمانگی و عدم افشا، اطلاعات سازمانی را محافظت نموده و مسوولیت امضا کنندگان را برای حفظ، بکارگیری و افشا اطلاعات به شیوه‌ای مسوولانه و تفویضی، گوشزد می‌کند.

ممکن است یک سازمان نیازمند نمونه های مختلفی از قراردادهای محرمانگی و عدم افشا در شرایط مختلف باشد.

1- Terms

۶-۱-۶ برقراری ارتباط با مراجع دارای اختیار

کنترل

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

راهنمای پیاده سازی

توصیه می‌شود سازمانها رویه هایی در اختیار داشته باشند که مشخص می‌کند در چه زمانی و با کدام یک از مراجع دارای اختیار (به عنوان مثال مجریان قانون، آتش نشانی، مراجع دارای اختیار نظارتی) تماس داشته باشند و چگونه توصیه می‌شود رخدادهای امنیت اطلاعات شناسایی شده در زمان مناسب گزارش دهی شوند، اگر این تردید وجود دارد که قانونی نقض شده است.

سازمانهای تحت شرایط حمله از طریق اینترنت ممکن است نیاز به شخص سوم بیرونی (به عنوان مثال یک ارایه کننده خدمت اینترنتی[1] یا اپراتور ارتباطاتی) برای اقدام در مقابل منبع حمله داشته باشند.

سایر اطلاعات

حفظ چنین ارتباطاتی ممکن است از ملزومات پشتیبانی از مدیریت رخدادهای امنیت اطلاعات (رجوع کنید به بخش ۱۳-۲) یا فرایند طرح‌ریزی استمرار کسب‌وکار و احتیاطی[2] (بخش ۱۴) ضروری باشد. همچنین تماس با نهادهای تنظیم مقررات[3]، برای پیش بینی و آمادگی برای تغییرات آتی در قوانین یا مقرراتی که توسط سازمان باید رعایت شوند، مفید است. تماس با دیگر مراجع دارای اختیار، شامل شرکت های خدماتی دولتی، خدمات اضطراری، و سلامت و ایمنی به عنوان مثال آتش نشانی (در رابطه با استمرار کسب وکار)، تامین کنندگان ارتباطاتی (در رابطه با مسیریابی خط و در دسترس پذیری)، تامین کنندگان آب (در رابطه با امکانات خنک‌کننده برای تجهیزات) می‌شود.

۶-۱-۷ برقراری ارتباط با گروههای بامنافع خاص

کنترل

توصیه می‌شود ارتباطات مناسب با گروه‌های دارای گرایش خاص یا سایر مجمع‌های[4] امنیتی تخصصی و انجمن‌های حرفه ای، حفظ شود.

راهنمای پیاده سازی

توصیه می‌شود، عضویت در گروه‌های دارای گرایش خاص یا مجمع ها به منظور زیر در نظر گرفته شود :

الف - توسعه دانش دربارهٔ بهترین تجربیات و بروز نگهداشتن اطلاعات مرتبط با امنیت اطلاعات؛

ب - اطمینان از اینکه درک از محیط امنیت اطلاعات کنونی[5] و کامل است؛

پ – دریافت پیش از موعد هشدارهای آماده‌باش[6]، توصیه‌ها و وصله[7]های مربوط به حملات و آسیب‌پذیری‌ها؛

1- Internet Service Provider
2- Contingency
3- Regulatory Bodies
4- Forums
5- Current
6- Alerts
7- Patch

ت - دسترسی به توصیه های تخصصی امنیت اطلاعات؛

ث - به اشتراک گذاری و تبادل اطلاعات درباره فن‌آوری ها، محصولات، تهدیدات یا آسیب پذیری های جدید؛

ج - تدارک نقاط ارتباطی مناسب در هنگام برخورد با رخدادهای امنیت اطلاعات (همچنین رجوع کنید به بند ۱۳- ۲-۱)؛

سایر اطلاعات

قراردادهای به اشتراک گذاری اطلاعات می‌تواند به منظور بهبود همکاری و هماهنگی در موضوعات امنیتی تدوین شوند. توصیه می‌شود این قبیل قراردادها نیازمندیهای محافظت از اطلاعات حساس را شناسایی نمایند.

۸-۱-۶ *بازنگری مستقل امنیت اطلاعات*

کنترل

توصیه می‌شود، رویکرد سازمان به امنیت اطلاعات و پیاده سازی آن (به عبارت دیگر اهداف کنترل، کنترل‌ها، خط‌مشی ها، فرایندها و رویه ها برای امنیت اطلاعات)، در فواصل زمانی طرح‌ریزی شده یا هنگامیکه تغییرات عمده ای در پیاده سازی امنیت اطلاعات رخ داد، مستقلاً بازبینی شود.

راهنمای پیاده سازی

توصیه می‌شود بازبینی مستقل توسط مدیریت آغاز شود. چنین بازبینی مستقلی برای اطمینان از تداوم مناسب بودن، کفایت و اثربخشی رویکرد سازمان به مدیریت امتیت اطلاعات ضروری است. توصیه می‌شود بازبینی شامل ارزیابی فرصتهای بهبود و نیاز به تغییرات رویکردی در امنیت که شامل خط‌مشی و اهداف کنترلی می‌شود، باشد. توصیه می‌شود این بازبینی توسط افرادی مستقل از حیطه بازبینی بعنوان مثال فعالیت ممیزی داخلی، یک مدیر مستقل یا سازمان ثالث متخصص در چنین بازبینی هایی انجام شود. افرادی که اینگونه بازبینی ها را انجام می‌دهند توصیه می‌شود از مهارت و تجربه مناسب برخوردار باشند.

توصیه می‌شود نتایج بازبینی های مستقل ثبت شده و به مدیریتی که آغازگر این بازبینی ها بوده است، گزارش شود. توصیه می‌شود این سوابق نگهداری شوند.

اگر بازبینی‌های مستقل نشان دهند که رویکرد سازمان و اجرای مدیریت امنیت اطلاعات کافی نبوده و یا با جهت‌گیری بیان شده در سند خط‌مشی امنیت اطلاعات منطبق نیست (رجوع کنید به بند ۵-۱-۱)، توصیه می‌شود مدیریت اقدامهای اصلاحی را در این موارد مد نظر قرار دهد.

سایر اطلاعات

حوزه‌ای که توصیه می‌شود مدیران بصورت منظم بازبینی کنند (رجوع کنید به بند ۱۵-۲-۱)، ممکن است مستقلاً بازبینی شود. روشهای بازبینی ممکن است شامل مصاحبه با مدیران، بررسی سوابق یا بازبینی اسناد خط‌مشی امنیت باشد. استاندارد ملی ایران ایزو ۱۹۰۱۱: سال ۱۳۸۶[۱]، رهنمودهایی برای ممیزی سیستم‌های مدیریت کیفیت و / یا زیست محیطی بوده و ممکن است همچنین برای انجام بازبینی مستقل، که شامل تدوین و

---

[۱]- منظور استاندارد ملی معادل استاندارد بین المللی ISO 19011:2002 می باشد.

پیاده‌سازی برنامه بازبینی است، راهنمای مفیدی را ارایه نماید. بخش ۱۵-۳ کنترل‌های مرتبط با بازبینی مستقل برای سیستم‌های اطلاعات عملیاتی و بکارگیری ابزارهای ممیزی سیستم را معین می‌کند.

۶-۲ اشخاص بیرونی

هدف : حفظ و نگهداری امنیت اطلاعات و امکانات پردازش اطلاعات سازمان که در دسترس طرفهای بیرونی قرار داشته یا توسط ایشان پردازش یا مدیریت شده یا با آنها مبادله می‌شوند.
توصیه می‌شود امنیت اطلاعات سازمانی و تجهیزات پردازش اطلاعات با ورود محصولات یا خدمات طرفهای بیرونی کاهش نیابد.
توصیه می‌شود هر دسترسی به امکانات پردازش اطلاعات سازمان و پردازش و ارتباط اطلاعاتی بوسیله طرف‌های بیرونی کنترل شود.
در جایی که نیاز کسب‌وکار،کارکردن با طرفهای بیرونی را بطلبد،که ممکن است نیاز به دسترسی اطلاعات سازمانی و امکانات پردازش اطلاعات، یا بدست آوردن یا تامین محصول یا خدمت از یا برای طرف بیرونی باشد، توصیه می‌شود برآورد ریسکی بمنظور تعیین عواقب امنیتی و الزامات کنترلی انجام شود. توصیه می‌شود، کنترل‌ها با طرف بیرونی مورد توافق قرار گرفته و در قراردادی با آنها تعریف شود.

۶-۲-۱ *شناسایی ریسک‌های مرتبط با اشخاص بیرونی*

کنترل

توصیه می‌شود ریسک‌های اطلاعات و امکانات پردازش اطلاعات سازمان ناشی از فرایندهای کسب‌وکار مرتبط با اشخاص بیرونی شناسایی شده و پیش از اعطای دسترسی، کنترل‌های مناسب پیاده سازی شوند.

راهنمای پیاده سازی

در جایی که نیاز به اجازه دسترسی شخص بیرونی به امکانات پردازش اطلاعات یا اطلاعات یک سازمان است، توصیه می‌شود برآورد ریسک (همچنین رجوع کنید به بخش ۴) بمنظور شناسایی هرگونه الزاماتی از کنترل‌های خاص صورت پذیرد. توصیه می‌شود شناسایی ریسک‌های مرتبط به دسترسی شخص بیرونی در زمینه های زیر مد نظر قرار گیرد :

الف - امکانات پردازش اطلاعاتی که نیاز است شخص بیرونی به آنها دسترسی داشته باشد؛

ب - نوع دسترسی که شخص بیرونی به تجهیزات پردازش اطلاعات خواهد داشت، به عنوان مثال :

۱ - دسترسی فیزیکی به عنوان مثال به دفاتر، اتاق‌های رایانه، کشوهای بایگانی[1]؛

۲ - دسترسی منطقی به عنوان مثال به پایگاه داده‌های سازمانی، سیستم‌های اطلاعاتی؛

۳ - شبکه ارتباطی بین سازمان و شبکه شخص بیرونی به عنوان مثال ارتباط دائم یا دسترسی از راه دور؛

۴ – آیا دسترسی از درون یا بیرون محیط کار اتفاق می افتد.

پ- ارزش و حساسیت اطلاعات و میزان حیاتی بودن آنها برای عملیات کسب‌وکار؛

1- Filing cabinets

ت - کنترل‌های لازم برای محافظت از اطلاعاتی که قرار نیست اشخاص بیرونی به آنها دسترسی داشته باشند؛

ث - کارکنان شخص بیرونی که با اطلاعات سازمانی سر و کار دارند.

ج - چگونه سازمان یا کارکنانی که مجاز به دسترسی، شناسایی می‌شوند، مجوزها چگونه تصدیق می‌شوند، چند وقت به چند وقت این نیازها مجدداً تایید می‌شوند.

چ - ابزارهای متفاوت و کنترل های به کار گرفته شده توسط شخص بیرونی در زمان ذخیره، پردازش، انتقال، اشتراک و تبادل اطلاعات؛

ح - پیامد دسترسی به شخص بیرونی که در زمان لازم در دسترس نباشد و شخص بیرونی که اطلاعات گمراه کننده یا غیردقیق را وارد یا دریافت می‌کند؛

خ - اقدامات و رویه های پرداختن به رخدادهای امنیت اطلاعات و آسیب های بالقوه و مفاد و شرایط استمرار دسترسی شخص بیرونی در صورت بروز یک رخداد امنیت اطلاعات؛

د - الزامات قانونی و مقرراتی و دیگر تعهدات قراردادی در رابطه با شخص بیرونی که توصیه می‌شود لحاظ شوند؛

ذ - این که منافع هر یک از ذینفعان دیگر ممکن است چگونه تحت تاثیر توافقات قرار می‌گیرد؛

توصیه می‌شود دسترسی اشخاص بیرونی به اطلاعات سازمان تا زمانی که کنترل های مناسب اجرا نشده‌اند و یا در صورت امکان تا زمانی که قراردادی که مفاد و شرایط ارتباط یا دسترسی را تعریف می‌کند، امضا نشده است، فراهم نشود. بطور کلی، توصیه می‌شود تمام الزامات امنیت اطلاعات که از کار با اشخاص بیرونی یا کنترل‌های داخلی ناشی می‌شوند از طریق قرارداد با شخص بیرونی منعکس شود (همچنین رجوع کنید به ۶-۲-۲ و۶-۲-۳). توصیه می‌شود از اینکه که شخص بیرونی از تعهداتش[1] آگاه است و مسوولیت ها و تعهدات[2] مربوط به دسترسی، پردازش، انتقال، یا مدیریت اطلاعات سازمان و تجهیزات پردازش اطلاعات را می پذیرد، اطمینان حاصل شود.

سایر اطلاعات

اطلاعات ممکن است توسط اشخاص بیرونی با مدیریت نامناسب امنیت به خطر بیفتد. توصیه می‌شود کنترل‌ها شناسایی شوند و برای ایجاد امکان دسترسی شخص بیرونی به تجهیزات پردازش اطلاعات به کار گرفته شوند. برای مثال، اگر نیاز خاصی به محرمانه بودن اطلاعات وجود دارد، می‌توان از قراردادهای عدم افشا استفاده کرد.

اگر بیشتر نیازها به منابع از خارج تامین شود، یا در جایی که چندین شخص خارجی نقش دارند، سازمان ها ممکن است با ریسک‌های مرتبط با فرایندها، مدیریت، و ارتباطات بین سازمانی روبرو شوند.

کنترل های ۶-۲-۲ و ۶-۲-۳ چیدمان‌های متفاوت توافقات شخص بیرونی را پوشش می دهند از جمله:

الف - ارایه دهندگان خدمات، نظیر ارایه دهندگان خدمات اینترنتی، ارایه کنندگان خدمات شبکه، خدمات تلفن، خدمات نگهداری و پشتیبانی

ب - خدمات امنیت مدیریت شده

پ - مشتریان

1- Obligations
2- Liabilty

ت – برون‌سپاری امکانات یا عملیات، به عنوان مثال سامانه های فن‌آوری اطلاعات، خدمات جمع آوری داده، عملیات مرکز تماس

ث - مشاوران مدیریت و بازرگانی، و ممیزان

ج - توسعه دهندگان و تامین کنندگان؛ به عنوان مثال تهیه‌کنندگان محصولات نرم‌افزاری و سیستم‌های فن‌آوری اطلاعات.

چ - نظافت، تدارکات[1] و سایر خدمات پشتیبانی برون سپاری شده.

ح - کارکنان موقت، جابجایی کارآموزان و دیگر انتصابات کوتاه مدت

این قراردادها می‌توانند به کاهش ریسک های مربوط به اشخاص بیرونی کمک کنند.

۶-۲-۲ *نشانی دهی امنیت هنگام سروکار داشتن با مشتریان*

کنترل

توصیه می‌شود، تمام الزامات امنیتی شناسایی شده، پیش از اعطای دسترسی به اطلاعات یا اموال سازمان به مشتری، مورد نشانی دهی شوند.

راهنمای پیاده سازی

توصیه می‌شود مفاد زیر برای پرداختن به امنیت قبل از ایجاد دسترسی به هر یک از دارایی‌های سازمان برای مشتریان در نظر گرفته شوند (بسته به نوع و وسعت دسترسی داده شده، ممکن همه آنها اعمال نشوند):

الف - محافظت از دارایی، شامل:

۱ - رویه هایی برای محافظت از دارایی‌های سازمان از جمله اطلاعات و نرم‌افزار و مدیریت آسیب پذیری های شناخته شده

۲- رویه هایی برای تعیین این که آیا خدشه ای به دارایی‌ها، به عنوان مثال از دست دادن یا تغییر داده‌ها رخ داده است یا نه.

۳- یکپارچگی

۴- محدودیت هایی درباره تکثیر و افشا اطلاعات

ب - توصیف محصول یا خدماتی که ارایه می‌شود

پ - دلایل، الزامات، و منافع متفاوت برای دسترسی مشتریان

ت - خط مشی کنترل دسترسی، پوشش دهنده:

۱- روش های دسترسی مجاز، و کنترل و استفاده از شناسه های منحصربه فردی نظیر شناسه کاربری و کلمه عبور

۲- یک فرایند مجوزدهی برای دسترسی کاربر و اختیارات ویژه

۳- بیانیه ای که تمام دسترسی هایی که صراحتاً مجوزدهی نشده اند، ممنوع هستند.

۴- فرایندی برای سلب حقوق دسترسی یا قطع ارتباط بین سیستم‌ها

1- Catering

ث - توافقاتی برای گزارش، اعلام، و بازرسی عدم دقت در اطلاعات(به عنوان مثال جزئیات شخصی)، رخدادهای امنیت اطلاعات و رخنه های امنیتی[1]

ج - شرح هر خدمتی که باید در دسترس قرار گیرد

چ - سطح مورد نظر[2] خدمت و سطوح غیر قابل قبول خدمات

ح - حق پایش، ابطال[3]، هر فعالیتی در رابطه با دارایی‌های سازمان

خ - ارتباطات بین هر سازمان و مشتری

د - مسوولیت هایی در رابطه با مورد قانونی و این که چگونه اطمینان حاصل می‌شود که الزامات قانونی برآورده می‌شوند؛ به عنوان مثال قوانین محافظت از داده‌ها، به خصوص احتساب سیستم‌های قانونی ملی متفاوت در صورتی که قرارداد دربرگیرنده همکاری با مشتریان در دیگر کشورها باشد. (همچنین رجوع کنید به ۱۵-۱)

ذ - حقوق مالکیت فکری و واگذاری حق تکثیر (رجوع کنید به ۱۵-۱-۲) و محافظت از هر کار مشترک (همچنین رجوع کنید به ۶-۱-۵)

سایر اطلاعات

الزامات امنیت اطلاعات در رابطه با دسترسی مشتریان به دارایی‌های سازمانی ممکن است بسته به امکانات پردازش اطلاعات و اطلاعاتی که مورد دسترسی قرار می‌گیرد، متفاوت باشد. این الزامات امنیتی را می‌توان با استفاده از قراردادهای مشتری که حاوی تمام ریسک های شناخته شده و الزامات امنیتی است، نشانی دهی کرد. (رجوع کنید به ۶-۲-۱)

قرارداد با اشخاص بیرونی، ممکن است همچنین دربرگیرنده اشخاص دیگر باشد. توصیه می‌شود، قراردادهایی که به شخص بیرونی امکان دسترسی می دهند شامل اجازه هایی برای تعیین دیگر اشخاص مجاز و شرایط برای دسترسی و مشارکت آنها باشند.

۶-۲-۳ *نشانی‌دهی امنیت در توافق‌های شخص‌سوم*

کنترل

توصیه می‌شود، توافق‌نامه های منعقده با اشخاص ثالثی که شامل اعطای دسترسی، پردازش، تبادل یا مدیریت اطلاعات یا امکانات پردازش اطلاعات سازمان، یا اضافه کردن محصولات یا خدمات به امکانات پردازش اطلاعات هستند، تمامی الزامات امنیتی مرتبط را پوشش دهند.

راهنمای پیاده سازی

توصیه می‌شود، قرارداد از اینکه که هیچ گونه سوء تفاهمی بین سازمان و شخص سوم وجود ندارد، اطمینان دهد.

توصیه می‌شود، سازمان ها خسارت خود را از شخص سوم به طور کامل اخذ نمایند.

توصیه می‌شود، مفاد زیر در قرارداد همکاری گنجانده شوند تا الزامات امنیتی شناخته شده را برآورده کنند. (رجوع کنید به ۶-۲-۱)

الف - خط مشی امنیت اطلاعات

1- Security Breaches
2- Target
3- Revoke

ب - کنترل هایی برای حصول اطمینان از محافظت از دارایی‌ها از جمله:

۱- رویه هایی برای محافظت از دارایی‌های سازمانی از جمله اطلاعات، نرم‌افزار، و سخت افزار

۲- هر گونه کنترل و سازوکار محافظت فیزیکی مورد نیاز

۳- کنترل‌هایی برای حصول اطمینان از محافظت در برابر نرم‌افزار مخرب (رجوع کنید به۱۰-۴-۱)

۴- رویه هایی برای تعیین این که آیا هیچگونه آسیب و خدشه ای به دارایی‌ها، از جمله از دست رفتن یا تغییر اطلاعات، نرم‌افزار، و سخت افزار وارد آمده است یا نه.

۵- کنترل هایی برای حصول اطمینان از بازگرداندن یا امحا اطلاعات و دارایی‌ها در پایان یا در یک زمان مورد توافق در طول زمان قرارداد.

۶- محرمانگی، یکپارچگی، در دسترس پذیری و هر گونه مالکیت مرتبط با دارایی‌ها (رجوع کنید به ۲-۱-۵)

۷- محدودیت هایی در رابطه با تکثیر و افشای اطلاعات و استفاده از قراردادهای محرمانه (رجوع کنید به ۶-۱-۵)

پ - آموزش کاربر و سرپرست درباره روش ها، رویه ها و امنیت

ت - حصول اطمینان از آگاهی کاربر از مسوولیت ها و مسائل امنیت اطلاعات

ث - تمهیداتی برای انتقال کارکنان در موارد مقتضی

ج - مسوولیت هایی در رابطه با نصب و نگهداری سخت افزار، و نرم‌افزار

چ - یک ساختار گزارش دهی واضح و قالب های گزارش دهی مورد توافق

ح - یک فرایند روشن و مشخص از مدیریت تغییر

خ - خط مشی کنترل دسترسی که موارد زیر را پوشش دهد:

۱- دلایل، الزامات، و منافع متفاوتی که دسترسی شخص سوم را ضروری می نماید.

۲- روش های دسترسی مجاز و کنترل و استفاده از شناسه های منحصربه فرد نظیر شناسه‌های کاربری و کلمات عبور.

۳- یک فرایند مجوزدهی برای دسترسی و اختیارات ویژه کاربران.

۴- یکی از الزامات برای حفظ فهرستی از افراد مجاز برای استفاده از خدماتی که در دسترس قرار می‌گیرد و این که حقوق و مزایای آنها در رابطه با این استفاده کدام است.

۵- بیانیه ای که تمام دسترسی هایی که صراحتاً مجوزدهی نشده اند، ممنوع هستند.

۶- فرایندی برای بازپس گیری حقوق دسترسی یا قطع ارتباط بین سیستم‌ها

د - هماهنگی هایی برای گزارش دهی، اطلاع، و بررسی رخدادهای امنیت اطلاعات و رخنه امنیتی و نیز تخلفات از الزامات بیان شده در قرارداد؛

ذ - توصیفی از محصول یا خدمتی که ارایه خواهد شد، و توصیفی از اطلاعاتی که در کنار این طبقه بندی امنیتی در دسترس قرار می‌گیرد(رجوع کنید به ۷-۲-۱)

ر - سطح هدف خدمات و سطوح غیرقابل قبول خدمات

ز - تعریف معیارهای عملکرد قابل تصدیق، پایش و گزارش دهی آنها

ژ - حق پایش، و ابطال هر فعالیت مربوط به دارایی‌های سازمان

س - حق ممیزی مسوولیت های تعریف شده در قرارداد، برای انجام این ممیزی ها توسط یک شخص سوم و لحاظ کردن حقوق آئین نامه ای ممیزان

ش – گنجاندن ماده ای برای فرایند حل مشکلات

ص - الزامات استمرار خدمات از جمله اقداماتی برای دسترسی و اطمینان پذیری در رابطه با اولویت های کسب وکار سازمان

ض - مسوولیت های مربوطه طرفین، نسبت به قرارداد

ط - مسوولیت هایی در رابطه با موضوعات قانونی و نحوه تضمین این که الزامات قانونی رعایت می‌شوند، مثلا قوانین محافظت از داده‌ها، به خصوص به حساب آوردن سیستم‌های قانونی ملی متفاوت در صورتی که قرارداد دربرگیرنده همکاری با سازمان های کشورهای دیگر است(همچنین رجوع کنید به ۱۵-۱)

ظ - حقوق مالکیت فکری و حق تکثیر(رجوع کنید به ۱۵-۱-۲) و محافظت از هر کار مشترک (همچنین رجوع کنید به ۶-۱-۵)

ع - مشارکت شخص سوم با پیمانکاران فرعی و کنترل های امنیتی که این پیمانکاران فرعی باید اجرا کنند.

غ - شرایطی برای مذاکره مجدد/خاتمه قراردادها

۱- توصیه می‌شود، در صورتی که هر یک از طرفین بخواهد رابطه را قبل از پایان قراردادها به پایان برساند برنامه احتیاطی، در نظر گرفته شود

۲- مذاکره مجدد درباره قراردادها در صورتی که الزامات امنیتی سازمان تغییر کند

۳- مستندسازی از فهرست دارایی‌ها، پروانه ها، قراردادهای حال حاضر یا حقوق مربوط به آنها

سایر اطلاعات

قراردادها ممکن است برای سازمان های متفاوت و در میان انواع مختلف اشخاص ثالث، متفاوت باشند. بنابراین، توصیه می‌شود که مراقب بود تمام ریسک‌ها شناخته شده و الزامات امنیتی در قراردادها گنجانده شوند (همچنین رجوع کنید به ۶-۲-۱). در صورت لزوم، کنترل ها و رویه های مورد نیاز را می‌توان در یک برنامه مدیریت امنیت گسترش داد.

توصیه می‌شود، اگر مدیریت امنیت اطلاعات برونسپاری شود، قرارداد به این بپردازد که شخص سوم چگونه تضمین خواهد کرد که امنیت مناسب همان طور که در برآورد ریسک تعریف شده است حفظ خواهد شد و امنیت چگونه برای شناسایی و پرداختن به ریسک‌ها رعایت خواهد شد.

بعضی از تفاوت های بین تامین منابع از بیرون و دیگر شکل های تامین خدمات توسط شخص سوم، شامل سوال درباره مسوولیت، طرح‌ریزی، دوره گذر و اختلال بالقوه در عملیات در طول آن دوره، برنامه ریزی سازگاری، هماهنگی ها و گزارش ها و جمع آوری و مدیریت اطلاعات درباره رخدادهای امنیتی می باشند. بنابراین مهم است که سازمان گذر به یک توافق برون سپاری شده را طرح‌ریزی ریزی و مدیریت کند و فرایند مناسبی را برای مدیریت تغییرات و مذاکره مجدد/خاتمه قراردادها داشته باشد.

رویه هایی برای استمرار پردازش در صورتی که شخص سوم از تامین خدماتش ناتوان باشد باید در قرارداد در نظر گرفته شود تا از هر گونه تاخیر در هماهنگ کردن خدمات جایگزینی اجتناب شود.

قرارداد با اشخاص ثالث ممکن است همچنین دربرگیرنده اشخاص ثالث دیگر نیز باشد. توصیه می‌شود، قراردادهایی که به اشخاص ثالث امکان دسترسی می دهد، شامل اجازه برای تعیین دیگر اشخاص مجاز و شرایطی برای دسترسی و مشارکت آنها باشد.
عموما، قراردادها توسط سازمان تدوین می‌شوند. ممکن است در بعضی مواقعی قراردادی طراحی شود و توسط یک شخص سوم به سازمان تحمیل شود. سازمان باید تضمین کند که امنیت تحت تاثیر الزامات قراردادهای تدوین شده شخص سوم، قرار نمی‌گیرد.

۷ مدیریت دارایی

۷-۱ مسوولیت داراییها

هدف: دستیابی به حفاظت مناسب از دارایی های سازمانی و ادامه دادن این کار.
توصیه می‌شود که برای همهٔ دارایی ها مالک مشخص شود و این دارایی ها برای مالک شمارش شوند.
توصیه می‌شود که مالکین برای همهٔ دارایی ها مشخص شده باشند و توصیه می‌شود که مسوولیت نگهداری کنترل‌های مناسب، واگذار شود. اجرای کنترل های خاص ممکن است توسط مالک (به یک شخص یا سازمان دیگر) محول شود، اما مالک، مسوول محافظت مناسب از دارایی ها باقی می ماند.

۷-۱-۱ *لیست موجودی اموال*

کنترل
توصیه می‌شود که تمام دارایی‌ها به وضوح شناسایی شوند و لیست موجودیی از تمام دارایی‌های مهم، تنظیم و نگهداری شود.
راهنمای پیاده سازی
توصیه می‌شود که سازمان تمام دارایی‌ها را شناسایی کرده و اهمیت این دارایی‌ها را مستند کند. توصیه می‌شود که این فهرست دارایی‌ها تمام اطلاعات لازم برای بازیابی پس از حادثه، از جمله نوع دارایی، قالب، محل، اطلاعات پشتیبان، اطلاعات گواهی، و یک ارزش تجاری را شامل باشد. توصیه می‌شود که لیست موجودی اموال، نسخه دوم از دیگر فهرست های غیرضروری نباشد، اما توصیه می‌شود که از به جا بودن محتوای آن، اطمینان حاصل شود.
به علاوه، توصیه می‌شود که مالکیت (رجوع کنید به ۷-۱-۲) و طبقه بندی اطلاعات (رجوع کنید به ۷-۲)، مورد توافق قرار گیرد و برای هر یک از دارایی‌ها، مستند شود. توصیه می‌شود که بر اساس اهمیت دارایی، ارزش تجاری آن و طبقه بندی امنیتی آن، سطوح محافظت متناسب با اهمیت دارایی‌ها، شناسایی شوند (اطلاعات بیشتر درباره نحوه ارزش گذاری دارایی‌ها با هدف بیان اهمیت آنها، در ISO/IEC 13335-3 قابل مشاهده است).
سایر اطلاعات
دارایی‌ها انواع بسیاری دارند، از جمله موارد زیر:

الف - اطلاعات: بانک‌های اطلاعاتی و فایل های داده، قراردادها و توافق‌نامه‌ها، مستندات سیستم، اطلاعات تحقیق، راهنماهای کاربر، محتوای آموزشی، رویه‌های عملیاتی یا پشتیبانی، طرح‌های استمرار کسب وکار، تفاهم نامه‌های پشتیبانی، گزارش‌های ممیزی، و اطلاعات کسب شده؛

ب – دارایی‌های نرم‌افزاری: نرم‌افزارهای کاربردی، نرم‌افزار سامانه، ابزارهای توسعه، و نرم‌افزارهای کمکی؛

پ – دارایی‌های فیزیکی: تجهیزات رایانه‌ای، تجهیزات ارتباطی، رسانه‌های قابل جابجایی، و سایر تجهیزات؛

ت - خدمات: خدمات محاسبه ای و ارتباطی، تجهیزات عمومی؛ مانند گرمایش، نور، برق و تهویه هوا

ث - افراد و صلاحیت، مهارت ها و تجربه های آنها؛

ج - موارد ناملموس مانند اعتبار و خوشنامی سازمان

فهرست دارایی‌ها کمک می‌کند تا این اطمینان ایجاد شود که از دارایی‌ها به نحو موثر محافظت می‌شود، و همچنین ممکن است برای دیگر اهداف تجاری نظیر سلامت و امنیت، بیمه یا دلایل مالی (مدیریت دارایی) لازم باشد. فرایند تدوین یک فهرست از دارایی‌ها، یک پیش نیاز مهم از مدیریت ریسک است (رجوع به بخش ۴).

۷-۱-۲ *مالکیت دارایی‌ها*

کنترل

توصیه می‌شود که تمام اطلاعات و دارایی‌های مرتبط با امکانات پردازش اطلاعات، در تملک[1] بخش معینی از سازمان باشند.

راهنمای پیاده سازی

توصیه می‌شود که مالک دارایی مسوول موارد زیر باشد:

الف - تضمین این‌که اطلاعات و دارایی‌های مربوط به تجهیزات پردازش اطلاعات به‌طور مناسب طبقه بندی شده‌اند.

ب - تعریف و بازنگری دوره‌ای محدودیت های دسترسی و طبقه‌بندی‌ها، به حساب آوردن خط‌مشی‌های کنترل دسترسی.

مالکیت ممکن است به موارد زیر اختصاص داده شود:

الف - یک فرایند تجاری؛

ب - مجموعه تعریف شده ای از فعالیت ها؛

پ - یک نرم‌افزار کاربردی؛ یا

ت – یک مجموعه تعریف شده از داده‌ها.

سایر اطلاعات

وظایف متداول را می‌توان واگذار کرد، مثلا به یک نگهبان که بصورت روزانه مراقب دارایی‌ها است، ولی مسوولیت به عهده مالک دارایی است.

۱- واژه "مالک" بعنوان موجودیت یا شخصی شناخته می‌شود که مسوولیت‌های تایید شده مدیریت را برای کنترل محصول، بهبود، حفظ و تگهداری، استفاده و امنیت داراییی ها، را دارد. واژه "مالک" به معنی شخصی که عملا حقوق مالکیت بر دارایی را دارد، نیست.

در سامانه های اطلاعاتی پیچیده، معین کردن گروه هایی از دارایی‌ها که با یکدیگر عمل می‌کنند تا یک وظیفه خاص تحت عنوان "خدمات" را ارایه کنند، ممکن است مفید باشد. در این نمونه، مسوولیت تحویل خدمت که شامل عملکرد دارایی‌های فراهم کننده آن خدمت نیز می باشد، بر عهده مالک خدمت است.

۷-۱-۳ *استفاده قابل قبول از دارایی‌ها*

کنترل

توصیه می‌شود که قوانینی برای استفادهٔ قابل قبول از اطلاعات و دارایی‌های مرتبط با امکانات پردازش اطلاعات، مشخص و مستندسازی و پیاده سازی شوند.

راهنمای پیاده سازی

توصیه می‌شود که تمام کارمندان، پیمانکاران، و کاربران شخص سوم از قوانین استفاده قابل قبول از اطلاعات و دارایی‌های مرتبط با تجهیزات پردازش اطلاعات، پیروی کنند. این قوانین شامل موارد زیر هستند:

الف - قوانین پست الکترونیک و استفاده از اینترنت (رجوع کنید به ۱۰-۸)

ب –رهنمودهای استفاده از دستگاه های متحرک/سیار به خصوص برای استفاده خارج از محوطه‌های سازمان (رجوع کنید به ۱۱-۷-۱)

توصیه می‌شود که قوانین خاص یا راهنمایی‌هایی توسط مدیریت، کارفرمایان و پیمانکاران مربوطه فراهم شوند.

توصیه می‌شود که کاربران اشخاص ثالثی که از دارایی‌های سازمان استفاده می‌کنند یا به آن دسترسی دارند، از محدودیت های موجود برای استفاده آنها از اطلاعات و دارایی‌های سازمان در رابطه با تجهیزات پردازش اطلاعات و منابع، آگاه باشند. توصیه می‌شود که این اشخاص برای استفاده خود از منابع پردازش اطلاعات و هر گونه کاربری انجام شده با مسوولیت آنها، مسوول شناخته شوند.

۷-۲ طبقه بندی اطلاعات

هدف: حصول اطمینان نسبت به اینکه، اطلاعات به سطح حفاظتی مناسبی رسیده اند.

توصیه می‌شود که اطلاعات برای نشان دادن نیاز، اولویت ها، و میزان محافظت مورد انتظار در زمان اداره اطلاعات، طبقه بندی شوند.

اطلاعات دارای درجه های حساسیت و بحرانی بودن متفاوتی هستند. بعضی موارد ممکن است نیازمند یک سطح محافظت اضافه یا اداره بصورت ویژه باشند. توصیه می‌شود که از یک طرح طبقه بندی اطلاعات برای تعریف مجموعه مناسبی از سطوح محافظت و تبادل اطلاعات مورد نیاز برای رسیدگی به موارد خاص، استفاده شود.

۷-۲-۱ *رهنمودهای طبقه بندی*

کنترل

توصیه می‌شود که اطلاعات باید با توجه به ارزش، الزامات قانونی، حساسیت و بحرانی بودن آن برای سازمان، طبقه بندی شوند.

راهنمای پیاده سازی

توصیه می‌شود که طبقه بندی ها و کنترل های حفاظتی مربوطه به اطلاعات، نیازهای تجاری برای اشتراک یا محدود کردن اطلاعات و پیامدهای تجاری مربوط به این نیازها را به حساب آورند.
توصیه می‌شود که رهنمود طبقه بندی، مفادی برای طبقه بندی مقدماتی و طبقه بندی مجدد با گذشت زمان؛ مطابق با خط مشی کنترل دسترسی از پیش تعیین شده (رجوع کنید به ۱۱-۱-۱) را شامل باشند.
توصیه می‌شود که تعریف طبقه بندی یک دارایی، مرور دوره ای آن و تضمین به روز بودن و در سطح مناسب نگهداری شدن آن، به عهده مالک دارایی باشد (رجوع کنید به ۷-۱-۲). توصیه می‌شود که طبقه بندی، تاثیر تجمع ذکر شده در ۱۰-۷-۲ را لحاظ کند.
توصیه می‌شود که تعداد گروه های طبقه بندی و منافعی که از به کار بردن آنها به دست می‌آید، مورد توجه قرار گیرند. استفاده از طرح های بیش از حد پیچیده، ممکن است طاقت فرسا و غیر اقتصادی باشد و یا اثبات شود که این طرح ها غیرعملی هستند. توصیه می‌شود که در تفسیر برچسب های طبقه بندی روی اسناد دریافتی از سایر سازمان ها دقت شود، زیرا ممکن است تعریف های متفاوتی برای برچسب های نامگذاری شده مشابه، داشته باشند.

سایر اطلاعات

سطح محافظت را می‌توان با تحلیل محرمانگی، یکپارچگی، و دردسترس پذیری و هر گونه الزامات دیگر برای اطلاعات مورد توجه، ارزیابی کرد.
اطلاعات اغلب پس از یک دوره زمانی، دیگر حساس و حیاتی قلمداد نمی‌شوند، مثلا هنگامی که اطلاعات در معرض دید عموم قرار داده شده باشند. توصیه می‌شود که این جنبه ها به حساب آورده شوند، چون طبقه بندی بیش از حد، ممکن است منجر به پیاده سازی کنترل های غیرضروری شود که به هزینه های اضافی منجر می‌شوند.
در هنگام تعیین کردن سطوح طبقه بندی، رسیدگی کردن به اسنادی که الزامات امنیتی مشابهی دارند همراه با هم، ممکن است به تسهیل کار طبقه بندی کمک کند.
به طور کلی، طبقه بندی اعطا شده به اطلاعات راهی اختصاری برای تعیین نحوه استفاده و محافظت از این اطلاعات است.

۷-۲-۲ برچسب‌گذاری و اداره‌کردن اطلاعات

کنترل

توصیه می‌شود که یک مجموعهٔ مناسب از رویه ها برای علامت‌گذاری و اداره‌کردن اطلاعات مطابق با طرح طبقه بندی اتخاذ شده توسط سازمان، توسعه یافته و پیاده سازی شود.

راهنمای پیاده سازی

رویه های برچسب زنی اطلاعات باید دارایی‌های اطلاعاتی را در قالب های فیزیکی و الکترونیکی پوشش دهند.
توصیه می‌شود که خروجی سیستم‌هایی که حاوی اطلاعاتی است که حساس یا حیاتی قلمداد می‌شوند، حامل یک برچسب مناسب طبقه بندی باشند (در خروجی). توصیه می‌شود که برچسب زدن، طبقه بندی را مطابق با قوانین تثبیت شده در ۷-۲-۱، انعکاس دهد. موارد قابل ملاحظه، شامل گزارش های چاپ شده، نمایش دهنده

های روی صفحه، رسانه‌های ضبط شده (مانند نوارها، دیسک ها، و سی دی ها)، پیام های الکترونیکی، و انتقال های فایل هستند.

توصیه می‌شود که برای هر سطح از طبقه بندی، رویه هایی از جمله پردازش امن، ذخیره، انتقال، برداشتن طبقه بندی، و تخریب، تعریف شود. توصیه می‌شود که رویه‌هایی برای کنترل دسترسی واقعه نگاری هر رویداد امنیتی مربوطه، نیز برای هر سطح از طبقه بندی در نظر گرفته شوند.

توصیه می‌شود که توافق نامه های منعقد شده با سازمان‌های دیگر که شامل اشتراک اطلاعات می‌باشند، رویه هایی برای شناسایی طبقه‌بندی آن اطلاعات و تفسیر برچسب‌های طبقه‌بندی دریافت شده از سازمان های دیگر را شامل باشند.

سایر اطلاعات

برچسب زدن و اداره امن اطلاعات طبقه بندی شده، یک الزام کلیدی برای هماهنگی های اشتراک اطلاعات است. برچسب های فیزیکی، نوع متداولی از برچسب زنی هستند. به هر حال، بعضی از دارایی‌های اطلاعاتی نظیر مستندات در شکل الکترونیکی را نمی‌توان به طور فیزیکی برچسب زنی کرد و باید از روش های برچسب زنی الکترونیکی استفاده شود. مثلا، برچسب زنی هشدار، ممکن است روی پرده یا صفحه نمایش ظاهر شود.

در جایی که برچسب زنی امکان پذیر نباشد می‌توان از دیگر ابزارهای نمایش طبقه بندی اطلاعات استفاده کرد، مثلا از طریق رویه ها یا فرا- داده[1].

1- Meta-Data

۸ امنیت منابع انسانی

۸-۱ پیش از اشتغال[۱]

هدف: اطمینان یافتن از این که کارکنان، پیمانکاران، و کاربران شخص ثالث، مسوولیت های خود را می دانند و برای نقش هایی که برای آنها در نظر گرفته شده اند و نیز برای کاهش خطر سرقت، تقلب و سوء استفاده از امکانات، مناسب هستند.

توصیه می‌شود که مسوولیت های امنیتی، قبل از استخدام در تشریح مشاغل به اندازه کافی و در اصطلاحات و شرایط استخدام، عنوان شوند.

توصیه می‌شود که تمام نامزدهای استخدام، پیمانکاران و کاربران شخص ثالث، به اندازه کافی - به خصوص در مشاغل حساس - کنترل شوند.

توصیه می‌شود که کارکنان، پیمانکاران، و کاربران شخص ثالث امکانات پردازش اطلاعات، توافق نامه ای درباره نقش‌ها و مسوولیت های امنیتی خود امضا کنند.

۸-۱-۱ *نقش ها و مسوولیت‌ها*

کنترل

توصیه می‌شود که نقش ها و مسوولیت‌های امنیتی کارکنان، پیمانکاران و کاربران شخص سوم، با توجه به خط‌مشی امنیت اطلاعات سازمان، تعریف و مستندسازی شوند.

راهنمای پیاده سازی

توصیه می‌شود که نقش ها و مسوولیت‌های امنیتی شامل الزاماتی باشند تا:

الف - مطابق با خط‌مشی های امنیت اطلاعات سازمان، پیاده سازی شده و اقدام کنند (رجوع کنید به ۱.۵)؛

ب - از دارایی‌ها دربرابر دسترسی غیرمجاز، افشا، تغییر، تخریب یا دخالت محافظت کنند؛

پ - فرایندها یا فعالیت های خاص امنیتی را اجرا کنند؛

ت - اطمینان دهند که مسوولیت اعمال انجام شده، به فردی که آنها را انجام داده است واگذار شده است؛

ث - رویدادهای امنیتی، یا رویدادهای بالقوه یا دیگر ریسک های امنیتی سازمان را گزارش کنند؛

توصیه می‌شود که نقش ها و مسوولیت‌های امنیتی در طول فرایند قبل از استخدام، تعریف شده و به طور واضح به نامزدهای مشاغل تفهیم شوند.

سایر اطلاعات

شرح مشاغل را می‌توان برای مستندسازی نقش ها و مسوولیت‌های امنیتی مورد استفاده قرار داد. توصیه می‌شود که نقش ها و مسوولیت‌های امنیتی برای افرادی که از طریق فرایند استخدام سازمان مشغول به کار نشده اند، مثلا از طریق یک سازمان شخص سوم به کار گرفته شده اند، نیز به طور واضح تعریف و تفویض شود.

۱- توضیح: کلمه "اشتغال" در اینجا به این صورت معنی شده است که همه وضعیت‌های مختلف ذیل را پوشش می دهد:
اشتغال افراد(موقت یا طولانی مدت)، انتصاب سمت‌های شغلی، تغییر سمت‌های شغلی، واگذار کردن قرارداد، و خاتمه دادن به هر یک از این توافق‌نامه‌ها

۸-۱-۲ گزینش

کنترل

توصیه می‌شود که پیشینه تمامی داوطلبن استخدام، پیمانکاران، و کاربران شخص سوم، با توجه به قوانین، مقررات و اصول اخلاقی مربوطه، و متناسب با الزامات کسب وکار، طبقه بندی اطلاعات مورد دسترسی و ریسک‌های مشاهده شده، تصدیق شود.

راهنمای پیاده سازی

توصیه می‌شود که بررسی های تصدیقی[1] درباره همه موارد مرتبط با حریم خصوصی انجام شود، محافظت از داده‌های شخصی و/یا قانون گذاری مبتنی بر استخدام را به حساب بیاورند و توصیه می‌شود که در جایی که اجازه داده می‌شود، شامل موارد زیر باشند:

الف - در دسترس بودن منابع کاراکتری رضایتبخش، به عنوان مثال یک تجاری و یک شخصی؛

ب - یک بررسی (برای کامل بودن و دقت) رزومهٔ فرد متقاضی؛

پ - تایید صلاحیت های حرفه ای و دانشگاهی ادعا شده؛

ت - بررسی مستقل هویت (گذرنامه یا سند مشابه)؛

ث - بررسی های جزئی تر نظیر بررسی‌های اعتبار یا بررسی‌های سوابق کیفری.

هنگامی که یک شغل، خواه در زمان انتصاب اولیه یا در زمان ترفیع، مستلزم دسترسی شخص به تجهیزات پردازش اطلاعات است و به خصوص اگر این تجهیزات، اطلاعات حساس را اداره می‌کنند، مانند اطلاعات مالی یا اطلاعات خیلی محرمانه، توصیه می‌شود که سازمان نیز بررسی‌هایی با جزئیات بیشتر را در نظر بگیرد.

توصیه می‌شود که رویه‌ها برای بررسی‌های تصدیق و صحه‌گذاری، معیارها و محدودیت‌هایی را تعریف کنند، مثلا این که چه کسی برای زیر نظر گرفتن افراد، واجد شرایط است، و چگونه، چه موقع و چرا بررسی‌های تصدیقی انجام می‌شوند.

توصیه می‌شود که یک فرایند کنترل برای پیمانکاران، و کاربران شخص سوم انجام شود. هنگامی که پیمانکاران از طریق یک آژانس تامین می‌شوند، توصیه می‌شود که قرارداد با آژانس به طور شفاف مسوولیت‌های آژانس را برای گزینش و رویه هایی آگاه سازی که در صورت کامل نشدن گزینش یا در صورتی‌که نتایج سبب شک و نگرانی شوند، پیمانکاران باید از آنها پیروی کنند را مشخص کند. به طریق مشابه توصیه می‌شود که قرارداد با شخص سوم (همچنین رجوع کنید به ۶-۲-۳)، به طور شفاف تمام مسوولیت‌ها و رویه‌های آگاه‌سازی را برای گزینش مشخص کند.

توصیه می‌شود که اطلاعات درباره تمام نامزدهایی که برای پست ها در سازمان در نظر گرفته می‌شوند، مطابق با هر یک از قوانین وضع شده مناسب موجود در حوزه قضایی مربوطه، جمع آوری شده و مورد استفاده قرار گیرند. توصیه می‌شود که بر حسب قوانین وضع شده و کاربردی، نامزدها از قبل درباره فعالیت های گزینشی آگاه شوند.

۸-۱-۳ ضوابط و شرایط استخدام

کنترل

توصیه می‌شود که کارکنان، پیمانکاران و کاربران شخص سوم، به عنوان بخشی از تعهد قراردادی خود، ضوابط و شرایط قرارداد استخدامی خود را قبول کرده و امضا کنند؛ توصیه می‌شود که این تعهد قراردادی، مسوولیت‌های کارکنان، پیمانکاران و کاربران شخص سوم، و سازمان در قبال امنیت اطلاعات را تعیین کند.

1- Verification checks

راهنمای پیاده سازی

توصیه می‌شود که مفاد و شرایط استخدام، علاوه بر منعکس کردن خط مشی امنیتی سازمان، موارد زیر را نیز تعیین کرده و توضیح دهند:

الف - این که تمام کارکنان، پیمانکاران و کاربران شخص سوم که به اطلاعات حساس دسترسی دارند، توصیه می‌شود که یک توافق نامه محرمانگی یا عدم افشا را قبل از دسترسی به امکانات پردازش اطلاعات، امضا کنند؛

ب - مسوولیت ها و حقوق قانونی کارکنان، پیمانکاران، و هر یک از کاربران دیگر، برای مثال در موضوع قوانین مالکیت معنوی یا قوانین وضع شده حفاظت از داده (همچنین رجوع کنید به ۱۵-۱-۱ و ۱۵-۱-۲)؛

پ - مسوولیت ها برای طبقه بندی اطلاعات و مدیریت دارایی‌های سازمانی مربوط به سیستم‌های اطلاعاتی و خدمات انجام شده توسط کارمند، پیمانکار، یا کاربر شخص سوم (همچنین رجوع کنید به ۷-۲-۱ و ۱۰-۷-۳)؛

ت - مسوولیت های کارمند، پیمانکار یا کاربر شخص سوم برای کار با اطلاعات دریافتی از سایر شرکت ها یا اشخاص بیرونی؛

ث - مسوولیت های سازمان برای کار با اطلاعات شخصی، شامل اطلاعات شخصی که در نتیجه یا در زمان همکاری با سازمان ایجاد شده است (همچنین رجوع کنید به ۱۵-۱-۴)؛

ج - مسوولیت هایی که به خارج از محوطه های سازمان و خارج از ساعات کار معمولی، توسعه داده می‌شوند، مثلا در مورد کار در خانه (همچنین رجوع کنید به ۹-۲-۵ و ۱۱-۷-۱)؛

چ - اقداماتی که در هنگام نادیده گرفتن الزامات امنیتی سازمان توسط کارکنان، پیمانکاران یا کاربران شخص سوم، انجام خواهند شد (همچنین رجوع کنید به ۸-۲-۳)؛

توصیه می‌شود که سازمان از موافق بودن کارکنان، پیمانکاران و کاربران شخص سوم با مفاد و شرایط مربوط به امنیت اطلاعات، متناسب با ماهیت و میزان دسترسی که به دارایی‌های سازمان در رابطه با سیستم‌های اطلاعاتی و خدمات خواهند داشت، اطمینان یابد.

توصیه می‌شود که در جای مناسب، مسوولیت های موجود در مفاد و شرایط استخدامی برای یک دوره تعیین شده پس از پایان استخدام، ادامه داده شوند. (همچنین رجوع کنید به ۸-۳)

سایر اطلاعات

می‌توان از یک کد رفتار برای پوشش دادن مسوولیت های کارمند، پیمانکار، یا شخص سوم در رابطه با محرمانگی، حفاظت از داده، اخلاقیات، استفاده مناسب از تجهیزات و امکانات سازمان، و نیز عملکردهای مربوط به خوش‌نامی سازمان - که مورد انتظار هستند - استفاده کرد. پیمانکار یا کاربران شخص سوم ممکن است با سازمانی بیرونی در ارتباط باشند، ممکن است لازم باشد که این سازمانی بیرونی نیز به نوبه خود در توافقات مربوط به قرارداد، به نمایندگی از طرف فرد دارای قرارداد، وارد شود.

۸-۲ حین خدمت

هدف: حصول اطمینان از اینکه کارکنان، پیمانکاران و کاربران شخص ثالث، از تهدیدها و نگرانی های امنیت اطلاعات و مسوولیت‌ها و تعهدات خود آگاه بوده و برای پشتیبانی از خط‌مشی امنیتی سازمان در انجام کارهای روزمره خود و کاهش ریسک ناشی از خطای انسانی، آماده شده اند.
توصیه می‌شود که مسوولیت‌های مدیریت تعریف شوند تا اطمینان حاصل شود که امنیت در سراسر مدت استخدام یک فرد در سازمان، اجرا می‌شود.
توصیه می‌شود که یک سطح کافی از آگاهی، آموزش، و پرورش در رویه های امنیتی و استفاده صحیح از امکانات پردازش اطلاعات، برای تمام کارکنان، پیمانکاران و کاربران شخص ثالث فراهم شود تا احتمال ریسک های امنیتی به حداقل برسد. توصیه می‌شود که یک فرایند انضباطی رسمی برای رسیدگی به رخنه های امنیتی، برقرار شود.

۸-۲-۱ *مسوولیت‌های مدیریت*

کنترل

توصیه می‌شود که مدیریت، اجرای امنیت مطابق با خط‌مشی ها و رویه های برقرار شدهٔ سازمان را برای کارکنان، پیمانکاران و کاربران شخص سوم الزامی‌کند.

راهنمای پیاده سازی

توصیه می‌شود که مسوولیت‌های مدیریت شامل حصول اطمینان از موارد زیر درباره کارکنان، پیمانکاران و کاربران شخص سوم، باشد:

الف - درباره نقش ها و مسوولیت‌های امنیت اطلاعات خود پیش از اعطای مجوز دسترسی به اطلاعات حساس یا سیستم‌های اطلاعاتی به طور مناسب توجیه شده اند؛

ب - رهنمودهایی برای تعیین انتظارات امنیتی از نقش خود در سازمان دریافت کرده اند؛

پ - برای رعایت سیاست های امنیتی سازمان، انگیزه مند شوند؛

ت - به سطحی از آگاهی درباره امنیت مرتبط با نقش ها و مسوولیت‌های خود در سازمان برسند (همچنین رجوع کنید به ۸-۲-۲)؛

ث - از مفاد و شرایط استخدام که شامل خط‌مشی امنیت اطلاعات سازمان و روش های مناسب کار می باشند، پیروی کنند؛

ج - همچنان به کسب مهارت ها و ویژگی های مناسب ادامه دهند.

سایر اطلاعات

اگر کارکنان، پیمانکاران، و کاربران شخص سوم از مسوولیت‌های امنیتی خود آگاه نشوند، می‌توانند باعث وارد شدن آسیب جدی به یک سازمان آسیب شوند. پرسنل دارای انگیزه، بیشتر قابل اطمینان هستند و رخدادهای امنیتی کمتری را سبب می‌شوند.

مدیریت ضعیف، ممکن است باعث شود تا پرسنل احساس کنند که سازمان کمتر از میزان لازم برای آنها ارزش قائل می‌شود و این مساله منجر به پیامد امنیتی منفی بر سازمان می‌شود. مثلا، مدیریت ضعیف ممکن است منجر به نادیده گرفته شدن امنیت یا سوء استفاده بالقوه از دارایی‌های سازمان شود.

۸-۲-۲ آگاهی رسانی، تحصیل و آموزش امنیت اطلاعات

کنترل

تمامی کارکنان سازمان و، در هنگام لزوم، پیمانکاران و کاربران شخص سوم، بایستی آموزش آگاه سازی مناسب و به روز رسانی قاعده مند خط‌مشی ها و رویه های سازمانی را دریافت کنند، آنگونه که به وظایف شغلی آنها مربوط است.

راهنمای پیاده سازی

توصیه می‌شود که آموزش آگاه سازی با یک فرایند مقدماتی رسمی آغاز شود که برای معرفی خط‌مشی های امنیتی سازمان و انتظارات، قبل از اعطای اجازه دسترسی به اطلاعات یا خدمات طراحی شده است.

توصیه می‌شود که آموزش مستمر دربرگیرنده الزامات امنیتی، مسوولیت‌های حقوقی و کنترل های تجاری و نیز آموزش استفاده صحیح از تجهیزات پردازش اطلاعات مانند رویه برقراری ارتباط با سیستم، استفاده از بسته های نرم‌افزاری و اطلاعات بر اساس فرایند انضباتی باشد (رجوع کنید به ۸-۲-۳).

اطلاعات دیگر

توصیه می‌شود که فعالیت های آگاه‌سازی، آموزش و تعلیم امنیت، با نقش، مسوولیت‌ها و مهارت های شخص متناسب و مرتبط باشد و توصیه می‌شود که شامل اطلاعاتی درباره تهدیدهای شناخته شده، فردی که برای دریافت مشاوره امنیتی بیشتر باید با او تماس گرفته شود و کانال های مناسب برای گزارش رخدادهای امنیت اطلاعات باشد (همچنین رجوع کنید به ۱۳-۱).

هدف از آموزش ارتقای آگاهی، این است که به افراد امکان داده شود تا مشکلات و رخدادهای امنیت اطلاعات را بشناسند و مطابق با نیازهای نقش کاری خود واکنش نشان دهند.

۸-۲-۳ فرایند انضباطی

کنترل

توصیه می‌شود که یک فرایند انضباطی رسمی برای کارکنانی که مرتکب یک نقض پیمان رخنه امنیتی می‌شوند، وجود داشته باشد.

راهنمای پیاده سازی

فرایند انضباطی نبایستی بدون تصدیق قبلی اینکه نقض پیمان امنیتی صورت گرفته است، آغاز شود. (برای مجموعه شواهد، همچنین رجوع کنید به ۱۳-۲-۳).

فرایند انضباطی رسمی بایستی اطمینان دهد که با کارکنانی که مظنون به ارتکاب نقض پیمان امنیتی هستند، برخوردی صحیح و عادلانه انجام می‌شود. فرایند انضباطی رسمی بایستی برای یک پاسخ آگاهانه که عواملی نظیر طبیعت و شدت نقض پیمان و پیامد آن بر کسب وکار، آیا این تخلف برای اولین بار اتفاق می افتد یا تکراری است، آیا نقض کننده به اندازه کافی آموزش دیده است یا خیر، قانون گذاری مرتبط، قراردادهای تجاری و دیگر عوامل مورد نیاز، آماده شوند. در موارد جدی سوء رفتار، این فرایند بایستی امکان حذف مستقیم وظایف، حقوق دسترسی و مجوزها، و اقدام سریع نگهبان برای همراهی فرد به خارج از محل را امکان پذیر سازد.

اطلاعات دیگر

فرایند انضباتی همچنین بایستی به عنوان عاملی برای بازداشتن کارکنان، پیمانکاران و کاربران شخص سوم از نقض خط‌مشی ها و رویه های امنیت سازمانی و هر نقض پیمان امنیتی دیگر، مورد استفاده قرار گیرد.

۸-۳ خاتمه استخدام یا تغییر شغل

هدف: حصول اطمینان از اینکه کارکنان، پیمانکاران و کاربران شخص ثالث، به روشی ضابطه مند سازمان را ترک کرده یا تغییر شغل می دهند.
توصیه می‌شود که مسوولیت‌هایی برای حصول اطمینان از اینکه خروج کارمند، پیمانکار یا کاربر شخص ثالث از سازمان، مدیریت می‌شود و اینکه بازگرداندن تمام تجهیزات و حذف تمام حقوق دسترسی، کامل می‌شود، در نظر گرفته شوند.
تغییر مسوولیت‌ها و استخدام ها در یک سازمان بایستی به عنوان خاتمه مسوولیت مربوطه یا استخدام، مطابق این بخش مدیریت شوند و هر گونه استخدام بایستی آنگونه که در بند ۱،۸ شرح داده شده است، مدیریت شود.

۸-۳-۱ *مسوولیت‌های خاتمه خدمت*

کنترل
مسوولیت های مربوط به اجرای خاتمه خدمت یا تغییر شغل، بایستی به وضوح تعریف شده و تخصیص داده شوند.

راهنمای پیاده سازی
ارتباطات مسوولیت‌های خاتمه توصیه می‌شود الزامات امنیتی جاری و مسوولیت‌های حقوقی و، در زمان مناسب، مسوولیت‌های موجود در هر توافق‌نامه محرمانگی (رجوع کنید به ۶-۱-۵) و مفاد و شرایط استخدام (رجوع کنید به ۸-۱-۳) را برای یک دوره تعیین شده پس از خاتمه استخدام کارکنان، پیمانکاران و کاربران شخص سوم ادامه می‌یابد، شامل باشد.
مسوولیت‌ها و وظایفی که پس از خاتمه خدمت همچنان معتبر هستند، بایستی در قراردادهای کارمند، پیمانکار یا کاربر شخص سوم گنجانده شوند.
تغییرات مسوولیت، یا استخدام بایستی به عنوان خاتمه مسوولیت یا استخدام مربوطه مدیریت شوند، و مسوولیت یا استخدام جدید بایستی آن‌گونه که در بند ۸-۱ شرح داده شده است، کنترل شود.

سایر اطلاعات
بخش منابع انسانی عموما مسوول کل فرایند خاتمه استخدام است و با مدیر سرپرست شخصی که سازمان را ترک می‌کند، همکاری می نماید تا جنبه های امنیتی رویه های مرتبط را مدیریت کند. در مورد یک پیمانکار، این فرایند مسوولیت خاتمه ممکن است توسط یک آژانس که مسوول پیمانکار است تقبل شود و در صورت وجود یک کاربر دیگر، این کار ممکن است توسط سازمان آنها انجام شود.
ممکن است لازم باشد که کارکنان، مشتریان، پیمانکاران یا کاربران شخص سوم از تغییرات در پرسنل و توافقات عملیاتی مطلع شوند.

۸-۳-۲ *عودت دارایی‌ها*

کنترل
تمامی کارکنان، پیمانکاران و کاربران شخص سوم بایستی به محض خاتمه استخدام قرارداد یا توافق‌نامه خود، تمامی دارایی‌های سازمان را که در اختیار آنها است، به سازمان عودت دهند.

راهنمای پیاده سازی

فرایند خاتمه بایستی رسمی‌شود تا بازگرداندن تمام نرم‌افزارهای ثبت شده، اسناد شرکتی، و تجهیزات را شامل شود. دیگر دارایی‌های سازمانی نظیر دستگاه‌های محاسبه سیار، کارت‌های اعتباری، کارت‌های دسترسی، نرم‌افزار، راهنماها، و اطلاعات ذخیره شده در رسانه های الکترونیکی نیز باید بازگردانده شوند.

در مواردی که یک کارمند، پیمانکار یا کاربر شخص سوم، تجهیزات سازمان را خریداری کند یا از تجهیزات شخصی خودش استفاده کند، بایستی رویه هایی دنبال شود تا اطمینان حاصل شود که تمام اطلاعات مرتبط به سازمان منتقل شده و به طور امن از تجهیزات پاک شده است (همچنین رجوع کنید به ۱۰-۷-۱).

در مواردی که یک کارمند، پیمانکار یا کاربر شخص سوم، دانشی دارد که برای انجام عملیات جاری مهم است، آن دانش بایستی مستندسازی شده و به سازمان منتقل شود.

۸-۳-۳ حذف حقوق دسترسی

کنترل

حقوق دسترسی تمام کارکنان، پیمانکاران و کاربران شخص سوم به اطلاعات و امکانات پردازش اطلاعات، بایستی به محض خاتمه استخدام، قرارداد یا توافق نامه آنها، حذف شده یا با تغییرات تطبیق داده شود.

راهنمای پیاده سازی

به محض خاتمه استخدام، بایستی حقوق دسترسی یک فرد به دارایی‌های مربوط به سیستم‌های اطلاعات و خدمات، مورد بازنگری قرار گیرد. این کار تعیین خواهد کرد که آیا لازم است تا حقوق دسترسی حذف شوند یا خیر. تغییرات یک استخدام بایستی در حذف تمام حقوق دسترسی که برای شغل جدید تایید نشده‌اند، انعکاس یابد. حقوق دسترسی که بایستی حذف یا تغییر داده شوند، شامل دسترسی فیزیکی و منطقی، کلیدها، کارت های شناسایی، تجهیزات پردازش اطلاعات (همچنین رجوع کنید به ۱۱-۲-۴)، تعهدات اشتراک و حذف تمام مستنداتی که این افراد یا پیمانکاران را به عنوان یک عضو جاری سازمان معرفی می‌کند، است. اگر کارمند، پیمانکار یا کاربر شخص سومی که در حال ترک شرکت است، کلمه های عبور حساب های کاربری که فعال باقی مانده اند را بداند، این کلمه های عبور بایستی به محض تغییر پست یا خاتمه قرارداد، تغییر داده شوند.

حقوق دسترسی برای دارایی‌های اطلاعاتی و تجهیزات پردازش اطلاعات، بایستی با توجه به ارزیابی عوامل ریسک، قبل از خاتمه یا تغییرات استخدام کاهش یافته یا حذف شوند. مانند:

الف - این که آیا خاتمه خدمت یا تغییر توسط کارمند، پیمانکار یا کاربر شخص سوم انجام شده است یا توسط مدیریت و نیز بیان دلیل خاتمه خدمت؛

ب - مسوولیت‌های فعلی کارمند، پیمانکار یا هر کاربر دیگر؛

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

اطلاعات دیگر

در شرایط خاص، ممکن است حقوق دسترسی برای دسترسی افراد دیگری غیر از کارمند، پیمانکار یا کاربر شخص سوم ترک کننده، نیز اختصاص داده شده باشند، مثلا، کارت های شناسایی گروهی. در چنین شرایطی، افراد ترک کننده بایستی از همه فهرست های دسترسی گروهی حذف شوند و بایستی تمهیداتی انجام شود تا به تمام کارکنان،

پیمانکاران و کاربران شخص سوم مربوط توصیه شود که این اطلاعات را بیش از این با شخصی که در حال ترک سازمان است، به اشتراک نگذارند.

در صورت خاتمه قرارداد توسط مدیریت، کارکنان، پیمانکاران و کاربران شخص سوم عزل شده، ممکن است عمدا اطلاعات را خراب کنند یا تجهیزات پردازش اطلاعات را منهدم کنند. در صورت استعفای افراد، آنها ممکن است وسوسه شوند تا اطلاعات را برای استفاده در آینده جمع آوری کنند.

۹ امنیت فیزیکی و محیطی

۹-۱ نواحی امن

هدف : پیشگیری از دسترسی فیزیکی غیر مجاز، خسارت و تعرض به ابنیه و اطلاعات سازمان.
توصیه می‌شود تجهیزات پردازش اطلاعات حیاتی یا حساس در نواحی امن نگهداری شوند و حفاظ‌های امنیتی مناسب و کنترل های تردد درباره آنها صورت گیرد. توصیه می‌شود آنها از نظر فیزیکی در برابر دسترسی غیرمجاز، آسیب، و مداخله محافظت شوند.
توصیه می‌شود محافظت انجام شده، با ریسک های شناسایی شده متناسب باشد.

۹-۱-۱ *حصار امنیت فیزیکی*

کنترل
توصیه می‌شود حفاظ‌های امنیتی (موانعی از قبیل حایل‌ها،دیوارها، درهای ورودی کنترل شده توسط کارت یا میزهای پذیرش)، برای حفاظت نواحی حاوی اطلاعات و امکانات پردازش اطلاعات، استفاده شوند.
راهنمای پیاده سازی
توصیه می‌شود دستورالعمل های زیر در هنگام لزوم برای حفاظ‌های امنیت فیزیکی در نظر گرفته شده و اجرا شوند.

الف - توصیه می‌شود حفاظ‌های امنیتی به دقت تعریف شوند و محل قرارگیری و توانایی هر یک از حفاظ‌ها باید متناسب با نیازهای امنیتی دارایی‌های آن محیط و نتایج ارزیابی ریسک آنها باشد.

ب - توصیه می‌شود فضای ساختمان یا سایت حاوی تجهیزات پردازش اطلاعات، از نظر فیزیکی مناسب باشد (به عبارت دیگر، توصیه می‌شود هیچ شکافی در حفاظ‌ها یا نواحی که ورود غیرقانونی بتواند اتفاق بیافتد، وجود نداشته باشد)؛ توصیه می‌شود دیوارهای بیرونی سایت استحکام مناسبی داشته باشند و توصیه می‌شود تمام درب ها به طور مناسب در برابر دسترسی غیرمجاز با مکانیسم های کنترل از جمله موانع، سیستم‌های هشدار دهنده، قفل ها و غیره محافظت شوند؛ توصیه می‌شود درب ها و پنجره ها زمانی که نیاز به محاظت بیرونی و کنترل‌های عدم حضور وجود دارد قفل شوند بخصوص برای پنجره هایی که در طبقات همکف قرار دارند.

پ - توصیه می‌شود یک ناحیه پذیرش یا هر ابزار مشابه دیگری برای کنترل دسترسی فیزیکی به سایت یا ساختمان‌ها در نظر گرفته شود؛ توصیه می‌شود دسترسی به سایت‌ها و ساختمان ها 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 درب های خروج اضطراری، موجود در حفاظ‌های امنیتی مجهز به سیستم هشدار دهنده و دوربین‌های کنترلی باشند و در ترکیب با دیوارها بررسی شوند تا سطح مقاومت مورد نیاز را مطابق با استانداردهای مناسب منطقه ای، ملی و بین المللی فراهم کنند؛ توصیه می‌شود آنها مطابق با استانداردهای محلی مقابله با حریق به گونه ای بی اشتباه عمل کنند؛

ج - توصیه می‌شود سیستم‌های کشف ورود غیرمجاز مطابق با استانداردهای ملی، منطقه ای و بین المللی نصب شوند و به طور منظم مورد آزمایش قرار گیرند تا تمام درب های بیرونی و پنجره ها را پوشش دهند. توصیه می‌شود فضاهای خالی همواره باید توسط سیستم هشدار دهنده کنترل شوند؛ همچنین توصیه می‌شود این پوشش برای فضاهای دیگر مانند اتاق رایانه یا اتاق های ارتباطات تامین گردد.

چ - توصیه می‌شود تجهیزات پردازش اطلاعات که توسط سازمان مدیریت می‌شوند از نظر فیزیکی از تجهیزاتی که توسط اشخاص ثالث دیگر مدیریت می‌شوند تفکیک شوند؛

اطلاعات دیگر

محافظت فیزیکی می‌تواند از طریق ایجاد یک یا چند مانع فیزیکی در اطراف ابنیه سازمان و تجهیزات پردازش اطلاعات آن حاصل شود؛ استفاده از چندین مانع امنیت بیشتری را فراهم می‌کند، و در صورت عمل نکردن یکی از موانع امنیت فیزیکی دچار اختلال نمی‌شود؛

یک ناحیه امن ممکن است یک دفتر کار قابل قفل شدن یا چندین اتاق باشد که توسط یک مانع فیزیکی داخلی یکپارچه احاطه شده است؛ موانع و حفاظهای دیگری برای کنترل دسترسی فیزیکی ممکن است بین نواحی داخلی با نیازهای امنیتی متفاوت مورد نیاز باشد.

توصیه می‌شود ملاحظات خاصی در راستای امنیت دسترسی فیزیکی برای ساختمان هایی که چندین سازمان مختلف در آن قرار دارند در نظر گرفته شود.

۹-۱-۲ کنترل‌های مداخل فیزیکی ورودی

کنترل

توصیه می‌شود نواحی امن، به منظور حصول اطمینان از اینکه فقط کارکنان مجاز، اجازه دسترسی دارند، توسط سیستم‌های کنترل ورودی مناسب، حفاظت شوند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر مدنظر قرار گیرند:

الف - توصیه می‌شود تاریخ و زمان ورود و خروج بازدیدکنندگان ثبت شود و توصیه می‌شود تمام مراجعه کنندگان تحت نظارت باشند مگر این که دسترسی آنها قبلا تایید شده باشد؛ توصیه می‌شود آنها فقط دسترسی برای اهداف خاص و مجاز را داشته باشند و دستورالعمل هایی در زمینه الزامات ایمنی ناحیه و رویه های مربوط به شرایط اضطراری به آنها اعلام شود.

ب - توصیه می‌شود دسترسی به نواحی که در آنجا، اطلاعات حساس مورد پردازش قرار می‌گیرد یا ذخیره می‌شود کنترل و برای افراد مجاز محدود شود؛ کنترل های دسترسی مانند کارت کنترل دسترسی باید برای مجاز و معتبر کردن تمام دسترسی ها مورد استفاده قرار گیرد؛ یک گزارش ممیزی از تمام دسترسی ها باید در محل امنی نگهداری شود.

پ - از تمام کارکنان، پیمانکاران و کاربران شخص ثالث و تمام بازدیدکنندگان باید خواسته شود تا نوعی علامت شناسایی قابل رویت را به لباس خود نصب کنند و در صورت مواجهه با بازدیدکنندگان بدون همراه و یا بدون علامت شناسایی توصیه می‌شود بلافاصله کارکنان امنیتی را مطلع کنند.

ت - توصیه می‌شود کارکنان خدمات پشتیبانی شخص ثالث امکان دسترسی محدود به نواحی امن یا تجهیزات پردازش اطلاعات حساس را فقط در صورت ضرورت داشته باشند؛ توصیه می‌شود این دسترسی مجاز و کنترل شده باشد؛

ث - توصیه می‌شود حقوق دسترسی به نواحی امن، به طور منظم بررسی و روزآمد شوند و در زمان لازم باطل شوند (رجوع کنید به ۸-۳-۳)؛

۹-۱-۳ ایمن‌سازی دفاتر، اتاق‌ها و امکانات

کنترل

توصیه می‌شود امنیت فیزیکی برای دفاتر، اتاق‌ها و امکانات، طراحی و بکار گرفته شود.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای تضمین امنیت دفاتر، اتاق ها و امکانات در نظر گرفته شود:

الف - توصیه می‌شود از مقررات سلامت و ایمنی مربوطه و استانداردها گزارشی تهیه شود؛

ب - توصیه می‌شود تجهیزات کلیدی از دسترس همگان دور نگه داشته شوند

پ - توصیه می‌شود در صورت امکان، ساختمان ها غیرقابل نفوذ باشند و حداقل نشانه ای از کاربردشان ارایه دهند و هیچ علایم واضحی خارج یا داخل ساختمان وجود نداشته باشد که وجود فعالیت های پردازش اطلاعات در آن را مشخص سازد؛

ت – راهنمای ساختمان و دفاتر تلفنی که محل قرارگیری تجهیزات پردازش اطلاعات حساس را نشان می‌دهند، توصیه می‌شود به سادگی در دسترس همگان قرار نداشته باشند؛

۹-۱-۴ محافظت در برابر تهدیدهای بیرونی و محیطی

کنترل

توصیه می‌شود برای مقابله با خسارت ناشی از آتش، سیل، زمین لرزه، انفجار، آشوب داخلی، و شکل های دیگری از حوادث طبیعی یا انسانی، حفاظت فیزیکی مناسب طراحی و بکار گرفته شود.

راهنمای پیاده سازی

توصیه می‌شود درمورد هر یک از تهدیدهای امنیتی که توسط اماکن مجاور متوجه ما می‌شود مانند آتش سوزی در ساختمان همسایه، نشت آب از سقف یا کف طبقات همکف یا انفجار در خیابان، ملاحظاتی صورت گیرد.

توصیه می‌شود رهنمودهای زیر برای اجتناب از آسیب در برابر آتش سوزی، سیل، زلزله، انفجار، شورش، و شکل‌های دیگر بلایای طبیعی یا انسانی به کار گرفته شود:

الف - توصیه می‌شود مواد خطرناک یا قابل اشتعال در فاصله ای مطمئن از نواحی امن نگه داشته شوند؛ توصیه می‌شود تجهیزات فله و باز در نواحی امن نگه داری نشوند

ب - توصیه می‌شود تجهیزات تهیه فایل‌های پشتیبان و محیط‌های ذخیره فایل‌های پشتیبان، در فاصله ای امن قرار گیرند تا از آسیب فجایعی که بر سایت اصلی تاثیر می گذارد در امان بمانند.

پ - توصیه می‌شود تجهیزات آتش نشانی مناسب فراهم و در محل مناسب قرار داده شود.

۹-۱-۵ کار در نواحی امن

کنترل

توصیه می‌شود برای کار در نواحی امن، حفاظت فیزیکی و رهنمودها، طراحی و بکار گرفته شوند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر مدنظر قرار گیرند.

الف - توصیه می‌شود کارکنان فقط در صورت لزوم، از وجود یا فعالیت های نواحی امن مطلع گردند.

ب - توصیه می‌شود از کارکردن بدون نظارت در نواحی امن به دلایل ایمنی و به منظور پیشگیری از فرصت انجام اقدامات خرابکارانه اجتناب شود.

پ - توصیه می‌شود نواحی امن خالی و بدون استفاده از نظر فیزیکی قفل شوند و به طور منظم بازدید شوند؛

ت - توصیه می‌شود تجهیزات عکس برداری، فیلم‌برداری، ضبط صوت یا دیگر تجهیزات ضبط کننده نظیر دوربین تلفن همراه، نباید اجازه ورود داشته باشند مگر این که برای آنها مجوز ورود صادر شود،

ملاحظات مربوط به کار در نواحی امن شامل کنترل هایی برای کارکنان، پیمانکاران و کاربران شخص ثالث و نیز فعالیت های سایر اشخاص، باید تهیه شود.

۹-۱-۶ نواحی دسترسی عمومی، نواحی تحویل و بارگیری

کنترل

توصیه می‌شود نقاط دسترسی از قبیل نواحی تحویل و بارگیری و سایر نقاطی که افراد غیر مجاز ممکن است وارد ساختمان ها شوند، تحت کنترل قرار گرفته و در صورت امکان، برای جلوگیری از دسترسی غیر مجاز، از امکانات پردازش اطلاعات، مجزا شوند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر، لحاظ شوند:

الف - توصیه می‌شود دسترسی به نواحی تحویل و بارگیری از خارج از ساختمان، محدود به اشخاص شناخته شده و مجاز باشد.

ب - توصیه می‌شود منطقه تحویل و بارگیری به گونه ای طراحی شود که بتوان بار را بدون دسترسی کارکنان تحویل به بخش های دیگر ساختمان تخلیه کرد؛

پ - توصیه می‌شود درب های خارجی نواحی تحویل و بارگیری، در زمانی که درب های داخلی باز می‌شوند ایمن شوند؛

ت - توصیه می‌شود مواد ورودی قبل از این که از منطقه تحویل و بارگیری به نقطه مورد استفاده انتقال داده شوند برای تهدیدهای احتمالی وارسی شوند (رجوع شود به ۹-۲-۱ مورد ت).

ث - توصیه می‌شود مواد ورودی مطابق با رویه های مدیریت دارایی در زمان ورود به محل ثبت شوند. (همچنین رجوع کنید به ۷-۱-۱)

ج - توصیه می‌شود محموله های ورودی و خروجی تا جایی که ممکن است، بصورت فیزیکی تفکیک شده باشند.

۹-۲ امنیت تجهیزات

هدف : پیشگیری از اتلاف، زیان، سرقت یا به خطر افتادن دارایی‌ها و ایجاد وقفه در فعالیت های سازمان.
توصیه می‌شود تجهیزات دربرابر تهدیدهای فیزیکی و محیطی محافظت شوند؛
محافظت از تجهیزات برای کاهش ریسک دسترسی غیرمجاز به اطلاعات و محافظت دربرابر آسیب یا خسارت ضروری است. توصیه می‌شود این ملاحظات، محل قرارگیری و تخلیه تجهیزات را هم در نظر بگیرد. کنترل های خاص ممکن است برای محافظت دربرابر تهدیدهای فیزیکی و محافظت از تجهیزات پشتیبان نظیر منبع برق و زیرساختار کابل کشی لازم باشد..

۹-۲-۱ *استقرار و حفاظت تجهیزات*

کنترل

توصیه می‌شود تجهیزات (در مکان مناسب) مستقر و محافظت شوند تا ریسک‌ها ناشی از تهدیدها و خطرات محیطی و فرصت‌های دسترسی غیر مجاز، کاهش یابند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای محافظت از تجهیزات مورد توجه قرا رگیرند:

الف - توصیه می‌شود تجهیزات به نحوی قرار گیرند که دسترسی غیرضروری به نواحی کاری به حداقل کاهش یابد؛

ب - توصیه می‌شود تجهیزات پردازش اطلاعات که با داده‌های حساس سروکار دارند، با زاویه دید محدود قرار گیرند تا ریسک رویت اطلاعات توسط اشخاص غیرمجاز در زمان استفاده کاهش یابد و تجهیزات دخیره اطلاعات برای جلوگیری از دسترسی غیر مجاز در جای امن قرار گیرند.؛

پ - توصیه می‌شود اجزایی که به محافظت خاص نیاز دارند جدا از سایر اقلام قرار گیرند تا سطح کلی محافظت مورد نیاز کاهش یابد

ت - توصیه می‌شود کنترل هایی برای کاهش ریسک تهدیدهای فیزیکی بالقوه مانند سرقت، آتش سوزی، انفجار، دود، آب، گرد و غبار، لرزش، تاثیرات شیمیایی، تداخل منابع برق، تداخل ارتباطات، تابش الکترومغناطیسی و دستکاری اتخاذ شود.

ث - توصیه می‌شود دستورالعمل های منع خوردن، آشامیدن، و سیگار کشیدن در نزدیکی تجهیزات پردازش اطلاعات تهیه شود.

ج - توصیه می‌شود شرایط محیطی نظیر دما و رطوبت برای شرایطی که ممکن است تاثیر منفی بر استفاده از تجهیزات اطلاعات بگذارند کنترل شوند

چ - توصیه می‌شود محافظت از اشتعال در تمام ساختمان ها به کار گرفته شود و توصیه می‌شود فیلترهایی برای حفاظت اشتعال در ورودی تمام خطوط ارتباطی و برق در نظر گرفته شود.

ح - توصیه می‌شود استفاده از روش های محافظت خاص، نظیر غشاهای صفحه کلید، برای تجهیزات مورد استفاده در محیط های صنعتی در نظر گرفته شوند؛

خ - توصیه می‌شود تجهیزاتی که اطلاعات حساس را پردازش می‌کنند محافظت شوند تا ریسک نشت اطلاعات در اثر سهل‌انگاری به حداقل برسد.

۹-۲-۲ امکانات و پشتیبانی

کنترل

توصیه می‌شود تجهیزات در برابر قطع برق و سایر اختلالات ناشی از نقص های امکانات پشتیبانی، محافظت شوند.

راهنمای پیاده سازی

توصیه می‌شود تمام امکانات پشتیبانی نظیر برق، آب، فاضلاب، گرمایش/تهویه و هواسازی برای سیستم‌هایی که مورد پوشش آنها قرار دارند بصورت مناسب فراهم شوند. توصیه می‌شود امکانات پشتیبانی به طور منظم بررسی و تست شوند تا عملکرد مناسب آنها تضمین شود و هر ریسکی ناشی از کارکرد نامناسب آنها کاهش یابد. توصیه می‌شود یک منبع برق مناسب تهیه شود که با مشخصات تولیدکننده تجهیزات تطابق داشته باشد.

یک منبع برق غیرقابل قطع[1]، برای تامین برق برای تجهیزاتی که عملیات حیاتی را پشتیبانی می‌کنند پیشنهاد می‌شود. توصیه می‌شود طرح‌های پیش‌آمدهای احتمالی مرتبط با برق، در زمان خرابی منبع برق غیرقابل قطع لحاظ شود. توصیه می‌شود یک ژنراتور پشتیبان، در صورتی که برای ادامه کار، تداوم پردازش اطلاعات لازم باشد در نظر گرفته شود. توصیه می‌شود یک منبع کافی سوخت در دسترس باشد تا تضمین نماید که ژنراتور می‌تواند برای دوره ای طولانی فعالیت کند. توصیه می‌شود تجهیزات منبع برق غیرقابل قطع و ژنراتورها به طور منظم بررسی شوند تا اطمینان حاصل شود که ظرفیت کافی را دارند و همچنین مطابق با پیشنهادات تولید کننده تست شوند. علاوه بر این، توصیه می‌شود چندین منبع برق مختلف تهیه شود یا اگر سایت بزرگ است یک ایستگاه برق جداگانه در نظر گرفته شود.

توصیه می‌شود کلیدهای قطع برق اضطراری در نزدیکی خروجی های اضطراری اتاق های تجهیزات قرار داده شوند تا قطع برق به سرعت در صورت وقوع شرایط اضطراری امکان‌پذیر شود. توصیه می‌شود روشنایی اضطراری برای مواقع قطع برق اصلی باید فراهم شود.

توصیه می‌شود منبع آب پایدار بوده و برای تامین آب سیستم‌های تهویه، تجهیزات مرطوب کننده، و اطفا حریق کافی باشد. نقص در سیستم تامین آب ممکن است به تجهیزات آسیب برساند یا از عملکرد مناسب سیستم اطفا حریق جلوگیری نماید. توصیه می‌شود یک سیستم هشدار دهنده برای کشف خرابی ها در امکانات پشتبانی تهیه و در صورت لزوم نصب شود.

توصیه می‌شود تجهیزات مخابرات حداقل توسط دو مسیر مختلف به ارایه دهنده خدمات متصل شوند تا خرابی در یک مسیر ارتباطات صوتی را دچار اختلال نکند. توصیه می‌شود خدمات صوتی حداقل نیازهای استانداردهای محلی را برای ارتباطات اضطراری برآورده سازد.

اطلاعات دیگر

گزینه‌هایی جهت دستیابی به منبع برق مستمر شامل استفاده از چندین منبع تغذیه برای اجتناب از وقوع قطعی در جریان برق..

۹-۲-۳ امنیت کابل کشی

کنترل

توصیه می‌شود کابل کشی های برق و ارتباطات مورد استفاده برای انتقال داده یا پشتیبانی از خدمات اطلاع رسانی، در برابر شنود، قطع شدن یا وارد آمدن خسارت، محافظت شوند.

1- Uninterruptible Power Supply (UPS)

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای امنیت کابل کشی مد نظر قرار گیرند:

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

ب - توصیه می‌شود کابل کشی شبکه، از مداخله غیرمجاز یا آسیب محافظت شود، مثلا با عبور از کانال و اجتناب از عبور از محل‌های عمومی

پ - توصیه می‌شود سیم های برق از سیم های مخابرات جدا شود تا از تداخل جلوگیری شود

ت - توصیه می‌شود از کابل هایی که به راحتی قابل تمایز است و از علایم مناسب استفاده شود تا خطاهای انسانی نظیر اتصال اشتباه کابل‌ها به حداقل برسد.

ث - توصیه می‌شود لیست مستند اتصالات برای کاهش احتمال خطا مورد استفاده قرار گیرد

ج - برای سیستم‌های حساس یا حیاتی کنترل های بیشتری لحاظ شود که عبارتند از:

۱- نصب مسیر های دارای حفاظ یا اتاق ها یا جعبه های قفل شده در نقاط بازرسی و ترمینال‌ها

۲ - استفاده از مسیرها و / یا رسانه های انتقال جایگزین جهت تامین امنیت مناسب

۳ - استفاده از کابل فیبر نوری

۴ - استفاده از محافظ های تداخل الکترو مغناطیسی برای محافظت از کابل ها

۵ - آغاز بررسی های فنی و فیزیکی برای یافتن تجهیزاتی که بصورت غیرمجاز به کابل ها وصل شده‌اند

۶ - کنترل دسترسی به پانل های اتصال و اتاق های اتصالات کابل ها

۹-۲-۴ *نگهداری تجهیزات*

کنترل

توصیه می‌شود تجهیزات به منظور حصول اطمینان از تداوم در دسترس بودن و حفظ اصالت آنها، به درستی نگهداری شوند.

راهنمای پیاده سازی

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

الف - توصیه می‌شود تجهیزات مطابق با فواصل زمانی و مشخصات فنی پیشنهادی تامین کننده نگهداری شوند

ب – تعمیر و سرویس تجهیزات باید فقط توسط کارکنان مجاز بخش نگهداری انجام شود

پ - توصیه می‌شود گزارش هایی از تمام خطاهای واقعی یا مشکوک و تمامی اقدامات نگهداری اصلاحی و پیشگیرانه نگهداری شود

ت - توصیه می‌شود کنترل های مناسب در زمان برنامه ریزی شده برای سرویس تجهیزات اجرا شود و به این مساله توجه شود که آیا این سرویس توسط کارکنان در داخل یا خارج از سازمان انجام می‌شود. همچنین در مواقع لازم، توصیه می‌شود اطلاعات حساس از تجهیزات پاک شود، یا کارکنان سرویس و نگهداری تجهیزات بازرسی بدنی شوند.

ث - توصیه می‌شود تمام تعهدات قید شده در بیمه نامه ها رعایت شوند.

۹-۲-۵ امنیت تجهیزات خارج از ابنیه اماکن سازمان

کنترل

توصیه می‌شود برای تجهیزات خارج از سایت، با توجه به ریسک‌ها مختلف ناشی از انجام کار در خارج از اماکن سازمان، ملاحظات امنیتی لازم بعمل آید..

راهنمای پیاده سازی

توصیه می‌شود صرف نظر از مالکیت تجهیزات، اجازه استفاده از تجهیزات پردازش اطلاعات در خارج از محوطه سازمان توسط مدیریت صادر شود.

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

الف - توصیه می‌شود تجهیزات و رسانه هایی که به خارج از محوطه سازمان برده می‌شوند بدون حضور فرد مذکور در محل های عمومی نشوند؛ توصیه می‌شود رایانه‌های قابل حمل به عنوان کیف دستی حمل شوند و در صورت امکان پنهان شوند

ب - توصیه می‌شود دستورالعمل های تولید کننده برای محافظت از تجهیزات همواره مورد توجه قرار گیرد؛ مثلا محافظت دربرابر قرارگرفتن در معرض میدان های الکترومغناطیسی قوی؛

پ - توصیه می‌شود کنترل های مربوط به کار در خانه توسط ارزیابی ریسک های مربوطه تهیه و در زمان مناسب اعمال شوند؛ مثلا قفسه‌هاب بایگانی قابل قفل شدن، سیاست میز پاک، کنترل دسترسی به رایانه‌ها و امنیت ارتباط با شبکه اداره

ت - توصیه می‌شود پوشش بیمه ای کافی برای محافظت از تجهیزات خارج از سایت تهیه گردد.

ریسک‌های امنیتی مانند آسیب، سرقت یا شنود ممکن است بین محل های مختلف متفاوت باشد لذا توصیه می‌شود مناسب ترین کنترل ها مورد استفاده قرار گیرد.

اطلاعات دیگر

تجهیزات ذخیره‌سازی و پردازش اطلاعات شامل انواع رایانه‌های شخصی، سازمان دهنده ها، تلفن های همراه، کارت های هوشمند، کاغذ یا سایر اشکال که برای کار در خانه یا انتقال به سایر نقاط دور از محل کار استفاده می‌شوند

اطلاعات بیشتر درباره جنبه های دیگر محافظت از تجهیزات متحرک را می‌توانید در ۱۱-۷-۱ پیدا کنید.

۹-۲-۶ امحا یا استفاده مجدد از تجهیزات به صورت ایمن

کنترل

توصیه می‌شود تمام اجزای تجهیزاتی که دارای رسانهٔ ذخیره‌سازی می باشند، پیش از امحا به منظور حصول اطمینان از اینکه هر دادهٔ حساس و نرم‌افزار دارای حق امتیاز روی آنها، حذف شده یا به شیوهٔ امنی دوباره نویسی شده اند، بررسی شوند.

راهنمای پیاده سازی

پیش از امحا دستگاه هایی که حاوی اطلاعات حساس هستند، توصیه می‌شود آنها از نظر فیزیکی تخریب شوند یا اطلاعات روی آنها توسط تکنیک هایی خراب، پاک یا حذف شود تا اطلاعات اصلی غیرقابل بازیابی باشد و هرگز نباید از عملکرد "حذف کردن[1]" یا "قالب بندی[1]" استاندارد استفاده کرد.

1- Delete

اطلاعات دیگر

در مورد دستگاه های آسیب دیده که حاوی داده‌های حساس هستند توصیه می‌شود ارزیابی ریسک بعمل آید تا تعیین شود که آیا لازم است که آنها را به جای ارسال برای تعمیر، بصورت فیزیکی نابود کرد یا خیر.

اطلاعات ممکن است از طریق دور ریختن بی دقت یا استفاده مجدد از تجهیزات، مورد دسترسی غیرمجاز قرار گیرد. (همچنین رجوع کنید به ۱۰-۷-۲)

۹-۲-۷ خروج اموال

کنترل

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

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر در نظر گرفته شوند:

الف - توصیه می‌شود تجهیزات، اطلاعات یا نرم‌افزارها بدون اجازه قبلی خارج نشوند

ب - توصیه می‌شود کارکنان، پیمانکاران، و کاربران شخص ثالث که حق دارند اجازه خروج اموال را صادر کنند، به روشنی مشخص شوند

پ - توصیه می‌شود محدودیت های زمانی برای بازگرداندن تجهیزات تعیین و تاریخ بازگشت کنترل شود.

ت - توصیه می‌شود در صورت امکان و لزوم تجهیزات در زمان خروج و بازگشت ثبت شوند.

اطلاعات دیگر

بازدیدهای سریع محلی که عهده‌دار آشکار کردن خروج غیر مجاز اموال است، ممکن است برای آشکار کردن تجهیزات ضبط غیرمجاز، سلاح و غیره نیز بعمل آید و از ورود آنها به سایت جلوگیری شود.

چنین بازدیدهای سریع محلی باید منطبق با ضوابط و قوانین باشد. افراد باید از وجود چنین بازدیدهای سریع محلی آگاه بوده و کنترل‌ها باید با مجوزهای مناسب صورت پذیرد تا با نیازهای قانونی و حقوقی منطبق باشد.

2- Format

۱۰ مدیریت ارتباطات و عملکرد

۱-۱۰ روش‌های اجرایی عملیاتی و مسوولیت‌ها

هدف : حصول اطمینان از عملکرد صحیح و امن امکانات پردازش اطلاعات توصیه می‌شود مسوولیت‌ها و رویه های مدیریت و اجرای تمام تجهیزات پردازش اطلاعات تثبیت شود. این شامل توسعه رویه های عملیاتی مناسب می‌باشد. توصیه می‌شود تفکیک وظایف در زمان ممکن اجرا شود تا مخاطره سوء استفاده سهوی یا عمدی از سیستم کاهش یابد.

۱۰-۱-۱ *روش‌های اجرایی عملیاتی مستند شده*

کنترل

توصیه می‌شود روش‌های اجرایی عملیاتی، مدون شده، نگهداری شوند و در دسترس تمام کاربرانی که به آنها نیاز دارند قرار گیرند.

راهنمای پیاده سازی

توصیه می‌شود روش‌های اجرایی مستند برای فعالیت‌های سیستم در رابطه با تجهیزات پردازش اطلاعات و ارتباطات نظیر رویه‌های روشن و خاموش کردن رایانه‌ها، تهیه فایل پشتیبان، نگهداری از تجهیزات، کار با محیط‌های ذخیره‌سازی اطلاعات، کنترل کار با رایانه‌ها و اتاق رایانه و ایمنی تهیه شود.

توصیه می‌شود رویه‌های عملیاتی دستورالعمل‌هایی را با جزییات کامل برای انجام وظایف هر شغل مشخص کنند از جمله:

الف - پردازش و کار با اطلاعات

ب – تهیه فایل‌های پشتیبان (رجوع کنید به ۱۰-۵)

پ - الزامات زمان‌بندی از جمله وابستگی‌های متقابل با سیستم‌های دیگر، زمان شروع اولین و خاتمه آخرین کار

ت - دستورالعمل‌هایی برای کنترل خطاها یا دیگر شرایط استثنایی که ممکن است در طول اجرای کار رخ دهد از جمله محدودیت‌های استفاده از امکانات سیستم‌ها (رجوع کنید به ۱۱-۵-۴)

ث – شماره تماس‌های پرسنل پشتیبانی در صورت بروز مشکلات فنی و عملیاتی

ج - خروجی خاص و دستورالعمل‌های کار با محیط‌های ذخیره‌سازی اطلاعات نظیر استفاده از محل خاص یا مدیریت خروجی‌های محرمانه شامل رویه‌هایی برای دور ریز ایمن خروجی از کارهایی که با مشکل مواجه شده اند. (رجوع کنید به ۱۰-۷-۲ و ۱۰-۷-۳)

چ - آغاز مجدد سیستم و رویه‌هایی بازگردانی در صورت نقص در عملکرد سیستم؛

ح – مدیریت ممیزی سیستم و اطلاعات وارده به آن(رجوع کنید به ۱۰-۱۰)

توصیه می‌شود رویه‌های عملیاتی و رویه‌های مستند برای فعالیت‌های سیستم به عنوان اسناد رسمی در نظر گرفته شوند و تغییرات آنها فقط با مجوز مدیریت انجام پذیرد. هر زمان که از نظر فنی امکان پذیر باشد، توصیه می‌شود سیستم‌های اطلاعات با استفاده از رویه‌ها، ابزارها و کاربردهای یکسان و به طور سازگار مدیریت شوند.

۱۰-۱-۲ مدیریت تغییر

کنترل

توصیه می‌شود تغییر در امکانات و سیستم‌های پردازش اطلاعات، تحت کنترل باشد.

راهنمای پیاده سازی

توصیه می‌شود سیستم‌های عملیاتی و نرم‌افزارها از نظر تغییرات تحت مدیریت کنترل شدید قرار گیرند.

به خصوص، موارد زیر توصیه می‌شود مد نظر قرار گیرد:

الف - شناسایی و ثبت تغییرات مهم

ب - برنامه ریزی و آزمون تغییرات مهم

پ- ارزیابی تاثیرات بالقوه، از جمله تاثیرات ایمنی این تغییرات؛

ت - رویه تایید رسمی برای انجام تغییرات پیشنهادی

ث – تبادل جزییات تغییرات با افراد مرتبط

ج - رویه‌های برگشت از تغییرات از جمله رویه‌ها و مسوولیت‌های توقف و بازگردانی موفق به حالت قبل از تغییرات در صورت وقوع وقایع پیش بینی نشده

توصیه می‌شود مسوولیت‌ها و رویه‌های مدیریت رسمی برای تضمین کنترل رضایت بخش تمام تغییرات در تجهیزات، نرم‌افزار یا رویه‌ها تعیین شود. زمانی که تغیرات انجام شد، توصیه می‌شود یک حساب ممیزی حاوی تمام اطلاعات مرتبط حفظ شود.

سایر اطلاعات

کنترل ناکافی تغییرات در تجهیزات و سیستم‌های پردازش اطلاعات، یکی از دلایل متداول ناکامی‌های سیستم یا امنیت است. قرار دادن یک سیستم در محیط عملیاتی به خصوص در زمان انتقال یک سیستم از مرحله توسعه به مرحله عملیاتی ممکن است بر قابلیت اطمینان برنامه‌های کاربردی تاثیر بگذارد. (همچنین رجوع کنید به ۱۲-۵-۱)

توصیه می‌شود تغییرات در سیستم‌های عملیاتی فقط زمانی انجام شود که دلیل کسب وکار معتبری برای انجام این کار وجود داشته باشد. مثلا افزایش ریسک سیستم. به روز رسانی سیستم‌ها با جدیدترین نسخه‌های سیستم‌های عامل همیشه از نظر کسب وکار به صرفه نیست زیرا ممکن است آسیب پذیری‌ها و ناپایداری بیشتری را در مقایسه با نسخه فعلی به همراه داشته باشد. همچنین ممکن است نیاز به آموزش تکمیلی و هزینه‌های دریافت مجوز استفاده، پشتیبانی، نگهداری و هزینه‌های بالاسری اجرا و سخت افزار جدید به خصوص در زمان انتقال وجود داشته باشد.

۱۰-۱-۳ تفکیک وظایف

کنترل

به منظور کاهش فرصت‌های دستکاری غیر عمد یا غیر مجاز، یا استفاده نابجا از دارایی‌های سازمان، توصیه می‌شود وظایف و حدود اختیارات تفکیک شوند.

راهنمای پیاده سازی

تفکیک وظایف روشی برای کاهش ریسک مربوط به سوء استفاده تصادفی یا عمدی از سیستم است. توصیه می‌شود مراقبت‌های لازم جهت کنترل دسترسی به دارایی‌ها و اصلاح، یا استفاده هر یک از افراد، بدون اطلاع و هماهنگی و یا

تشخیص بعمل آید. توصیه می‌شود انجام هر امری از مجوز انجام آن مجزا باشد. توصیه می‌شود احتمال تبانی در طراحی کنترل‌ها در نظر گرفته شود.
سازمان‌های کوچک ممکن است انجام تفکیک وظایف را دشوار بدانند اما توصیه می‌شود این اصل همیشه تا حد امکان و به هر میزان که ممکن است رعایت شود. هر زمان که تفکیک وظایف دشوار باشد، توصیه می‌شود کنترل‌های دیگر نظیر کنترل فعالیت‌ها، ممیزی امور و نظارت‌های مدیریتی بکار برده شود. آنچه مهم است مستقل بودن ممیزی امنیت است.

۱۰-۱-۴ جداسازی امکانات توسعه، آزمون و عملیاتی

کنترل

توصیه می‌شود امکانات مربوط به سیستم‌های درحال توسعه، تحت آزمایش و عملیاتی، به منظور کاهش ریسک ناشی از دسترسی غیر مجاز یا تغییرات در سیستم‌های عملیاتی، تفکیک شوند.

راهنمای پیاده سازی

توصیه می‌شود سطح تفکیک بین محیط‌های عملیاتی، تحت آزمایش و درحال توسعه که برای پیشگیری از مشکلات عملیاتی لازم است، توصیه می‌شود که شناسایی شده و کنترل‌های مناسب اعمال شود.
توصیه می‌شود موارد زیر مد نظر قرار گیرد:

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

ب - توصیه می‌شود نرم‌افزارهای تحت توسعه و عملیاتی، روی رایانه‌های متفاوت و یا پردازشگرهای متفاوت یک رایانه و از دامنه و پوشه‌های مختلف اجرا شوند.

پ - توصیه می‌شود همگردان‌ها[1]، ویراستارها و دیگر ابزار توسعه از سیستم‌های عملیاتی در زمانی‌که لازم نیستند قابل دسترسی نباشند.

ت - توصیه می‌شود محیط سیستم‌های تحت آزمایش تا حد امکان با محیط عملیاتی شباهت داشته باشد.

ث - توصیه می‌شود کاربران از نمایه‌های کاربری متفاوتی برای کار در محیط سیستم‌های تحت آزمایش و عملیاتی استفاده کنند و توصیه می‌شود تا منوهایی برای کاهش ریسک خطا، نمایه کاربری مورد استفاده را نمایش دهند.

ج - توصیه می‌شود داده‌های حساس، به محیط سیستم، تحت آزمایش کپی نشوند. (رجوع کنید به ۱۲-۴-۲)

اطلاعات دیگر

فعالیت‌های تست و توسعه می‌توانند باعث بروز مشکلات جدی مانند تغییر ناخواسته ی فایل‌ها یا محیط سیستم و یا خرابی سیستم شوند. در این صورت، باید محیط شناخته شده و پایداری حفظ شود که در آن، تست معنا دار انجام شود و از دسترسی نامناسب توسعه دهند نرم‌افزاری جلوگیری به عمل آید.
در جایی که کاربران سیستم‌های تحت توسعه و یا آزمون به سیستم‌های عملیاتی و اطلاعات آن دسترسی دارند، ممکن است باعث اعمال کد غیرمجاز و تست نشده‌ای شده و یا داده‌های عملیاتی را تغییر دهند. در بعضی از سیستم‌ها، این قابلیت ممکن است باعث سوءاستفاده شده یا کد غیرمجازی وارد شود که باعث مشکلات عملیاتی مهمی شود.

1- Compilers

کاربران توسعه و آزمون سیستم‌ها برای محرمانگی اطلاعات سیستم‌های عملیاتی تهدید یک به حساب می‌آیند. اگرفعالیت‌های توسعه و آزمون سیستم‌ها در محیط محاسباتی مشترکی انجام شود ممکن است تغییرات ناخواسته‌ای را برای نرم‌افزار یا اطلاعات ایجاد کند. بنابراین تفکیک تجهیزات محیط‌های عملیاتی، تحت توسعه و آزمون برای کاهش ریسک تغییرات تصادفی یا دسترسی غیرمجاز به نرم‌افزار عملیاتی و داده‌های کسب وکار ضروری است. (برای حفاظت از داده‌های آزمون، همچنین رجوع کنید به ۱۲-۴-۲)

۱۰-۲ مدیریت تحویل خدمت شخص سوم

هدف : پیاده سازی و نگهداری سطح مناسب امنیت اطلاعات و تحویل خدمت، در راستای توافق‌نامه‌های تحویل خدمت شخص ثالث. توصیه می‌شود سازمان اجرای توافقات را بررسی نماید، مطابقت با توافقات را کنترل نماید و تغییرات را مدیریت نماید تا تضمین شود که خدمات ارایه شده تمام الزامات توافق شده با شخص ثالث را برآورده می سازد.

۱۰-۲-۱ *تحویل خدمت*

کنترل

توصیه می‌شود از پیاده‌سازی، عملیاتی شدن و نگهداری کنترل‌های امنیتی، تعاریف خدمت و سطوح تحویل مندرج در توافق‌نامه تحویل خدمت اشخاص ثالث،اطمینان حاصل شود.

راهنمای پیاده سازی

وصیه می‌شود توافقنامه ارایه خدمات اشخاص ثالث باید دربرگیرنده قراردادهای امنیتی توافق شده، تعاریف خدمات و جنبه‌های مدیریت خدمات باشد. در صورت واگذاری خدمات به بیرون از سازمان، توصیه می‌شود سازمان مراحل انتقال (اطلاعات، تجهیزات پردازش اطلاعات و سایر امکانات دیگر) به داخل سازمان را تعریف نموده و توصیه می‌شود تضمین نماید که امنیت اطلاعات درزمان سراسر زمان انتقال حفظ می‌شود.

توصیه می‌شود سازمان از توانایی اشخاص ثالث در ارایه خدمات با کیفیت مطلوب و داشتن برنامه کاری مناسب جهت تداوم ارایه سطح خدمات لازم و عدم وقوع وقفه در ارایه خدمات حساس اطمینان حاصل نماید.(رجوع کنید به۱۴-۱)

۱۰-۲-۲ *پایش و بازبینی خدمات شخص سوم*

کنترل

وصیه می‌شود خدمات، گزارشات و سوابق تهیه شده توسط اشخاص ثالث، به صورت قاعده مند پایش و بازبینی شده، و توصیه می‌شود ممیزی‌ها به صورت منظم انجام شوند.

راهنمای پیاده سازی

توصیه می‌شود کنترل و بررسی خدمات ارایه شده اشخاص ثالث تضمینی بر رعایت مفاد و شرایط مربوط به امنیت اطلاعات در قراردادها و مدیریت مطلوب حوادث و مشکلات امنیت اطلاعات است. توصیه می‌شود این موضوع دربرگیرنده رابطه و فرایند مدیریت خدمات بین سازمان و اشخاص ثالث باشد تا:

الف - سطوح ارایه خدمات را جهت کنترل رعایت مفاد قرارداد بررسی نماید؛

ب - گزارش‌های خدمات ارایه شده توسط اشخاص ثالث را بررسی نماید و جلسات منظمی را برای بررسی تطابق روند پیشرفت کار با مفاد قرارداد ترتیب دهد.

پ - اطلاعاتی در رابطه با حوادث امنیت اطلاعات ارایه دهد و این اطلاعات را جهت بررسی توسط شخص ثالث و سازمان در صورتی که در قرارداد یا هر یک از دستورالعمل‌ها و رویه‌ها ذکر شده باشد در اختیار آنها قرار دهد.

ت - گزارش‌های ممیزی شخص ثالث و گزارش‌های حوادث امنیتی، مشکلات عملیاتی ناکامی‌ها و ردیابی تقصیرات و اختلالات در رابطه با خدمات ارایه شده را بررسی کند.

ث - هر مشکل تشخیص داده شده ای را حل و مدیریت کند.

توصیه می‌شود مسوولیت مدیریت روابط با با اشخاص ثالث به یک فرد منصوب شده یا تیم مدیریت خدمات سپرده شود. به علاوه، توصیه می‌شود سازمان باید از واگذاری مسوولیت امکان بررسی رعایت مفاد قرارداد توسط اشخاص ثالث اطمینان حاصل نماید. توصیه می‌شود مهارت و منابع فنی کافی در دسترس قرار گیرد تا رعایت الزامات قرارداد به خصوص الزامات امنیت اطلاعات کنترل شوند(رجوع کنید به ۶-۲-۳). توصیه می‌شود اقدامات لازم زمانی که نقصی در ارایه خدمات مشاهده شد صورت گیرد.

توصیه می‌شود سازمان در تمام جنبه‌های مربوط به اطلاعات حساس و حیاتی یا تجهیزات پردازش اطلاعات که مورد دسترسی یا مدیریت اشخاص ثالث قرار دارند، ابزارهای کنترلی خود را حفظ نموده و اطمینان حاصل کند که امکان پایش را در فعالیت‌های امنیتی نظیر مدیریت تغییرات، شناسایی آسیب پذیری‌ها و حوادث امنیت اطلاعات از طریق دریافت گزارشات تعریف شده با ساختار و شکل مشخص دارا می‌باشد.

اطلاعات دیگر

در صورت واگذاری خدمات به بیرون، سازمان باید آگاه باشد که هنوز مسوولیت نهایی اطلاعات پردازش شده به عهده سازمان است.

۱۰-۲-۳ مدیریت تغییرات در خدمات شخص سوم

کنترل

توصیه می‌شود تغییرات در ارایه خدمات شامل نگهداری و بهبود خط‌مشی‌های امنیت اطلاعات، روش‌های اجرایی و کنترل‌های موجود، توصیه می‌شود با توجه به میزان بحرانی بودن سیستم‌های کسب‌وکار و فرایندهای مرتبط و برآورد مجدد ریسک‌ها، مدیریت شوند.

راهنمای پیاده سازی

در فرایند مدیریت تغییرات خدمات اشخاص ثالث باید موارد زیر در نظر گرفته شود:

الف - تغییرات ایجاد شده توسط سازمان:

۱-بهبود هر یک از کاربردها و سیستم‌های جاری

۲-توسعه هر یک از کاربردها و سیستم‌های جدید؛

۳- اصلاحات یا ارتقای خط مشی‌ها و رویه‌های سازمان

۴- کنترل‌های جدید برای حل حوادث امنیت اطلاعات و بهبود امنیت

ب - تغییرات در خدمات اشخاص ثالث:

۱-تغییر و بهبود شبکه

۲-استفاده از فن‌آوری‌های جدید
۳- استفاده از محصولات جدید یا مدل‌ها و نسخه‌های جدیدتر محصول
۴- ابزارها و محیط جدید توسعه
۵- تغییرات در محل فیزیکی تجهیزات خدمات
۶- تغییر محصول

۱۰-۳ طرح‌ریزی و پذیرش سیستم

هدف : کمینه کردن مخاطرات ناشی از خرابی سیستم‌ها.
برنامه ریزی و آماده سازی پیشرفته ای برای تضمین دسترسی به ظرفیت و منابع کافی برای ارائه عملکرد مورد نیاز سیستم لازم است.
پیش بینی لازم در مورد ظرفیت مورد نیاز آینده به عمل آید تا مخاطره تحمیل بار زیادی به سیستم کاهش یابد.
توصیه می‌شود نیازهای عملیاتی سیستم‌های جدید در نظر گرفته و مستند شود و قبل از پذیرش و استفاده از آنها تست شود.

۱۰-۳-۱ *مدیریت ظرفیت*

کنترل
توصیه می‌شود استفاده از منابع پایش و تنظیم شده و ظرفیت مورد نیاز در آینده به گونه ای پیش بینی شود که از کارایی مورد نیاز سیستم، اطمینان حاصل شود.
راهنمای پیاده سازی
توصیه می‌شود برای هر فعالیت جدید و جاری، توصیه می‌شود نیازهای ظرفیتی شناسایی شود. توصیه می‌شود سیستم‌ها تنظیم و پایش شوند تا از تداوم عملکرد و مطلوبیت کارایی آنها در هنگام نیاز اطمینان حال شود و در صورت لزوم بهبود یابد. توصیه می‌شود از کنترل‌های شناسایی استفاده شود تا مشکلات در زمان مناسب تشخیص داده شوند. توصیه می‌شود پیش بینی الزامات ظرفیتی آینده، الزامات کسب وکار و سیستمی جدید و گرایش‌های جاری و پیش بینی شده را در قابلیت‌های پردازش اطلاعات سازمان در نظر بگیرد.
باید توجه خاصی به منابعی که زمان طولانی یا هزینه بالایی جهت تهیه دارند نمود. بنابراین توصیه می‌شود مدیران نحوه استفاده از منابع کلیدی سیستم‌ها را زیرنظر بگیرند. توصیه می‌شود آنها باید روند استفاده را به خصوص در رابطه با کاربردهای کسب وکار یا ابزارهای سیستم اطلاعات مدیریت بررسی کنند.
توصیه می‌شود مدیران از این اطلاعات برای شناسایی و اجتناب از تنگناهای احتمالی و وابستگی به کارکنان کلیدی که ممکن است برای امنیت سیستم یا خدمات تهدید به حساب آیند استفاده کرده و اقدامات مناسب را برنامه ریزی نمایند.

۱۰-۳-۲ *پذیرش سیستم*

کنترل

توصیه می‌شود معیار پذیرش برای سیستم‌های اطلاعاتی جدید، ارتقا سیستم‌های جاری و نسخه‌های جدید ایجاد شده و در حین توسعه و پیش از پذیرش سیستم، آزمایش‌های مناسب انجام پذیرند.

راهنمای پیاده سازی

توصیه می‌شود مدیران مطمئن شوند که الزامات و معیارهای پذیرش سیستم‌های جدید به طور شفاف تعریف شده، مورد توافق قرار گرفته، مستند و تست می‌شوند. توصیه می‌شود عملیاتی شدن سیستم‌های اطلاعاتی جدید، به روز رسانی سیستم‌های جاری و استفاده از نسخه جدید سیستم‌ها پس از پذیرش رسمی آن صورت پذیرد.

توصیه می‌شود موارد زیر قبل از پذیرش رسمی سیستم‌ها مورد توجه قرار گیرد:

الف - نیازهای ظرفیتی و کارایی رایانه‌ها

ب - رویه‌های بازیابی خطا و آغاز مجدد و برنامه‌های همسوسازی

پ - آماده سازی و تست رویه‌های عملیاتی متداول با استانداردهای تعریف شده

ت - مجموعه کنترل‌های امنیتی تایید شده

ث – روش‌های اجرایی دستی موثر

ج - هماهنگی‌های استمرار تجارت(رجوع کنید به ۱۴-۱)

چ - شواهدی که نشان می دهند نصب سیستم جدید تاثیری منفی بر سیستم‌های فعلی به خصوص در زمان‌های اوج پردازش نظیر پایان ماه نخواهد داشت.

ح - شواهدی که نشان می دهد به تاثیر سیستم جدید بر کل امنیت سازمان توجه کافی شده است.

خ - آموزش بهره بردار ی و استفاده از سیستم‌های جدید

د - سهولت استفاده؛ زیرا بر عملکرد کاربر تاثیر گذاشته و از خطای انسانی جلوگیری می‌کند.

برای توسعه سیستم‌های مهم و جدید، توصیه می‌شود توابع عملیاتی و کاربران در مراحل مختلف فرایند توسعه مورد مشاوره قرار گیرند تا از بازدهی طراحی سیستم پیشنهادی اطمینان حاصل شود. توصیه می‌شود تست‌های مناسب برای تایید رعایت کامل تمام معیارهای پذیرش انجام شود.

اطلاعات دیگر

پذیرش ممکن است شامل یک فرایند صدور گواهی و تایید صلاحیت برای تصدیق رعایت الزامات امنیتی باشد.

۱۰-۴ حفاظت در برابر کدهای مخرب و سیار

هدف : حفاظت از یکپارچگی نرم افزارها و اطلاعات

برای جلوگیری از ورود وکشف کدهای بدخواهانه و سیار غیرمجاز باید ملاحظات احتیاطی لازم بعمل آید.

نرم‌افزارها و تجهیزات پردازش اطلاعات نسبت به ورود کد بدخواهانه، مانند ویروس‌های کامپیوتری، کرم‌های شبکه، اسب‌های تروجان و بمب‌های منطقی آسیب‌پذیر هستند. توصیه می‌شود به کاربران در مورد خطرات کدهای بدخواهانه هشدار داده شود. توصیه می‌شود مدیران در زمان مناسب کنترل‌هایی را برای جلوگیری، کشف و رفع کدهای بدخواهانه و کنترل کدهای سیار، در نظر بگیرند.

۱۰-۴-۱ *کنترل هایی در برابر کدهای مخرب*

کنترل

توصیه می‌شود کنترل‌های لازم برای تشخیص کدهای مخرب، پیشگیری و ترمیم در برابر آنها، و روش‌های اجرایی مناسب برای آگاه‌سازی کاربران بکار برده شود.

راهنمای پیاده سازی

توصیه می‌شود محافظت دربرابر کدهای مخرب بر اساس نوع کد کشف شده و نرم‌افزار مقابله با آن، آگاهی‌های امنیتی، و راهکارهای دسترسی مناسب به سیستم و کنترل مدیریت تغییرات باشد.

توصیه می‌شودرهنمودهای زیر در نظر گرفته شود:

الف – تدوین یک خط‌مشی رسمی برای جلوگیری از استفاده از نرم‌افزارهای غیرمجاز (رجوع کنید به ۱۵-۱-۲)

ب - تدوین یک خط‌مشی رسمی برای محافظت در برابر ریسک‌های مربوط به دستیابی به فایل‌ها و نرم‌افزارها از طریق شبکه‌های بیرونی یا هر رسانه دیگر که نشان دهنده روش‌های پیشگیری مورد اتخاذ هم باشد.

پ - انجام بررسی‌های منظم نرم‌افزارها و محتوای اطلاعات سیستم‌هایی که فرایندهای حیاتی کسب وکار را پشتیبانی می‌کنند؛ توصیه می‌شود حضور هر فایل تایید نشده یا تغییر غیرمجاز رسما بررسی شود.

ت - نصب و به روز رسانی منظم نرم‌افزارهای کشف و ترمیم کدهای مخرب برای اسکن رایانه‌ها و رسانه‌ها به عنوان یک کنترل احتیاطی توصیه می‌شود کنترل‌های انجام شده شامل موارد زیر باشد:

۱- بررسی هر فایل روی رسانه‌های الکترونیکی یا نوری و فایل‌های دریافت شده از طریق شبکه‌ها برای کنترل وجود کدهای مخرب قبل از استفاده.

۲- کنترل ضمیمه‌های نامه‌های الکترونیکی برای کنترل کدهای مخرب قبل از استفاده؛ توصیه می‌شود این بررسی در محل‌های مختلف مثلا در سرویسگرهای پست الکترونیکی، رایانه‌های رومیزی، و در زمان ورود به شبکه سازمان انجام شود؛

۳- بررسی صفحات وب برای کد مخرب

ث - تعریف رویه‌ها و مسوولیت‌های مدیریت جهت محافظت سیستم‌ها در مقابل کدهای مخرب، آموزش استفاده از آنها، گزارش و بازیابی اطلاعات پس از وقوع حملات کدهای مخرب (رجوع کنید به۱۳-۱ و ۱۳-۲)

ج - آماده سازی برنامه‌های استمرار کسب وکار مناسب برای بازیابی اطلاعات پس از وقوع حملات کدهای مخرب از جمله تمام داده‌ها و نرم‌افزارها و فایل‌های پشتیبان (رجوع کنید به بند ۱۴)

چ - پیاده‌سازی روش‌های اجرایی برای جمع‌آوری منظم اطلاعات، مانند درخواست اشتراک در لیست‌های ارسال نامه و/ یا بررسی سایت‌های اینترنتی که اطلاعاتی درباره کدهای مخرب می‌دهد

ح - اجرای رویه‌هایی برای بررسی صحت اطلاعات مربوط به کدهای مخرب و تضمین این که اطلاعات بولتن‌های هشدار دهنده، دقیق و جامع هستند؛ مدیران باید تضمین کنند که منابع واجد شرایط، مانند مجلات معتبر، سایت‌های اینترنتی قابل اطمینان، یا تامین کنندگانی که نرم‌افزارهایی تولید می‌کنند که در برابر کدهای مخرب محافظت می‌کند، برای تمایز بین توهمات و کدهای مخرب واقعی مورد استفاده قرار می‌گیرند. توصیه می‌شود تمام کاربران از مساله توهمات و این که در زمان دریافت آنها چه کار باید انجام دهند مطلع شوند.

اطلاعات دیگر:

استفاده از دو یا چند محصول نرم‌افزاری از شرکت‌های متفاوت که در برابر کدهای مخرب، محیط پردازش اطلاعات را محافظت می‌کنند می‌تواند تاثیر محافظت در برابر کدهای مخرب را بهبود بخشند.
نرم‌افزارهای محافظت در برابر کدهای مخرب را می‌توان به گونه ای نصب کرد که بصورت اتوماتیک فایل‌های تعریف و موتور بررسی خود را به‌روز رسانی کند تا از به روز بودن آن اطمینان حاصل شود. به علاوه، این نرم‌افزارها را می‌توان روی هر رایانه‌ای نصب نمود تا کنترل‌ها بصورت اتوماتیک انجام شود.
در زمان تعمیرات یا انجام روال‌های اضطراری که کنترل‌های معمول مراقبت در مقابل کدهای مخرب معلق می‌شوند در مقابل ورود کدهای مخرب باید مراقب بود.

۱۰-۴-۲ *کنترل هایی در برابر کدهای سیار*

کنترل

توصیه می‌شود جایی‌که استفاده از کدهای سیار مجاز است، پیکربندی به نحوی باشد که از انطباق عملکرد کد سیار، با خط‌مشی امنیتی ای که به صورت شفاف تعریف شده، بتوان اطمینان حاصل نمود، و توصیه می‌شود از اجرای کد سیار غیر مجاز نیز پیشگیری شود.

راهنمای پیاده سازی

توصیه می‌شود ملاحظات زیر برای محافظت در برابر انجام فعالیت‌های غیرمجاز کدهای سیار در نظر گرفته شود:

الف - اجرای کد سیار در یک محیط مجزا
ب - جلوگیری از استفاده از هر گونه کد سیار
پ - جلوگیری از دریافت کد سیار
ت - استفاده از تمهیدات فنی موجود در یک سیستم خاص برای مدیریت کدهای سیار
ث - کنتر ل منابع قابل دسترسی توسط کد سیار
ج -استفاده از روش‌های رمزنگاری برای احراز هویت کدهای سیار

اطلاعات دیگر

کد سیارکدی نرم‌افزاری است که از یک رایانه به رایانه دیگر حرکت می‌کند و سپس به طور اتوماتیک عملکرد خاصی را بدون تعامل کاربر اجرا می‌کند. کد سیار با تعدادی از خدمات واسط در ارتباط است.
علاوه بر کسب اطمینان از این که کدهای سیار حاوی کدهای مخرب نیستند، کنترل کد سیار آنها برای اجتناب از استفاده غیرمجاز یا اختلال در سیستم، شبکه، یا سایر منابع و دیگر نقض‌های امنیت اطلاعات حیاتی است.

۱۰-۵ نسخه‌های پشتیبان

هدف : حفظ یکپارچگی و در دسترس بودن به اطلاعات و امکانات پردازش اطلاعات
توصیه می‌شود رویه‌های منظم برای اجرای خط‌مشی و راهبردهای تهیه فایل پشتیبان به منظور داشتن نسخه‌های پشتیبان از داده‌ها و ذخیره به موقع آنها تهیه شود.(همچنین رجوع کنید به ۱۴-۱)

۱۰-۵-۱ *ایجاد پشتیبان از اطلاعات*

کنترل

توصیه می‌شود تهیه فایل پشتیبان از اطلاعات و نرم‌افزارها، با توجه به خط‌مشی توافق شده نسخه‌های پشتیبان، به صورت منظم انجام و آزمایش شوند.

راهنمای پیاده سازی

توصیه می‌شود تجهیزات لازم برای تهیه فایل پشتیبان و بازیابی آن، فراهم شود تا تضمین شود که تمام اطلاعات ضروری و نرم‌افزارها را می‌توان پس از یک حادثه یا خرابی رسانه‌ها بازیابی نمود.

توصیه می‌شود موارد زیر برای تهیه فایل پشتیبان از اطلاعات در نظر گرفته شود:

الف - اطلاعاتی که باید از آنها فایل پشتیبان تهیه شود مشخص شوند.

ب - توصیه می‌شود سوابق دقیق و کامل از فایل‌های پشتیبان و مستندات مربوط به نحوه بازگردانی آنها تهیه شود.

پ - توصیه می‌شود نوع و فواصل زمانی تهیه فایل پشتیبان بر اساس الزامات کسب وکار سازمان، میزان حساسیت و حیاتی بودن اطلاعات برای فعالیت‌های سازمان باشد.

ت - توصیه می‌شود فایل‌های پشتیبان در یک محل دیگر و با فاصله کافی از سایت اصلی برای اجتناب از هر گونه آسیب ناشی از وقوع حادثه در سایت اصلی ذخیره شوند.

ث - توصیه می‌شود فایل‌های پشتیبان باید دارای سطح مناسبی از محافظت فیزیکی و محیطی باشند که با استانداردهای مربوطه همخوانی داشته باشد. توصیه می‌شود کنترل‌های حفاظتی استفاده شده در مورد رسانه‌های سایت اصلی در سایت پشتیبان هم به کار برده شوند(رجوع کنید به بند ۹)

ج - توصیه می‌شود رسانه‌های ذخیره فایل‌های پشتیبان به طور منظم تست شوند تا اطمینان حاصل شود که میتوان برای استفاده اضطراری در زمان لازم به آنها تکیه کرد

چ - توصیه می‌شود رویه‌های بازیابی اطلاعات به طور منظم بررسی و تست شود تا تضمین شود که آنها قابل استفاده بوده و از طریق آنها طی زمان مشخص شده در سیاست‌های امنیتی اطلاعات قابل بازگردانی هستند.

ح - توصیه می‌شود در شرایطی که محرمانگی اطلاعات اهمیت دارد، فایل‌های پشتیبان بصورت رمز نگهداری شوند.

توصیه می‌شود تهیه فایل پشتیبان برای تک تک سیستم‌ها به طور منظم تست شود تا تضمین شود که آنها الزامات برنامه‌های استمرار کسب وکار را برآورده می سازند(رجوع کنید به بند ۱۴). توصیه می‌شود برای سیستم‌های حیاتی،از تمام اطلاعات، کاربردها، و داده‌هاکه برای بازگردانی کامل سیستم در صورت بروز حادثه به آنها نیاز است، فایل پشتیبان تهیه شود.

توصیه می‌شود زمان نگهداری اطلاعات حیاتی کسب وکار و نیز هر الزام دیگری که برای نگهداری مناسب کپی‌های آرشیو لازم است تعیین شود. (رجوع کنید به ۱۵-۱-۳)

اطلاعات دیگر

تهیه فایل پشتیبان را می‌توان اتوماتیک نمود تا فرایند تهیه فایل پشتیبان و بازیابی آن تسهیل شود. توصیه می‌شود عملکرد این راه حل‌های اتوماتیک قبل از اجرا و در فواصل منظم تست شوند.

۱۰-۶ مدیریت امنیت شبکه

هدف : حصول اطمینان از حفاظت اطلاعات در شبکه‌ها و زیر ساختارهای پشتیبانی کننده آنها.
مدیریت امن شبکه‌ها که ممکن است مرزهای سازمانی را در نوردد نیازمند ملاحظه دقیق جریان داده، آثار حقوقی، کنترل و محافظت آن می‌باشد. کنترل‌های تکمیلی ممکن است برای محافظت از عبور اطلاعات حساس در شبکه‌های همگانی لازم باشد.

۱۰-۶-۱ *کنترل های شبکه*

کنترل

توصیه می‌شود شبکه‌ها به منظور حفاظت در برابر تهدیدها و برای حفظ امنیت سیستم‌ها و برنامه‌های کاربردی که از شبکه استفاده می‌کنند (شامل اطلاعات در گردش)، به میزان کفایت، مدیریت و کنترل شوند.

راهنمای پیاده سازی

توصیه می‌شود مدیران شبکه‌ها کنترل‌هایی را اجرا کنند تا امنیت اطلاعات در شبکه‌ها تضمین شده و خدمات شبکه در قبال دسترسی غیر مجاز حفظ شوند. به خصوص، توصیه می‌شود موارد زیر در نظر گرفته شود:

الف - توصیه می‌شود مسوول عملیاتی شبکه‌ها هر جا که ممکن بود از مسوول عملیاتی رایانه‌ها تفکیک شود. (رجوع کنید به ۱۰-۱-۳)

ب - مسوولیت‌ها و رویه‌های مدیریت تجهیزات راه دور از جمله تجهیزاتی که توسط کاربر مورد استفاده قرار می‌گیرد توصیه می‌شود تدوین و اجرا شود

پ - توصیه می‌شود کنترل‌های خاصی برای محافظت از محرمانگی و یکپارچگی داده‌هایی که از شبکه‌های همگانی یا شبکه‌های بی سیم عبور می‌کند پیش بینی شود و از سیستم‌ها و کاربردهای مرتبط محافظت شود؛ کنترل‌های خاصی نیز ممکن است برای حفظ دسترسی به خدمات شبکه و رایانه‌های متصل لازم باشد(رجوع کنید به ۱۱-۴ و ۱۲-۳)

ت - توصیه می‌شود از ابزار مشاهده و ثبت وقایع مناسب استفاده شود تا ثبت وقایع امنیتی امکان‌پذیر شود.

ث - توصیه می‌شود فعالیت‌های مدیریتی به‌دقت هماهنگ شود تا خدمات مربوط به سازمان بهینه شده و همچنین از بکار گیری مناسب کنترل‌ها در زیرساختار پردازش اطلاعات اطمینان حاصل شود.

اطلاعات دیگر

اطلاعات تکمیلی درباره امنیت شبکه را می‌توانید در ISO/IEC 18028T، روش‌های امنیت فن‌آوری اطلاعات- امنیت شبکه IT، مطالعه فرمایید.

۱۰-۶-۲ *امنیت خدمات شبکه*

کنترل

توصیه می‌شود ویژگی‌های امنیتی، سطوح خدمات، و الزامات مدیریتی تمامی خدمات شبکه، شناسایی شده و در هر توافق‌نامهٔ خدمات شبکه، اعم از اینکه این خدمات در داخل انجام یا برون سپاری می‌شود، لحاظ شود.

راهنمای پیاده سازی

توصیه می‌شود توانایی‌های ارایه کننده خدمات شبکه در مدیریت خدمات موردتوافق به گونه ای مطمئن، تعیین شود و به طور منظم مورد نظارت قرار گیرد و توصیه می‌شود حق ممیزی برای کارفرما مورد تاکید قرار گیرد.
توصیه می‌شود هماهنگی‌های امنیتی مورد نیاز برای خدات خاص مانند ویژگی‌های امنیتی، سطوح خدمات، و الزامات مدیریت شناسایی شوند. توصیه می‌شود سازمان اطمینان حاصل کند که ارایه کنندگان خدمات شبکه توانایی انجام این خدمات را دارند.

اطلاعات دیگر

خدمات شبکه می‌تواند شامل پیش‌بینی و تامین ارتباطات، خدمات شبکه خصوصی، شبکه‌های ارزش افزوده و راه‌حل‌های امنیت شبکه نظیر دیوارهای آتش و سیستم‌های کشف ورود غیرمجاز باشد.
این خدمات ممکن است از ارایه عرض باند مدیریت نشده ساده تا خدمات ارزش افزوده پیچیده متغیر باشد.
ویژگی‌های امنیتی خدمات شبکه می‌تواند شامل موارد زیر باشد:

الف - فن‌آوری به کار رفته برای امنیت خدمات شبکه نظیر مجوز دهی، رمزنگاری و کنترل‌های امنیت شبکه
ب - پارامترهای فنی موردنیاز برای ارتباط امن با خدمات شبکه مطابق با قوانین ارتباطات شبکه و امنیت
پ - رویه‌هایی برای استفاده از خدمات شبکه جهت محدود کردن دسترسی به خدمات یا کاربردهای شبکه در صورت لزوم

۱۰-۷ اداره‌کردن محیطهای ذخیره‌سازی

هدف : پیشگیری از افشاء، دستکاری، خروج یا تخریب غیر مجاز دارایی‌ها و وقفه در فعالیتهای کسب‌وکار.
توصیه می‌شود محیطهای ذخیره‌سازی اطلاعات کنترل و بصورت فیزیکی محافظت شوند.
توصیه می‌شود روش‌های اجرایی عملیاتی مناسب برقرار بکار برده شود تا از مدارک و محیطهای ذخیره‌سازی (برای مثال، نوارها، دیسک‌ها)، داده های ورودی/خروجی و مستندات سیستم در برابر افشاء، تغییر، حذف و جابجایی غیرمجاز حفاظت بعمل آید.

۱۰-۷-۱ *مدیریت محیطهای ذخیره‌سازی قابل جابجایی*

کنترل

توصیه می‌شود برای مدیریت محیط‌های ذخیره‌سازی قابل جابجایی، روش‌های اجرایی اتخاذ شود.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای مدیریت رسانه های قابل انتقال در نظر گرفته شود:

الف - توصیه می‌شود محتوای هر یک از رسانه‌های چندبار مصرف که مورد نیاز نیستند و باید از سازمان دور ریخته شوند. توصیه می‌شود به نحوی از روی رسانه پاک شوند که دیگرقابل بازیابی نباشند
ب - هر زمان که لازم و امکان پذیر باشد، توصیه می‌شود دور ریختن رسانه‌ها و محیط‌های ذخیره اطلاعات با اخذ مجوز انجام پذیرد و یک نسخه از آن مجوز در سوابق و مستندات حفظ شود.
پ - توصیه می‌شود تمام رسانه‌ها و محیط‌های ذخیره اطلاعات در یک محیط امن و ایمن مطابق با مشخصات تولید کننده نگهداری شوند.

ت - توصیه می‌شود اطلاعات ذخیره شده در رسانه‌ها که باید بیش از طول عمر رسانه در دسترس باقی بمانند (مطابق با مشخصات سازندگان) توصیه می‌شود در جای دیگری نیز نگهداری شوند تا از آسیب به اطلاعات به دلیل خرابی رسانه جلوگیری شود

ث - توصیه می‌شود تعداد و مشخصات محیط‌های ذخیره اطلاعات که قابل انتقال هستند در محلی ثبت شود تا احتمال از دست رفتن اطلاعات به دلیل انتقال آنها به محل دیگر کاهش یابد.

ج - توصیه می‌شود درایوهای مربوط به محیط‌های ذخیره اطلاعات قابل انتقال فقط زمانی فعال باشند که دلیل خاصی در کسب وکار برای آن وجود داشته باشد.

توصیه می‌شود تمام رویه ها و سطوح ارابه مجوز به طور شفاف مستند شود.

اطلاعات دیگر

رسانه‌های قابل انتقال شامل نوارها، دیسک‌ها، حافظه‌های کوچک، دیسک‌های سخت قابل انتقال، سی دی‌ها، دی وی دی‌ها و رسانه‌های چاپی هستند.

۱۰-۷-۲ امحای محیطهای ذخیره‌سازی

کنترل

محیط‌های ذخیره‌سازی که دیگر مورد نیاز نیستند، توصیه می‌شود با بکارگیری روش‌های اجرایی رسمی، به صورت امن و محافظت شده، امحا شوند.

راهنمای پیاده سازی

توصیه می‌شود با بکارگیری رویه‌های رسمی برای دور ریختن امن رسانه‌ها، خطر نشت اطلاعات حساس به افراد غیرمجاز را کاهش دهید. رویه‌های مورد استفاده برای دور ریز امن رسانه‌هایی که حاوی اطلاعات حساس هستند، توصیه می‌شود باید 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، به گونه ای امن و ایمن نگهداری و یا دور ریخته شوند؛ برای مثال بوسیله سوزاندن یا تکه تکه کردن، یا پاک کردن کامل داده‌ها برای استفاده در کاربرد دیگری در داخل سازمان

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

پ - ممکن است جمع آوری و امحاء امن و مطمئن و دسته جمعی تمام رسانه‌هایی که باید دور ریخته شوند راحت تر از جدا سازی رسانه‌های حاوی اطلاعات حساس و امحاء جداگانه آنها باشد.

ت - بسیاری از سازمان‌ها خدمات جمع آوری و دور ریز رسانه‌های کاغذی خود را به پیمانکاران خارج از سازمان واگذار می‌کنند؛ توصیه می‌شود در انتخاب پیمانکار مناسب و با تجربه کافی، دقت لازم به عمل آید.

ث - توصیه می‌شود در صورت امکان دورریختن موارد حساس ثبت شود تا سوابق آنها وجود داشته باشد.

در زمان انباشته کردن اطلاعات برای دورریختن، توصیه می‌شود ملاحظات کافی در مورد تاثیر تجمعی آن بعمل آید تا حجم زیاد اطلاعات غیر حساس به اطلاعات حساس تبدیل نشوند.

اطلاعات دیگر

اطلاعات حساس ممکن است بواسطه دور ریختن بی دقت رسانه‌ها افشا شوند (برای کسب اطلاعات درباره دور ریختن تجهیزات، رجوع کنید به ۹-۲-۶)

۱۰-۷-۳ روش‌های اجرایی جابجایی اطلاعات

کنترل

توصیه می‌شود روش‌های اجرایی انتقال و انبارش اطلاعات، برای حفاظت این اطلاعات در برابر افشای غیر مجاز یا استفاده نابجا، تدوین شوند.

راهنمای پیاده سازی

توصیه می‌شود رویه‌هایی برای رفتار، پردازش، ذخیره، و انتقال اطلاعات مطابق با طبقه‌بندی آنها در نظر گرفته شود (رجوع کنید به ۷-۲). توصیه می‌شود موارد زیر مورد توجه قرار گیرد:

الف - برچسب زدن و رفتار با تمام رسانه‌ها بر اساس سطح طبقه‌بندی آنها.

ب – اعمال محدودیت‌های دسترسی برای پیشگیری از دسترسی کارکنان غیرمجاز

پ - نگهداری سوابق رسمی رسید داده‌ها بصورت مجاز

ت - اطمینان از ورود کامل داده‌ها و تکمیل پردازش به طور مناسب و سنجش صحت داده‌های خروجی.

ث - محافظت از داده‌های خاص که منتظر ورود به سطحی سازگارتر با حساسیت خود هستند.

ج - نگهداری از رسانه‌ها مطابق با مشخصات تولید کنندگان

چ - حفظ توزیع داده‌ها در سطح حداقل ممکن

ح - علامت گذاری واضح تمام نسخ رسانه‌ها برای توجه دریافت کننده مجاز

خ - بررسی فهرست‌های توزیع کنندگان و دریافت کنندگان مجاز در فواصل زمانی منظم

اطلاعات دیگر

این رویه‌ها در مورد اطلاعات مستند، سیستم‌های رایانه‌ی، شبکه‌ها، تجهیزات محاسبه متحرک، تجهیزات ارتباطی متحرک، نامه‌ها، ارتباطات صوتی به هر شکل آن، خدمات چند رسانه‌ای، امکانات و خدمات پستی، استفاده از دستگاه‌های نمابر و هر مورد حساس دیگر مانند چک‌های بانکی و فاکتورها به کار می روند.

۱۰-۷-۴ امنیت مستندات سیستم

کنترل

توصیه می‌شود مستندات سیستم در برابر دسترسی غیر مجاز، حفاظت شوند.

راهنمای پیاده سازی

برای ایمن سازی مستندسازی سیستم‌ها توصیه می‌شود موارد زیر مدنظر قرار گیرد:

الف - توصیه می‌شود مستندات سیستم‌ها به صورت مطمئن نگهداری شوند.

ب - توصیه می‌شود فهرستی حداقلی از افراد مجاز دارای دسترسی به مستندات سیستم‌ها توسط مالک آن برنامه کاربردی تهیه شود.

پ - توصیه می‌شود مستندات سیستم‌هایی که در شبکه‌های عمومی نگه داشته می‌شوند یا از طریق یک شبکه عمومی تامین می‌شوند باید به طور مناسب محافظت شوند.

اطلاعات دیگر

مستندات یک سیستم ممکن است شامل دامنه‌ای از اطلاعات حساس مانند شرح کاربردها، فرایندها، رویه‌ها، ساختارهای داده‌ها و فرایندهای مجوز دهی باشد.

۱۰-۸ تبادل اطلاعات

هدف : حفظ امنیت اطلاعات و نرم‌افزارهای قابل تبادل یک سازمان با هر موجودیت بیرونی.
توصیه می‌شود مبادلات اطلاعات و نرم‌افزارها بین سازمان‌ها براساس خط‌مشی رسمی مبادلات باشد، که هم‌راستا با توافق‌نامه‌های مبادله بوده و با قوانین حقوقی تطابق دارد (به بند ۱۵ رجوع کنید)
توصیه می‌شود روش‌های اجرایی و استانداردهایی برای حفاظت از اطلاعات و رسانه فیزیکی حاوی اطلاعات درحال عبور، اعمال شود.

۱۰-۸-۱ *خط‌مشی‌ها و روش‌های اجرایی تبادل اطلاعات*

کنترل

توصیه می‌شود برای حفاظت تبادل اطلاعات از طریق هر نوع محیط ارتباطی، خط‌مشی‌ها و روش‌های‌اجرایی رسمی تبادل اطلاعات تدوین شود.

راهنمای پیاده‌سازی

رویه‌ها و کنترل‌هایی که باید در زمان استفاده از تجهیزات ارتباطات الکترونیکی برای تبادل اطلاعات مورد توجه قرار گیرند عبارتند از:

الف - رویه‌های طراحی شده برای محافظت از اطلاعات در برابر دستبرد، نسخه برداری، تغییر، گمراه کردن و تخریب؛

ب - رویه‌هایی برای کشف و محافظت در برابر کدهای مخرب که ممکن است با استفاده از ارتباطات الکترونیکی منتقل شوند (رجوع کنید به بند ۱۰-۴-۱)؛

پ - رویه‌هایی برای محافظت از اطلاعات الکترونیکی حساس مبادله شده که به شکل فایل ضمیمه هستند.

ت - خط مشی یا دستورالعمل‌هایی که استفاده قابل قبول از تجهیزات ارتباطات الکترونیکی را تعریف می‌کنند (رجوع کنید به بند ۷-۱-۳).

ث – روش‌های اجرایی برای استفاده از ارتباطات بی‌سیم، با در نظر گرفتن ریسک‌های مربوطه

ج – تعیین مسوولیت، کارکنان، پیمانکاران، و هر کاربر دیگر برای این که به سازمان آسیب نرساند، مثلا از طریق بدنام کردن، آزار رسانی، جعل هویت، رد کردن نامه ای زنجیره ای، خرید غیرمجاز، و...؛

چ – استفاده از روش‌های رمزنگاری؛ برای مثال، برای حفاظت از محرمانگی، تمامیت و صحت اطلاعات (رجوع کنید به بند۱۲-۳)

ح - دستورالعمل‌های حفظ و دور ریز برای تمام مکاتبات کسب وکار از جمله پیام‌ها، مطابق با قوانین و مقررات ملی و محلی؛

خ - عدم رها کردن اطلاعات حساس در تجهیزات چاپ، مانند دستگاه تکثیر، چاپگر، و دستگاه‌های نمابر، زیرا این اطلاعات ممکن است توسط افراد غیرمجاز مورد دسترسی قرار گیرد.

د - کنترل‌ها و محدودیت‌های مربوط به هدایت امکانات ارتباطی مانند انتقال خودکار نامه الکترونیکی به نشانی‌های خارجی

ذ - یادآوری به کارکنان درباره رعایت احتیاط لازم. مثلا در حین مکالمات تلفنی اطلاعات حساس را علنی نسازند تا از دستبرد به آن توسط موارد زیر اجتناب شود:

۱ - افرادی که در نزدیکی آنها هستند به خصوص در زمان استفاده از تلفن همراه

۲ - استراق سمع و شکل‌های دیگر شنود از طریق دسترسی فیزیکی به گوشی تلفن یا خط تلفن با استفاده از تجهیزات شنود خط

۳ - افرادی که در طرف دیگر خط هستند

ر - عدم ارسال پیام‌هایی که حاوی اطلاعات حساس هستند به دستگاه‌های پاسخگو، زیرا این اطلاعات ممکن است توسط اشخاص غیرمجاز مورد دسترسی قرار گیرند و یا در سیستم‌های اشتراکی ذخیره شوند یا در اثر شماره گیری اشتباه در جای دیگری ذخیره شوند؛

ز - یادآوری به کارکنان درباره مشکلات استفاده از دستگاه‌های نمابر مخصوصا موارد ذیل :

۱ - دسترسی غیرمجاز به پیام‌های ذخیره شده و بازیابی پیام‌ها

۲ - برنامه ریزی عمدی یا تصادفی ماشین‌ها برای ارسال پیام‌ها به شماره‌های خاص

۳ - ارسال اسناد و پیام‌ها به شماره اشتباه از طریق شماره گیری اشتباه یا شماره ای که به اشتباه ذخیره شده است.

ژ - یادآوری به کارکنان درباره عدم ذخیره داده‌های مربوط به مشخصات افراد نظیر نشانی پست الکترونیکی یا دیگر اطلاعات کارکنان در هر نرم‌افزار برای اجتناب از دسترسی سایر افراد و استفاده غیرمجاز

س - یادآوری به کارکنان درباره این که ماشین‌های نمابر و تکثیر مدرن در صورت خطای کاغذی یا خطا در انتقال قابلیت ذخیره اطلاعات دارند و به محض رفع مشکل اطلاعات قابل چاپ می باشد.

به علاوه، توصیه می‌شود به کارکنان یادآوری شود که مکالمات محرمانه خود را در مکان‌های عمومی یا اماکنی که بدون دیوار و باز هستند و در مکان‌هایی که دیوارها دارای عایق صوتی نمی‌باشند انجام ندهند.

توصیه می‌شود تجهیزات تبادل اطلاعات، الزامات قانونی مربوطه را رعایت نمایند (رجوع کنید به بند ۱۵).

اطلاعات دیگر

تبادل اطلاعات ممکن است با استفاده از تعدادی از انواع مختلف تجهیزات تبادل اطلاعات از جمله پست الکترونیکی، خدمات صوتی، نمابر و ویدیو انجام شود.

تبادل نرم‌افزارها ممکن است از طریق تعدادی از رسانه‌های مختلف از جمله دریافت از اینترنت و خرید از فروشندگانی که این محصولات را می فروشند انجام شود.

توصیه می‌شود روال‌های قانونی و امنیتی تبادل اطلاعات الکترونیکی، تجارت الکترونیکی، و ارتباطات الکترونیکی مربوط به کسب وکار و الزامات لازم برای اعمال کنترل‌ها، تهیه و اجرا شوند.

اطلاعات ممکن است به دلیل فقدان آگاهی، خط‌مشی و روش‌های اجرایی مربوط به استفاده از تجهیزات تبادل اطلاعات مثلا شنیده شدن مکالمه با تلفن همراه در اماکن عمومی، اشتباه در ارسال نامه‌های الکترونیکی یا ارسال تصادفی نمابر به تجهیزات مقصد اشتباه، مورد دسترسی غیر مجاز قرار گیرد.
در صورت خرابی تجهیزات ارتباطی یا اعمال بار اضافه به آنها و یا وقفه در عملکرد آنها عملیات کسب وکار ممکن است مختل شده و امنیت اطلاعات به مخاطره بیفتد.(رجوع کنید به ۱۰-۳ و بند ۱۴). اطلاعات می‌توانند به‌خطر بیافتند در صورتی که بوسیله کاربران غیرمجاز مورد دسترسی قرار گیرند (رجوع کنید به بند ۱۱).

۱۰-۸-۲ *توافق‌نامه‌های تبادل*

کنترل

برای تبادل اطلاعات و نرم‌افزار بین سازمان‌ها و مخاطبان بیرونی آنها، توصیه می‌شود توافق‌نامه‌هایی تهیه شود.

راهنمای پیاده‌سازی

توصیه می‌شود در قراردادهای تبادل ملاحظات امنیتی زیر لحاظ شوند:

الف - مسیولیت‌های مدیریت در زمینه کنترل و اعلام انتقال، ارسال و دریافت

ب - رویه‌هایی برای مطلع ساختن فرستنده از انتقال،ارسال و دریافت

پ - رویه‌هایی برای تضمین قابلیت پیگیری و عدم انکار

ت - حداقل استانداردهای فنی برای بسته بندی و انتقال

ث - قراردادهای وجه الضمان

ج - استانداردهای شناسایی پیک

چ - مسوولیت‌ها و تعهدات در صورت بروز حوادث امنیت اطلاعات نظیر آسیب به داده‌ها

ح - استفاده از یک سیستم برچسب زنی مورد توافق برای اطلاعات حساس یا حیاتی، و اطمینان از این که معنای برچسب بلافاصله فهمیده می‌شود و این که اطلاعات به طور مناسب مورد پشتیبانی قرار می‌گیرد.

خ - مالکیت و مسوولیت‌هایی برای محافظت از داده‌ها، حق تکثیر، رعایت پروانه‌های نرم‌افزاری و ملاحظات مشابه (رجوع کنید به بند ۱۵-۱-۲ و ۱۵-۱-۴)

د - استانداردهای فنی برای ثبت و خواندن اطلاعات و نرم‌افزارها

ذ - هر کنترل خاصی که ممکن است برای محافظت از موارد حساس نظیرکلیدهای رمزگشایی لازم باشد. (رجوع کنید به بند ۱۲-۳)

توصیه می‌شود خط مشی‌ها، رویه‌ها و استانداردهایی برای محافظت از اطلاعات و رسانه‌های فیزیکی در انتقال، ایجاد و اعمال شود (همچنین رجوع کنید به بند ۱۰-۸-۳) و توصیه می‌شود در قراردادهای تبادل به آنها اشاره شود. توصیه می‌شود محتوای امنیتی هر قرارداد نشان دهنده حساسیت اطلاعات کسب وکار مربوطه باشد.

اطلاعات دیگر

قراردادها می‌توانند الکترونیکی یا دستی و به شکل قراردادها یا مفاد استخدام رسمی باشند. توصیه می‌شود برای اطلاعات حساس مکانیسم‌های خاص به‌کار رفته برای تبادل برای تمام سازمان‌ها و انواع قراردادها یکسان باشد.

۱۰-۸-۳ محیط‌های ذخیره‌سازی (رسانه) فیزیکی، حین حمل‌ونقل

کنترل

توصیه می‌شود محیط‌های ذخیره‌سازی حاوی اطلاعات در هنگام حمل‌ونقل خارج از مرزهای فیزیکی سازمان، در برابر دسترسی غیر مجاز، استفاده نابجا یا صدمه، محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود دستورالعمل‌های زیر برای محافظت از رسانه‌هایی که بین سایت‌های مختلف انتقال داده می‌شوند رعایت شود:

الف - توصیه می‌شود از حمل یا پیک قابل اطمینان استفاده شود

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

پ – توصیه می‌شود روش‌های اجرایی برای بررسیِ هویت پیک‌ها تدوین شود.

ت - توصیه می‌شود از بسته بندی مناسب برای محافظت از محتویات بسته‌ها دربرابر هر گونه آسیب فیزیکی احتمالی در طول حمل و مطابق با تمام مشخصات تولید کننده استفاده شود، مثلا محافظت در برابر هر فاکتور محیطی که ممکن است به محتوی رسانه‌ها خسارت وارد نماید نظیر قرار گرفتن در معرض گرما، رطوبت یا میدان‌های الکترومغناطیسی.

ث - توصیه می‌شود کنترل‌هایی در صورت امکان به کار گرفته شوند تا از اطلاعات حساس دربرابر افشا غیرمجاز یا تغییرات محافظت کنند، مثلا:

۱ - استفاده از جعبه‌های قفل‌شده

۲ - تحویل دستی

۳ - بسته بندی غیرقابل دستکاری، که هر گونه اقدامی برای دسترسی را نشان می‌دهد.

۴ - در موارد خاص، تقسیم محموله به بیش از یک محموله و ارسال از مسیرهای مختلف

اطلاعات دیگر

اطلاعات ممکن است دربرابر دسترسی غیر مجاز، سوء استفاده، یا اختلال در طول حمل فیزیکی مثلا در زمان ارسال رسانه‌ها از طریق خدمات پست یا یک پیک آسیب‌پذیر باشد.

۱۰-۸-۴ پیام‌رسانی الکترونیکی

کنترل

توصیه می‌شود اطلاعات مورد بحث در پیام‌رسانی الکترونیکی به صورت مناسبی حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیتی برای پیام‌های الکترونیکی شامل موارد زیر رعایت شود:

الف - محافظت از پیام‌ها در برابر دسترسی غیرمجاز، تغییرات، یا جلوگیری از ارایه خدمات

ب - اطمینان از آدرس‌دهی و حمل صحیح پیام،

پ - قابلیت اطمینان عمومی و دسترسی به خدمات

ت - ملاحظات حقوقی مثلا الزاماتی برای امضاهای الکترونیکی

ث - کسب مجوز قبل از استفاده از خدمات همگانی نظیر پیام سریع یا اشتراک شبکه‌ها

ج - سطوح قوی‌تر تعیین هویت جهت دسترسی به شبکه‌های عمومی

اطلاعات دیگر

انتقال پیام الکترونیکی نظیر پست الکترونیکی، تبادل اطلاعات الکترونیکی. پیام رسانی الکترونیکی نقش مهمی در تبادلات تجاری امروز دارند که البته ریسک‌های آن در مقایسه با ارتباطات کاغذی متفاوت است.

۱۰-۸-۵ سیستم‌های اطلاعاتی کسب‌وکار

کنترل

توصیه می‌شود به منظور حفاظت اطلاعات مربوط به ارتباطات داخلی سیستم‌های اطلاعاتی کسب‌وکار، خط‌مشی‌ها و روش‌های اجرایی مربوطه ایجاد و پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات مربوط به آثار امنیتی و کسب وکار ارتباط این تجهیزات شامل موارد زیر باشد:

الف - آسیب‌پذیری‌های شناخته شده در سیستم‌های اجرایی و حسابداری در جایی که اطلاعات بین بخش‌های مختلف سازمان متفاوت است؛

ب - آسیب‌پذیری‌های اطلاعات در سیستم‌های ارتباطات کسب وکار مثلا درباره تماس‌های تلفنی یا کنفرانس مکالمات، محرمانگی تماس‌ها، ذخیره نمابرها، بازکردن و توزیع نامه‌ها

پ - خط مشی و کنترل‌های مناسب برای مدیریت اشتراک اطلاعات

ت - خارج ساختن طبقاتی از اطلاعات حساس کسب وکار و اسناد طبقه بندی شده در صورتی که سیستم سطح مناسبی از محافظت را ارایه نمی‌کند. (رجوع کنید به بند ۷-۲)

ث – محدود کردن دسترسی به گزارشات روزانه افراد خاص؛ برای مثال، کارکنانی که در پروژه‌های حساس کار می‌کنند.

ج – رده‌بندی کارکنان، پیمانکاران یا شرکای کسب وکار مجاز به استفاده از سیستم و محل‌هایی که ممکن است سیستم از آنجا مورد دسترسی قرار گیرد (رجوع کنید به بند ۶-۲ و بند ۶-۳)؛

ج - محدود کردن دسترسی به اطلاعات دفتر یادداشت افراد خاص مانند کارکنانی که در پروژه‌های حساس کار می‌کنند؛

چ - شناسایی وضعیت کاربران مانند کارکنان سازمان یا پیمانکاران در دفاتر یادداشت برای استفاده کاربران دیگر

ح - حفظ و کپی‌پشتیبانی گرفتن از اطلاعاتی که در سیستم‌ها نگهداری می‌شود (رجوع کنید به بند ۱۰-۵-۱)

خ - الزامات و تنظیمات انجام مجدد (رجوع کنید به بند ۱۴)

اطلاعات دیگر

سیستم‌های اطلاعات اداری فرصت‌هایی هستند برای انتشار و اشتراک سریع تر اطلاعات کسب وکار با استفاده از ترکیبی از اسناد، رایانه‌ها، محاسبه گرهای سیار، ارتباطات سیار، پست، پیام صوتی، ارتباطات صوتی در هر شکل آن خدمات و امکانات پستی، ماشین‌های نمابر.

۱۰-۹ خدمات تجارت الکترونیک

هدف: حصول اطمینان از امنیت خدمات تجارت الکترونیکی و استفاده ایمن از آنها.
توصیه می‌شود تاثیرات امنیتی در رابطه با استفاده از خدمات تجارت الکترونیکی، از جمله تعاملات برخط، و الزامات کنترلی مربوطه، در نظر گرفته شود. همچنین توصیه می‌شود یکپارچگی و در دسترس بودن به اطلاعاتی که به صورت الکترونیکی از طریق سیستم‌های عمومی منتشر می‌شوند، در نظر گرفته شود.

۱۰-۹-۱ *تجارت الکترونیک*

کنترل

اطلاعات مورد استفاده در تجارت الکترونیکی که از شبکه‌های عمومی عبور می‌کنند، توصیه می‌شود در برابر اقدامات کلاه برداری، مناقشات در قرارداد، و افشا و دستکاری غیر مجاز، محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیتی برای تجارت الکترونیکی شامل موارد زیر باشد:

الف - سطح اطمینان مورد نیاز هر یک از طرفین نسبت به هویت مورد ادعای طرف دیگر مثلا از طریق مجوز دهی.

ب - فرایند مجوز دهی در رابطه با هر کسی که ممکن است قیمت‌ها را تعیین کند و اسناد مهم کسب وکار را صادر یا امضا کند؛

پ - حصول اطمینان از این که شرکای کسب وکار کاملا از اختیارات خود مطلع هستند؛

ت - تعیین و رعایت الزامات محرمانگی، یکپارچگی، اثبات ارسال و دریافت اسناد کلیدی، و عدم دستکاری قراردادها مثلا در رابطه با فرایندهای مناقصه یا قرارداد

ث - سطح اطمینانی که در یکپارچگی لیست قیمت‌های اعلام شده لازم است

ج - محرمانگی هر یک از داده‌ها یا اطلاعات حساس

چ - محرمانگی و یکپارچگی هر یک از تعاملات، اطلاعات پرداخت، جزییات نشانی تحویل، و تایید رسیدها

ح - تعیین سطح مناسب کنترل اطلاعات پرداخت که توسط مشتری ارایه شده است.

خ - انتخاب مناسب ترین نحوه پرداخت برای محافظت در برابر تقلب و کلاه‌برداری

د - سطح محافظت مورد نیاز برای حفظ محرمانگی و یکپارچگی اطلاعات سفارش

ر - اجتناب از خرابی یا تکرار در اطلاعات تعاملات

ز - مسوولیت در قبال انجام تعاملات جعلی

ج - الزامات بیمه

بسیاری از ملاحظات فوق را می‌توان با استفاده از کنترل‌های رمزگشایی(رجوع کنید به بند ۱۲-۳) با احتساب رعایت الزامات قانونی مورد رسیدگی قرار داد (رجوع کنید به بند ۱۵-۱، مخصوصا بند ۱۵-۱-۶ برای وضع قوانین رمزنگاری). توصیه می‌شود توافقات تجارت الکترونیکی بین شرکای کسب وکار، توسط یک قرارداد مستند که هر دو طرف را به رعایت مفاد مورد توافق تجارت، از جمله جزییات اختیارات ملزم کند پشتیبانی شود (رجوع کنید به مورد ب در بالا). قراردادهای دیگری هم با ارایه دهندگان خدمات اطلاعاتی و خدمات ارزش افزوده شبکه ممکن است ضروری باشد.

توصیه می‌شود سیستم‌های تجارت همگانی، مفاد تجارت خود را به اطلاع مشتریان برسانند.
توصیه می‌شود ملاحظات لازم برای ایجاد انعطاف پذیری در سیستم در برابر حمله به سایت میزبان مورد استفاده برای تجارت الکترونیکی و الزامات امنیتی هر یک از ارتباطات متقابل شبکه که برای اجرای خدمات تجارت الکترونیکی لازم است مورد توجه قرار گیرد. (رجوع کنید به بند ۱۱-۴-۶)

اطلاعات دیگر

تجارت الکترونیکی در مقابل تعدادی از تهدیدهای شبکه ای که ممکن است منجر به کلاهبرداری، اختلاف در قرارداد، و افشا یا تغییر اطلاعات شوند آسیب‌پذیر است.
تجارت الکترونیکی، می‌تواند از روش‌های امن احراز اصالت استفاده کند. برای مثال می‌تواند از رمز نگاری کلید همگانی و امضاهای دیجیتال(رجوع کنید به بند ۱۲-۳) برای کاهش ریسک استفاده کند. همچنین از اشخاص ثالث امین می‌توان در زمانی که به این خدمات نیاز است استفاده کرد.

۱۰-۹-۲ *تراکنش های برخط*

کنترل

توصیه می‌شود اطلاعات مورد استفاده در داد و ستدهای برخط، به منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه، تغییر یافتن غیر مجاز پیغام، افشای غیر مجاز، بازگرداندن یا تکرار غیر مجاز پیغام، حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیتی برای تعاملات برخط، شامل موارد زیر باشد:

الف - استفاده از امضاهای الکترونیکی توسط هر یک از طرفین دخیل در معامله

ب – رعایت تمام جنبه‌های معامله برای اطمینان حصول اطمینان از اینکه:

۱ - مدارک طرفین معتبر و تایید شده است

۲ - معامله محرمانه باقی می ماند؛ و

۳ - محرمانگی اطلاعات مربوط به تمام طرفین حفظ می‌شود

پ - مسیر ارتباطی بین تمام طرفین رمز می‌شود.

ت - پروتکل‌های به‌کار رفته برای ارتباط بین تمام طرفین ایمن است؛

ث - اطمینان از قرارگیری جزییات معامله در مکانی خارج از دسترسی عموم مثلا در یک سکوی ذخیره سازی که در اینترانت سازمان قرار دارد، و نه بر روی رسانه‌هایی که مستقیما در دسترس همگان است.

ج - در جایی که از یک مرجع مورد اطمینان استفاده می‌شود (مثلا، برای صدور و حفظ امضاهای دیجیتال و/یا گواهینامه‌های دیجیتال)، امنیت در سراسر فرایند مدیریت انتهابه‌انتهای امضا/گواهینامه، اعمال شود.

اطلاعات دیگر

میزان کنترل‌های به‌کار رفته باید با سطح ریسک‌های مربوط به هر معامله برخط تناسب داشته باشد.
تراکنش‌ها باید با قوانین، احکام و مقررات قضایی جایی که در آن ایجاد یا پردازش و یا نگهداری می‌شوند مطابقت داشته باشند.
بسیاری از شکل‌های معاملاتی وجود دارند که ممکن است به گونه ای برخط اجرا شوند مثلا قراردادی، مالی و غیره.

۱۰-۹-۳ *اطلاعات قابل دسترس عموم*

کنترل

توصیه می‌شود یکپارچگی اطلاعاتی که در یک سیستم در قابل دسترس عموم قرار می‌گیرد، به منظور پیشگیری از دستکاری غیر مجاز، باید محافظت شود.

راهنمای پیاده‌سازی

توصیه می‌شود نرم‌افزارها، داده‌ها، و اطلاعات دیگری که نیازمند سطح بالایی از یکپارچگی هستند و در یک سیستم قابل دسترس عموم قرار دارند توسط مکانیسم‌های مناسب مثلا امضاهای دیجیتال محافظت شوند (رجوع کنید به بند ۱۲-۳). برای سیستمی که در دسترس همگان قرار می گیرد، توصیه می‌شود قبل از ارایه دسترسی باید ضعف‌ها و مشکلات کاملا بررسی شود.

توصیه می‌شود یک فرایند تایید رسمی قبل از این که اطلاعات در معرض دید همگان قرار گیرد وجود داشته باشد. بعلاوه، توصیه می‌شود، همه ورودی‌های تامین شده از خارج از سیستم تصدیق و تایید شوند.

توصیه می‌شود سیستم‌های انتشار الکترونیکی به خصوص سیستم‌هایی که انعکاس و ورود مستقیم اطلاعات را امکان پذیر می‌کنند به دقت کنترل شوند به گونه ای که:

الف - اطلاعات مطابق با مقررات محافظت از داده‌ها به دست آید (رجوع کنید به بند ۱۵-۱-۴)؛

ب - اطلاعات ورودی به سیستم انتشار و اطلاعاتی که توسط آن پردازش می‌شود به طور کامل و دقیق و به موقع پردازش شوند؛

پ - اطلاعات حساس در طول زمان جمع آوری، پردازش، و ذخیره سازی محافظت شوند.

ت – ساختار دسترسی به سیستم انتشار، اجازه دسترسی غیر عمدی به شبکه‌هایی که سیستم به آنها متصل است را نمی‌دهد.

اطلاعات دیگر

اطلاعات روی یک سیستم قابل دسترس عموم مانند اطلاعات سرور شبکه که از طریق اینترنت قابل دسترسی است، ممکن است نیازمند رعایت قانون و مقررات حوزه قضایی محل قرارگیری سرور، یا محل انجام معاملات و یا در جایی که مالک (ها) سکونت دارند باشد. تغییر غیرمجاز اطلاعات منتشر شده ممکن است به خوش‌نامی سازمان منتشر کننده آسیب برساند.

۱۰-۱۰ پایش

هدف: تشخیص فعالیتهای غیر مجاز پردازش اطلاعات.

توصیه می‌شود بر فعالیت سیستم‌ها نظارت شده و توصیه می‌شود اتفاقات امنیت اطلاعات ضبط شود. توصیه می‌شود اطلاعات ثبت وقایع کاربر و ثبت وقایع خرابی برای اطمینان از اینکه مشکلات سیستم اطلاعاتی شناسایی شده‌اند مورد استفاده قرار گیرند.

توصیه می‌شود سازمان تمام الزامات قانونی در رابطه با نظارت و ثبت وقایع را رعایت کند.

توصیه می‌شود یک سیستم نظارت برای بررسی میزان اثربخشی کنترل های بکار رفته و تایید سهولت استفاده از مدل سیاست دسترسی، مورد استفاده قرار گیرد.

۱۰-۱۰-۱ واقعه‌نگاری ممیزی

کنترل

توصیه می‌شود سوابق ممیزی مشتمل بر فعالیت‌های کاربر، استثناها و وقایع امنیت اطلاعات، برای یک بازهٔ زمانی توافق شده، ایجاد و نگهداری شوند تا در رسیدگی‌های آتی و پایش کنترل دسترسی، مورد استفاده قرار گیرند.

راهنمای پیاده‌سازی

توصیه می‌شود گزارش‌های ممیزی شامل موارد زیر باشند:

الف - هویت کاربر

ب - تاریخ، زمان، و جزییات وقایع کلیدی، مانند ورود به/ خروج از سیستم

پ – شناسه یا محل ترمینال در صورت امکان

ت - سوابق مربوط به دسترسی‌های موفق و غیر موفق به سیستم

ث – سوابق مربوط به دسترسی‌های موفق و غیر موفق به داده‌ها و سایر منابع سیستم

ج - تغییرات در پیکربندی سیستم

چ - استفاده از حقوق دسترسی

ح - استفاده از کاربردها و امکانات سیستم

خ - فایل‌های مورد پردازش و نوع دسترسی

د - نشانی‌ها و پروتکل‌های شبکه

ذ - هشدارهای ایجادشده توسط سیستم کنترل دسترسی

ر – فعال‌سازی و غیرفعال‌سازی سیستم‌های مراقبت نظیر سیستم‌های ضد ویروس و سیستم‌های کشف مزاحمت

اطلاعات دیگر

گزارش‌های ممیزی ممکن است حاوی داده‌های شخصی افراد باشد. توصیه می‌شود اقدامات مناسب برای محافظت از محرمانگی این گزارشات به کار گرفته شود (همچنین رجوع کنید به بند ۱۵-۱-۴). توصیه می‌شود در صورت امکان، مجریان سیستم اجازه پاک کردن یا غیرفعال کردن گزارش‌های فعالیت خودشان را نداشته باشند (رجوع کنید به بند ۱۰-۱-۳).

۱۰-۱۰-۲ پایش کاربرد سیستم

توصیه می‌شود روش‌های‌اجرایی برای پایش کاربرد امکانات پردازش اطلاعات، ایجاد شده و نتایج فعالیت‌های پایش، به صورت منظم، بازبینی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود سطح مراقبت مورد نیاز برای تک تک تجهیزات از طریق ارزیابی ریسک تعیین شود. توصیه می‌شود سازمان از تمام الزامات قانونی مربوطه در مورد فعالیت‌های کنترلی اش پیروی کند. توصیه می‌شود موضوعاتی که باید مورد توجه قرار گیرند عبارتند از:

الف - دسترسی مجاز، از جمله جزییاتی نظیر

۱ - هویت کاربر

۲ - تاریخ و زمان وقایع کلیدی

۳ - نوع وقایع

۴ - فایل‌های مورد دسترسی

۵ – برنامه/امکانات استفاده شده

ب - تمام فعالیت‌های ویژه شامل :

۱ - استفاده از شناسه‌های کاربری ویژه مانند ناظر[1]، ریشه[2]، راهبر

۲ - راه اندازی و توقف سیستم

۳ - اتصال/جداکردن دستگاه I/O

پ - اقدامات دسترسی غیرمجاز نظیر:

۱ - فعالیت‌های مشکل دار یا رد شده

۲ - فعالیت‌های مشکل دار یا ردشده ای که از داده‌ها و سایر منابع استفاده می‌کنند.

۳ - تخلف از خط مشی دسترسی و هشدارهای مربوط به دروازه شبکه و دیوار آتش

۴ – هشدار از سیستم‌های کشف مزاحمت

ت - هشدارها یا خرابی‌های سیستم‌نظیر:

۱ - هشدارها یا پیام‌های کنسول

۲ - گزارش استثناها سیستم

۳ - هشدارهای مدیریت شبکه

۴ – هشدارهای ارایه شده توسط سیستم کنترل دسترسی

ث - تغییرات یا اقدام برای تغییر تنظیم سیستم امنیت و کنترل‌های آن

فواصل زمانی بررسی فعالیت‌های سیستم نظارتی باید منطبق با ریسک مرتبط با آن باشد. توصیه می‌شود عوامل ریسک در نظر گرفته شده شامل این موارد باشند:

الف - میزان حساسیت فرایندهای کاربردها

ب - ارزش، حساسیت، و حیاتی بودن اطلاعات به‌کار رفته؛

پ - تجربه گذشته نفوذ و سوء استفاده و فراوانی آسیب‌پذیری‌هایی که کشف می‌شوند؛

ت - میزان ارتباطات داخلی سیستم (بخصوص شبکه‌های عمومی)

ث - امکانات ثبت وقایع غیر فعال شده.

اطلاعات دیگر

استفاده از سیستم‌های نظارتی برای حصول اطمینان از اینکه کاربران فقط کارهایی را انجام می دهند که باید انجام دهند الزامی است.

بررسی سوابق نظارتی باعث درک تهدیدهای پیش روی سیستم و نحوه ایجاد آنها است. مثال‌های مربوط به وقایعی که ممکن است نیازمند بررسی بیشتر در صورت وقوع حوادث امنیت اطلاعات باشند در ۱۳-۱-۱ آمده است.

1- Supervisor
2- Root

۱۰-۱۰-۳ حفاظت از اطلاعات ثبت شدهٔ وقایع

کنترل

توصیه می‌شود امکانات واقعه‌نگاری و اطلاعات ثبت وقایع، در برابر دسترسی پنهانی و غیر مجاز، حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود هدف کنترل‌ها، محافظت از تغییرات غیرمجاز و مشکلات عملیاتی در تجهیزات ثبت وقایع باشد که شامل موارد زیر است:

الف - تغییرات در انواع پیام‌هایی که ثبت می‌شوند؛

ب - فایل‌های ثبت شده ای که ویرایش یا حذف می‌شوند

پ – محدودیت در ظرفیت رسانه‌های ثبت وقایع، که منجر به ناکامی در ثبت وقایع یا دوباره کاری وقایع ثبت شده در گذشته می‌شود.

بعضی از گزارش‌های ممیزی ممکن است به عنوان بخشی از خط‌مشی نگهداری گزارش وقایع یا به دلیل الزامات خاص، جمع آوری و بایگانی شوند. (همچنین رجوع کنید به بند ۱۳-۲-۳)

اطلاعات دیگر

گزارش‌های سیستم حاوی حجم وسیعی از اطلاعات است که بسیاری از آن برای کنترل امنیت، استفاده ای نداشته باشد. توصیه می‌شود برای کمک به شناسایی وقایع مهم کنترل امنیت، پیام‌های مربوط بصورت اتوماتیک به یک گزارش دیگر کپی شوند و/یا از ابزارهای ممیزی مناسب که فایل را بررسی و وقایع مهم را جدا می‌کنند استفاده شود. گزارشات ثبت وقایع سیستم باید محافظت شود زیرا اگر داده‌ها را بتوان تغییر داده و یا حذف نمود، وجود آنها ممکن است احساس نادرستی از امنیت ایجاد کند.

۱۰-۱۰-۴ اطلاعات ثبت‌شده وقایع مربوط‌به راهبر و اپراتور سیستم

کنترل

توصیه می‌شود وقایع فعالیت‌های راهبر و اپراتور سیستم ثبت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود گزارش‌ها شامل موارد زیر باشد:

الف - زمان وقوع حادثه

ب - اطلاعات مربوط به واقعه (فایل‌های مورد استفاده قرار گرفته) یا ناکامی (خطای اتفاق افتاده و اقدامات اصلاحی)

پ - کدام شناسه‌های کاربری، راهبر و اپراتور شرکت داشته اند.

ت - کدام فرایندها نقش داشتند

توصیه می‌شود گزارش‌های راهبر و اپراتور سیستم به صورت منظم بررسی شوند.

اطلاعات دیگر

یک سیستم کشف مزاحمت که خارج از کنترل راهبران سیستم و شبکه مدیریت می‌شود، را می‌توان برای کنترل فعالیت‌های راهبر شبکه و سیستم مورد استفاده قرار داد.

۱۰-۱۰-۵ واقعه‌نگاری خرابی

کنترل

توصیه می‌شود وقایع خرابی‌ها ثبت و تحلیل شده و اقدام مناسبی در رفع آنها انجام شود.

راهنمای پیاده‌سازی

توصیه می‌شود خطاهای گزارش شده توسط کاربران یا توسط برنامه‌های سیستم در رابطه با مشکلات پردازش اطلاعات یا سیستم‌های ارتباطات، ثبت شوند. توصیه می‌شود قوانین روشنی برای رسیدگی به خطاها وجود داشته باشد از جمله:

الف - بررسی گزارش‌های خطا برای تضمین این که خطاها به صورت رضایت بخش حل شده اند

ب - بررسی اقدامات اصلاحی برای تضمین این که کنترل‌ها نادرست نبوده اند و اینکه اقدام انجام شده کاملا مجاز است

اگر این امکان در سیستم وجود دارد باید از فعال بودن سیستم ثبت خطاها اطمینان حاصل نمود.

اطلاعات دیگر

ثبت خطاها و اشکالات ممکن است بر عملکرد یک سیستم تاثیر بگذارد. توصیه می‌شود این ثبت توسط کارکنان ذی‌صلاح انجام شود و سطح ثبت مورد نیاز برای تک تک سیستم‌ها توصیه می‌شود توسط یک ارزیابی ریسک با احتساب کاهش سطح عملکرد تعیین شود.

۱۰-۱۰-۶ همزمان‌سازی ساعت‌ها

کنترل

توصیه می‌شود ساعت‌های تمامی سیستم‌های پردازش اطلاعات مرتبط در درون یک سازمان یا دامنهٔ امنیتی، توصیه می‌شود با یک منبع زمانی دقیق توافق شده، همزمان شوند.

راهنمای پیاده‌سازی

در جایی که یک رایانه یا دستگاه ارتباطی قابلیت راه اندازی یک ساعت زمان واقعی را داشته باشد، توصیه می‌شود این ساعت، مطابق با یک استاندارد مورد توافق مثلا زمان جهانی هماهنگ[1]. یا زمان استاندارد محلی تنظیم شود، همانطور که بعضی از ساعت‌ها با زمان تغییر می‌کنند توصیه می‌شود رویه‌ای باشد که هر گونه تغییرمهم را اصلاح کند.

تفسیر صحیح فورمت تاریخ زمان، برای تضمین این که ثبت کننده زمان نشان دهنده زمان واقعی است، مهم است. توصیه می‌شود تغییرات ساعت تابستانی مد نظر قرار گیرد.

اطلاعات دیگر

تنظیم صحیح ساعت‌رایانه‌ها برای تضمین دقت گزارش‌های ممیزی مهم است و نشان دهنده دقت گزارش است و ممکن است لازم باشد در تحقیقات و یا دادگاه به آن استناد شود.

گزارش‌های ممیزی غیردقیق، ممکن است مانع از این بررسی‌ها شود و به اعتبار این شواهد خدشه وارد کند. ساعتی که با ساعت یک فرستنده رادیویی مرتبط به ساعت اتمی ملی همزمان است، می‌تواند به عنوان یک ساعت اصلی برای سیستم‌های ثبت کننده مورد استفاده قرار گیرد. یک پروتکل زمان شبکه را می‌توان برای حفظ تمام سرورها به صورت همزمان با ساعت اصلی مورد استفاده قرار داد.

1- Coordinated Universal Time (UTC)

۱۱ کنترل دسترسی

۱-۱۱ الزامات کسب‌وکار برای کنترل دسترسی

هدف: کنترل دسترسی به اطلاعات.

توصیه می‌شود دسترسی به اطلاعات، امکانات پردازش اطلاعات و پردازش‌های تجاری براساس الزامات امنیتی و تجاری کنترل شود.

توصیه می‌شود در قوانین کنترل دسترسی خط مشی های مربوط به انتشار و تایید اطلاعات لحاظ شوند.

۱-۱-۱ *خط‌مشی کنترل دسترسی*

کنترل

توصیه می‌شود یک خط‌مشی کنترل دسترسی بر مبنای الزامات کسب‌وکار و الزامات امنیتی در خصوص دسترسی، ایجاد، مدون و بازنگری شود.

راهنمای پیاده‌سازی

توصیه می‌شود قوانین و مقررات کنترل دسترسی برای هر کاربر یا گروه کاربران، به روشنی در یک خط‌مشی کنترل دسترسی بیان شود. کنترل‌های دسترسی هم منطقی و هم فیزیکی هستند(همچنین رجوع کنید به بخش ۹) و توصیه می‌شود اینها با هم در نظر گرفته شوند. توصیه می‌شود کاربران و ارایه کنندگان خدمات بیانیه روشنی از الزامات کسب و کار توسط کنترل‌های دسترسی رعایت شوند دریافت کنند.

توصیه می‌شود در خط مشی موارد زیر لحاظ شود:

الف - الزامات امنیتی هر یک از برنامه های کاربردی تجاری

ب - شناسایی تمام اطلاعات مربوط به برنامه های کاربردی تجاری و ریسک‌هایی که اطلاعات با آنها مواجه خواهند بود.

پ - خط‌مشی هایی برای انتشار و تایید اطلاعات مانند قاعده نیاز به دانستن، و سطوح امنیتی و طبقه بندی اطلاعات (رجوع کنید به بند ۷-۲)

ت - سازگاری بین کنترل دسترسی و خط‌مشی های طبقه بندی اطلاعات سیستم‌ها و شبکه‌های مختلف

ث - قوانین مربوطه و هر یک از الزامات قراردادی درباره محافظت از دسترسی به داده‌ها یا خدمات (رجوع کنید به بند ۱۵-۱)

ج - شرح حال‌های دسترسی کاربر استاندارد برای قوانین شغل متعارف در سازمان

چ - مدیریت حقوق دسترسی در یک محیط توزیع شده و شبکه ای که تمام انواع اتصالات موجود را به رسمیت می شناسد.

ح - تفکیک نقش‌های کنترل دسترسی مانند، تقاضای دسترسی، تایید دسترسی، اجرای دسترسی

خ - الزامات مجوز دهی رسمی تقاضاهای دسترسی (رجوع کنید به بند ۱۱-۲-۱)

د - الزامات بررسی دوره ای کنترل‌های دسترسی (رجوع کنید به بند ۱۱-۲-۴)

ذ - از بین بردن حقوق دسترسی (رجوع کنید به بند ۸-۳-۳)

اطلاعات دیگر

توصیه می‌شود در زمان تعیین قوانین کنترل دسترسی موارد زیر لحاظ گردند:

الف - تمایز قائل شدن بین قوانینی که باید همیشه اجرا شوند و رهنمودهایی که اختیاری یا مشروط هستند؛
ب - تثبیت قوانین بر اساس این فرض "هر چیزی به طور کلی ممنوع است مگر این که صریحا اجازه داده شود" به جای این فرض که "هر چیزی عموما مجاز است مگر این که صریحا ممنوع شود"
پ - تغییرات در برچسب‌های اطلاعات(رجوع کنید به بند ۷-۲) که به طور خودکار توسط تجهیزات پردازش اطلاعات ایجاد می‌شوند و آنهایی که به اختیار کاربر ایجاد می‌شوند؛
ت – تغییراتِ مجوزهای کاربر که بطور خودکار توسط سیستم اطلاعاتی ایجاد می‌شود و آنهایی که بوسیله راهبر سیستم ایجاد می‌شود.
ث - قوانینی که نیازمند تایید ویژه قبل از اعمال می‌باشند و قوانینی که نیازمند تایید ویژه قبل از اعمال نمی‌باشند.

توصیه می‌شود قوانین کنترل دسترسی توسط روش‌های اجرایی رسمی و مسوولیت‌های تعیین شده پشتیبانی شوند. (برای مثال، رجوع کنید به بند ۶-۱-۳، ۱۱-۳، ۱۰-۴-۱، ۱۱-۶)

۱۱-۲ مدیریت دسترسی کاربر

هدف: حصول اطمینان از دسترسی کاربر دارای مجوز و پیشگیری از دسترسی غیر مجاز به سیستم‌های اطلاعاتی.
توصیه می‌شود روش‌های اجرایی رسمی برای کنترل تخصیص حقوق دسترسی به سیستم‌ها و خدمات اطلاعات در نظر گرفته شوند.
توصیه می‌شود روش‌های اجرایی تمام مراحل چرخه دسترسی کاربر را از ثبت اولیه کاربران جدید تا پایان ثبت نهایی کاربرانی که دیگر نیاز به دسترسی به سیستم‌ها و خدمات اطلاعاتی ندارند را پوشش دهند. توصیه می‌شود توجه خاصی در زمان مناسب به نیاز به کنترل تخصیص حقوق دسترسی برتر معطوف شود که به کاربران اجازه می‌دهد کنترل‌های سیستم را طی کنند.

۱۱-۲-۱ ثبت کاربر

کنترل

توصیه می‌شود برای اعطا یا لغو دسترسی به سیستم‌ها و خدمات اطلاعاتی، یک روش‌اجرایی رسمی ثبت و حذف کاربر وجود داشته باشد.

راهنمای پیاده‌سازی

توصیه می‌شود روش‌های اجرایی کنترل دسترسی برای ثبت و حذف کاربران شامل موارد زیر باشد:
الف - استفاده از شناسه های منحصر به فرد کاربر برای ایجاد امکان پذیرش مسوولیت فعالیت‌های کاربران توسط خود آنها؛ توصیه می‌شود استفاده از شناسه های گروهی فقط در صورتی مجاز شود که به دلایل کاری یا عملیاتی لازم باشد و توصیه می‌شود که تایید و مستند شوند.
ب - بررسی این که کاربر از مالک سیستم برای استفاده از سیستم و خدمات اطلاعات مجوز دارد؛ کسب تایید جداگانه از مدیریت برای حقوق دسترسی نیز می‌تواند مناسب باشد.

پ - بررسی این که سطح دسترسی اعطا شده متناسب با اهداف کاری (رجوع کنید به بند ۱۱-۱) و با خط‌مشی امنیت سازمانی سازگار است به عنوان مثال به تفکیک وظایف آسیب نمی‌رساند (رجوع کنید به بند ۱۰-۱-۳).

ت - ارایه یک بیانیه کتبی از حقوق دسترسی کاربران به آنها

ث - تقاضا از کاربران برای امضا بیانیه‌ای که نشان می‌دهد آنها شرایط دسترسی را درک کرده اند؛

ج - حصول اطمینان از این که ارایه کنندگان خدمات دسترسی را تا زمانی که روش‌های اجرایی مربوطه بطور کامل به انجام برسند، ارایه نمی‌کنند.

چ - حفظ مدرکی رسمی از تمام اشخاصی که برای استفاده از خدمات ثبت شده اند.

ح - حذف یا توقیف از حقوق دسترسی کاربرانی که نقش‌ها یا وظایف را تغییر داده اند یا سازمان را ترک کرده‌اند.

خ- بررسی دوره‌ای، و حذف یا مسدود کردن شناسه‌ها یا حساب‌های کاربری زائد (رجوع کنید به بند ۱۱-۲-۴)

د- حصول اطمینان از اینکه شناسه ها و حسابهای کاربری مازاد به دیگر کاربران ارایه نمی‌شود؛

اطلاعات دیگر

توصیه می‌شود به تثبیت نقش‌های دسترسی کاربر بر مبنای الزامات کسب وکار که تعدادی از حقوق دسترسی را به شرح‌های دسترسی کاربر معمولی خلاصه می‌کنند، ملاحظه زیادی شود. تقاضاها و بررسی‌های دسترسی (رجوع کنید به بند ۱۱-۲-۴) در سطح این نقش‌ها ساده تر از سطح حقوق خاص مدیریت می‌شوند.

توصیه می‌شود بعنوان ملاحظات بندهایی در قراردادهای پرسنل و بندهای خدمات گنجانده شود که در صورتی که دسترسی غیرمجاز توسط پرسنل یا عوامل خدمات سعی می‌شود محرومیت‌هایی در نظر گرفته شود. (همچنین رجوع کنید به بند ۶-۱-۵، ۸-۱-۳ و ۸-۲-۳)

۱۱-۲-۲ مدیریت اختیارات ویژه

کنترل

توصیه می‌شود تخصیص و بکارگیری اختیارات ویژه، محدود و کنترل شده باشد.

راهنمای پیاده‌سازی

توصیه می‌شود سیستم‌های چندکاربره، که نیازمند محافظت در برابر دسترسی غیر مجاز، دارای تخصیص مزایا که از طریق یک فرایند رسمی کنترل می‌شود، باشند. توصیه می‌شود مراحل زیر در نظر گرفته شود:

الف - مزایای دسترسی در رابطه با هر یک از محصولات سیستم، مانند سیستم عامل، سیستم مدیریت بانک داده و هر یک از کاربردها و کاربرانی که باید به آنها ختصاص داده شود توصیه می‌شود شناسایی شوند.

ب - توصیه می‌شود مزایایی به هر کاربر بر مبنای نیاز به استفاده و بر مبنای واقعه به واقعه در راستای خط‌مشی کنترل دسترسی؛ به عبارت دیگر حداقل الزامات نقش عملکردی آنها فقط در زمان مورد نیاز اختصاص یابد؛

پ - توصیه می‌شود یک فرایند تایید اعتبار و گزارشی از تمام مزایای اختصاص یافته، نگهداری شود. توصیه می‌شود مزایا تا زمانی که فرایند صدور مجوز به طور کامل به انجام برسد، ارایه نشود؛

ت - توصیه می‌شود توسعه و استفاده از روتین‌های سیستم ارتقا یابد تا از نیاز به اعطای مزایا به کارکنان اجتناب شود؛

ث - توصیه می‌شود توسعه و استفاده از برنامه‌هایی که از نیاز به اجرا با مزایا اجتناب می‌کنند ارتقا یابد؛

ج - توصیه می‌شود مزایایی به کاربران متفاوت در نظر گرفته شود در مقایسه با آنهایی که برای استفاده کسب وکار عادی مورد استفاده قرار گرفتند.

اطلاعات دیگر

استفاده نامناسب از مزایای اجرای سیستم (هر ویژگی یا امکانی از یک سیستم اطلاعاتی که این امکان را به کاربر می‌دهد تا کنترل‌ها را باطل کند) می‌تواند عامل موثری برای خرابی یا رخنه در سیستم‌ها باشد.

۱۱-۲-۳ مدیریت کلمهٔ عبور کاربر

کنترل

توصیه می‌شود تخصیص کلمات عبور، از طریق یک فرایند مدیریت رسمی، کنترل شود.

راهنمای پیاده‌سازی

توصیه می‌شود این فرایند شامل الزامات زیر باشد:

الف - توصیه می‌شود از کاربران خواسته شود بیانیه ای را برای محرمانه نگه داشتن کلمات عبور و حفظ کلمات عبور فقط در میان اعضای گروه امضا کنند؛ این بیانیه امضا شده را می‌توان در مفاد و شرایط استخدام گنجاند (رجوع کنید به بند ۸-۱-۳)

ب - زمانی که از کاربران خواسته می‌شود کلمات عبور خود را حفظ کنند، توصیه می‌شود ابتدا یک شماره رمز موقت و امن (رجوع کنید به بند ۱۱-۳-۱) به آنها داده شود که مجبور شوند بلافاصله کلمه عبور خود را به آن تغییر دهند.

پ - تثبیت روش‌های اجرایی برای تصدیق هویت یک کاربر قبل از ارایه کلمه عبور جدید، جابجایی یا کلمه عبور موقت؛

ت - توصیه می‌شود کلمات عبور موقت به صورتی ایمن به کاربران داده شود؛ توصیه می‌شود استفاده از پیام‌های الکترونیکی اشخاص ثالث یا محافظت نشده اجتناب شود؛

ث - توصیه می‌شود کلمات عبور برای هر فرد، منحصر به فرد باشد و توصیه می‌شود قابل حدس نباشد؛

ج - توصیه می‌شود کاربران دریافت کلمه عبور خود را اعلام کنند؛

چ - توصیه می‌شود کلمات عبور هرگز در سیستم‌های رایانه‌ی به گونه ای محافظت نشده ذخیره نشوند

ح - توصیه می‌شود کلمات عبور فروشندگان پس از نصب سیستم‌ها یا نرم‌افزار تغییر یابد.

اطلاعات دیگر

کلمات عبور ابزارهای متداولی برای تصدیق هویت یک کاربر قبل از دسترسی به یک سیستم اطلاعات یا سرویس مطابق با تایید اعتبار کاربر است. فن‌آوری‌های دیگر برای شناسایی کاربر و تایید اعتبار، نظیر زیست سنجی مانند تصدیق اثر انگشت، تصدیق امضا، و استفاده از نشانه‌های سخت افزاری، مانند کارت‌های هوشمند، موجود هستند و توصیه می‌شود در صورت مناسب بودن در نظر گرفته شوند.

۱۱-۲-۴ بازنگری حقوق دسترسی کاربر

کنترل

توصیه می‌شود مدیریت با استفاده از یک فرایند رسمی، حقوق دسترسی کاربران را در فواصل زمانی منظم، بازنگری کند.

راهنمای پیاده‌سازی

توصیه می‌شود در بررسی حقوق دسترسی رهنمودهای زیر مد نظر قرار گیرد :

الف - توصیه می‌شود حقوق دسترسی کاربران در فواصل منظم مثلا در دوره‌های شش ماهه، و پس از هر تغییر نظیر ارتقا، تنزل رتبه، یا خاتمه استخدام بررسی شوند(رجوع کنید به بند ۱۱-۲-۱)؛

ب - توصیه می‌شود حقوق دسترسی کاربران در زمان جابجایی از یک کارمند به کارمند دیگر در همان سازمان بررسی شود و مجددا اختصاص یابد؛

پ - اختیارات برای حقوق دسترسی دارای مزیت خاص(رجوع کنید به بند ۱۱-۲-۲)، توصیه می‌شود در فواصل کمتر مثلا به صورت ۳ ماهه بررسی شود؛

ت - تخصیص مزایا توصیه می‌شود در فواصل منظم بررسی شود تا اطمینان حاصل شود که مزایای غیر مجاز احراز نشده است؛

ث - تغییر در حساب‌های برتر توصیه می‌شود برای بررسی دوره ای ثبت شود

اطلاعات دیگر

لازم است که حقوق دسترسی کاربران برای حفظ کنترل موثر بر دسترسی به داده‌ها و خدمات اطلاعات بررسی شود.

۱۱-۳ مسوولیت‌های کاربر

هدف: پیشگیری از دسترسی کاربر غیر مجاز، و به خطر افتادن یا سرقت اطلاعات و امکانات پردازش اطلاعات.

همکاری کاربران مجاز برای امنیت موثر لازم است.

توصیه می‌شود کاربران درباره مسوولیت‌های شان برای حفظ کنترل‌های دسترسی موثر، به خصوص در رابطه با استفاده از کلمات عبور و امنیت تجهیزات کاربران آگاه شوند.

توصیه می‌شود یک خط‌مشی کنترل آشکار برای کاهش خطر دسترسی غیرمجاز یا آسیب به ورقه‌ها، رسانه ها، و تجهیزات پردازش اطلاعات اجرا شود.

۱۱-۳-۱ استفاده از کلمهٔ عبور

کنترل

توصیه می‌شود کاربران در انتخاب و بکارگیری کلمهٔ عبور، به تبعیت از شیوه‌های امنیتی صحیح، ملزم شوند.

راهنمای پیاده‌سازی

توصیه می‌شود به تمام کاربران توصیه شود که:

الف - کلمات عبور را محرمانه نگه دارند

ب - از نگهداری سابقه ای (مثلا، کاغذ، فایل نرم‌افزاری، یا وسیله دستی) از کلمات عبور مگر زمانی که بتوان آن را به طور ایمن ذخیره کرد و روش ذخیره بهبود مورد تأیید اجتناب کنند؛

پ - کلمات عبور را هر زمان که نشانه‌ای از سوء استفاده احتمالی از سیستم یا کلمه عبور باشد؛ تغییر دهند

ت - کلمات عبور با کیفیت را با حداقل طول انتخاب کنند که:

۱ - حفظ کردن شان ساده باشد؛

۲ - به چیزخاصی مربوط نباشد که شخص دیگری بتواند به سادگی آن را حدس بزند یا با استفاده از اطلاعات شخصی فرد آن را پیدا کند؛ مثلا، نام، شماره تلفن، و تاریخ تولد؛

۳ - نسبت به حملات واژه‌نامه آسیب‌پذیر نباشد؛ مثلا متشکل از واژگانی که در واژه‌نامه آمده است، نباشد.

۴ - از حروف مشابه، تماما عددی یا تماما الفبایی استفاده نشود.

ث - کلمات عبور را در فواصل منظم یا بر اساس تعداد دسترسی‌ها تغییر دهند (توصیه می‌شود کلمات عبور برای حساب‌های ممتاز با تکرار بیشتری نسبت به حساب‌های معمولی تغییر کنند) و از استفاده مجدد از کلمات عبور قدیمی اجتناب کنند.

ج - کلمات عبور موقت را در اولین ارتباط با سیستم تغییر دهند.

چ - کلمات عبور را در هیچ فرایندی که به طور اتوماتیک با سیستم مرتبط می‌شود قرار ندهند مثلا در کلید ماکرو ذخیره نکنند؛

ح - کلمات عبور را بین افراد به اشتراک نگذارند.

خ - از کلمه عبور مشابه برای اهداف کاری و غیر کاری استفاده نکنند.

اگر کاربران نیاز به دسترسی به چندین سرویس، سیستم یا الگو داشته باشند از آنها خواسته شود که چندین کلمه عبور جداگانه را حفظ کنند، باید به آنها توصیه شود که می‌توانند از یک کلمه عبور منفرد و باکیفیت (رجوع کنید به مورد ت) برای تمام خدمات استفاده کنند، زمانی که به کاربران اطمینان داده شد که سطح معقولی از محافظت برای ذخیره کلمه عبور در هر سرویس، سیستم یا الگو تثبیت شده است.

اطلاعات دیگر

مدیریت سیستم کمکی که به کلمات عبور گم شده یا فراموش شده می پردازد، نیازمند مراقبت خاص است زیرا این ممکن است همچنین وسیله ای برای حمله به سیستم کلمه عبور باشد.

۱۱-۳-۲ *تجهیزات بدون مراقبت کاربر*

کنترل

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

راهنمای پیاده‌سازی

توصیه می‌شود تمام کاربران از الزامات امنیتی و روش‌های اجرایی محافظت از تجهیزات رها شده و نیز مسوولیت شان برای اجرای این محافظت آگاه شوند. توصیه می‌شود به کاربران توصیه شود که:

الف - جلسات فعالی را در پایان به خاتمه برسانند مگر این که بتوان آنها را از طریق یک مکانیسم قفل مناسب مانند یک برنامه محافظ صفحه نمایش محافظت نمود.

ب - از رایانه‌های پردازنده مرکزی، سرورها، و رایانه‌های اداری در زمانی که جلسه بـه پایـان مـی رسـد، قطـع ارتباط نمایند.

پ - رایانه‌ها یا پایانه‌ها را از استفاده غیرمجاز توسط یک قفل کلیددار یا یک کنتـرل معـادل ماننـد دسترسـی توسط کلمه عبور در زمانی‌که در حال استفاده نیست محافظت کنند (همچنین رجوع کنید به بند ۱۱-۳-۳).

اطلاعات دیگر

تجهیزات نصب شده در محیط‌های کاربر، برای مثال ایستگاه‌های کاری، سرویس دهنده‌های فایل ممکن است نیازمند حفاظت خاص دربرابر دسترسی غیرمجاز وقتی که برای مدت مدیدی بدون متصدی باقی می‌مانند.

۱۱-۳-۳ خط‌مشی میز پاک و صفحهٔ پاک

کنترل

توصیه می‌شود یک خط‌مشی میز پاک برای کاغذها و محیط‌های ذخیره‌سازی قابل جابجایی و یک خط‌مشی صـفحهٔ پاک برای امکانات پردازش اطلاعات، مورد پذیرش واقع شوند.

راهنمای پیاده‌سازی

توصیه می‌شود خط‌مشی میز پاک و صفحه پاک در طبقه‌بنـدی اطلاعـات(رجـوع کنیـد بـه ۷-۲)، الزامـات قـانونی و قراردادی(رجوع کنید به ۱۵-۱)، و ریسک‌های مشابه و جنبه‌های فرهنگیِ سازمان، درنظرگرفته شود. توصیه می‌شـود رهنمودهای زیر در نظر گرفته شود:

الف – توصیه می‌شود اطلاعات کسب وکار حیاتی یا حساس، برای مثـال روی کاغـذ یـا رسـانه ذخیـره‌سـازی الکترونیکی، وقتی که به آنها نیاز نیست بطور ایده‌ال در یک گاوصندوق یا قفسه یا سایر شکل‌هـای وسـایل حفاظتی نگهداری شود، مخصوصا وقتی که اداره تعطیل است.

ب – توصیه می‌شود رایانه‌ها و پایانه‌ها بصورت قطع ارتباط یا حفاظت شده با یک ساز و کار قفل صفحه کلید و نمایش کنترل شده با کلمه عبور، کلمه رمز یا ساز و کار احراز اصالت کاربر مشابه، رها شوند وقتی که بدون متصدی هستند و توصیه می‌شود با قفل رمزی، کلمه عبور یا سـایر کنتـرل‌هـا وقتـی کـه مـورد اسـتفاده نیستند، محافظت شوند

پ – توصیه می‌شود نقاط پستی ورودی و خروجی و ماشین‌های نمابر بدون متصدی محافظت شوند.

ت – توصیه می‌شود از استفاده غیرمجاز از تجهیزات نسخه‌برداری و سایر فن‌آوری‌های تکثیـر (مـثلا اسـکنرها، دوربین‌های عکاسی) جلوگیری شود.

ث – توصیه می‌شود مدارک حاوی اطلاعات طبقه‌بندی شده و حساس سریعا از چاپگرها برداشته شوند.

اطلاعات دیگر

یک خط‌مشی میز پاک/صفحه پاک ریسک‌های دسترسی غیرمجاز، از دست دادن، یا آسیب به اطلاعات را در حـین و خارج از ساعات کاری عادی را کاهش می دهد. همچنین گاوصندوق ها یا سایر اشکال امکانات نگهـدای امـن ممکـن است از اطلاعات نگهداری شده در آنها در برابر بلاهایی مانند آتش، زمین لرزه، سیل یا انفجار حفاظت نمایند.

۱۱-۴ کنترل دسترسی به شبکه

هدف: پیشگیری از دسترسی غیر مجاز به خدماتی که تحت شبکه ارائه می‌شوند.
توصیه می‌شود دسترسی به خدمات شبکه ای درونی و بیرونی کنترل شود.
توصیه می‌شود دسترسی کاربران به شبکه‌ها و خدمات با استفاده از موارد زیر به امنیت خدمات شبکه ای آسیب نرساند:
الف - واسط های مناسب بین شبکه سازمان و شبکه‌های دیگر سازمان‌ها و شبکه‌های همگانی برقرار است.
ب - ساز و کارهای سنجش اعتبار مناسب برای کاربران و تجهیزات به کار گرفته می‌شوند:
پ - کنترل دسترسی کاربر به خدمات اطلاعات اجرا می‌شود.

۱۱-۴-۱ *خط‌مشی استفاده از خدمات شبکه*

کنترل
توصیه می‌شود کاربران تنها به خدماتی که مشخصاً استفاده از آنها برایشان مجاز شده، دسترسی داشته باشند.
راهنمای پیاده‌سازی
توصیه می‌شود یک خط‌مشی درباره استفاده از شبکه‌ها و خدمات شبکه ای تدوین شود. توصیه می‌شود این خط‌مشی دربرگیرنده موارد زیر باشد:
الف - شبکه‌ها و خدمات شبکه ای که دسترسی به آنها مجاز است؛
ب - روش‌های اجرایی مجوزدهی برای تعیین این که 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 به‌کار رفته برای دسترسی به شبکه‌ها و خدمات شبکه ای (برای مثال، شرایطی برای دسترسی از طریق شماره‌گیری برای دسترسی به تامین کننده سرویس اینترنت یا سیستم راه دور)
توصیه می‌شود خط‌مشی استفاده از خدمات شبکه ای با خط‌مشی کنترل دسترسی کسب وکار همخوانی داشته باشد(رجوع کنید به بند ۱۱-۱).
اطلاعات دیگر
ارتباطات غیرمجاز و ناامن به خدمات شبکه می‌تواند بر کل سازمان تاثیر بگذارد. این کنترل به خصوص برای ارتباطات شبکه‌ها به نرم‌افزارهای کاربردی کسب وکار حساس و حیاتی یا برای کاربران در مکان‌های با ریسک بالا مانند نواحی عمومی یا بیرونی که خارج از کنترل و مدیریت سازمان است مهم است.

۱۱-۴-۲ *احراز اصالت (تصدیق هویت) کاربر برای اتصالات بیرونی*

کنترل
توصیه می‌شود برای کنترل دسترسی کاربران راه دور، روش‌های مناسب تصدیق هویت بکار گرفته شوند.

راهنمای پیاده‌سازی

تعیین اعتبار کاربران راه دور را می‌توان مثلا با استفاده از یک فن مبتنی بر رمزنگاری، نشانه‌های سخت افزاری، یا یک پروتکل چالش/پاسخ به دست آورد. اجرای مناسب این روشها را می‌توان در انواع راه حل های شبکه های خصوصی مجازی یافت. خطوط اختصاصی خصوصی را نیز می‌توان برای حصول اطمینان از منبع اتصالات مورد استفاده قرار داد. روش‌های اجرایی و کنترل‌های شماره گیری مثلا استفاده از مودم‌های شماره گیر، می‌تواند محافظتی دربرابر ارتباطات غیرمجاز و ناخواسته به تجهیزات پردازش اطلاعات یک سازمان ایجاد کند. این نوع کنترل اصالت کاربرانی را که سعی می‌کنند ارتباطی با شبکه یک سازمان از مکان‌های دور برقرار کنند احراز می‌کند. در زمان استفاده از این پروتکل، توصیه می‌شود یک سازمان از خدمات شبکه ای که شامل انتقال تماس است استفاده نکند یا اگر این کار این کار را می‌کند، توصیه می‌شود آنها استفاده از این ویژگی‌ها را برای اجتناب از ضعف‌های مربوط به انتقال تماس غیرفعال کنند. توصیه می‌شود فرایند تماس مجدد تضمین کند که قطع ارتباط واقعی در طرف سازمان رخ می‌دهد. در غیر این صورت، کاربر راه دور ممکن است خط را باز نگه دارد و وانمود کند که تصدیق تماس انجام شده است. توصیه می‌شود روش‌های اجرایی و کنترل‌های تماس عمیقا برای مقابله با این احتمال آزموده شود.

تعیین اعتبار گره، می‌تواند به عنوان یک ابزار جایگزین تعیین اعتبار گروه‌های کاربران راه دور در زمانی که به تجهیزات رایانه‌ی امن و مشترک متصل هستند عمل کند. روشهای رمزنگاری مثلا بر اساس گواهی دهی ماشینی می‌تواند برای تعیین اعتبار گره مورد استفاده قرار گیرد. این بخشی از راه حل‌های مبتنی بر شبکه خصوصی مجازی است.

توصیه می‌شود کنترل‌های اضافه تعیین اعتبار، برای کنترل دسترسی به شبکه‌های بی سیم اجرا شوند. به خصوص، در انتخاب کنترل‌هایی برای شبکه‌های بی سیم به دلیل فرصت‌های بزرگتر برای مداخله کشف نشده و واردکردن ترافیک شبکه لازم است.

اطلاعات دیگر

ارتباطات خارجی پتانسیل دسترسی غیرمجاز به اطلاعات کسب وکار را مثلا از طریق روش‌های شماره گیری ایجاد می‌کنند. انواع مختلف روش‌های سنجش اعتبار وجود دارد که بعضی از آنها سطح بالاتری از محافظت را در مقایسه با بقیه ارایه می‌کنند مثلا روش‌هایی بر اساس استفاده از روشهای رمزنگاری می‌توانند سنجش اعتباری قوی ایجاد کنند. مهم است که با یک ارزیابی ریسک، سطح محافظت لازم تعیین شود. این برای انتخاب مناسب یک روش تعیین اعتبار لازم است.

یکی از راه‌های تسهیل ارتباط با یک رایانه راه دور ممکن است راهی برای دستیابی به دسترسی غیرمجاز به یک عملکرد کسب وکار باشد. این بخصوص زمانی مهم است که اتصال از شبکه ای استفاده کند که خارج از کنترل مدیریت امنیت سازمان است.

۱۱-۴-۳ *شناسایی تجهیزات در شبکه‌ها*

کنترل

توصیه می‌شود شناسایی خودکار تجهیزات، به عنوان وسیله ای برای احراز اصالت اتصالات از مکان‌ها و تجهیزات مشخص، در نظر گرفته شود.

راهنمای پیاده‌سازی

شناسایی تجهیزات باید زمانی انجام شود که مهم باشد ارتباطات فقط می‌تواند از یک محل یا تجهیزات خاص آغاز شود. یک شناسایی کننده تجهیزات می‌تواند برای نشان دادن این که آیا تجهیزات اجازه دارد با شبکه اتصال برقرار کند یا نه مورد استفاده قرار گیرد. اگر بیش از یک شبکه وجود دارد و بخصوص اگر این شبکه‌ها حساسیت‌های متفاوت دارند. توصیه می‌شود این شناسایی کنندگان به روشنی نشان دهند که تجهیزات اجازه اتصال به کدام شبکه را دارند. ممکن است لازم باشد که محافظت فیزیکی از تجهیزات را برای حفظ امنیت شناسایی کننده تجهیزات در نظر داشته باشیم.

اطلاعات دیگر

این کنترل می‌تواند با روش‌های دیگری برای احراز اصالت کاربر تجهیزات (رجوع کنید به بند ۱۱-۴-۲) تکمیل شود. شناسایی تجهیزات می‌تواند علاوه بر تعیین اعتبار کاربر مورد استفاده قرار گیرد.

۱۱-۴-۴ حفاظت از درگاه عیب‌یابی و پیکر بندی راه دور

کنترل

توصیه می‌شود دسترسی فیزیکی و منطقی به درگاه‌های عیب‌یابی و پیکربندی، تحت کنترل باشد.

راهنمای پیاده‌سازی

دسترسی فیزیکی و منطقی به پورت های عیب یابی و پیکربندی دربرگیرنده استفاده از یک قفل و رویه روش‌های اجرایی پشتیبان برای کنترل دسترسی فیزیکی به درگاه است. مثالی از چنین روش‌های اجرایی پشتیبان، تضمین آن است که درگاه‌های عیب یابی و پیکربندی فقط توسط هماهنگی بین مدیر خدمات رایانه و پرسنل پشتیبانی نرم‌افزار/سخت افزار است که به دسترسی نیاز دارند.

درگاه‌ها، خدمات، و تجهیزات مشابهی که روی یک رایانه یا دستگاه شبکه ای نصب می‌شوند، و به طور خاص برای کارایی کسب وکار لازم نیستند، توصیه می‌شود غیرفعال شوند یا حذف شوند.

اطلاعات دیگر

بسیاری از سیستم‌های رایانه‌ی، سیستم‌های شبکه، و سیستم‌های ارتباطات، با یک تجهیزات عیب یابی و پیکربندی راه دور برای استفاده توسط مهندسان نگهداری نصب می‌شوند.

اگر این درگاه‌های عیب یابی محافظت نشده باشند، به ابزاری برای دسترسی غیرمجاز تبدیل می‌شوند.

۱۱-۴-۵ تفکیک در شبکه‌ها

کنترل

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

راهنمای پیاده‌سازی

یکی از روش‌های کنترل امنیت شبکه‌های بزرگ تقسیم آنها به حوزه‌های شبکه منطقی جداگانه مانند حوزه‌های شبکه داخلی یک سازمان و حوزه‌های شبکه خارجی است که هر کدام توسط یک محیط امنیتی تعریف شده محافظت می‌شوند. یک مجموعه مدرج از کنترل‌ها را می‌توان در حوزه‌های شبکه‌های منطقی مختلف برای تفکیک بیشتر محیط‌های امنیتی شبکه، مثلا سیستم‌هایی که برای همگان قابل دسترسی هستند، شبکه‌های داخلی، و دارایی‌های حیاتی مورد استفاده قرار داد. توصیه می‌شود حوزه‌ها بر اساس یک ارزیابی ریسک و الزامات مختلف امنیتی در هر یک از دوره‌ها تعریف شوند.

چنین محیط‌های شبکه را می‌توان از طریق نصب یک دروازه امن بین دو شبکه که برای کنترل دسترسی و جریان اطلاعات بین دو حوزه متصل می‌شوند اجرا کرد. توصیه می‌شود این دروازه برای فیلتر کردن ترافیک بین این حوزه‌ها (رجوع کنید به بند ۱۱-۴-۶ و ۱۱-۴-۷) و مسدود کردن دسترسی غیرمجاز مطابق با خط‌مشی کنترل دسترسی سازمان پیکربندی گردد (رجوع کنید به بند ۱۱-۱). مثالی از این نوع دروازه، چیزی به نام دیوار آتش است. روش دیگر روش حوزه‌های منطقی جداگانه محدودکردن دسترسی شبکه با استفاده از شبکه‌های خصوصی مجازی برای گروه‌های کاربر در سازمان است.

شبکه‌ها، را همچنین می‌توان با استفاده از کارایی دستگاه شبکه، مثلا با سوئیچ کردن پروتکل اینترنت[1] تفکیک کرد. حوزه‌های جداگانه را آن گاه می‌توان با کنترل جریان‌های داده‌های شبکه با استفاده از قابلیت‌های مسیریابی/ راه‌گزینی[2] نظیر فهرست‌های کنترل دسترسی اجرا کرد.

توصیه می‌شود معیارهای تفکیک شبکه ها به دامنه ها براساس خط مشی کنترل دسترسی و الزامات دسترسی باشد (رجوع کنید به ۱۰-۱)، و همچنین درنظر گرفتن هزینه مربوطه و پیامد عملکرد متحد کردن فن‌آوری دروازه یا مسیریابی مناسب شبکه (رجوع کنید به ۱۱-۴-۶ و ۱۱-۴-۷).

بعلاوه، توصیه می‌شود تفکیک شبکه ها بر اساس ارزش و طبقه‌بندیِ اطلاعات نگهداری شده یا پردازش شده در شبکه، سطوح اعتماد، یا خطوط کسب وکار برای کاهش پیامد کلی قطع سرویس.

توصیه می‌شود ملاحظاتی برای تفکیک شبکه های بی‌سیم از شبکه های داخلی و خصوصی درنظر گرفته شود. از آنجا که فضای احاطه شده توسط شبکه بی‌سیم بخوبی تعریف نشده است، توصیه می‌شود یک ارزیابی ریسک در این شرایط برای شناسایی کنترل ها انجام شود (برای مثال، احراز اصالت قوی، روش‌های رمزنگاری، و انتخاب فرکانس) تا از وضعیت مناسب تفکیک شبکه اطمینان حاصل آید.

اطلاعات دیگر

شبکه ها بطور فزاینده در حال توسعه یافتن، فراتر از مرزهای سنتی سازمانی هستند، از آنجایی که شرکای کسب وکار به صورتی شکل گرفته اند که ممکن است به اتصال میانی یا اشتراک پردازش میانی و تجهیزات شبکه نیاز داشته باشند. این توسعه ها ممکن است ریسک دسترسی غیرمجاز به سیستم‌های اطلاعاتی موجود را که از شبکه استفاده می‌کند افزایش دهد؛ تعدادی از آنها ممکن است نیاز به حفاظت در برابر کاربران شبکه های دیگر داشته باشند، بخاطر حیاتی بودن یا حساس بودن آنها.

۱۱-۴-۶ کنترل اتصال به شبکه

کنترل

برای شبکه‌های اشتراکی، به ویژه آنهایی که در محدوده‌های سازمان، گسترش می یابند، قابلیت کاربران برای اتصال به شبکه، توصیه می‌شود در راستای خط‌مشی کنترل دسترسی و الزامات برنامه‌های کاربردی کسب‌وکار، محدود شود (رجوع کنید به بند ۱۱-۱)

راهنمای پیاده‌سازی

توصیه می‌شود حقوق دسترسی کاربران به شبکه طبق نیاز خط‌مشی کنترل دسترسی حفظ و روزآمد شود. (رجوع کنید به بند ۱۱-۱-۱)

1- Internet Protocol (IP)
1- Switching/Routing

قابلیت ارتباط کاربران را می‌توان از طریق دروازه های شبکه که تردد را با استفاده از جدول‌ها یا قوانین از پیش تعیین شده فیلتر می‌کنند محدود کرد. مثال‌های کاربردهایی که توصیه می‌شود محدودیت‌ها به آنها اعمال می‌شوند شامل موارد زیر است:

الف - پیام‌رسانی؛ مثلا پست الکترونیکی

ب - انتقال فایل

پ - دسترسی تعاملی

ت - دسترسی به برنامه های کاربردی

توصیه می‌شود پیوند حقوق دسترسی شبکه به تاریخ ها یا زمان‌های خاصی از روز در نظر گرفته شود.

اطلاعات دیگر

به کارگیری کنترل‌هایی برای محدود کردن قابلیت اتصال کاربران ممکن است توسط خط‌مشی کنترل دسترسی برای شبکه‌های مشترک به خصوص شبکه‌هایی که در فراسوی مرزهای سازمانی بسط می یابند مورد نیاز باشد.

۱۱-۴-۷ کنترل مسیر یابی در شبکه

کنترل

توصیه می‌شود کنترل‌های مسیریابی برای شبکه‌ها پیاده‌سازی شوند، تا اطمینان حاصل شود که اتصالات رایانه ای و جریان‌های اطلاعاتی، خط‌مشی کنترل دسترسی به برنامه‌های کاربردی کسب‌وکار را نقض نمی‌کنند.

راهنمای پیاده‌سازی

توصیه می‌شود کنترل های مسیریابی بر ساس ساز و کار های بررسی آدرس مقصد و منبع مثبت باشد.

مداخل امنیت را می‌توان برای اعتبار بخشی نشانی‌های مقصد و منبع در نقاط کنترل شبکه داخلی و بیرونی در صورتی که میان بر و یا فن‌آوری ترجمه نشانی شبکه مورد استفاده قرار می‌گیرند. توصیه می‌شود مجریان از قدرت و نارسایی‌های هر یک از ساز و کارهای به‌کار رفته آگاه باشند. توصیه می‌شود الزامات کنترل مسیریابی شبکه بر اساس خط‌مشی دسترسی باشد. (رجوع کنید به بند ۱۱-۱)

اطلاعات دیگر

شبکه‌های مشترک، به خصوص شبکه‌هایی که ماورای مرزهای سازمانی گسترش دارند ممکن است نیازمند کنترل‌های مسیریابی اضافی باشند. این به خصوص در جایی که شبکه‌ها با کاربران شخص سوم مشترک هستند اعمال می‌شود.

۱۱-۵ کنترل دسترسی به سیستم عامل

هدف: پیشگیری از دسترسی غیر مجاز به سیستم‌های عامل.

توصیه می‌شود تجهیزات امنیتی برای محدود کردن دسترس به سیستم‌های عامل به کاربران مجاز مورد استفاده قرار گیرد. توصیه می‌شود تجهیزات قابلیت‌های زیر را داشته باشند:

الف - تصدیق اعتبار کاربران مجاز مطابق با یک خط‌مشی کنترل دسترسی تعریف شده

ب - ثبت تلاشهای موفق و ناموفق تصدیق اعتبار سیستم

پ - ثبت استفاده از مزایای ویژه سیستم

ت - صدور هشدارهایی در زمانی‌که خط مشی‌های امنیتی سیستم نقض می‌شوند

ث - ارائه ابزارهای مناسب برای تصدیق اعتبار

ج - در جای مناسب، محدود کردن زمان ارتباط کاربران

۱۱-۵-۱ *روش‌های اجرایی برقراری ارتباط امن*

کنترل

توصیه می‌شود دسترسی به سیستم‌های عامل، از طریق یک روش‌اجرایی برقراری ارتباط امن با سیستم، کنترل شود.

راهنمای پیاده‌سازی

توصیه می‌شود روش اجرایی ورود به یک سیستم عامل برای کاهش فرصت دسترسی غیرمجاز طراحی شود. بنابراین توصیه می‌شود این روش اجرایی برقراری ارتباط حداقل اطلاعات را درباره سیستم افشا کند تا از ارایه کمک غیرمجاز به یک کاربرد غیرمجاز اجتناب شود. توصیه می‌شود یک روش اجرایی خوب برای برقراری ارتباط:

الف - سیستم یا شناساننده‌های برنامه کاربردی را تا زمانی که فرایند برقراری ارتباط با موفقیت به پایان نرسیده است نشان ندهد.

ب - یک هشدار عمومی را نمایش دهد که توصیه می‌شود رایانه فقط توسط اشخاص مجاز مورد دسترسی قرار گیرد.

پ - پیام‌های کمک را در طول روش اجرایی برقراری ارتباط ارایه نکند که به کاربران غیرمجاز کمک شود.

ت - اطلاعات برقراری ارتباط را پس از تکمیل تمام داده‌های ورودی اعتبار بخشی نماید. اگر خطایی سرزند، توصیه می‌شود سیستم نشان ندهد که کدام بخش از داده‌ها صحیح و کدام بخش صحیح نیست.

ث - تعداد تلاشهای برقراری ارتباط ناموفق مجاز را محدود کند؛ مثلا به سه بار و موارد زیر را در نظر گیرد:

۱ - ثبت تلاشهای موفق و ناموفق

۲ - ایجاد یک تاخیر زمانی قبل از این که به تلاشهای برقراری ارتباط بیشتر اجازه داده شود یا هر تلاشی بدون مجوز خاص رد شود.

۳ - قطع ارتباط داده‌ها

۴ - ارسال یک پیام هشدار به مرکز فرمان سیستم اگر تعداد تلاشها برای برقراری ارتباط به میزان حد اکثر خود رسید.

۵ - تعیین تعداد (تلاشهای مکرر وارد کردن کلمه عبور در ارتباط با حداقل طول کلمه عبور و ارزش سیستمی که محافظت می‌شود

ج - حداکثر و حداقل زمان مجاز برای روش اجرایی برقراری ارتباط را محدود کند. توصیه می‌شود اگر از حد انتظار فراتر رفت، سیستم برقراری ارتباط را خاتمه دهد.

چ - اطلاعات زیر را درباره تکمیل یک برقراری ارتباط موفق نمایش دهد:

۱ - تاریخ و زمان برقراری ارتباط موفق قبلی

۲ - جزئیات هر تلاش ناموفق برای برقراری ارتباط از زمان آخرین برقراری ارتباط موفق

ح - کلمه عبوری را که وارد می‌شود نمایش ندهد یا کاراکترهای کلمه عبور را توسط نمادهایی نشان دهد.

خ - کلمات عبور را در یک متن آشکار در یک شبکه منتقل نکند

اطلاعات دیگر

اگر کلمات عبور در طول جلسه برقراری ارتباط در یک شبکه در یک متن آشکار منتقل شوند، می‌توان آنها را توسط یک برنامه کشف کننده شنود تحت شبکه در شبکه به دست آورد.

۱۱-۵-۲ *شناسایی و احراز اصالت کاربر*

کنترل

توصیه می‌شود تمامی کاربران یک شناسهٔ منحصر به فرد (شناسهٔ کاربر) برای استفاده شخصی خودشان داشته باشند و توصیه می‌شود یک فن مناسب تصدیق هویت، به منظور اثبات هویت ادعا شده توسط یک کاربر، انتخاب شود.

راهنمای پیاده‌سازی

توصیه می‌شود این کنترل برای تمام انواع کاربران به کار گرفته شود (شامل پرسنل پشتیبانی فنی، اپراتورها، راهبران شبکه، برنامه نویسان سیستم، و راهبران بانک داده)

توصیه می‌شود هویت کاربر برای ردیابی فعالیت‌ها در مورد افراد مسوول مورد استفاده قرار گیرد. توصیه می‌شود فعالیت‌های منظم کاربر از طریق حساب‌های با امتیازات ویژه انجام نشود.

در مواقع استثنایی، در جایی که منفعت کاری آشکاری وجود دارد، می‌توان از شناسه کاربری مشترک برای گروهی از کاربران یا یک شغل خاص استفاده کرد. توصیه می‌شود تایید مدیریت برای این موارد مستند شود. کنترل‌های اضافی ممکن است برای حفظ پاسخگویی لازم باشد.

توصیه می‌شود شناسه‌های عمومی برای استفاده توسط یک فرد فقط در صورتی مجاز است که یا در جایی که عملکردهای در دسترسی یا فعالیت‌های انجام شده توسط نام کاربری نیازی به ردیابی شدن ندارند (برای مثال، دسترسی فقط خواندنی)، یا در جایی که کنترل‌های دیگری در حال اجرا است مورد استفاده قرار گیرند (برای مثال، کلمه عبور برای یک شناسه کلی فقط برای یک شخص و در یک زمان و برای واقعه نگاری آن لحظه صادر می‌شود)

در جایی که احراز اصالت و تصدیق هویت قوی لازم است، توصیه می‌شود روش‌های تایید اعتبار که جایگزین کلمه عبور می‌شوند، نظیر ابزارهای رمزنگاری، کارت‌های هوشمند، علائم یا ابزارهای زیست سنجی مورد استفاده قرار گیرند.

اطلاعات دیگر

کلمات عبور (همچنین رجوع کنید به بند ۱۱-۳-۱ و بند ۱۱-۵-۳) راهی بسیار معمول برای ارایه شناسایی و اعتبار بر اساس یک رمز هستند که فقط کاربر آن را می‌داند. همین را می‌توان با ابزار رمزنگاری و پروتکل‌های تایید اعتبار به

دست آورد. توصیه می‌شود شدت شناسایی کاربر و تایید اعتبار او با حساسیت اطلاعاتی که قرار است مورد دسترسی قرار گیرد همخوانی داشته باشد.
مواردی نظیر علائم و کارتهای هوشمند، که کاربر آنها را دارد، نیز می‌توانند برای شناسایی و تعیین اعتبار مورد استفاده قرار گیرند. فن‌آوری‌های زیست سنجی تعیین اعتبار که از ویژگی‌های منحصر به فرد یا ویژگی‌های یک فرد هستند نیز می‌توانند برای احراز اصالت یک شخص مورد استفاده قرار گیرد. ترکیبی از فن‌آوری‌ها و ساز و کارهایی که پیوند محکمی با هم دارند منجر به شناسایی قوی‌تر خواهد شد.

۱۱-۵-۳ سیستم مدیریت کلمهٔ عبور

کنترل

توصیه می‌شود سیستم‌های مدیریت کلمات عبور، تعاملی بوده و توصیه می‌شود کیفیت کلمات عبور را تضمین نمایند.

راهنمای پیاده‌سازی

توصیه می‌شود یک سیستم مدیریت کلمه عبور:

الف - استفاده از هویت‌های کاربر و کلمات عبور را برای حفظ پاسخگویی اجبار کند

ب - به کاربران اجازه دهد کلمه عبور خود را انتخاب کنند و تغییر دهند، و روش اجرایی تاییدی را برای خطاهای وارده بگنجاند

پ - انتخاب کلمات عبور با کیفیت را انجام دهد. (رجوع کنید به بند ۱۱-۳-۱)

ت - تغییرات در کلمات عبور را اجبار کند (رجوع کنید به بند ۱۱-۳-۱)

ث - کاربران را وادار کند کلمات عبور موقت را در اولین برقراری ارتباط تغییر دهند. (رجوع کنید به بند ۱۱-۳-۲)

ج - سابقه ای 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 دیگر داده‌های سیستم کاربردی ذخیره کند.

خ - کلمات عبور را در فرم‌های محافظت شده ذخیره کند یا منتقل کند.

اطلاعات دیگر

کلمات عبور یکی از ابزارهای اساسی اعتباربخشی مجوز کاربران در دسترسی به یک سرویس رایانه‌ی هستند.
بعضی از برنامه های کاربردی نیازمند کلمات عبور هستند که توسط مراجع مستقل تعیین می‌شوند؛ در چنین مواردی نکات ب، ت، و ث از راهنمای فوق به‌کار نمی‌روند. در اکثر موارد کلمات عبور توسط کاربران انتخاب و حفظ می‌شوند.
بخش ۱۱-۳-۱ را برای راهنمای درباره استفاده از شبکه‌ها ببینید.

۱۱-۵-۴ استفاده از برنامه‌های کمکی سیستم

کنترل

توصیه می‌شود استفاده از برنامه‌های کمکی سیستم که ممکن است قادر به ابطال کنترل‌های سیستم و برنامهٔ کاربردی باشند، محدود و به شدت کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رهنمودهای زیر برای استفاده از برنامه های کاربردی سیستم در نظر گرفته شود:

الف - استفاده از روش‌های اجرایی شناسایی، احراز اصالت، و مجوز دهی برای برنامه های کمکی سیستم
ب - تفکیک برنامه های کمکی سیستم از نرم‌افزارهای کاربردی
پ - محدودکردن استفاده از برنامه های کمکی سیستم به حداقل تعداد کاربردی کاربران مجاز و مورد اطمینان(رجوع کنید به بند ۱۱-۲-۲)
ت – اجازه برای استفاده تک کاره از ابزارهای سیستم‌ها
ث - محدودکردن دسترسی به سطوح تایید مجوز برای کاربردهای سیستم
ج – واقعه نگاریِ همه استفاده ها از ابزارهای سیستم.
چ – محدودسازی دسترسی به ابزارهای کمکی سیستم، برای مثال برای دوره از یک تغییر مجاز
ح - از بین بردن با غیرفعال کردن نرم‌افزارهای غیرضروری بر اساس برنامه های کمکی و نرم‌افزار سیستمی
خ - عدم اجازه دسترسی به کاربرانی که به برنامه های کمکی در یک سیستم دسترسی دارند در زمانی که تفکیک وظایف لازم است.

اطلاعات دیگر

اکثر نصب‌های رایانه‌ی یک یا چند برنامه کمکی سیستم دارند که ممکن است منجر به ابطال کنترل‌های سیستم و برنامه های کاربردی شوند.

۱۱-۵-۵ خروج زمانی از لایه ارتباطی

کنترل

توصیه می‌شود لایه‌های ارتباطی غیر فعال پس از یک بازهٔ زمانی تعریف شده برای غیر فعال بودن، بسته و قطع شوند.

راهنمای پیاده‌سازی

توصیه می‌شود یک دستگاه اتمام وقت صفحه جلسه را روشن کند و احتمالا بعدا، هر دو عملکرد و جلسات شبکه را پس از یک دوره تعریف شده عدم فعالیت ببندد. توصیه می‌شود تاخیر اتمام وقت، نشانگر ریسک های امنیتی منطقه، طبقه بندی اطلاعاتی که مورد استفاده قرار می‌گیرند و کاربردهای مورد استفاده و ریسک های مربوط به تجهیزات باشد.

شکل محدودی از تجهیزات اتمام وقت را می‌توان برای بعضی از سیستم‌ها ارایه کرد که صفحه را روشن می‌کند و از دسترسی غیرمجاز جلوگیری می‌کند اما کارایی یا جلسات شبکه را نمی بندد.

اطلاعات دیگر

کنترل به خصوص در محل‌هایی که ریسک بالایی دارند مهم است، که شامل مناطق همگانی یا بیرونی خارج از مدیریت امنیت سازمان است. توصیه می‌شود جلسات برای جلوگیری از دسترسی اشخاص غیرمجاز و جلوگیری از حمله به خدمات خاموش شود.

۱۱-۵-۶ محدودسازی زمان اتصال

کنترل

به منظور فراهم آوری امنیت بیشتر برای برنامه‌های کاربردی با ریسک بالا، توصیه می‌شود محدودیت‌هایی در زمان‌های اتصال اعمال گردد.

راهنمای پیاده‌سازی

توصیه می‌شود کنترل‌های زمان ارتباط برای برنامه‌های کاربردی رایانه‌ی حساس در نظر گرفته شود، به خصوص از محل‌های با ریسک بالا مانند مناطق عمومی یا بیرونی که خارج از مدیریت امنیت سازمان هستند. مثال‌های این محدودیت‌ها عبارتند از:

الف - استفاده از علائم زمانی از پیش تعیین شده مثلا برای انتقال یا جلسات عادی کوتاه

ب - محدودکردن زمان‌های اتصال به ساعات اداری عادی اگر الزامی برای عملیات مازاد زمان یا عملیات ساعات اضافه وجود ندارد.

پ - در نظر گرفتن تایید مجدد اعتبار در فواصل زمان بندی شده

اطلاعات دیگر

محدود کردن دوره ای که در طول آن، ارتباطات با خدمات رایانه امکان پذیر می‌شوند فرصت دسترسی غیرمجاز را کاهش می‌دهد. محدود کردن طول جلسات فعال، از برگزاری جلساتی که برای پیشگیری از تایید اعتبار مجدد باز هستند جلوگیری می‌کند.

۱۱-۶ کنترل دسترسی به برنامه‌های کاربردی و اطلاعات

هدف: پیشگیری از دسترسی غیر مجاز به اطلاعات نگهداری شده در سیستم‌های کاربردی.

توصیه می‌شود تجهیزات امنیتی برای محدودکردن دسترسی به سیستم‌های کاربرد مورد استفاده قرار گیرند.

توصیه می‌شود دسترسی منطقی به نرم‌افزار و اطلاعات محدود به کاربران مجاز باشد.

توصیه می‌شود سیستم‌های کاربرد:

الف - دسترسی کاربر را به اطلاعات و سیستم‌های کاربردی مطابق با یک خط‌مشی کنترل دسترسی تعریف شده کنترل کنند؛

ب - محافظت در برابر دسترسی غیرمجاز را توسط هر نرم افزارکمکی، نرم‌افزار سیستم عامل، و نرم‌افزار را مخربی که توانایی حذف و یا عبور از کنترلهای برنامه های کاربردی و یا سیستمی دارد را ایجاد کند.

پ - به دیگر سیستم‌هایی که منابع اطلاعاتی با آنها در ارتباط هستند، اختلال وارد نکنند.

۱۱-۶-۱ *محدودیت دسترسی به اطلاعات*

کنترل

مطابق با خط مشی کنترل دسترسی تعریف شده، توصیه می‌شود دسترسی کاربران و کارکنان پشتیبانی کننده به اطلاعات و کارکردهای سیستم کاربردی، محدود شود.

راهنمای پیاده‌سازی

توصیه می‌شود محدودیت در دسترسی بر اساس الزامات عملکرد کسب وکار فردی باشد. توصیه می‌شود خط‌مشی کنترل دسترسی همچنین با خط‌مشی دستریس سازمانی همسو باشد. (رجوع کنید به بند ۱۱-۱)

توصیه می‌شود به کارگیری رهنمودهای زیر به منظور پشتیبانی الزامات محدودیت دسترسی در نظر گرفته شود:

الف - ارایه منوهایی برای کنترل دسترسی به وظایف سیستم کاربردی

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

پ - کنترل حقوق دسترسی نرم‌افزارهای کاربردی دیگر

ت – حصول اطمینان از این که خروجی سیستم‌های کاربردی که اطلاعات حساس را اجرا می‌کنند فقط حاوی اطلاعات مرتبط برای استفاده از خروجی می‌باشند و فقط به پایانه ها و محل‌های مجاز فرستاده می‌شوند. توصیه می‌شود این شامل بررسی‌های دوره ای از این خروجی‌ها برای تضمین این باشد که اطلاعات زائد حذف می‌شود.

۱۱-۶-۲ *جداسازی سیستم‌های حساس*

کنترل

توصیه می‌شود سیستم‌های حساس یک محیط محاسباتی اختصاصی (مجزا)، داشته باشند.

راهنمای پیاده‌سازی

توصیه می‌شود نکات زیر برای جداسازی سیستم حساس در نظر گرفته شود:

الف - توصیه می‌شود حساسیت سیستم کاربردی صریحا شناسایی و توسط مالک سیستم کاربردی شناسایی و مستند شود مستند شود(رجوع کنید به بند ۷-۱-۲).

ب - زمانی که یک نرم‌افزار کاربردی حساس در حال اجرا در یک محیط مشترک است، سیستم‌های کاربردی که این نرم‌افزار دارای منابع مشترک با آنها است، توصیه می‌شود توسط مالک نرم‌افزار کاربردی حساس شناسایی و پذیرفته شوند.

اطلاعات دیگر

بعضی از سیستم‌های کاربردی، به اندازه کافی به آسیب بالقوه که نیازمند اجرای خاص هستند حساس هستند.

حساسیت ممکن است نشان دهد که سیستم کاربردی:

الف - توصیه می‌شود در یک رایانه اختصاصی اجرا شود

ب - توصیه می‌شود فقط منابع را با سیستم‌های کاربردی مورداطمینان در اشتراک داشته باشد.

جداسازی را می‌توان با استفاده از روش‌های فیزیکی یا منطقی به دست آورد. (همچنین رجوع کنید به بند ۱۱-۴-۵)

۱۱-۷ محاسبهٔ سیار و کار از راه دور

هدف: حصول اطمینان از امنیت اطلاعات در هنگام استفاده از امکانات محاسبهٔ سیار و کار از راه دور.

در زمان استفاده از محاسبه سیار، رسیک‌های کار در یک محیط محافظت نشده توصیه می‌شود (توصیه می‌شود ریسک‌های کار در یک محیط محافظت نشده) در نظر گرفته شود و توصیه می‌شود محافظت مناسب به کار گرفته شود. در مورد کار از راه دور، توصیه می‌شود سازمان از محافظت برای محل کار از راه دور استفاده کند و تضمین کند که مقررات مناسب برای این نوع کار کردن وجود دارند.

۱۱-۷-۱ *محاسبه و ارتباطات سیار*

کنترل

به منظور حفاظت در برابر ریسک‌های بکارگیری امکانات محاسبه و ارتباطات سیار، توصیه می‌شود یک خط‌مشی رسمی بکار گرفته شود و توصیه می‌شود معیارهای امنیتی مناسبی اختیار شوند.

راهنمای پیاده‌سازی

در زمان استفاده از تجهیزات محاسبه و ارتباط سیار، مانند رایانه‌های کیفی، رایانه‌های دستی، رایانه‌های روپایی، کارت‌های هوشمند، و تلفن‌های همراه توصیه می‌شود که مراقبت شود که تضمین شود اطلاعات کسب وکار مورد دستبرد قرار نمی‌گیرند. توصیه می‌شود خط‌مشی محاسبه سیار به حساب آوردند، ریسک‌های کار با تجهیزات محاسبه سیار در محیط‌های محافظت نشده را مد نظر قرار دهند.

توصیه می‌شود خط‌مشی محاسبه سیار، شامل الزاماتی برای محافظت فیزیکی، کنترل‌های دسترسی، روشهای رمزنگاری، نسخه های پشتیبان و محافظت دربرابر ویروس باشد. توصیه می‌شود خط‌مشی همچنین شامل قوانین و نکاتی درباره تجهیزات ارتباط سیار برای شبکه‌ها و راهنمایی درباه استفاده از این تجهیزات در مکان‌های عمومی باشد.

توصیه می‌شود در زمان استفاده از تجهیزات محاسبه سیار در مکان‌های عمومی، اتاق‌های جلسات، و مناطق محافظت نشده خارج از حوزه‌های سازمان مراقبت شود. توصیه می‌شود محافظت برای اجتناب از دسترسی غیرمجاز یا افشای اطلاعات ذخیره شده و پردازش شده توسط تجهیزات به کار گرفته شود. برای مثال استفاده از روش‌های رمزنگاری (رجوع کنید به بند ۱۲-۳)

توصیه می‌شود کاربران تجهیزات محاسبه سیار، در مکان‌های عمومی مراقب باشند تا از ریسک دیده شدن توسط اشخاص غیرمجاز اجتناب شود. توصیه می‌شود روش‌های اجرایی دربرابر نرم‌افزارهای نامناسب در نظر گرفته شود و به‌روز شود. (رجوع کنید به بند ۱۰-۴)

توصیه می‌شود نسخه های پشتیبان اطلاعات کسب وکار حیاتی به طور منظم گرفته شود. توصیه می‌شود تجهیزات برای امکان پذیر کردن پشتیبان گیری سریع و ساده از اطلاعات در دسترس باشد. توصیه می‌شود این نسخه های پشتیبان محافظت کافی را در برابر سرقت یا آسیب به اطلاعات داشته باشند.

توصیه می‌شود محافظت مناسب در استفاده از تجهیزات سیار مرتبط با شبکه‌ها در نظر گرفته شود. توصیه می‌شود دسترسی راه دور به اطلاعات کسب وکار در سراسر شبکه همگانی با استفاده از تجهیزات محاسبه سیار فقط پس از شناسایی و مجوز دهی و با مکانیسم کنترل دسترسی مناسب رخ دهند. (رجوع کنید به بند ۱۱-۴)

توصیه می‌شود تجهیزات محاسبه سیار، همچنین از نظر فیزیکی در برابر سرقت به خصوص در زمانی که مثلا در ماشین و انواع دیگر حمل‌ونقل، اتاق‌های هتل‌ها، مراکز کنفرانس، و مکان‌های همایش محافظت شوند. توصیه می‌شود رویه ای خاص که الزامات امنیتی قانونی، بیمه و... سازمان را مد نظر قرار می‌دهد برای موارد سرقت یا آسیب به تجهیزات محاسبه سیار تثبیت شود.

توصیه می‌شود تجهیزاتی که اطلاعات حساس، مهم و یا حیاتی را حمل می‌کنند بی توجه رها نشود و در صورت امکان توصیه می‌شود از نظر فیزیکی قفل شود و توصیه می‌شود برای امنیت تجهیزات مورد استفاده قرار گیرد. (رجوع کنید به بند ۹-۲-۵)

توصیه می‌شود آموزش برای پرسنلی که از محاسبه سیار برای افزایش آگاهی آنها درباره ریسک‌های ناشی از این نوع کار و کنترل‌هایی که توصیه می‌شود اجرا شوند هماهنگ شود.

اطلاعات دیگر

اتصالات بی سیم شبکه سیار، شبیه به انواع دیگر ارتباطات شبکه است، اما تفاوت‌های مهمی دارد که توصیه می‌شود در زمان شناسایی کنترل‌ها در نظر گرفته شود.

تفاوت‌های معمول عبارتند از:

الف - بعضی از پروتکل‌های امنیتی بی سیم ناکافی هستند و ضعف‌های مشهودی دارند.

ب - اطلاعات ذخیره شده در رایانه‌های سیار را به دلیل عرض باند محدود شبکه و یا به این دلیل که تجهیزات سیار ممکن است در زمان‌هایی که پشتیبان‌گیری زمان بندی می‌شود متصل نباشند، نمی‌توان پشتیبان گرفت.

۱۱-۷-۲ کار از راه دور

کنترل

توصیه می‌شود برای عملیات‌های کار از راه دور، یک خط‌مشی، طرح‌های عملیاتی و روش‌های اجرایی، ایجاد و پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان‌ها فقط فعالیت‌های کار از راه دور را در صورتی که مطمئن شدند هماهنگی‌های امنیتی مناسب در حال اجرا است و این‌ها با خط‌مشی امنیت سازمان مطابقت دارد مجاز کنند.

توصیه می‌شود محافظت مناسب از محل کار از راه دور مثلا در مقابله با سرقت از تجهیزات و اطلاعات، افشای غیرمجاز اطلاعات، دسترسی راه دور غیرمجاز به سیستم‌های داخلی سازمان یا سوءاستفاده از تجهیزات در نظر گرفته شود. توصیه می‌شود فعالیت‌های کار از راه دور، توسط مدیریت مجوز داده و کنترل شود و توصیه می‌شود که از مدنظر قرار دادن هماهنگی های مناسب برای این نوع کار اطمینان حاصل شود.

توصیه می‌شود موضوعات زیر در نظر گرفته شود:

الف - امنیت فیزیکی فعلی محل کار از راه دور با احتساب امنیت فیزیکی ساختمان و محیط محلی؛

ب - محیط فیزیکی پیشنهادی کار از راه دور

پ - الزامات امنیت ارتباطات با احتساب نیاز به دسترسی راه دور به سیستم‌های داخلی سازمان، حساسیت اطلاعاتی که مورد دسترسی قرار خواهد گرفت و از لینک های ارتباطی عبور می‌کند و حساسیت سیستم داخلی؛

ت - تهدید دسترسی غیرمجاز به اطلاعات یا منابع از اشخاص دیگر از طریق اسکان، مثلا دوستان و خانواده؛

ث - استفاده از شبکه‌های خانگی و الزامات یا محدودیت‌هایی درباره پیکربندی خدمات شبکه بی سیم؛

ج - خط‌مشی‌ها و روش‌های اجرایی برای جلوگیری از اختلافات درباره حقوق مالکیت مجازی که درباره تجهیزات کاملا خصوصی

چ - دسترسی به تجهیزات خصوصی (برای بررسی امنیت ماشین یا حین یک تجسس) که ممکن است از نظر قانونی ممنوع باشد.

ح - توافقنامه های مجوزهای نرم‌افزاری که به گونه ای هستند که سازمان ممکن است مسوول تایید مجوز برای نرم‌افزارها یا ایستگاه‌های کاری کارفرما باشد که مالکیت آن با کارکنان، پیمانکاران یا کاربران شخص سوم است

خ - محافظت آنتی ویروس و الزامات دیوار آتش

توصیه می‌شود در رهنمودها و ضمائم قرارداد موارد زیر در نظر گرفته شوند:

الف - تهیه تجهیزات مناسب و منابع ذخیره برای فعالیت‌های کار از راه دور، در جایی که استفاده از تجهیزات خصوصی که تحت کنترل سازمان نیست مجاز نیست؛

ب - تعریفی از کار مجاز، ساعات کار، طبقه بندی اطلاعاتی که ممکن است در سیستم‌های داخلی نگه داشته شـود و خدماتی که کاربر راه دور مجاز به دسترسی به آنها است؛

پ - تدارک تجهیزات ارتباطی مناسب، از جمله روش‌هایی برای تامین امنیت دسترسی راه دور

ت - امنیت فیزیکی

ث - قوانین و راهنمایی برای اعضا و دسترسی بازدید کننده به تجهیزات و اطلاعات

ج - تدارک پشتیبانی و نگهداری سخت افزار و نرم‌افزار

چ - تدارک بیمه

ح - روش‌های اجرایی برای پشتیبانی گرفتن از داده‌ها و استمرار کسب وکار

خ - ممیزی و کنترل امنیت

د - پس گرفتن حقوق دسترسی و اجازه و بازگرداندن تجهیزات در زمانی که فعالیت‌های کار راه دور خاتمه می‌یابند.

اطلاعات دیگر

کار راه دور از فن‌آوری ارتباطات برای قادر ساختن پرسنل به کار از راه دور از یک محل ثابت خـارج از سـازمان آنهـا استفاده می‌کند.

۱۲ اکتساب، بهبود، حفظ و نگهداری سیستم‌های اطلاعاتی

۱-۱۲ الزامات امنیتی سیستم‌های اطلاعاتی

هدف: حصول اطمینان از اینکه امنیت، یک جزء جدائی ناپذیر از سیستم‌های اطلاعاتی است.
سیستم‌های اطلاعاتی شامل سیستم‌های عامل، زیرساخت‌ها، برنامه های کاربردی کسب و کار، محصولات در دسترس، خدمات و برنامه های کاربردی توسعه یافته توسط کاربر است. طراحی و پیاده سازی سیستم اطلاعاتی که از فرایند تجاری پشتیبانی می‌کند، می‌تواند برای امنیت حیاتی باشد. توصیه می‌شود الزامات امنیتی قبل از بهبود و/یا پیاده سازی سیستم‌های اطلاعات، شناسایی شده و مورد توافق قرار گیرند.
توصیه می‌شود تمامی الزامات امنیتی در مرحله الزامات یک پروژه شناسایی شده، و به عنوان بخشی از کل حالت کسب و کار برای یک سیستم اطلاعاتی مورد دفاع قرار گرفته، توافق شده و مستند شود.

۱-۱-۱۲ *مشخصات و تحلیل الزامات امنیتی*

کنترل

توصیه می‌شود، بیانه های الزامات کسب وکار برای سیستم‌های اطلاعاتی جدید، یا توسعه سیستم‌های اطلاعاتی موجود، الزاماتی برای کنترل های امنیتی مشخص کنند.

راهنمای پیاده‌سازی

توصیه می‌شود مشخصاتِ الزاماتِ کنترل‌ها، کنترل‌های خودکار را بصورت آمیخته شده در سیستم اطلاعاتی، و نیاز برای پشتیبانی کنترل‌های دستی، در نظر بگیرند. توصیه می‌شود ملاحظات مشابه در زمان ارزشیابی بسته‌های نرم‌افزاری، بهبود یافته یا خریداری شده، برای برنامه های کاربردی کسب وکار به کار گرفته شود.
توصیه می‌شود الزامات و کنترل‌های امنیتی منعکس کننده ارزش کسب وکار دارایی‌های اطلاعاتی درگیر (همچنین به ۷-۲ رجوع کنید)، و آسیب کسب وکار بالقوه، که ممکن است ناشی از خرابی یا فقدان امنیت باشد.
توصیه می‌شود الزامات سیستم برای امنیت اطلاعات و فرایندها برای پیاده سازی امنیت، در مراحل اولیه پروژه‌های سیستم اطلاعات گنجانده شود. کنترل های معرفی شده در مرحله طراحی بصورت قابل توجه کم ارزش تر از پیاده سازی و حفظ آن کنترل هایی هستند که در حین و پس از پیاده سازی گنجانده می‌شوند.
اگر محصولات خریداری شوند، توصیه می‌شود یک فرایند آزمون و اکتساب رسمی، دنبال شود. توصیه می‌شود قراردادها با تامین کننده به الزامات امنیتی شناخته شده اشاره داشته باشند. در جایی که عاملیت امنیت در یک محصول پیشنهادی، الزامات مشخص شده را برآورده نمی‌کند؛ توصیه می‌شود ریسک مطرح شده و کنترل های مربوط، مجددا قبل از خرید محصول، مورد ملاحظه قرار گیرد. در جایی که کارا بودن افزودنی، در جایی که عاملیت افزودنی تامین می‌شود و باعث ایجاد یک ریسک امنیتی می‌شود، توصیه می‌شود این موضوع غیرفعال شود یا توصیه می‌شود ساختار کنترل پیشنهادی مورد بازنگری قرار گیرد تا تعیین که آیا مزیت را می‌توان از عاملیت پیشرفته در دسترس به دست آورد.

اطلاعات دیگر

اگر مثلا به دلایل هزینه ای مناسب در نظر گرفته شود، مدیریت ممکن است بخواهد از محصولاتی که به طور مستقل ارزشیابی و گواهی شده‌اند، استفاده کند. اطلاعات بیشتر درباره معیارهای ارزشیابی برای محصولات امنیتی فن‌آوری

اطلاعات را می‌توان در ISO/IEC 15408 یا دیگر استانداردهای ارزشیابی یا صدور گواهی بطوری که مناسب باشد، پیدا کرد.

ISO/IEC TR 13335-3 راهنمایی‌هایی درباره استفاده از فرایندهای مدیریت ریسک برای شناسایی الزاماتِ کنترل‌های امنیتی فراهم می‌کند.

۱۲-۲ پردازش صحیح در برنامه‌های کاربردی

هدف: پیشگیری از خطاها، گم شدن، دستکاری غیر مجاز یا استفاده نابجا از اطلاعات در برنامه‌های کاربردی.

توصیه می‌شود کنترل‌های مناسب در برنامه های کاربردی از جمله برنامه های کاربردی توسعه یافته توسط کاربر، طراحی شود تا از پردازش صحیح اطمینان حاصل شود. توصیه می‌شود این کنترل‌ها شامل صحه گذاری داده ورودی، پردازش داخلی و داده خروجی باشد.

ممکن است کنترل‌های افزودنی برای سیستم‌هایی که پردازش انجام می دهند، یا پیامدی روی اطلاعات حساس، با ارزش یا حیاتی دارند، لازم باشد. توصیه می‌شود چنین کنترل هایی بر پایه الزامات امنیتی و ارزیابی ریسک تعیین شوند.

۱۲-۲-۱ *صحه‌گذاری داده ورودی*

کنترل

توصیه می‌شود داده ورودی به برنامه‌های کاربردی، اعتباردهی شوند تا از درستی و تناسب این داده اطمینان حاصل شود.

راهنمای پیاده‌سازی

توصیه می‌شود بررسی‌هایی بر روی ورودی تراکنش های کسب وکار، داده دائمی (برای مثال، نام ها و آدرس ها، محدودیت های اعتباری، شماره های ارجاع مشتری)، و جداول پارامتری(برای مثال، قیمت های فروش، نرخ های تبدیل پول رایج، نرخ های مالیات) به کار گرفته شود. توصیه می‌شود رهنمودهای زیر در نظر گرفته شود:

الف - بررسی‌های ورودی دوگانه یا ورودی دیگر، نظیر بررسی مرز یا محدود کردن میدان ها به گستره مشخصی از داده ورودی، تا خطاهای زیر آشکار شود:

۱ - ارزش‌های خارج از گستره

۲ - کاراکترهای غیرمعتبر در میدان‌های داده

۳ - داده مفقودشده یا غیرکامل

۴ - تجاوز کردن از محدوده‌های بالا و پایین حجم داده

۵ - داده کنترلی غیرمجاز یا متناقض

ب - بازنگری دوره‌ای محتوای میدان‌های کلیدی یا فایل های داده برای تایید اعتبار و تمامیت آنها

پ - بازبینی مدارک چاپی ورودی برای تغییرات غیرمجاز (توصیه می‌شود همه تغییرات به مدارک ورودی مجاز باشند)

ت – روش های اجرایی برای پاسخ به خطاهای صحه گذاری

ث - روش های اجرایی برای آزمون معقول بودن داده ورودی

ج - تعریف مسوولیت‌های تمامی پرسنل درگیر در فرایند ورود داده

چ - ایجاد اطلاعات ثبت شده وقایع از فعالیتهای درگیر در فرایند ورود داده (رجوع کنیدبه ۱۰-۱۰-۱)

اطلاعات دیگر

امتحان خودکار و صحه گذاری داده ورودی در جایی که قابل اجرا است، می‌تواند در نظر گرفته شود، تا ریسک خطا ها را کاهش دهد و از حملات استاندارد شامل سرریز حافظه میانجی و تزریق کد جلوگیری بعمل آورد.

۱۲-۲-۲ *کنترل پردازش درونی*

کنترل

توصیه می‌شود بررسی های صحه گذاری در برنامه های کاربردی گنجانده شود تا هر خرابی اطلاعات درحین پردازش خطاها یا اقدامات عمدی آشکار شود.

راهنمای پیاده‌سازی

توصیه می‌شود طراحی و پیاده سازی برنامه های کاربردی، اطمینان دهد که ریسک های خرابی های پردازش که منجر به از دست رفت تمامیت می‌شود، حداقل شود. نواحی مشخص که مد نظر قرار می‌گیرند عبارتند از:

الف - استفاده از توابع اضاافه کردن، تغییر دادن و حذف برای پیاده سازی تغییرات در داده

ب – روش های اجرایی برای جلوگیری از برنامه هایی که در ترتیب انجام غلط در حال اجرا هستند یا پس از خطا در پردازش قبلی اجرا می‌شوند (همچنین رجوع کنید به بند ۱۰-۱-۱)

پ - استفاده از برنامه های مناسب برای بازیابی خرابی ها بمنظور اطمینان دهی از پردازش صحیح داده

ت - حفاظت در برابر حمله‌هایی که از اجراهای بیش از حد/ سرریزهای حافظه میانجی بهره می‌گیرد.

توصیه می‌شود یک چک لیست مناسب آماده شود، فعالیت‌ها مستند شوند و توصیه می‌شود نتایج امن نگه داشته شوند. مثال‌های بررسی‌هایی که می‌توانند مورد استفاده قرار گیرند عبارتند از:

الف - جلسه یا کنترل‌های گروهی، برای سازگار کردن فایل‌های داده‌ها پس از روزآمد شدن معاملات

ب - کنترل‌های تعادلی برای بررسی تعادل‌ها در مقایسه با تعادل‌های قبلی به عبارت دیگر:

۱ - کنترل‌های اجرا به ا جرا

۲ - کل بروزرسانی فایل ها

۳ - کنترل‌های برنامه به برنامه

پ - صحه گذاری داده‌های ورودی که در سیستم تولید شده اند(رجوع کنید به بند ۱۲-۲-۱):

ت - بررسی درباره یکپارچگی، موثق بودن، یا هر گونه ویژگی امنیتی داده‌ها یا نرم‌افزارهای بارگیری‌شده، یا بارگیری شده، بین رایانه‌های مرکزی و راه دور.

ث - کل سوابق و فایل‌ها بصورت درهم

ج - بررسی‌هایی برای تضمین این که برنامه‌های کاربرد در زمان صحیح اجرا می‌شوند

چ - بررسی‌هایی برای تضمین این که برنامه‌ها با ترتیب صحیح اجرا می‌شوند و در صورت بروز خطا پایان می‌یابند و این که پردازش بیشتر تا زمانی که مشکل حل شود متوقف می‌شود.

ه - ایجاد اطلاعات ثبت شده از فعالیت‌های موجود در پردازش(رجوع کنید به بند ۱۰-۱۰-۱)

اطلاعات دیگر

داده‌هایی که به درستی وارد شده اند ممکن است از طریق خطاهای سخت افـزاری، خطاهـای پـردازش یـا از طریـق فعالیت‌های عمدی مختل شوند. بررسی‌های اعتباردهی موردنیاز به ماهیت کاربرد و پیامد کسب وکار هر گونه اختلال در داده‌ها بستگی خواهد داشت.

۱۲-۲-۳ تمامیت پیغام

کنترل

توصیه می‌شود الزاماتی برای اطمینان از سندیت و حفاظت از یکپارچگی پیغام در برنامه‌های کاربردی، شناسایی شده و کنترل‌های مناسبی شناسایی و پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ارزیابی ریسک‌های امنیتی برای تعیین این که آیا یکپارچگی پیام لازم است و برای شناسایی مناسـب ترین روش اجرا انجام شود.

اطلاعات دیگر

روشهای رمزنگاری(رجوع کنید به بند ۱۲-۳) را می‌توان به عنوان ابزار مناسبی برای اجرای تعیین اعتبار پیـام مـورد استفاده قرار داد.

۱۲-۲-۴ صحه‌گذاری داده خروجی

کنترل

توصیه می‌شود به منظور حصول اطمینان از اینکه پردازش اطلاعات ذخیره شده، صحیح بوده و شرایط مناسبی دارد، داده‌های خروجی برنامه‌های کاربردی، صحه‌گذاری شوند.

راهنمای پیاده‌سازی

صحه‌گذاری خروجی ممکن است شامل موارد زیر باشد:

الف - بررسی‌های امکان پذیری برای آزمون این که آیا داده‌های خروجی معقول هستند:

ب - هماهنگ کردن حساب‌های کنترلی برای تضمین پردازش تمام داده‌ها

پ – ارایه اطلاعات کافی برای یک خواننده یا سیستم پردازش متعاقب آن برای تعیـین دقـت، کامـل بـودن، و طبقه بندی اطلاعات

ت - روش‌های اجرایی برای پاسخگویی به آزمون‌های صحه‌گذاری خروجی

ث - تعریف مسوولیت‌های تمام اشخاص دخیل در فرایند خروجی داده‌ها

ج - ایجاد اطلاعات ثبت شده از فعالیت‌ها در فرایند صحه‌گذاری خروجی داده‌ها

اطلاعات دیگر

معمولا سیستم‌ها و کاربردها با این فرض ساخته می‌شوند که پس از گذراندن صحه‌گذاری، تصـدیق، و آزمـون لازم و مناسب، نتیجه همیشه صحیح خواهد بود. به هر حال، این فرض همیشه معتبر نیست، به عبارت دیگر سیسـتم‌هـایی که آزموده شده اند ممکن است با این حال در بعضی شرایط خروجی نادرستی بدهند.

۱۲-۳ کنترل‌های رمزنگاری

هدف: حفاظت از محرمانگی، سندیت یا یکپارچگی اطلاعات، توسط مفاهیم رمزنگاری.
توصیه می‌شود یک خط‌مشی درباره استفاده از کنترل‌های رمزنگاری طراحی شود. توصیه می‌شود مدیریت کلیدی برای پشتیبانی از استفاده از روشهای رمزنگاری به کار گرفته شود.

۱۲-۳-۱ 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 توسعه یک خط‌مشی رمز نگاری موارد زیر در نظر گرفته شود:

الف - رویکرد مدیریت در قبال استفاده از کنترل‌های رمزنگاری در سازمان، از جمله اصول کلی که توصیه می‌شود اطلاعات کسب وکار تحت آن محافظت شود(همچنین رجوع کنید به بند ۵-۱-۱)

ب - بر اساس یک ارزیابی ریسک، توصیه می‌شود سطح مورد نیاز محافظت با احتساب نوع، مقاومت، و کیفیت الگوریتم رمزنگاری مورد نیاز شناسایی شود.

پ - استفاده از رمزنگاری برای محافظت از اطلاعات حساس که توسط رسانه‌های سیار یا قابل جابجایی، دستگاه‌ها یا خطوط ارتباطی حمل می‌شود.

ت - رویکرد در قبال مدیریت کلیدی، از جمله روش‌هایی برای پرداختن به محافظت از کلیدهای رمزنگاری و بازیابی اطلاعات رمزنگاری شده در صورت آسیب، خدشه یا صدمه

ث - نقش‌ها و مسوولیت‌ها مثلا این که چه کسی مسوول موارد زیر است:

۱ - اجرای خط‌مشی

۲ - مدیریت کلیدی از جمله تولید کلید (همچنین رجوع کنید به بند ۱۲-۳-۲)

ج - استانداردهایی که باید برای اجرای موثر در تمام سازمان مورداستفاده قرار گیرد. (که چه راه حلی برای چه فرایندهای کسب وکار استفاده می‌شود)

چ –پیامد استفاده از اطلاعات رمزنگاری شده درکنترل‌هایی که بر بررسی محتوا تکیه دارند. (برای مثال، آشکارسازی ویروس)

توصیه می‌شود در زمان اجرای خط مشی رمزنگاری سازمان، به مقررات و محدودیت‌های ملی که ممکن است در مورد استفاده از روشهای رمزنگاری در بخش‌های مختلف جهان اعمال شود و نیز به مسائل جریان گسترده اطلاعات رمزنگاری شده ملاحظه شود(همچنین رجوع کنید به بند ۱۵-۱-۶).

کنترل‌های رمزنگاری را می‌توان برای دستیابی به اهداف امنیت اطلاعات مورد استفاده قرار داد مثلا:

الف- محرمانگی: استفاده از رمزنگاری اطلاعات برای محافظت از اطلاعات حساس و حیاتی خواه ذخیره شده خواه منتقل شده؛

ب - یکپارچگی/موثق بودن: استفاده از امضاهای دیجیتال یا کدهای تایید پیام برای محافظت از موثق بودن و یکپارچگی اطلاعات حساس یا حیاتی ذخیره شده یا منتقل شده؛

پ - عدم انکار: استفاده از روش‌های رمز نگاری برای به دست آوردن شاهدی بر وقوع یا عدم وقوع یک واقعه یا فعالیت

اطلاعات دیگر

توصیه می‌شود تصمیم گیری درباره این که آیا راه حل رمزنگاری مناسب است، به عنوان بخشی از فرایند گسترده تر ارزیابی خطر و انتخاب کنترل‌ها در نظر گرفته شوند. این ارزیابی را سپس می‌توان برای تعیین این که آیا کنترل رمزنگاری مناسب است یا نه، چه نوع کنترلی توصیه می‌شود که به کار گرفته شود و برای کدام اهداف و فرایندهای کسب وکار به کار گرفته شود انجام داد.

سیاستی درباره استفاده از کنترل‌های رمزنگاری برای افزایش منافع و کاهش ریسک‌ها استفاده از روشهای رمزنگاری و اجتناب از استفاده نامناسب یا غیرصحیح لازم است. توصیه می‌شود در زمان استفاده از امضاهای دیجیتال به هر گونه قوانین مربوطه به خصوص قوانینی که شرایطی را توصیف می‌کنند که تحت آن، امضای دیجیتال قانونا الزام آور است ملاحظه شود(رجوع کنید به بند ۱۵-۱).

توصیه می‌شود مشاوره تخصصی برای شناسایی سطح مناسب محافظت و تعریف مشخصات مناسبی که محافظت مورد نیاز را ارایه خواهند کرد و اجرای یک سیستم مدیریت کلیدی ایمن را پشتیبانی خواهندکرد انجام شود.

ISO/IEC JTC1 SC27 چندین استاندارد را در رابطه با کنترل‌های رمزنگاری طراحی کرده است. اطلاعات بیشتر را همچنین می‌توانید در IEEE P1363 و رهنمودهای OECD در باره رمزنگاری پیدا کنید. (همچنین رجوع کنید به بند ۱۲-۳-۲)

۱۲-۳-۲ مدیریت کلید

کنترل

توصیه می‌شود به منظور پشتیبانی استفاده سازمان از فنون رمزنگاری، یک سیستم مدیریت کلید ایجاد شود.

راهنمای پیاده‌سازی

توصیه می‌شود تمام کلیدهای رمزنگاری در مقابل تغییر، آسیب و خرابی محافظت شوند. به علاوه، کلیدهای رمزی و خصوصی نیازمند محافظت در برابر دسترسی غیرمجاز دارند. توصیه می‌شود تجهیزات به‌کار رفته برای تولید ذخیره، و بایگانی کلیدها از نظر فیزیکی محافظت شود.

توصیه می‌شود یک سیستم مدیریت کلیدی بر اساس مجموعه مورد توافق استانداردها، رویه‌ها و روش‌های امن باشد برای:

الف - تولید کلید برای سیستم‌های رمزنگاری مختلف و کاربردهای مختلف

ب - تولید و به دست آوردن گواهینامه های کلیدی همگانی

پ - توزیع کلیدها بین کاربرهای مورد نظر از جمله این که توصیه می‌شود کلیدها چگونه در زمان دریافت فعال شوند؛

ت - ذخیره کلیدها از جمله این که چگونه کاربران مجاز به کلیدها دسترسی پیدا می‌کنند؛

ث - تغییر یا روزآمد کردن کلیدها از جمله نقش‌ها درباره این که توصیه می‌شود چه زمانی کلیدها تغییر کنند و این کار چگونه باید انجام شود.

ج - رسیدگی به کلیدهای خدشه واردشده

چ - پس گرفته کلیدها از جمله این که توصیه می‌شود چگونه کلیدها مسترد شوند یا غیرفعال شوند، مثلا زمانی که کلیده‌ها مورد آسیب قرار گرفته اند یا زمانی که یک کاربر از سازمان می رود. (در چه حالتی توصیه می‌شود که کلیدها بایگانی شوند)

ح - بازیابی کلیدهایی که گم می‌شوند یا مختل می‌شوند به عنوان بخشی از مدیریت استمرار کسب وکار مثلا برای بهبود اطلاعات رمزنگاری شده

خ - بایگانی کلیدها مثلا برای اطلاعات بایگانی شده یا کپی پشتیبان گرفته شده

د - تخریب کلیدها

ذ - واقعه نگاری و ممیزی فعالیت‌های مرتبط با مدیریت کلید

توصیه می‌شود به منظور کاهش احتمال آسیب، فعالی سازی و غیرفعال سازی، تاریخ‌هایی برای کلیدها تعریف شوند تا کلیدها را فقط بتوان برای دوره محدودی از زمان مورد استفاده قرار داد. توصیه می‌شود دوره زمان وابسته به شرایطی باشد که کنترل رمزنگاری تحت آن مورد استفاده قرار می‌گیرد.

علاوه بر مدیریت مطمئن کلیدهای خصوصی و رمزی، توصیه می‌شود اصیل بودن کلیدهای عمومی نیز در نظر گرفته شود. این فرایند احراز اصالت می‌تواند با استفاده از گواهینامه های کلید عمومی که معمولا توسط یک مرجع دارای اختیار صدور گواهی صادر می‌شود، -که توصیه می‌شود یک نهاد به رسمیت شناخته شده با کنترل ها و روش های اجرایی مناسب و بجا برای تامین درجه اطمینان مورد نیاز باشد-؛ انجام شود.

توصیه می‌شود محتوای قراردادها یا توافق‌نامه های سطح خدمات با تامین کنندگان بیرونی خدمات رمزنگاری - مثلا با یک مرجع دارای اختیار صدور گواهی-، موضوعات مسوولیت، اطمینانِ از خدمات، و زمان های پاسخ برای فراهم کردن خدمات را پوشش دهد(رجوع کنید به بند ۶-۲-۳).

اطلاعات دیگر

مدیریت کلیدهای رمزنگاری برای استفاده موثر از روشهای رمزنگاری لازم است.

ISO/IEC 11770 اطلاعات بیشتری را درباره مدیریت کلید ارایه می‌کند. دو نوع تکنیک رمزنگاری عبارتند از:

الف - روشهای کلید رمزی، در جایی که دو یا چند طرف، یک کلید را در اشتراک دارند و این کلید هم برای رمزنگاری و هم برای رمزگشای اطلاعات مورد استفاده قرار می‌گیرد. این کلید باید سری نگه داشته شود زیرا هر کسی که به کلید دسترسی داشته باشد می‌تواند تمام اطلاعاتی را که با آن کلید رمزنگاری می‌شود رمزگشایی کند یا اطلاعات غیرمجاز را با استفاده از کلید عرضه کند:

ب - روشهای کلید همگانی که در آن هر کاربر یک جفت کلید دارد؛ یک کلید همگانی و یک کلید خصوصی(که باید محرمانه نگهداری شود)؛ روشهای کلید همگانی را می‌توان برای رمزنگاری و تولید امضاهای دیجیتال مورد استفاده قرار داد (همچنین رجوع کنید به ISO/IEC 9796 و ISO/IEC 14888)

تهدید جعل یک امضای دیجیتال با جایگزین کردن یک کلید همگانی کاربر وجود دارد. این مشکل با استفاده از یک گواهینامه کلید همگانی مورد رسیدگی قرار می‌گیرد.

روشهای رمزنگاری را همچنین می‌توان برای محافظت از کلیدهای رمزنگاری مورد استفاده قرار داد. روش‌های اجرایی ممکن است برای پرداختن به تقاضاهای دسترسی به کلیدهای رمزنگاری وجود داشته باشد مثلا ممکن است لازم باشد اطلاعات رمزنگاری شده به شکلی رمزنگاری نشده مانند مدرکی در یک دادگاه در دسترس قرار گیرند.

۱۲-۴ امنیت فایل های سیستم

هدف: حصول اطمینان از امنیت پرونده‌های سیستم.
توصیه می‌شود دسترسی به فایل‌های سیستم و کد منبع برنامه کنترل شوند و پروژه‌های فن‌آوری اطلاعات و فعالیت‌های پشتیبانی به گونه‌ای ایمن انجام شوند. توصیه می‌شود مراقبت شود که از قرارگرفتن داده حساس در محیط‌های آزمون اجتناب شود.

۱۲-۴-۱ کنترل نرم‌افزار عملیاتی

کنترل
توصیه می‌شود به منظور کنترل نصب نرم‌افزار بر روی سیستم‌های عملیاتی، روش‌های اجرایی ایجاد شوند.
راهنمای پیاده‌سازی
توصیه می‌شود به منظور کاهش خطر اختلال در سیستم‌های عملیاتی رهنمودهای زیر، برای کنترل تغییرات در نظر گرفته شوند:

الف - توصیه می‌شود روزآمدسازی نرم‌افزار عملیاتی، عملکردها، و کتابخانه‌های برنامه فقط توسط مجریان آموزش دیده پس از تایید مدیریتی مناسب انجام شود(رجوع کنید به بند ۱۲-۴-۳)

ب - توصیه می‌شود سیستم‌های عملیاتی فقط کد قابل‌اجرای تایید شده را در اختیار بگیرند و نه کد توسعه یا همگردان‌ها را.

پ- توصیه می‌شود برنامه های کاربردی و نرم‌افزار سیستم عامل فقط پس از آزمون گسترده و موفقیت آمیز اجرا شود؛ توصیه می‌شود آزمون‌ها شامل آزمون‌هایی درباره قابل استفاده بودن، امنیت، تاثیرات بر دیگر سیستم‌ها و مناسب نبودن برای کاربر باشند و توصیه می‌شود درباره سیستم‌های جداگانه انجام شوند(رجوع کنید به بند ۱۰-۱-۴)؛ توصیه می‌شود تضمین شود که تمام کتابخانه‌های منبع برنامه متناظر روزآمد شده اند؛

ت - توصیه می‌شود سیستم کنترل پیکربندی برای حفظ کنترل تمام نرم‌افزارهای اجرا شده و نیز مستندات سیستم مورد استفاده قرار گیرند.

ث - توصیه می‌شود یک راهبرد کاهنده قبل از اجرای تغییرات در نظر گرفته شود.

ج - توصیه می‌شود اطلاعات ثبت شده حسابرسی از تمام روزآمدسازی‌های کتابخانه‌های برنامه عملیاتی نگهداری شود

چ - توصیه می‌شود نسخه‌های قبلی نرم‌افزار عملکرد، به عنوان یک اقدام همسوسازی حفظ شود.

ح - توصیه می‌شود نسخه‌های قدیمی نرم‌افزار، به همراه اطلاعات مورد نیاز و پارامترها، رویه‌ها، جزئیات پیکربندی، و نرم‌افزار پشتیبان برای مدت زمانی که داده‌ها در آرشیو نگهداری می‌شوند ذخیره شوند.

توصیه می‌شود نرم‌افزارهای تامین شده توسط فروشندگان که در سیستم‌های عملیاتی مورد استفاده قرار گرفتند، در سطح پشتیبانی شده توسط تامین کننده نگهداری شوند. با گذشت زمان، فروشندگان نرم‌افزار نسخه‌های قدیمی تر نرم‌افزار را پشتیبانی نمی‌کنند. توصیه می‌شود سازمان ریسک‌ها تکیه بر نرم‌افزار پشتیبانی نشده را در نظر بگیرد.

توصیه می‌شود هر تصمیمی برای روزآمدسازی به یک نسخه جدید الزامات کسب وکار را برای تغییر و امنیت نسخه جدید به حساب آورد، به عبارت دیگر معرفه یک کارایی جدید امنیتی یا تعداد و شدت مشکلات امنیتی که بر این مدل تاثیر می گذارند. توصیه می‌شود بسته‌های نرم‌افزاری در زمانی که می‌توانند به از بین بردن یا کاهش ضعف‌های امنیتی کمک کنند به کار گرفته شوند(همچنین رجوع کنید به بند ۱۲-۶-۱).

توصیه می‌شود دسترسی فیزیکی یا منطقی فقط به تامین کنندگان برای اهداف پشتیبانی در زمان لازم و با تایید مدیریت داده شود. توصیه می‌شود فعالیت‌های تامین کننده کنترل شوند.

نرم‌افزار رایانه‌ی ممکن است بر نرم‌افزارو مدول‌های ارایه شده از خارج تکیه داشته باشند که توصیه می‌شود برای اجتناب از تغییرات غیرمجازکه ممکن است ضعف‌های امنیتی ایجاد کند کنترل شوند.

اطلاعات دیگر

توصیه می‌شود سیستم‌های عامل فقط زمانی که لازم است روزآمد شوند مثلا اگر نسخه فعلی سیستم عامل دیگر الزامات کسب وکار را پشتیبانی نمی‌کند. توصیه می‌شود روزآمدسازی‌ها فقط به این دلیل که نسخه جدیدی از سیستم عامل موجود است رخ ندهند. نسخه‌های جدید سیستم‌های عامل ممکن است امنیت کمتری داشته باشندو کمتر از سیستم‌های فعلی درک شوند.

۱۲-۴-۲ *حفاظت از داده‌های آزمون سیستم*

کنترل

توصیه می‌شود داده‌های آزمون، به دقت انتخاب شده، محافظت و کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود استفاده از بانک‌های داده عملیاتی که حاوی اطلاعات شخصی است یا هر اطلاعات حساس دیگر برای اهداف آزمون اجتناب شود. اگر اطلاعات شخصی یا به هر جهت حساس برای اهداف تست(آزمون) مورد استفاده قرار گیرد، توصیه می‌شود تمام جزئیات حساس و محتوای حساس قبل از استفاده حذف شوند یا تغییر کنند. توصیه می‌شود رهنمودهای زیر برای محافظت از داده‌های عملیاتی زمانی که برای اهداف آزمونی له کار می روند به کار گرفته شود:

الف - رویه‌های کنترل دسترسی که در سیستم‌های کاربرد عملیاتی مورد استفاده قرار می‌گیرند نیز توصیه می‌شود در سیستم‌های آزمون عملکرد قرار گیرند.

ب - توصیه می‌شود هر زمان که اطلاعات عملیاتی روی یک سیستم عملیاتی آزمون کپی می‌شود مجوز جداگانه ای لازم باشد

پ - توصیه می‌شود اطلاعات عملیاتی از یک سیستم عملیاتی آزمون بلافاصله پس از کامل شدن آزمون حذف شوند.

ت - توصیه می‌شود کپی کردن و استفاده از اطلاعات عملیاتی واقعه‌نگاری شود تا بعنوان داده ممیزی در دسترس قرار گیرد.

اطلاعات دیگر

آزمون پذیرش و سیستم معمولا نیازمند حجم‌های مهمی از داده‌های آزموده هستند که تا حد امکان به داده‌های عملیاتی نزدیک هستند.

۱۲-۴-۳ 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 مربوطه (مانند طراحی ها، مشخصات، طرح های تصدیق، طرح های صحه گذاری)، شدیدا کنترل شود تا از امکان کارایی غیرمجاز جلوگیری شود و از تغییرات غیرعمدی اجتناب شود. برای کد منبع برنامه، این را می‌توان از طریق ذخره مرکزی کنترل شده این کد، ترجیحا در کتاب‌خانه‌های منبع برنامه به دست آورد. رهنمودهای زیر، باید برای کنترل دسترسی به این کتابخانه‌های منبع برنامه به منظور کاهش پتانسیل اختلال برنامه‌های رایانه‌ی در نظر گرفته شوند(همچنین رجوع کنید به ۱۱):

الف - توصیه می‌شود در هر جایی که ممکن باشد، کتابخانه‌های منبع برنامه در سیستم‌های عملیاتی نگهداری نشوند

ب - توصیه می‌شود کد منبع برنامه و کتابخانه‌های منبع برنامه مطابق با رویه‌های تثبیت شده مدیریت شوند

پ - توصیه می‌شود پرسنل پشتیبانی دسترسی نامحدود به کتابخانه‌های منبع برنامه نداشته باشند.

ت - توصیه می‌شود روزآمدسازی کتابخانه‌های منبع برنامه و زمان‌های مربوطه، و صدور منابع برنامه برای برنامه ریزها فقط پس از دریافت تایید مناسب انجام شوند.

ث - توصیه می‌شود فهرست‌های برنامه در یک محیط ایمن نگهداری شوند. (رجوع کنید به بند ۱۰-۷-۴)

ج - توصیه می‌شود اطلاعات ثبت شده حسابرسی از تمام دسترسی‌ها به کتابخانه‌های منبع برنامه نگهداری شوند

چ - توصیه می‌شود نگهداری و کپی کتابخانه‌های منبع برنامه منوط به رویه‌های شدید کنترل تغییر باشد(رجوع کنید به بند ۱۲-۵-۱)

اطلاعات دیگر

کد منبع برنامه کدی است که توسط برنامه نویس‌ها نوشته می‌شود و برای ایجاد موارد قابل‌اجرا تدوین (و پیوند) می‌شود. زبان‌های برنامه نویسی خاص به طور رسمی بین کد منبع و موارد قابل‌اجرا تمایز قائل نمی‌شوند زیرا قابل‌اجراها در زمانی که فعال می‌شوند ایجاد می‌شوند.

استانداردهای ISO10007 و ISO/IEC 12207 اطلاعات بیشتری را درباره مدیریت پیکربندی و فرایند چرخه نرم‌افزار ارایه می‌کنند.

۱۲-۵ امنیت در فرایندهای بهبود و پشتیبانی

هدف: حفظ امنیت نرم‌افزار و اطلاعات سیستم کاربردی.

توصیه می‌شود محیط‌های پروژه و پشتیبانی شدیدا کنترل شوند.

توصیه می‌شود مدیرانی که مسئول سیستم‌های کاربرد هستند مسوول امنیت پروژه یا محیط پشتیبانی باشند.

توصیه می‌شود آنها تضمین کنند که تمام تغییرات سیستم‌های پیشنهادی بررسی می‌شوند تا بررسی شود که آنها به امنیت سیستم یا محیط عملکرد خدشه وارد نمی‌کنند.

۱۲-۵-۱ روش‌های اجرایی کنترل تغییر

کنترل

توصیه می‌شود با استفاده از روش‌های اجرایی رسمی کنترل تغییر، پیاده‌سازی تغییرات کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رویه‌های کنترل تغییرات رسمی به منظور کاهش اختلال سیستم‌های اطلاعاتی مستند و اجرا شوند.

توصیه می‌شود عرضه سیستم‌های جدید و تغییرات عمده در سیستم‌های فعلی یک فرایند رسمی مستندسازی، مشخص سازی، آزمون، کنترل کیفیت و اجرای مدیریت شده را دنبال کند.

توصیه می‌شود این فرایند شامل یک ارزیابی ریسک، تحلیل پیامدهای تغییرات، و مشخصات کنترل‌های امنیتی موردنیاز باشد. توصیه می‌شود این فرایند همچنین تضمین نماید که رویه‌های فعلی امنیت و کنترل، مختل نمی‌شوند و برنامه نویس‌ها دسترسی را فقط به بخش‌هایی از سیستم دارند که برای کارشان لازم است و این که قرارداد و تایید رسمی برای هر تغییر کسب می‌شود.

توصیه می‌شود در صورت امکان، رویه‌های تغییر عملیاتی و عملکرد یکپارچه باشند(همچنین رجوع کنید به بند ۱۰-۱-۲). توصیه می‌شود رویه‌های تغییرات شامل موارد زیر باشند:

الف - حفظ گزارشی از سطوح تایید مورد توافق

ب - تضمین تغییرات توسط کاربران مجاز ارایه می‌شوند.

پ - بررسی کنترل‌ها و رویه‌های یکپارچگی برای تضمین این که آنها بواسطه تغییرات مختل نخواهند شد.

ت- شناسایی همه نرم‌افزارها، اطلاعات، موجودیت های بانک داده، و سخت افزار که اصلاحاتی را نیاز دارند.

ث - به دست آوردن تایید رسمی برای پیشنهادهای مفصل قبل از آغاز کار

ج - تضمین این که کاربران مجاز تغییرات را قبل از اجرای آنها می پذیرند.

چ - تضمین این که مجموعه مستندسازی سیستم پس از تکمیل هر تغییر روزآمد می‌شود و این که مستندسازی بایگانی می‌شود یا دور ریخته می‌شود

ح - حفظ یک نسخه کنترل برای تمام روزآمدسازی‌های نرم‌افزار

خ - حفظ یک گزارش ممیزی از تمام تقاضاهای تغییرات

د - تضمین این که مستندسازی عملیات(رجوع کنید به بند ۱۰-۱-۱) و رویه‌های کاربر در زمان لازم تغییر می‌کنند تا مناسب باقی بمانند.

ذ - تضمین این که اجرای تغییرات در زمان صحیح رخ می‌دهد و فرایندهای کسب وکار مربوطه را مختل نمی‌کند

اطلاعات دیگر

تغییر نرم‌افزار می‌تواند بر محیط عملیاتی تاثیر بگذارد.

عملکرد خوب شامل آزمون نرم‌افزار جدید در محیطی است که هم از محیط تولید و هم از محیط توسعه جدا شده باشد(همچنین رجوع کنید به بند ۱۰-۱-۴). این ابزاری برای کنترل بر نرم‌افزار جدید و ایجاد محافظت اضافه اطلاعات عملیاتی که برای اهداف آزمون مورد استفاده قرار می‌گیرد ایجاد می‌کند. توصیه می‌شود این شامل بسته‌های خدمات، و دیگر روزآمدسازی‌ها باشد. توصیه می‌شود روزآمدسازی‌های اتوماتیک در سیستم‌های حیاتی انجام نشوند زیرا بعضی روزآمدسازی‌ها ممکن است باعث ایجاد مشکل در کاربردهای حیاتی شوند (رجوع کنید به بند ۱۲-۶)

۱۲-۵-۲ بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات سیستم عامل

کنترل

توصیه می‌شود در هنگام تغییر سیستم‌های عامل، به منظورحصول اطمینان از عدم وجود پیامد سوء بر عملیات یا امنیت سازمانی، نرم‌افزارهای کاربردی حیاتی کسب‌وکار بازنگری و آزموده شوند.

راهنمای پیاده‌سازی

توصیه می‌شود این فرایند موارد زیر را پوشش دهد:

الف - بررسی کنترل کاربرد و رویه‌های یکپارچگی برای تضمین این که آنها از طریق تغییرات در سیستم عامل مختل نشده‌اند.

ب - تضمین این که برنامه و بودجه پشتیبانی سالانه بررسی‌ها و آزمون سیستم را که از تغییرات سیستم عامل ناشی می‌شوند پوشش خواهد داد.

ت - تضمین این که اعلام تغییرات سیستم عامل به موقع انجام می‌شود تا آزمون‌ها و بررسی‌های مناسب قبل از اجرا امکان پذیر شوند.

ث - تضمین این که تغییرات مناسب در برنامه‌های استمرار کسب وکار انجام می‌شوند(رجوع کنید به بند ۱۴).

توصیه می‌شود یک گروه یا فرد خاص مسوولیت کنترل آسیب‌پذیری‌ها و پخش بسته‌ها توسط فروشنده را به عهده داشته باشد (رجوع کنید به بند ۱۲-۶).

۱۲-۵-۳ محدودسازی در اعمال تغییرات در بسته‌های نرم‌افزاری

کنترل

توصیه می‌شود از دستکاری در بسته‌های نرم‌افزاری، اجتناب شده، محدود به تغییرات ضروری باشد، و توصیه می‌شود تمامی تغییرات به شدت کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود تا حد امکان بسته‌های نرم‌افزاری تهیه شده توسط فروشندگان بدون تغییر مورد استفاده قرار گیرد.

توصیه می‌شود هر زمان که یک بسته نرم‌افزاری تغییر کند، نکات زیر باید رعایت شود:

الف - خطر کنترل‌های درونی و فرایندهای یکپارچه ای که مختل می‌شوند

ب - توصیه می‌شود این که آیا رضایت فروشنده کسب شود یا نه

پ - احتمال دریافت تغییرات لازم از فروشنده به صورت روزآمدسازی‌های برنامه استاندارد

ت –پیامد این که اگر سازمان مسوول نگهداری نرم‌افزار در نتیجه تغییر در آینده شود

اگر تغییرات لازم باشد توصیه می‌شود نرم‌افزار اصلی تهیه شود و تغییرات به یک نسخه ای که کاملا شناسایی شده است اعمال شود. یک فرآیند مدیریت روزآمدسازی نرم‌افزار، توصیه می‌شود برای تضمین این که روزآمدترین بسته‌های تایید شده و روزآمدسازی‌های کاربرد برای تمام نرم‌افزار مجاز نصب می‌شوند اجرا شود(رجوع کنید به بند ۱۲-۶). توصیه می‌شود تمام تغییرات به طور کامل آزموده و مستند شود به گونه ای که آنها را بتوان در صورت لزوم در روزآمدسازی‌های نرم‌افزاری آینده مجددا به کار برد. در صورت لزوم، توصیه می‌شود تغییرات توسط یک نهاد ارزیابی مستقل آزموده و اعتبار بخشی شود.

۱۲-۵-۴ نشت اطلاعات

کنترل

توصیه می‌شود از فرصتهای نشت اطلاعات، پیشگیری شود.

راهنمای پیاده‌سازی

توصیه می‌شود موارد زیر برای محدود کردن ریسک نشت اطلاعات مثلا از طریق استفاده از کانال‌های مخفی در نظر گرفته شود:

الف - جستجوی رسانه‌ها و ارتباطات خارج از باند برای اطلاعات مخفی

ب – پنهان کردن و مدوله کردن سیستم و رفتار ارتباطات برای کاهش احتمال این که یک شخص سوم بتواند اطلاعات را از چنین رفتاری استنباط کند

پ - استفاده از سیستم‌ها و نرم‌افزاری که یکپارچگی بالایی دارند مثلا استفاده از محصولات ارزیابی شده (رجوع کنید به بند ISO/IEC 15408)

ت - کنترل منظم فعالیت‌های پرسنل و سیستم در صورت مجاز بودن تحت مقررات موجود

ث - کنترل استفاده از منابع در سیستم‌های رایانه‌ی

اطلاعات دیگر

کانال‌های پنهان مسیرهایی هستند که هدف از ایجادشان هدایت جریان اطلاعات ناست اما ممکنم است با این حال در یک سیستم یا یک شبکه وجود داشته باشند. مثلا دستکاری بیت‌ها در بسته‌های پروتکل ارتباطات را می‌توان به عنوان روشی مخفی برای سیگنال دهی مورد استفاده قرار داد. به دلیل ماهیت شان، پیشگیری از وجود تمام کانال‌های پنهان اگر غیرممکن نباشد مشکل خواهد بود. به هر حال استفاده از این کانال‌ها اغلب توسط کد تروجان انجام می‌شود(همچنین رجوع کنید به بند ۱۰-۴-۱). بنابراین اقداماتی برای محافظت از کد تروجان ریسک استفاده از کانال‌های پنهان را کاهش می‌دهد.

پیشگیری از دسترسی غیرمجاز به شبکه(۱۱-۴) و نیز سیاست‌ها و رویه‌های جلوگیری از سوء استفاده از خدمات اطلاعات توسط پرسنل(۱۵-۱-۵) به محافظت دربرابر کانال‌های پنهان کمک می‌کند.

۱۲-۵-۵ بهبود نرم‌افزار برون‌سپاری شده

کنترل

توصیه می‌شود توسعهٔ نرم‌افزار برون‌سپاری شده، توسط سازمان، نظارت و پایش شود.

راهنمای پیاده‌سازی

در جایی که توسعه نرم‌افزار از بیرون تامین می‌شود، توصیه می‌شود نکات زیر مد نظر قرار گیرد:

الف - تایید قراردادها، مالکیت کد، و حقوق مالکیت فکری (رجوع کنید به بند ۱۵-۱-۲)

ب – گواهی کردن کیفیت و دقت و صحت کار انجام شده

پ - مدیریت وجه الضمان‌ها در صورت کوتاهی شخص سوم

ت - حقوق دسترسی برای ممیزی کیفیت و دقت کار انجام شده

ث - الزامات قراردادی برای کارایی کیفیت و امنیت کد

ج - آزمون قبل از نصب برای کشف کد نامناسب و تروجان

۱۲-۶ مدیریت آسیب‌پذیری فنی

هدف: کاهش مخاطرات منتج از سوء استفاده از آسیب‌پذیری‌های فنی منتشر شده.
توصیه می‌شود مدیریت آسیب‌پذیری فنی به گونه ای موثر، سیستماتیک و قابل تکرار با اقدامات انجام شده در جهت تایید تاثیر آن انجام شود. توصیه می‌شود این ملاحظات شامل سیستم‌های عامل، و هر کاربرد دیگری که در حال استفاده است باشند.

۱۲-۶-۱ کنترل آسیب‌پذیری‌های فنی

کنترل

اطلاعات بهنگام در خصوص آسیب پذیری‌های فنی سیستم‌های اطلاعاتی مورد استفاده، توصیه می‌شود که کسب شده، قرار گرفتن سازمان در معرض چنین آسیب‌پذیری‌هایی ارزیابی شده، و معیارهای مناسبی برای نشان دهی ریسک‌ها مربوطه، برگزیده شوند.

راهنمای پیاده‌سازی

یک لیست موجودی جدید و کامل از دارایی‌ها(رجوع کنید به بند ۷-۱) پیش نیاز مدیریت موثر آسیب‌پذیری فنی است. اطلاعات خاص مورد نیاز برای پشتیبانی مدیریت آسیب‌پذیری فنی شامل فروشنده نرم‌افزار، تعداد نسخه‌ها، وضعیت فعلی استقرار (برای مثال چه نرم‌افزاری روی چه سیستمی نصب می‌شود)، و شخص یا اشخاص دخیل در سازمان که مسوول نرم‌افزار هستند است.

توصیه می‌شود فعالیت مناسب و به موقع در پاسخ به شناسایی آسیب پریری‌های فنی بالقوه صورت گیرد. توصیه می‌شود راهنمایی‌های زیر برای تثبیت یک فرایند مدیریت موثر برای آسیب‌پذیری‌های فنی دنبال شوند:

الف - توصیه می‌شود سازمان نقش‌ها و مسوولیت‌های مربوط به مدیریت آسیب‌پذیری فنی از جمله کنترل آسیب‌پذیری، ارزیابی ریسک آسیب‌پذیری، بسته بندی، ردیابی دارایی‌ها، و هر هماهنگی مورد نیاز را تعریف و ایجاد کند.

ب - منابع اطلاعات که برای شناسایی آسیب‌پذیری‌های فنی مربوطه و حفظ آگاهی درباره آنها مورد استفاده قرار خواهد گرفت توصیه می‌شود برای نرم‌افزار و فن‌آوری دیگر شناسایی شود. (بر اساس لیست موجودی دارایی‌ها، رجوع کنید به بند ۷-۱-۱)؛ توصیه می‌شود این منابع اطلاعات بر اساس تغییرات در لیست موجودی یا در زمانی که منابع جدید یا مفیدی پیدا می‌شوند روزآمد شوند.

پ - توصیه می‌شود برای واکنش به اعلام آسیب‌پذیری‌های فنی مربوطه یک زمان بندی تعریف شود

ت - به محض این که یک آسیب‌پذیری فنی بالقوه شناسایی شد، توصیه می‌شود سازمان ریسک‌های مربوطه و فعالیت‌های مورد نیاز را شناسایی کند. این فعالیت‌ها ممکن است دربرگیرنده دسته بندی گروه‌های آسیب‌پذیر و یا به کارگیرِ کنترل‌های دیگر باشد

ث - با توجه به این که یک آسیب‌پذیری فنی با چه اولویتی باید مورد رسیدگی قرار گیرد، توصیه می‌شود فعالیت‌های انجام شده مطابق با کنترل‌های مربوط به مدیریت تغییر (رجوع کنید به بند ۱۲-۵-۱) یا با پیروی از رویه‌های واکنش به رخدادهای امنیتی اطلاعات انجام شوند (رجوع کنید به بند ۱۳-۲).

ج - اگر یک وصله[1] در دسترس باشد، توصیه می‌شود ریسک‌های مربوط به نصب دسته‌های جدید ارزیابی شود (برای مثال، توصیه می‌شود ریسک‌های مطرح شده بوسیله آسیب پذیری سیستم با ریسک‌های نصب وصله مقایسه شود)

چ - توصیه می‌شود دسته‌ها قبل از این که نصب شوند آزموده و ارزیابی شوند تا تضمین شود که آنها موثر هستند و منجر به عوارض جانبی غیرقابل تحمل نمی‌شود. اگر هیچ دسته ای موجود نباشد، توصیه می‌شود کنترل‌های دیگر در نظر گرفته شود نظیر:

۱ - متوقف کردن خدمات یا قابلیت‌های مربوط به آسیب‌پذیری

۲ - استفاده یا اضافه کردن کنترل‌های دسترسی مانند دیوارهای آتش در مرزهای شبکه(رجوع کنید به بند ۱۱-۴-۵)

۳ - افزایش نظارت برای کشف یا پیشگیری از حملات واقعی

۴ - افزایش آگاهی از آسیب‌پذیری

ح - توصیه می‌شود اطلاعات ثبت شده حسابرسی برای تمام رویه‌های مورد نظر نگهداری شود

خ - توصیه می‌شود فرایند مدیریت آسیب‌پذیری فنی به طور منظم نظارت شود و به منظور تضمین تاثیر و بازدهی اش ارزیابی شود.

د - توصیه می‌شود سیستم‌هایی که در معرض ریسک بالا قرار دارند ابتدا مورد رسیدگی قرار گیرند.

اطلاعات دیگر

عملکرد صحیح یک فرایند مدیریت آسیب‌پذیری فنی سازمان برای بسیاری از سازمان‌ها حیاتی است و بنابراین توصیه می‌شود به طور منظم کنترل شود. یک لیست موجودی دقیق برای تضمین این که آسیب‌پذیری‌های فنی مربوطه شناسایی می‌شوند لازم است.

مدیریت آسیب‌پذیری فنی را می‌توان به عنوان یک عملکرد فرعی مدیریت تغییر دانست و بدین ترتیب می‌تواند از مزیت فرایندها و رویه‌های مدیریت تغییر استفاده کند(رجوع کنید به بند ۱۰-۱-۲ و ۱۲-۵-۱)

فروشندگان اغلب زیر فشار زیادی برای پخش بسته‌ها در سریع ترین زمان ممکن قرار دارند. بنابراین، یک دسته نمی‌تواند به مشکل به اندازه کافی برسد و ممکن است تاثیرات جانبی منفی داشته باشد. همچنین در بعضی موارد، برداشتن یک دسته ممکن است به سادگی به محض استفاده از دسته امکان پذیر نباشد.

اگر آزمون کافی از دسته‌ها ممکن نباشد، مثلا به دلیل هزینه یا نبود منابع، تاخیری در دسته بندی را می‌توان برای ارزیابی ریسک‌های مربوطه بر اساس تجربه گزارش شده توسط کاربران دیگر در نظر گرفت.

1- Patch

۱۳ مدیریت رخدادهای امنیت اطلاعات

۱-۱۳ گزارش‌دهی وقایع و ضعف‌های امنیت اطلاعات

هدف: حصول اطمینان از اینکه وقایع و ضعف‌های امنیت اطلاعات مربوط به سیستم‌های اطلاعاتی، به شیوه ای به اطلاع برسد که اجازهٔ اقدام اصلاحی بهنگام را بدهد.

توصیه می‌شود گزارش رسمی وقایع و رویه‌های افزایشی به کار گرفته شود. توصیه می‌شود تمام کارکنان، پیمانکاران، و کاربران شخص ثالث از رویه‌های گزارش انواع مختلف وقایع و ضعف‌هایی که ممکن است بر امنیت دارایی‌های سازمان تاثیر بگذارند مطلع شوند. توصیه می‌شود از آنها خواسته شود هر واقعه و ضعف امنیت اطلاعات را در اسرع وقت به نقطه تماس تعیین شده گزارش کنند.

۱-۱-۱۳ گزارش‌دهی وقایع امنیت اطلاعات

کنترل

توصیه می‌شود وقایع امنیت اطلاعات در کوتاهترین زمان ممکن، از طریق مجاری مدیریتی مناسب، گزارش شوند.

راهنمای پیاده‌سازی

توصیه می‌شود یک رویه گزارش رسمی وقایع امنیت اطلاعات ایجاد شود و رویه ای برای واکنش به رخدادها نیز باید ایجاد شود که فعالیت‌هایی را که باید در زمان دریافت گزارشی مبنی بر یک واقعه امنیت اطلاعات انجام شود تعریف می‌کند. توصیه می‌شود یک محل گزارش‌دهی برای گزارش وقایع امنیت اطلاعات ایجاد شود. توصیه می‌شود که تضمین شود که این محل گزارش‌دهی در سراسر سازمان، شناخته شده است و همیشه در دسترس بوده و توانایی ارایه واکنش کافی و به موقع را دارد.

توصیه می‌شود تمام کارکنان، پیمانکاران، و کاربران شخص سوم از مسوولیت شان در گزارش هر واقعه امنیت اطلاعات در اسرع وقع آگاه باشند. توصیه می‌شود آنها از رویه گزارش وقایع امنیت اطلاعات و محل گزارش‌دهی آگاه باشند. توصیه می‌شود رویه‌های گزارش شامل موارد زیر باشد:

الف - فرآیندهای انعکاس مناسب برای تضمین این که کسانی که وقایع امنیت اطلاعات را گزارش می‌کنند از نتایج پس از رسیدگی به مساله آگاه هستند

ب - فرم‌های گزارش وقایع امنیت اطلاعات برای پشتیبانی فعالیت گزارش و برای کمک به شخص گزارش کننده برای به یاد داشتن تمام فعالیت‌های لازم در صورت وقوع حادثه امنیت اطلاعات

پ - رفتار صحیح که باید در صورتی که یک حادثه امنیت اطلاعات رخ داد؛ انجام شود

۱ - اعلام فوری تمام جزئیات مهم (برای مثال، نوع عدم انطباق یا نقض، پدیدآمدن عیب فنی، پیغام های روی صفحه نمایش، رفتار عجیب)

۲ - عدم انجام هر گونه فعالیت خودسرانه اما گزارش آنی آن به محل گزارش‌دهی

ت - اشاره به فرآیند انضباطی رسمی تثبیت شده برای برخورد با کارکنان، پیمانکاران، یا کاربران شخص سومی که مرتکب رخنه امنیتی شده اند.

در محیط‌های پر خطر، یک هشدار اجباری ممکن است ارایه شود تا از طریق آن، شخص، تحت اجبار بتواند این مشکلات را نشان دهد. توصیه می‌شود رویه‌هایی پاسخگویی به هشدارهای اجبار نشان دهنده شرایط پرخطری باشد که این هشدارها نشان می‌دهند.

اطلاعات دیگر

مثال‌های رخدادهای امنیت اطلاعات عبارتند از:

الف - آسیب به خدمات، تجهیزات یا تاسیسات

ب - عملکرد نامناسب یا سرریز کردن سیستم

پ - خطاهای انسانی

ت - عدم انطباق با خط‌مشی‌ها و رهنمودها

ث - نقض هماهنگی‌های امنیت فیزیکی

ج - تغییرات کنترل نشده سیستم

چ - عملکرد نامناسب نرم‌افزار یا سخت افزار

ح - نقض دسترسی

با مراقبت مناسب از جنبه‌های محرمانگی، رخدادهای امنیت اطلاعات را می‌توان در آموزش آگاهانه کاربران به کاربرد(رجوع کنید به بند ۸-۲-۲)، مثلا در آموزش آنچه که ممکن است رخ دهد، نحوه واکنش به این رخدادها و نحوه اجتناب از آنها در آینده است. برای ایجاد امکان پرداختن به رخدادهای امنیت اطلاعات به طور مناسب، ممکن است لازم باشد که شواهد در اسرع وقت پس از وقوع جمع آوری شوند. (رجوع کنید به بند ۱۳-۲-۳)

عملکرد نامناسب یا دیگر رفتارهای نامناسب سیستم ممکن است نشان دهنده یک حمله امنیتی یا رخنه امنیتی باشد و بنابراین توصیه می‌شود همیشه به عنوان واقعه امنیت اطلاعات گزارش شود.

اطلاعات بیشتر درباره گزارش رخدادهای امنیت اطلاعات و مدیریت وقایع امنیت اطلاعات را می‌توان در ISO/IECTR 18044 پیدا کرد.

۱۳-۱-۲ گزارش‌دهی ضعف‌های امنیتی

کنترل

توصیه می‌شود تمامی کارکنان، پیمانکاران و کاربران شخص سوم سیستم‌ها و خدمات اطلاعاتی، نسبت به یادداشت و گزارش‌دهی هر ضعف امنیتی مشاهده شده یا مورد سوء ظن در سیستم‌ها یا خدمات، ملزم شوند.

راهنمای پیاده‌سازی

توصیه می‌شود تمام کارمندان، پیمانکاران و کابران شخص سوم این موضوعات را در اولین فرصت ممکن یا به مدیران‌شان و یا به بطور مستقیم به تامین کننده سرویس‌شان گزارش کنند تا از ریسک‌های رخدادهای امنیت اطلاعات جلوگیری شود. توصیه می‌شود ساز و کار گزارش، ساده و تا حد امکان قابل دسترسی باشد. همچنین توصیه می‌شود آنها مطلع شوند که در هیچ شرایطی سعی نکنند یک ضعف مشکوک را به اثبات برسانند.

اطلاعات دیگر

به کارکنان، پیمانکاران و کاربران شخص سوم باید توصیه شود سعی نکنند ضعف‌های امنیتی مشکوک را اثبات کنند. آزمون ضعیف ممکن است به عنوان سوء استفاده احتمالی از سیستم تلقی شود و همچنین ممکن است باعث آسیب به سیستم اطلاعات یا خدمات شود و منجر به ایجاد مسوولیت قانونی برای شخصی شود که آزمون را انجام می‌دهد.

۱۳-۲ مدیریت رخدادها و بهبودهای امنیت اطلاعات

هدف: حصول اطمینان از اینکه رویکردی استوار و موثر برای مدیریت رخدادهای امنیت اطلاعات، بکار گرفته شده است.

توصیه می‌شود مسوولیت‌ها و رویه‌هایی برای پرداختن به وقایع و ضعف‌های امنیت اطلاعات به محض این که گزارش شدند در نظر گرفته شود. توصیه می‌شود یک فرآیند بهبود مداوم برای واکنش، کنترل، ارزیابی و مدیریت رخدادهای امنیت اطلاعات به کار گرفته شود.

توصیه می‌شود هر زمان که شواهدی لازم است، جمع آوری شود تا انطباق با الزامات قانونی تضمین شود

۱۳-۲-۱ مسوولیت‌ها و روش‌های اجرایی

کنترل

توصیه می‌شود به منظور حصول اطمینان از یک پاسخ سریع، موثر و منظم به رخدادهای امنیت اطلاعات، مسوولیت‌های مدیریتی و روش‌های اجرایی ایجاد شوند.

راهنمای پیاده‌سازی

علاوه بر گزارش رخدادها و ضعف‌های امنیت اطلاعات (همچنین رجوع کنید به بند ۱۳-۱)، توصیه می‌شود کنترل سیستم‌ها، هشدارها، و آسیب‌پذیری‌ها (۱۰-۱۰-۲) برای کشف رخدادهای امنیت اطلاعات مورد استفاده قرار گیرند.

توصیه می‌شود رهنمودهای زیر برای اجرای رویه‌های مدیریت وقایع امنیت اطلاعات در نظر گرفته شوند:

الف - توصیه می‌شود رویه‌هایی برای رسیدگی به انواع مختلف رخدادهای امنیت اطلاعات تثبیت شود که شامل موارد زیر است:

۱ - خرابی‌های سیستم اطلاعات و آسیب به خدمات

۲ - کد نامناسب (رجوع کنید به بند ۱۰-۴-۱)

۳ - انکار خدمات

۴ - خطاهایی که از داده‌های کسب وکار ناقص یا غیردقیق ناشی می‌شوند.

۵ - رخنه در محرمانگی و یکپارچگی

۶ - سوء استفاده از سیستم‌های اطلاعات

ب - علاوه بر برنامه‌های عادی(رجوع کنید به بند ۱۴-۱-۳)، توصیه می‌شود رویه‌هایی موارد زیر را پوشش دهند(همچنین رجوع کنید به بند ۱۳-۲-۲):

۱ - تحلیل و شناسایی علت دقیق رخداد

۲ - محدودسازی

۳ - برنامه ریزی و اجرای فعالیت اصلاحی برای پیشگیری از وقوع مجدد در صورت لزوم؛

۴ - ارتباط با آنهایی که تحت تاثیر رخداد قرار دارند یا در آن مشارکت دارند

۵ - گزارش فعالیت به مرجع مناسب

پ - توصیه می‌شود گزارش‌های ممیزی و شواهد مشابه جمع آوری شوند (رجوع کنید به بند ۱۳-۲-۳) و امنیت شان تامین شود که برای موارد زیر مناسب باشند:

۱- تحلیل مسایل داخلی
۲ - استفاده به عنوان شواهد دادگاهی در رابطه با نقض احتمالی قرارداد یا الزامات قانونی یا در واقعه غیرنظامی یا اقدامات جنایی مثلا در شرایط سوء استفاده از رایانه یا قوانین محافظت از داده‌ها
۳ - مذاکره برای دریافت خسارت از تامین کنندگان نرم‌افزار و خدمات

ت - توصیه می‌شود فعالیت‌هایی برای نجات از رخنه های امنیتی و اصلاح خطاهای سیستم با دقت و به طور رسمی‌کنترل شود. توصیه می‌شود این رویه‌ها تضمین کنند که:

۱ - فقط کارکنانی که شناخته شده و مجاز هستند اجازه دسترسی به سیستم‌های زنده و داده‌ها را دارند(همچنین برای دسترسی خارجی، رجوع کنید به بند ۶-۲)
۲ - تمام فعالیت‌های اضطراری به طور مفصل مستند می‌شوند
۳ - فعالیت اضطراری به مدیریت گزارش می‌شود و به صورت منظم بررسی می‌شود
۴ - یکپارچگی سیستم‌های کسب وکار و کنترل‌ها با حداقل تاخیر تایید می‌شود.

توصیه می‌شود اهداف مدیریت رخدادهای امنیت اطلاعات با مدیریت مورد توافق قرار گیرد و توصیه می‌شود که تضمین شود که کسانی که مسوول مدیریت رخدادهای امنیت اطلاعات هستند اولویت‌های سازمان را برای پرداختن به رخدادهای امنیت اطلاعات درک می‌کنند.

اطلاعات دیگر

رخدادهای امنیت اطلاعات ممکن است از مرزهای سازمانی و ملی فرا رود. به منظور واکنش به این رخدادها نیاز فزاینده ای به هماهنگ کردن در ارایه عکس‌العمل و اشتراک اطلاعات درباره این رخدادها با سازمان‌های بیرونی در زمان مناسب وجود دارد.

۱۳-۲-۲ یادگیری از رخدادهای امنیت اطلاعات

کنترل

توصیه می‌شود برای اینکه نوع، حجم و هزینه‌های رخدادهای امنیتی، قابل اندازه گیری و پایش باشند، ساز و کارهای لازم ایجاد شوند.

راهنمای پیاده‌سازی

توصیه می‌شود اطلاعات به دست آمده از ارزیابی رخدادهای امنیت اطلاعات برای شناسایی رخدادهای پرتکرار یا با تاثیر زیاد مورد استفاده قرار گیرد. (رجوع کنید به بند ۵-۱-۲)

اطلاعات دیگر

ارزیابی اطلاعات رخدادهای امنیت اطلاعات ممکن است نشان دهنده نیاز به افزایش کنترل برای محدود کردن فراوانی، آسیب، و هزینه وقایع آینده یا در نظر گرفته شدن در فرآیند بررسی خط‌مشی امنیت باشد.

۱۳-۲-۳ گردآوری شواهد

کنترل

هنگامی‌که پیگرد علیه یک فرد یا سازمان، پس از یک رخداد امنیت اطلاعات، منجر به اقدام قانونی (اعم از مدنی یا جنایی) می‌شود، توصیه می‌شود شواهد منطبق با قواعد اقامهٔ شواهد در حوزه‌های قضایی مرتبط، گردآوری، نگهداری و ارایه شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رویه‌های داخلی توسعه یابند و در زمان جمع آوری و ارایه شواهد برای اهداف فعالیت انضباطی در یک سازمان دنبال شوند.

به طور کلی، قوانین شواهد موارد زیر را پوشش می‌دهند:

الف - قابل پذیرش بودن شواهد: این که آیا شواهد را می‌توان در دادگاه مورد استفاده قرار داد؛

ب - وزن شواهد: کیفیت و کامل بودن شواهد

توصیه می‌شود به منظور دستیابی به شواهد قابل قبول، سازمان تضمین نماید که سیستم‌های اطلاعاتی آنها با هر استاندارد منتشر شده یا آئین نامه تولید شواهد قابل پذیرش، مطابقت دارد.

توصیه می‌شود وزن شواهد ارایه شده با تمام الزامات موجود مطابقت داشته باشد. به منظور دستیابی به شواهد معتبر، توصیه می‌شود کیفیت و کامل بودن کنترل‌های به‌کار رفته برای محافظت صحیح و مستمر از شواهد (به عبارت دیگر شواهد کنترل فرآیند) در سراسر دوره ای که شواهد بازیابی، ذخیره و پردازش می‌شوند، با شواهدی قوی نشان داده شود. به طور کلی، این گزارش قوی باید تحت شرایط زیر ایجاد شود:

الف - برای اسناد کاغذی: نسخه اصل به طور ایمن با سوابقی از فردی که سند را پیدا کرده، محل پیدا شدن سند، زمان پیدا شدن سند، و کسی که شاهد این پیدا شدن است نگهداری می‌شود؛ توصیه می‌شود هر گونه بررسی که تضمین می‌کند نسخه‌های اصل مشکل پیدا نمی‌کنند؛ در نظر گرفته شود

ب - برای اطلاعات موجود در رسانه‌های رایانه‌ی؛ توصیه می‌شود تصاویر برابر اصل یا نسخه‌برداری (بسته به الزامات قابل کاربردی) از هر یک از رسانه‌های قابل جابجایی، اطلاعات موجد در دیسک‌های سخت یا در حافظه برای تضمین امنیت موجود باشند. توصیه می‌شود اطلاعات ثبت شده تمام فعالیت‌ها در زمان فرآیند نسخه‌برداری نگهداری شود و فرآیند مشاهده شود؛ توصیه می‌شود رسانه‌های اصل و اطلاعات ثبت شده (اگر این ممکن نیست، حداقل یک تصویر برابر اصل یا کپی) به طور ایمن و دست نخورده نگه داشته شوند.

توصیه می‌شود هر گونه کار کارشناسی فقط روی نسخه‌های کپی انجام شود. توصیه می‌شود یکپارچگی تمام مطالب موجود در مدارک محافظت شود. توصیه می‌شود نسخه برداری از شواهد توسط کارکنان قابل اعتماد نظارت شود و اطلاعات درباره مکان و زمان انجام نسخه برداری فردی که فعالیت‌های نسخه برداری را انجام می‌دهد و ابزارها و برنامه‌هایی که مورد استفاده قرار گرفته اند ثبت شود.

اطلاعات دیگر

زمانی که یک واقعه امنیت اطلاعات برای نخستین بار کشف می‌شود، ممکن است دقیقا معلوم نباشد که آیا این حادثه منجر به اقدام دادگاهی شود. بنابراین این خطر وجود دارد که شواهد لازم عمدا یا تصادفا قبل از تشخیص جدی بودن رخداد خراب شود. توصیه می‌شود از یک وکیل یا پلیس در مراحل اولیه هر اقدام حقوقی مشورت خواسته شود و توصیه‌های او اجرا شود.

شواهد ممکن است از مرزهای سازمان یا حوزه قضایی فراتر روند. در این موارد، توصیه می‌شود که تضمین شود سازمان حق دارد اطلاعات لازم را به عنوان شاهد جمع آوری کند. توصیه می‌شود الزامات حوزه‌های قضایی مختلف نیز برای افزایش شانس پذیرش فراسوی مرزهای قضایی مربوطه در نظر گرفته شود.

۱۴ مدیریت استمرار کسب‌وکار

۱۴-۱ جنبه‌های امنیت اطلاعات مدیریت استمرار کسب‌وکار

هدف : خنثی کردن وقفه های فعالیتهای کسب و کار و حفاظت از فرآیندهای بحرانی کسب و کار در برابر اثرات ناشی از خرابی های عمدهٔ سیستم‌های اطلاعاتی یا سوانح و حصول اطمینان به از سرگیری به موقع آنها.
توصیه می‌شود یک فرآیند مداوم مدیریت استمرار کسب و کار برای کاهش پیامد بر سازمان و بازیابی از آسیب به دارایی های اطلاعاتی که میتوانند ناشی از حوادث طبیعی، نقایص فیزیکی سخت افزارها و یا خسارتهای عمدی باشند تا سطح مطلوبی از طریق آمیزه ای از کنترل های پیشگیرانه و بازیابی انجام شود. توصیه می‌شود، این فرآیند فرآیندهای تجاری مهم را شناسایی کند و الزامات مدیریت امنیت اطلاعات استمرار کسب و کار را با دیگر الزامات مربوط به جنبه هایی از جمله عملیات، استخدام، تجهیزات، حمل و نقل و امکانات یکپارچه سازد.
پیامدهای فجایع، اختلالات امنیتی، آسیب به خدمات و دسترسی به خدمات باید تابع یک روش تحلیل آسیب‌های کسب و کار قرار گیرند. توصیه می‌شود برنامه های استمرارکسب و کار طراحی شوند و برای تضمین از سرگیری به موقع عملیات حیاتی اجرا شوند. توصیه می‌شود امنیت اطلاعات جزء لاینفک یک فرآیند تداوم تجاری و دیگر فرآیندهای مدیریتی در سازمان باشد.
توصیه می‌شود مدیریت استمرار کسب و کار شامل کنترل هایی برای شناسایی و کاهش ریسک ها به علاوه فرآیند ارزیابی ریسک های کلی باشد، پیامدهای رخدادهای آسیب رسان را محدود کند و تضمین کند که اطلاعات مورد نیاز برای فرآیندهای کسب و کار به سادگی در دسترس است.

۱۴-۱-۱ لحاظ کردن امنیت اطلاعات در فرایند مدیریت استمرار کسب‌وکار

کنترل

توصیه می‌شود فرآیند مدیریت شده ای به منظور استمرار کسب وکار در سراسر سازمان، ایجاد و پیاده سازی شود که الزامات امنیت اطلاعات مورد نیاز استمرار کسب وکار سازمان را نشانی دهی کند.

راهنمای پیاده‌سازی

توصیه می‌شود این فرآیند ارکان مهم مدیریت استمرار کسب و کار شامل موارد زیر را در کنار هم داشته باشد:

الف - درک ریسک هایی که یک سازمان با آن روبرو است، از نظر احتمال رخداد و میزان پیامد آنها در زمان شامل شناسایی و اولویت بندی فرآیندهای کسب و کار مهم (رجوع کنید به بند ۱۴-۱-۲)

ب - شناسایی تمام داراییهای موجود در فرآیندهای حیاتی کسب و کار (رجوع کنید به بند ۷-۱-۱)

پ - درک پیامدی که اختلالات رخدادهای امنیت اطلاعات احتمالا بر کسب و کار، تثبیت اهداف کسب وکار و تجهیزات پردازش اطلاعات ایجاد کردند (این موضوع مهم است که راه حل هایی پیدا شود تا رخدادهای منجر به پیامدهای کوچکتر را اداره کنند، به اندازه رخدادهای جدی که می‌تواند دوام سازمان را تهدید کند)

ت - در نظر گرفتن بیمه مناسب که ممکن است بخشی از فرآیند استمرار کسب و کار و نیز بخشی از مدیریت عملیاتی ریسک باشد.
ث - شناسایی و در نظر گرفتن کنترل های پیشگیرانه و اصلاحی اضافی
ج - شناسایی منابع مالی، سازمانی، فنی، و زیست محیطی برای اشاره به الزامات شناخته شده امنیت اطلاعات.
چ - تضمین ایمنی کارکنان و محافظت از تجهیزات پردازش اطلاعات و اموال سازمانی
ح - فرمول بندی و مستندسازی برنامه های استمرار کسب و کار که به الزامات امنیت اطلاعات در راستای راهبرد استمرار کسب و کار مورد توافق اشاره دارد (رجوع کنید به بند ۱۴-۱-۳)
خ - آزمون و بروزسازی منظم برنامه ها و فرآیندهای پیاده سازی شده (رجوع کنید به بند ۱۴-۱-۵)
د - تضمین این که مدیریت استمرار کسب و کار در فرآیندها و ساختار سازمان به کار گرفته می‌شود، توصیه می‌شود مسوولیت فرآیند مدیریت استمرار کسب وکار در سطح مناسب در سازمان تعیین شود. (رجوع کنید به بند ۶-۱-۱)

۱۴-۱-۲ *استمرار کسب‌وکار و ارزیابی ریسک*

کنترل

توصیه می‌شود وقایعی که می‌توانند موجب وقفه در فرآیندهای کسب وکار شوند، با توجه به احتمال بروز و آسیب ناشی از چنین وقفه هایی و پیامدهای آنها بر امنیت اطلاعات، شناسایی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود جنبه های امنیت اطلاعات استمرار کسب و کار بر اساس شناسایی حوادثی باشد که باعث اختلال در فرآیندهای کسب وکار سازمان ها می‌شود، مثلا خرابی تجهیزات، خطاهای انسانی، سرقت، آتش سوزی، بلایای طبیعی، و اقدامات تروریستی. توصیه می‌شود این فعالیت‌ها با یک فرآیند ارزیابی ریسک به منظور تعیین احتمال و پیامد این اختلالات از نظر زمانی، میزان آسیب و دوره از سر گیری فرآیند دنبال شود.

توصیه می‌شود ارزیابی ریسک استمرار کسب و کار با مشارکت کامل تمام مالکان منابع و فرآیندهای تجاری انجام شود. توصیه می‌شود این ارزیابی تمام فرآیندهای کسب وکار را در برگیرد و به تجهیزات پردازش اطلاعات محدود نباشد، لیکن باید شامل نتایج خاص امنیت اطلاعات باشد. مهم است که جنبه های مختلف به هم پیوند داده شوند تا تصویر کاملی از الزامات استمرار کسب و کار سازمان به دست آید. توصیه می‌شود ارزیابی ریسک ها را در مقایسه با معیارها و اهداف مربوط به سازمان از جمله، منابع مهم، پیامدهای اختلالات، زمان های مجاز قطعی سرویس و اولویت های بازیابی؛ شناسایی، سنجش و اولویت بندی کند.

بسته به نتایج ارزیابی ریسک، توصیه می‌شود یک راهبرد استمرار کسب و کار برای تعیین رویکرد کلی در قبال استمرار کسب و کار در نظر گرفته شود. پس از ایجاد این راهبرد، لازم است مدیریت سازمان آن را تایید نموده و به گونه‌ای برنامه‌ریزی نماید تا این راهبرد اجرا شود.

۱۴-۱-۳ *ایجاد و پیاده‌سازی طرح‌های استمرار دربرگیرندهٔ امنیت اطلاعات*

کنترل

در پی وقفه و یا بروز نقص در فرآیندهای بحرانی کسب وکار، به منظور نگهداری یا از سرگیری عملیـات و اطمینـان از دسترس پذیری اطلاعات در سطح و دوره زمانی قابل قبول، توصیه می‌شود طرح هایی ایجاد و پیاده سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود فرآیند برنامه ریزی استمرار کسب و کار موارد زیر را در نظر گیرد:

الف - شناسایی و توافق درباره مسوولیت ها و رویه های استمرار کسب و کار

ب- شناسایی حد قابل قبول آسیب به اطلاعات و خدمات

پ- اجرای رویه هایی برای امکان پذیر کردن بازیابی و نگهداری عملیات کسب وکار و دسترسی به اطلاعات در مقیاسهای زمانی مورد نیاز؛ توجه خاصی باید به ارزیابی وابستگی های داخلی و خارجی کسب و کار و قراردادهای موجود شود؛

ت- رویه های عملیاتی به منظور پیگیری تکمیل بازیابی و ذخیره سازی در آینده؛

ث- مستندسازی رویه ها و فرآیندهای مورد توافق

ج- آموزش مناسب کارکنان درخصوص رویه ها و فرآیندهای مورد توافق از جمله مدیریت بحران

چ- تست و ارتقاء برنامه ها

توصیه می‌شود فرآیند برنامه ریزی بر اهداف کسب وکار از جمله حفظ خدمات ارتباطی خاص مشتریان در زمان قابل قبول تاکید کند. همچنین توصیه می‌شود خدمات و منابعی که این امر را تسهیل می‌کنند شناسایی شوند که از آن جمله می‌توان به استخدام، منابع پردازش غیراطلاعاتی، و نیز هماهنگی های پشتیبانی برای تجهیزات پردازش اطلاعات اشاره کرد. این فعالیت‌ها ممکن است شامل هماهنگی با شخص های ثالث به شکل قراردادهای دوجانبه یا خدمات اشتراک کسب وکار باشد.

توصیه می‌شود برنامه های تداوم کسب و کار به آسیب پذیری های سازمانی اشاره کنند و بنابراین ممکن است شامل اطلاعات حساسی باشند که باید به طور مناسب محافظت شوند. توصیه می‌شود نسخه های برنامه های استمرار کسب و کار در محلی دیگر با فاصله کافی برای جلوگیری از هر گونه آسیب ناشی از حوادث قرار داده شوند. توصیه می‌شود مدیریت تضمین کند که نسخه های برنامه های استمرار کسب وکار به روز هستند و با سطح مشابه امنیت به کار رفته در محل اصلی محافظت می‌شوند. موارد دیگری که برای اجرای برنامه های استمرار کسب و کار لازم هستند توصیه می‌شود در محلی دور ذخیره شوند.

اگر محل های موقت جایگزین مورد استفاده قرار می‌گیرند، توصیه می‌شود سطح کنترل های امنیتی اجرا شده در این محل ها مشابه محل اصلی باشد.

اطلاعات دیگر

باید اشاره شود که برنامه ها و فعالیت های مدیریت بحران ممکن است با مدیریت استمرار کسب و کار متفاوت باشد؛ به عبارت دیگر ممکن است بحرانی رخ دهد که بتوان آن را با رویه های مدیریتی رفع کرد

۴-۱-۱۴ چارچوب طرح‌ریزی استمرار کسب‌وکار

کنترل

به منظور حصول اطمینان از سازگاربودن تمامی طرح ها، نشان دهی بدون تناقض الزامات امنیت اطلاعات، و شناسایی اولویت های آزمون و نگهداری، توصیه می‌شود یک چارچوب واحد از طرح های استمرار کسب وکار ایجاد و نگهداری شود.

راهنمای پیاده‌سازی

توصیه می‌شود هر برنامه استمرار کسب و کار رویکرد استمرار را مثلا رویکرد تضمین اطلاعات یا دسترسی و امنیت سیستم اطلاعات را بیان کند. توصیه می‌شود هر برنامه همچنین یک برنامه برای موارد اضطراری را مشخص و شرایط فعال سازی آن را تعیین کند، و نیز افراد مسوول اجرای هر جزء از برنامه را مشخص شوند. زمانی که الزامات جدید شناسایی شدند، توصیه می‌شود هر گونه رویه اضطراری[1] موجود مثلا، برنامه های تخلیه محل[2] به طور مناسب اصلاح شوند. توصیه می‌شود رویه هایی در برنامه مدیریت تغییر سازمان گنجانده شوند تا تضمین شود که موضوعات استمرار همیشه به طور مناسب مورد اشاره و رسیدگی قرار می‌گیرند.

توصیه می‌شود هر برنامه یک مالک خاص داشته باشد. توصیه می‌شود رویه های اضطراری، برنامه هایی با اجرای دستی برای شرایط اضطرار[3]، و برنامه های از سرگیری[4] در حوزه مسوولیت مالک منابع یا فرآیندهای کسب وکار مربوطه باشند. توصیه می‌شود قراردادهای پشتیبانی برای خدمات فنی جایگزین، نظیر تجهیزات پردزاش اطلاعات و ارتباطات معمولا در حیطه مسوولیت ارایه کنندگان خدمات باشد.

توصیه می‌شود یک چارچوب برنامه ریزی استمرار کسب و کار الزامات امنیت اطلاعات شناسایی شده را مورد اشاره قرار دهد و موارد زیر را در نظر گیرد:

الف - شرایط فعال سازی برنامه هایی که باید قبل از فعال سازی آنها فرآیندی اجرا شود(برای مثال چگونگی ارزیابی موقعیت، اینکه چه کسانی در برنامه دخیل هستند)؛ بیان می‌کند.

ب - رویه های اضطراری که توصیف کننده فعالیت هایی هستند که باید پس از وقوع یک رخداد که عملیات کسب وکار را به خطر می اندازد؛ اجرا گردند

پ - رویه های پشتیبانی که فعالیت هایی را که برای انجام فعالیت های کسب وکار مهم یا حمایت از خدمات پشتیبانی جایگزین باید در نظر گرفته شوند بیان می‌کند و فرآیندها را عملیاتی می‌کنند.

ت - رویه های عملیاتی موقت برای تکمیل فرآیند ذخیره و بازیابی

ث - رویه های از سر گیری که فعالیت هایی را که برای بازگشتن به عملیات عادی کسب و کار اتخاذ شوند را بیان می‌کنند

ج - یک برنامه زمانبندی نگهداری که مشخص می‌کند چگونه و در چه موقعی برنامه و فرآیند نگهداری از برنامه باید آزموده شود.

چ - فعالیت های آگاه‌سازی، آموزش، و تعلیم که برای ایجاد درکی از فرآیندهای استمرار کسب و کار و تضمین این که فرآیند همچنان موثر خواهند بود نیاز می‌باشند

ح - مسوولیت‌های افراد به گونه ای که بیان کند چه کسی مسوول اجرای چه جزئی از برنامه است. توصیه می‌شود گزینه‌ها بر حسب نیاز در نظر گرفته شوند؛

1- Escalation plan
2- Evacuation plan
3- Manual fallback plans
4- Resumption plans

خ - دارایی‌های حیاتی و منابع مورد نیاز برای انجام رویه های اضطراری، پشتیبانی و از سر گیری

۱۴-۱-۵ حفظ و نگهداری آزمون و ارزیابی مجدد طرح‌های استمرار کسب‌وکار

کنترل

توصیه می‌شود طرح های استمرار کسب وکار، به منظور حصول اطمینان از اینکه به روز و موثر هستند، به طورمنظم مورد آزمون قرار گرفته و بهنگام شوند.

راهنمای پیاده‌سازی

توصیه می‌شود آزمون‌های برنامه استمرار کسب و کار تضمین کنند که اعضاء تیم بازیابی و دیگر کارکنان مربوطه از برنامه ها و مسوولیت شان برای استمرار کسب و کار و امنیت اطلاعات آگاهند و نقش خود را در زمان هر پیشامد می‌دانند.

توصیه می‌شود جدول آزمون برای برنامه (های) استمرار کسب و کار نشان دهد که توصیه می‌شود چگونه و چه موقع هر جزء از برنامه آزموده شود. توصیه می‌شود هر جزء برنامه (ها) به کرات آزموده شود.

توصیه می‌شود انواع تکنیک ها به منظور تضمین اینکه برنامه ها در محیط واقعی عملیاتی می‌شوند مورد استفاده قرار گیرند. توصیه می‌شود موارد زیر شامل شوند:

الف - آزمون به موقع سناریوهای مختلف (مطرح کردن تمهیدات بازسازی کسب وکار با بکار بردن وقفه‌های نمونه)

ب - شبیه سازی‌ها (بطور مشخص برای آموزش افراد در نقش های مدیریتی بحران/ رخدادها در آینده)

پ - آزمون بازیابی فنی (اطمینان از اینکه سیستم‌های عملیات بازیابی اطلاعات بطور موثر بازیابی شوند)

ت - بازیابی آزمون در محل‌های متفاوت (اجرای فرایندهای کسب وکار همزمان با عملیات بازیابی، جدا از سایت اصلی)

ث - آزمون‌های تجهیزات و خدمات تامین کننده (اطمینان از اینکه سرویس ها و محصولات تامین شده خارجی، تعهدات قراردادی را برآورده می‌کنند)

ج - تست‌های سازگاری (آزمون اینکه سازمان، کارکنان، تجهیزات، امکانات و فرایندها می‌توانند بر وقفه ها فائق آیند)

این تکنیک ها را می‌توان در هر سازمانی مورد استفاده قرار داد. توصیه می‌شود آنها به گونه ای به کار گرفته شوند که مرتبط با برنامه بازیابی خاصی باشد. توصیه می‌شود نتایج آزمون‌ها ثبت شود و اقداماتی برای بهبود برنامه ها در صورت لزوم باید اتخاذ شود.

توصیه می‌شود مسوولیت‌ها برای بررسی های منظم هر برنامه استمرار کسب و کار تعیین شود. توصیه می‌شود شناسایی تغییرات در محیط های کسب وکار که تا به حال در برنامه های استمرار کسب و کار منعکس نشده اند از طریق روزآمدسازی مناسب برنامه دنبال شود. همچنین توصیه می‌شود این فرآیند کنترل تغییر رسمی تضمین کند که برنامه های روزآمد شده از طریق بررسی های منظم توزیع و تقویت شده اند.

مثال هایی از تغییراتی که بروزسازی برنامه های استمرار کسب و کار در نظر میگیرند عبارتند از دستیابی به تجهیزات جدید، بروزسازی سیستم‌ها و تغییرات در موارد زیر است:

الف - کارکنان

ب - نشانی‌ها و شماره‌های تماس

پ - راهبرد کسب وکار
ت - محل، تجهیزات و منابع
ث - مقررات
ج - قراردادها، تامین کننده‌ها و مشتریان کلیدی
چ - فرایندها یا فرایندهای جدید یا کنارگذاشته شده
خ - ریسک (عملیاتی و مالی)

۱۵ انطباق

۱۵-۱ انطباق با الزامات قانونی

هدف : پرهیز از نقض هر نوع قانون، مقررات، تعهدات آیین نامه ای یا قراردادی و هر الزام امنیتی.
طراحی، عملکرد، استفاده و مدیریت سیستم‌های اطلاعات ممکن است منوط به الزامات آئین نامه ای، مقرراتی، و قراردادی باشد.
توصیه می‌شود الزامات قانونی خاص از مشاوران حقوقی سازمان یا دست اندرکاران حقوقی خاص و واجد شرایط درخواست شود. الزامات قانونی در کشورهای مختلف متفاوتند و ممکن است برای اطلاعات ایجاد شده در یک کشور که به کشور دیگر منتقل می‌شود تغییر کنند. (بعبارت دیگر جریان داده عبوری از مرز)

۱۵-۱-۱ شناسایی قوانین قابل‌اجرا

کنترل

تمامی مقررات، الزامات آیین نامه ای و قراردادی مرتبط و رویکرد سازمان نسبت به برآورده سازی این الزامات، باید برای هر سیستم اطلاعاتی و سازمان، به وضوح تعریف شده، مدون شده و به روز نگه داشته شوند.

راهنمای پیاده‌سازی

توصیه می‌شود کنترل های خاص و مسوولیت های فردی برای رعایت این الزامات تعریف و مستند شود.

۱۵-۱-۲ حقوق مالکیت فکری[1]

توصیه می‌شود به منظور حصول اطمینان از انطباق با الزامات قانون گزار، الزامات آیین نامه ای و قراردادی در استفاده از کالاهایی که ممکن است دارای حقوق مالکیت فکری باشد، و در هنگام استفاده از محصولات نرم‌افزاری دارای حقوق انحصاری، روشهای اجرایی مناسب، پیاده سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رهنمودهای زیر برای محافظت از هر کالائی که ممکن است مالکیت فکری در نظر گرفته شود رعایت شود:

الف - انتشار خط مشی انطباق با حقوق مالکیت فکری که استفاده قانونی از محصولات نرم‌افزاری و اطلاعاتی را تعریف می‌کند

ب - دستیابی به نرم‌افزار فقط از طریق منابع شناخته شده و معتبر برای تضمین این که حق تکثیر نقض نمی‌شود.

پ - حفظ و آگاهی از خط مشی ها به منظور محافظت از حقوق مالکیت فکری و دادن اطلاعیه درباره برخورد انضباطی در برابر نقض آنها.

ت - نگهداری گزارش های مناسب از دارایی‌ها و شناسایی تمام آنها با الزامات مرتبط به منظور محافظت از حقوق مالکیت فکری

ث - حفظ شواهد و مدارک مالکیت گواهی‌ها و پروانه‌ها، دیسک‌های اصلی و راهنماها

1- Intellectual property rights (IPR)

ج - اجرای کنترل هایی برای تضمین این که حداکثر استفاده کنندگان مجاز از حد خاصی فراتر نمی رود.
چ - انجام بررسی هایی که فقط نرم‌افزارهای مجاز و محصولات دارای مجوز نصب می‌شوند
ح - ارایه خط مشی برای حفظ شرایط مناسب گواهی
خ - ارایه خط مشی برای دور ریز یا انتقال نرم‌افزار به دیگران
د - استفاده از ابزارهای مناسب ممیزی
ذ –مطابقت مفاد و شرایط نرم‌افزار و اطلاعات به دست آمده از شبکه‌های همگانی
ر - عدم تکثیر، تبدیل به قالب دیگر یا چکیده گرفتن غیر از مواردی که در قانون حق تکثیر مجاز دانسته شده‌اند
ز - عدم کپی برداری کامل یا جزئی از کتاب ها، مقالات، گزارش ها و دیگر مستندات غیر از مواردی که در قانون حق تکثیر مجاز دانسته شده اند..

اطلاعات دیگر

حقوق مالکیت فکری شامل حق تکثیر نرم‌افزار یا مستندات، حقوق طراحی، علائم تجاری، حق انحصاری، و گواهی های کد منبع است.

محصولات نرم‌افزاری اختصاصی معمولا در قالب یک قرارداد دارای مجوز تامین می‌شوند که مفاد و شرایط گواهی را مثلا برای محدود کردن استفاده از محصولات در ماشین های خاص یا محدود کردن کپی برداری برای ایجاد نسخه های پشتیبان مشخص می‌کند. شرایط حقوق مالکیت معنوی یک نرم‌افزار که توسط سازمان طراحی شده است باید برای کارکنان روشن شود.

الزامات قانونی، مقرراتی و قراردادی ممکن است محدودیت‌هایی در تکثیر مطالب اختصاصی ایجاد کند. به خصوص، ممکن است آنها این گونه حکم کنند که فقط مطالبی که توسط سازمان طراحی شده است یا توسط سازنده طی یک مجوز به سازمان داده شده است می‌تواند مورد استفاده قرار گیرد. نقض حق تکثیر ممکن است منجر به اقدام حقوقی شود که دربرگیرنده محاکمه کیفری است.

۱۵-۱-۳ حفاظت از سوابق سازمانی

کنترل

توصیه می‌شود سوابق مهم، با توجه به مقررات، الزامات آئین نامه ای، قراردادی و کسب وکار، در برابر گم شدن، تخریب و تحریف، محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود گزارش ها در بخش‌های مختلف گروه بندی شوند بعنوان مثال گزارش های حسابداری، گزارش های پایگاه داده‌ها، اطلاعات ثبت شده معاملات، اطلاعات ثبت شده ممیزی و رویه های عملیاتی که هر کدام جزئیاتی از دوره نگهداری و نوع رسانه ذخیره مثلا، کاغذ، میکروفیلم، مغناطیسی یا نوری را نشان می دهند. هر گونه مطلب و برنامه رمزنگاری و نسخه برداری مربوطه در رابطه با بایگانی های نسخه برداری شده یا امضاهای دیجیتال (رجوع کنید به ۱۲-۳) همچنین توصیه می‌شود برای ایجاد امکان رمزگشایی از گزارش‌ها برای طول دوره زمانی که گزارش‌ها نگهداری می‌شوند ذخیره شوند.

توصیه می‌شود درباره احتمال خرابی رسانه های به کار رفته به منظور ذخیره گزارش ها تمهیداتی اندیشیده شود. توصیه می‌شود رویه های ذخیره و استفاده، مطابق با پیشنهادات تولیدکننده اجرا شوند. توصیه می‌شود برای ذخیره بلندمدت، استفاده از کاغذ و میکروفیلم در نظر گرفته شود.

در جایی که رسانه های ذخیره‌سازی الکترونیکی انتخاب می‌شوند، توصیه می‌شود رویه هایی برای تضمین توانایی دسترسی به داده‌ها در سراسر دوره نگهداری گنجانده شود تا در برابر آسیب به دلیل تغییر فن‌آوری در آینده محافظت شود.

توصیه می‌شود سیستم‌های ذخیره‌سازی داده‌ها به گونه ای انتخاب شود که داده‌های مورد نیاز را بتوان در یک شکل و بازه زمانی قابل قبول با توجه به الزامات موجود نگهداری کرد.

توصیه می‌شود سیستم ذخیره اطلاعات کار شناسایی دقیق اسناد و دوره های حفظ آنها را به گونه ای که در مقررات یا قوانین ملی و منطقه ای تعریف شده است تضمین کند. این سیستم باید تخریب مناسب گزارش ها را پس از آن دوره در صورتی که سازمان به آنها نیاز ندارد مجاز شمارد.

به منظور رعایت این اهداف محافظتی، توصیه می‌شود مراحل زیر در یک سازمان انجام شوند:

الف – توصیه می‌شود رهنمود هایی درباره حفظ، ذخیره و کار و دور ریز گزارش‌ها و اطلاعات صادر شود.

ب - توصیه می‌شود یک جدول زمانی نگهداری برای شناسایی گزارش‌ها و دوره زمانی که برای آن نگهداری شده اند تهیه شود.

پ - توصیه می‌شود لیست موجودی از منابع اطلاعات کلیدی نگهداری شود

ت - توصیه می‌شود کنترل‌های مناسبی برای محافظت از گزارش‌ها و اطلاعات در برابر آسیب، تخریب، و تقلب اجرا شود.

اطلاعات دیگر

بعضی گزارش ها ممکن است نیازمند این باشند که به گونه ای امن حفظ شوند تا الزامات آئین نامه ای، مقرراتی یا قراردادی رعایت شوند و نیز فعالیت های ضروری کسب و کار پشتیبانی شوند.

به عنوان مثال گزارش هایی هستند که ممکن است به عنوان شواهدی که یک سازمان در چارچوب قوانین عمل می‌کند مورد نیاز باشند تا دفاع کافی دربرابر اقدامات غیر حقوقی یا حقوقی یا تایید وضعیت مالی یک سازمان در قبال سهام داران، 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 ISO 15489-1 بیابید.

۱۵-۱-۴ حفاظت داده‌ها و حریم خصوصی اطلاعات شخصی

کنترل

توصیه می‌شود حفاظت داده‌ها و حریم خصوصی آنگونه که در مقرارت و آئین نامه های مرتبط، و در صورت قابلیت اعمال، شرایط قراردادی، الزام شده، تضمین شود.

راهنمای پیاده‌سازی

توصیه می‌شود یک خط مشی سازمانی محافظت از داده‌ها طراحی و حریم خصوصی اجرا شود. توصیه می‌شود این خط مشی به تمام اشخاصی که در پردازش اطلاعات شخصی نقش دارند اطلاع داده شود.

انطباق با این خط مشی و تمام قوانین محافظت از داده‌های مربوطه و مقررات نیازمند ساختار و کنترل مدیریتی مناسب می باشند. اغلب این امر به بهترین نحو توسط انتصاب یک شخص مسوول مانند یک مامور محافظت از داده‌ها انجام می‌شود که توصیه می‌شود این شخص راهنمایی را برای مدیران، کاربران، و ارایه کنندگان خدمات درباره مسوولیت فردی و رویه های خاصی که توصیه می‌شود دنبال شود ارایه کند. توصیه می‌شود مسوولیت کار با اطلاعات شخصی و تضمین آگاهی از اصول مراقبت از داده‌ها مطابق با قوانین و مقررات مربوطه مورد توجه قرار گیرد. توصیه می‌شود اقدامات فنی و سازمانی مناسب برای محافظت از اطلاعات شخصی اجرا شود.

اطلاعات دیگر

تعدادی از کشورها مقرراتی دارند که کنترل هایی را درباره جمع آوری، پردازش و انتقال داده‌های شخصی اعمال می‌کند. با توجه به مقررات ملی مربوطه این کنترل ها ممکن است وظایفی را برای افراد جمع آوری کننده، پردازش کننده و منتشر کننده اطلاعات شخصی ایجاد کند و ممکن است امکان انتقال داده‌ها را به کشورهای دیگر محدود کند.

۱۵-۱-۵ پیشگیری از استفاده نابجا از امکانات پردازش اطلاعات

کنترل

توصیه می‌شود کاربران از بکارگیری امکانات پردازش اطلاعات برای مقاصد غیر مجاز، بازداشته شوند.

راهنمای پیاده‌سازی

توصیه می‌شود مدیریت استفاده از تجهیزات پردازش اطلاعات را تایید کند. هر گونه استفاده از این تجهیزات برای اهداف غیرکسب وکار بدون تایید مدیریت (رجوع کنید به بند ۶-۱-۴) یا برای هر گونه هدف غیرمجاز توصیه می‌شود به عنوان استفاده غیرمجاز از تجهیزات قلمداد شود. اگر هر فعالیت غیرمجازی از طریق کنترل یا طرق دیگر شناسایی شود، توصیه می‌شود این فعالیت به اطلاع مدیر خاص مربوطه برای بررسی اقدام حقوقی و یا انضباطی مناسب، برسد.

توصیه می‌شود مشاوره قانونی قبل از اجرای رویه های کنترل مورد استفاده قرار گیرد.

توصیه می‌شود تمام کاربران از هدف و دامنه کاربرد دقیق دسترسی مجازشان و کنترل‌های موجود برای کشف استفاده غیرمجاز آگاه باشند. این امر ممکن است از طریق اجازه دادن کتبی به کاربران، که توصیه می‌شود نسخه ای از آن توسط کاربر امضا شود و در اختیار سازمان باشد انجام شود. توصیه می‌شود که به کارکنان یک سازمان، پیمانکاران و کاربران شخص ثالث یادآوری شود که فقط دسترسی مجاز امکان پذیر است.

در زمان برقراری ارتباط با یک سیستم، توصیه می‌شود یک پیام هشدار ارایه شود که نشان می دهد که تجهیزات پردازش اطلاعاتی که کاربر وارد آن شده است متعلق به سازمان است و این که دسترسی غیرمجاز ممکن نیست. توصیه می‌شود کاربر اظهار کند که پیام را مشاهده کرده است تا بتواند در فرآیند برقراری ارتباط به کار خود ادامه دهد. (رجوع کنید به بند ۱۱-۵-۱).

اطلاعات دیگر

تجهیزات پردازش اطلاعات، یک سازمان عمدتا و منحصرا برای اهداف کسب وکار می باشد. کشف ورود غیرمجاز، بررسی محتوا و دیگر ابزارهای کنترلی می‌توانند به پیشگیری و کشف سوء استفاده از تجهیزات پردازش اطلاعات کمک کنند.

بسیاری از کشورها مقرراتی برای محافظت دربرابر سوء استفاده از رایانه دارند. استفاده از یک رایانه برای اهداف غیرمجاز ممکن است یک تخلف کیفری محسوب شود.
قانونی بودن کنترل استفاده در کشورهای مختلف متفاوت است و ممکن است نیازمند این باشد که مدیریت به تمام کاربران این کنترل را اطلاعات دهد و موافقت آنها را کسب کند.
در جایی که سیستم مورد استفاده برای دسترسی همگانی مورد استفاده قرار می‌گیرد (برای مثال، یک سرویس دهنده عمومی وب)، و در معرض کنترل امنیتی است باید پیامی روی صفحه ظاهر شود و این را نشان دهد.

۱۵-۱-۶ مقرارت کنترل‌های رمزنگاری

کنترل

توصیه می‌شود کنترل‌های رمزنگاری در انطباق با تمامی‌توافق نامه ها، قوانین و مقررات مرتبط، بکارگرفته شوند.

راهنمای پیاده‌سازی

توصیه می‌شود موارد زیر برای انطباق با قراردادها، قوانین، و مقررات مربوطه در نظر گرفته شود:

الف - محدودیت‌های ورود و/یا صدور سخت افزار و نرم‌افزار رایانه برای اجرای عملکردهای رمزنگاری

ب - محدودیت‌هایی درباره ورود یا خروج نرم‌افزار و سخت افزار رایانه‌ی که برای اضافه شدن کارایی رمزنگاری طراحی شده اند.

پ - محدودیت‌هایی درباره استفاده از رمزنگاری

ت - روش های اجباری یا اختیاری دسترسی به اطلاعات رمزنگاری شده توسط سخت افزار یا نرم‌افزار برای تضمین محرمانگی محتوا

توصیه می‌شود مشاوره قانونی برای تضمین انطباق با قوانین و مقررات ملی انجام شود. قبل از این که اطلاعات رمزنگاری شده یا کنترل های رمزنگاری به کشور دیگری منتقل شود توصیه می‌شود مشاوره قانونی انجام شود.

۱۵-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی، و انطباق فنی

هدف : حصول اطمینان از انطباق سیستم‌ها با خط مشی ها و استانداردهای امنیتی سازمانی.
توصیه می‌شود امنیت سیستم‌های اطلاعات به طور منظم بررسی شود.
توصیه می‌شود این بررسی ها در قبال خط مشی های امنیتی مناسب و الگوهای فنی انجام شوند و توصیه می‌شود سیستم‌های اطلاعات برای انطباق با استانداردهای امنیتی حاکم و کنترل های امنیتی مستند مورد ممیزی قرار گیرند.

۱۵-۲-۱ انطباق با خط‌مشی‌ها و استانداردهای امنیتی

کنترل

برای حصول انطباق با خط مشی ها و استانداردهای امنیتی، توصیه می‌شود مدیران از اینکه تمامی روش‌های اجرایی امنیتی، در حیطهٔ مسوولیت شان، به درستی اجرا می‌شوند، اطمینان حاصل نمایند.

راهنمای پیاده‌سازی

توصیه می‌شود مدیران انطباق پردازش اطلاعات را در حوزه مسوولیت خود با خط مشی ها، استانداردها و دیگر الزامات امنیتی مناسب بررسی کنند.

اگر هر گونه عدم انطباق در نتیجه بررسی مشاهده شود، توصیه می‌شود مدیران:

الف - علل عدم انطباق را تعیین کنند

ب – ارزشیابی نیاز به اقداماتی برای اطمینان از عدم وقوع مجدد عدم انطباق

پ - اقدام اصلاحی مناسب را تعیین واجرا کنند

ت - اقدامات اصلاحی انجام شده را بررسی کنند.

توصیه می‌شود نتایج بررسی ها و اقدامات اصلاحی انجام شده توسط مدیران ثبت شود و توصیه می‌شود این گزارش ها نگهداری شوند. توصیه می‌شود مدیران نتایج را به اشخاصی که بررسی های مستقل (رجوع کنید به بند ۶-۱-۸) را انجام می دهند در زمانی که بررسی های مستقل در حوزه مسوولیت شان انجام می‌شود گزارش کنند.

اطلاعات دیگر

کنترل عملیاتی استفاده از سیستم در ۱۰-۱۰ آمده است.

۱۵-۲-۲ بررسی انطباق فنی

کنترل

توصیه می‌شود به منظور انطباق با استانداردهای پیاده سازی امنیت، سیستم‌های اطلاعاتی به طور منظم بررسی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود بررسی انطباق فنی یا به طور دستی (اگر لازم باشد، پشتیبانی شده بوسیله ابزارهای نرم‌افزاری مناسب)توسط یک مهندس با تجربه سیستم و/یا با کمک ابزارهای اتوماتیک که گزارش فنی را برای تفسیر متعاقب توسسط یک متخصص فنی آماده می‌کند انجام شوند.

اگر آزمون‌های نفوذ یا ارزیابی‌های آسیب‌پذیری مورد استفاده قرار می‌گیرند، توصیه می‌شود احتیاط شود زیرا این فعالیت‌ها ممکن است منجر به نقض امنیت سیستم شوند. توصیه می‌شود این آزمون‌ها برنامه ریزی شده، مستند و قابل تکرار باشند.

توصیه می‌شود هر بررسی انطباق فنی فقط بوسیله اشخاص مجاز وشایسته انجام شود، یا تحت نظارت چنین افرادی صورت گیرد.

اطلاعات دیگر

بررسی انطباق فنی دربرگیرنده بررسی سیستم‌های عملیاتی برای تضمین این است که کنترل‌های سخت افزاری و نرم‌افزاری به طور صحیح اجرا شده اند. این نوع بررسی‌های انطباق نیازمند تخصص فنی یک متخصص است.

بررسی انطباق همچنین مثلا آزمون نفوذ و ارزیابی‌های آسیب‌پذیری را شامل می‌شود که ممکن است توسط کارشناسان مستقلی که به طور خاص برای این منظور در نظر گرفته شده اند انجام شود. این ممکن است در کشف آسیب‌پذیری‌ها در سیستم و برای بررسی این که کنترل‌ها در پیشگیری از دسترسی غیرمجاز به دلیل این آسیب‌پذیری‌ها تا چه حد موثر هستند مفید باشد.

آزمون نفوذ و ارزیابی‌های آسیب‌پذیری مجرایی برای یک سیستم در زمان خاص ایجاد می‌کنند. این محدود به بخش‌هایی از سیستم است که در واقع در طول اقدامات نفوذ آزموده می‌شوند. آزمون نفوذ و ارزیابی‌های آسیب‌پذیری جایگزین ارزیابی ریسک نیستند.

۱۵-۳ ملاحظات ممیزی سیستم‌های اطلاعاتی

هدف : بیشینه کردن اثربخشی و کمینه کردن اختلال در فرآیند ممیزی سیستم‌های اطلاعاتی.
توصیه می‌شود برای محافظت از سیستم‌های عملیاتی و ابزارهای بازرسی در طول بازرسی سیستم‌های اطلاعات کنترل هایی موجود باشد.
محافظت همچنین برای حفظ یکپارچگی و پیشگیری از سوء استفاده از ابزارهای ممیزی لازم است.

۱۵-۳-۱ کنترل‌های ممیزی سیستم‌های اطلاعاتی

کنترل

توصیه می‌شود الزامات و فعالیت های ممیزی مرتبط با بررسی های سیستم‌های عملیاتی، به دقت طرح‌ریزی و مورد توافق قرار گیرند تا ریسک‌های ناشی از توقف در فرآیندهای کسب وکار، کمینه شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رهنمودهای زیر رعایت شوند:

الف - توصیه می‌شود الزامات بازرسی با مدیریت مناسب مورد توافق قرار گیرند.

ب - توصیه می‌شود هدف و دامنه کاربرد بررسی‌ها مورد توافق قرار گرفته و کنترل شود.

پ - توصیه می‌شود بررسی‌ها محدود به دسترسی فقط خواندنی به نرم‌افزار یا داده‌ها باشد

ت - توصیه می‌شود دسترسی غیر از فقط خواندنی فقط برای نسخه‌های جدا شده فایل‌های سیستم، مجاز شوند که توصیه می‌شود در زمانی که بازرسی کامل می‌شود پاک شوند. یا در صورتی که الزامی به حفظ این فایل‌ها تحت شرایط مستندسازی بازرسی وجود دارد محافظت مناسب از آنها به عمل آید.

ث - توصیه می‌شود منابع مورد نیاز جهت اجرای بررسی ها صریحا شناسایی شده و در دسترس قرار گیرد.

ج - توصیه می‌شود الزامات پردازش اضافه، شناسایی شده مورد توافق قرار گیرد

چ - توصیه می‌شود تمام دسترسی کنترل و ثبت شود تا یک گزارش مرجع موجود باشد؛ استفاده از گزارش‌های ممهور باید برای اطلاعات یا سیستم‌های حیاتی در نظر گرفته شود.

ح - توصیه می‌شود تمام رویه‌ها، الزامات و مسوولیت‌ها مستند شوند

خ - توصیه می‌شود شخص یا اشخاصی که بازرسی را انجام می‌دهند از فعالیت‌های مورد بازرسی مستقل باشد.

۱۵-۳-۲ حفاظت از ابزارهای ممیزی سیستم‌های اطلاعاتی

کنترل

توصیه می‌شود به منظور پیشگیری از هرگونه استفادهٔ نابجا یا به خطر افتادن احتمالی، دسترسی به ابزارهای ممیزی سیستم‌های اطلاعاتی، محافظت شده باشد.

راهنمای پیاده‌سازی

توصیه می‌شود ابزارهای کنترل سیستم‌های اطلاعات مانند نرم‌افزارها یا فایل های داده‌ها، از سیستم‌های توسعه و عملیاتی تفکیک شوند و در کتابخانه های نوار یا مناطق کاربر نگهداری نشوند مگر این که سطح مناسبی از محافظت اضافه را دریافت کنند.

اطلاعات دیگر

اگر اشخاص ثالث در بازرسی شرکت دارند، ممکن است خطر سوء استفاده از ابزارهای حسابرسی توسط این اشخاص ثالث وجود داشته باشد، و اطلاعات توسط این سازمان شخص سوم مورد دسترسی قرار گیرد. توصیه می‌شود کنترل هایی نظیر ۶-۲-۱ (برای ارزیابی ریسک ها) و ۹-۱-۲ (برای محدودسازی دسترسی فیزیکی) را می‌توان برای پرداختن به ریسک و هر گونه پیامد آن نظیر کلمات عبوری که فورا تغییر می‌کنند و در معرض دید بازرسی کننده ها قرار دارند باید در نظر گرفته شود.

کتابنامه

۱- استاندارد ملی ایران ۱-۹۹۷۰: سال ۱۳۸۶، فن‌آوری اطلاعات - تکنیک‌های امنیت - مدیریت امنیت تکنولوژی ارتباطات و اطلاعات – قسمت اول: مفاهیم و مدل‌های مدیریت امنیت تکنولوژی ارتباطات و اطلاعات

۲- استاندارد ملی ایران ایزو ۱۹۰۱۱: سال ۱۳۸۶، رهنمودهایی برای ممیزی سیستم‌های مدیریت کیفیت و/یا زیست محیطی

3- ISO/IEC Guide 2:1996, Standardization and related activities – General vocabulary

4- ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards

5- ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security

6- ISO/IEC 13888-1: 1997, Information technology – Security techniques – Non-repudiation – Part 1: General

7- ISO/IEC 11770-1:1996 Information technology – Security techniques – Key management – Part 1: Framework

8- ISO/IEC 9796-2:2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

9- ISO/IEC 9796-3:2000 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

10- ISO/IEC 14888-1:1998 Information technology – Security techniques – Digital signatures with appendix – Part 1: General

11- ISO/IEC 15408-1:1999 Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model

12- ISO/IEC 14516:2002 Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services

13- ISO 15489-1:2001 Information and documentation – Records management – Part 1: General

14- ISO 10007:2003 Quality management systems – Guidelines for configuration management

15- ISO/IEC 12207:1995 Information technology – Software life cycle processes

16- OECD Guidelines for the Security of Information Systems and Networks: ‘Towards a Culture of Security’, 2002

17- OECD Guidelines for Cryptography Policy, 1997
18- IEEE P1363-2000: Standard Specifications for Public-Key Cryptography

19- ISO/IEC 18028-4 Information technology – Security techniques – IT Network security – Part 4: Securing remote access

20- ISO/IEC TR 18044 Information technology – Security techniques – Information security incident

ICS: 35.040

صفحه : ۱۲۵