ISIRI-ISO-IEC

17799

1st. edition

Identical with
ISO/IEC 17799:2005

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

استاندارد ایران- ایزو- آی ای سی

۱۷۷۹۹

چاپ اول

فن‌آوری اطلاعات- فنون امنیتی- آیین‌کار مدیریت امنیت اطلاعات

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

ICS:35.040

به نام خدا

آشنایی با سازمان استاندارد و تحقیقات صنعتی ایران

سازمان استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان 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 کمیسیون‌های فنی مرکب از کارشناسان سازمان[۱]، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که سازمان استاندارد تشکیل می‌دهد به تصویب رسیده باشند.

سازمان استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[۲] کمیسیون بین‌المللی الکتروتکنیک (IEC)[۳] و سازمان بین‌المللی اندازه شناسی قانونی (OIML)[۴] است و به عنوان تنها رابط[۵] کمیسیون کدکس غذایی (CAC) [۶] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان استاندارد این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامه تأیید صلاحیت به آنها اعطا و بر عملکرد آنها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

۱- سازمان استاندارد و تحقیقات صنعتی ایران

2 - International organization for Standardization

3 - International Electro technical Commission

4 - International Organization for Legal Metrology (Organization International de Metrology Legal)

5 - Contact point

6 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

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

رئیس:	**سمت و/ یا نمایندگی**
قرایی، محمدحسن (کارشناسی ارشد مخابرات - سیستم)	گروه مهندسین فن آوری نوین ۵۲ (سهامی خاص)
دبیران:	
رضایی، امید (کارشناسی ارشد مخابرات - رمز)	گروه مهندسین فن آوری نوین۵۲ (سهامی خاص)
میرمطهری، نوید (کارشناسی ارشد مهندسی مخابرات - سیستم)	گروه مهندسین فن آوری نوین۵۲ (سهامی خاص)
اعضاء: (اسامی به ترتیب حروف الفبا)	
احمدلو، یعقوب (کارشناسی ارشد مدیریت فناوری اطلاعات	کارشناس ارشد دفتر مرکزی حراست بانک کشاورزی
ارومیه‌چی‌ها، محمد علی (کارشناسی ارشد مخابرات - رمز)	کارشناس ارشد شرکت صنایع الکترونیک زعیم
بلند قامت، حسین (کارشناسی ارشد کامپیوتر - نرم افزار)	کارشناس ارشد سازمان بیمه ایران
تدین، محمد حسام (دکتری ریاضی کاربردی)	عضو هیات علمی مرکز تحقیقات مخابرات ایران
حمزه لویی منفرد، حسن (کارشناسی ریاضی کاربردی)	مدیر عامل شرکت مهندسی ایمن رایانه شرق (سهامی خاص)
کریمی، علیرضا (کارشناسی ارشد مخابرات - رمز)	مدیر حوزه اجرایی آزمایشگاه و مرکز تخصصی آپا رمز

قاسمی، حسین (کارشناسی ارشد مخابرات - رمز)	کمیته ملی برق والکترونیک ایران (INEC)
قرایی، نرجس (کارشناسی برق - قدرت)	کارشناس گروه مهندسین فن‌آوری نوین۵۲ (سهامی خاص)
میری، سید امیر مسعود (دکتری مهندسی برق - الکترونیک)	عضو هیات علمی دانشگاه امام حسین (ع)
یزدیان، علی (دکتری مهندسی برق)	عضو هیات علمی دانشگاه تربیت مدرس

فهرست مندرجات

پیش گفتار

استاندارد "فن‌آوری اطلاعات - فنون امنیتی - آیین‌کار مدیریت امنیت اطلاعات" که پیش‌نویس آن در کمیسیون فنی مربوط، توسط مرکزتحقیقات مخابرات ایران، برمبنای روش تنفیذ مورد اشاره **در راهنمای ISO/IEC Guide21-1 (پذیرش منطقه‌ای یا ملی استانداردهای "بین‌المللی/ منطقه‌ای" و دیگر مدارک استاندارد)** به عنوان استاندارد ملی ایران، تهیه شده و در هشتاد و هفتمین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده ها مورخ ۱۳۸۸/۱۰/۲۳ مورد تصویب قرارگرفته‌است اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌گردد.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهدشد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرارخواهدگرفت. بنابراین همواره از آخرین تجدیدنظر آنها استفاده‌خواهدشد.

این استاندارد ملی براساس پذیرش استاندارد بین‌المللی به شرح زیر است:

ISO/IEC 17799:2005, “Information technology - Security techniques - Code of practice for information security management” + Cor:2007

مقدمه

۰-۱ امنیت اطلاعات چیست؟

اطلاعات، دارایی[1] است همانند سایر دارایی‌های مهم کسب‌وکار که برای کسب‌وکار سازمان دارای اهمیت است، و درنتیجه باید بگونه‌ای مناسب محافظت شود. این موضوع در محیطی که تعاملات کسب‌وکار در آن رو به افزایش است، دارای اهمیت ویژه‌ای است. در نتیجه این اتصالات در حال افزایش، اکنون اطلاعات در معرض تهدیدات[2] و آسیب‌پذیری‌هایی[3] قرار گرفته است که از نظر تعداد و تنوع در حال افزایش هستند (رهنمودهای[4] "سازمان همکاری و توسعه اقتصادی"[5] برای امنیت "سامانه‌های اطلاعاتی"[6] و شبکه‌ها را نیز ببینید).

اطلاعات می‌تواند به اشکال گوناگون وجود داشته باشد. اطلاعات می‌تواند بر روی کاغذ چاپ یا نوشته شده باشد، به‌صورت الکترونیکی ذخیره شده باشد، با پست یا با استفاده از وسایل الکترونیکی ارسال شود، از طریق فیلم به نمایش درآید، یا در مکالمه بیان شود. اطلاعات به هر شکلی که باشد، یا به هر روشی که به اشتراک[7] گذاشته یا ذخیره[8] شود، همیشه باید از آن به‌گونه‌ای مناسب حفاظت شود.

امنیت اطلاعات، حفاظت از اطلاعات در برابر طیف گسترده‌ای از تهدیدات است و به منظور اطمینان از "استمرار کسب‌وکار"[9]، کمینه کردن "ریسک کسب‌وکار"[10] و بیشینه کردن "بازگشت سرمایه‌گذاری‌ها"[11] و "فرصت‌های کسب‌وکار"[12] است.

امنیت اطلاعات، با پیاده‌سازی مجموعه‌ای از کنترل‌های مناسب شامل خط‌مشی‌ها[13]، فرایندها[14]، رویه‌ها[15]، "ساختارهای سازمانی"[16] و کارکردهای نرم‌افزاری و سخت‌افزاری، قابل دستیابی است. این کنترل‌ها در موارد لازم باید مستقر[17]، پیاده‌سازی[18]، پایش[19] و بازبینی[20] شده و بهبود[21] یابند تا از برآورده‌شدن اهداف خاص

---

1 - Asset
2 - Threats
3 - Vulnerabilities
4 - Guidelines
5 - Organization for Economic Co-operation and Development (OECD)
6 - Information Systems
7 - Share
8 - Store
9 - Business continuity
10 - Business risk
11 - Return on investments
12 - Business opportunities
13 - Policies
14 - Processes
15 - Procedures
16 - Organizational structures
17 - Establish
18 - Implement
19 - Monitor
20 - Review
21 - Improve

امنیتی و کسب‌وکار در سازمان، اطمینان حاصل شود. توصیه می‌شود که این موارد در راستای سایر فرایندهای مدیریت کسب‌وکار انجام شوند.

۲-۰ چرا امنیت اطلاعات لازم است؟

اطلاعات و "فرایندهای پشتیبان"[۱]، سامانه‌ها و شبکه‌ها، دارایی‌های مهم کسب‌وکار هستند. تعریف[۲]، دستیابی[۳]، نگهداری[۴] و بهبود امنیت اطلاعات می‌تواند تاثیر به‌سزایی بر ماندگاری در عرصه رقابت، "گردش مالی"[۵]، سودآوری[۶]، "پایبندی به قانون"[۷] و "وجهه تجاری"[۸] داشته باشد.

سازمان‌ها و سامانه‌های اطلاعاتی و شبکه‌های آنها با تهدیدات امنیتی از منابع گوناگون، از قبیل "کلاهبرداری رایانه‌ای"[۹]، جاسوسی[۱۰]، "خرابکاری عمدی"[۱۱]، "خرابکاری ضداجتماعی"[۱۲]، آتش‌سوزی و سیل مواجه هستند.

دلایل بروز خسارت از قبیل "کد مخرب"[۱۳]، "رخنه‌گری رایانه‌ای"[۱۴]، و "حملات ممانعت از سرویس"[۱۵]، متداول‌تر و زیاده‌خواهانه‌تر[۱۶] و به‌صورت فزاینده‌ای پیچیده‌تر شده‌اند.

امنیت اطلاعات، برای کسب‌وکار بخش‌های خصوصی و عمومی و نیز برای حفاظت از "زیرساخت‌های حیاتی"[۱۷] اهمیت دارد. امنیت اطلاعات در هر دو بخش به‌عنوان یک توانمندساز[۱۸]، مثلاً برای دستیابی به دولت الکترونیک یا کسب‌وکار الکترونیک و اجتناب از ریسک‌های مرتبط یا کاهش آن ریسک‌ها، عمل خواهد کرد. اتصال بین شبکه‌های عمومی و خصوصی و به اشتراک گذاشتن منابع اطلاعاتی، دشواری دستیابی به "کنترل دسترسی"[۱۹] را افزایش می‌دهد. گرایش به "محاسبات توزیع شده"[۲۰] نیز تاثیر کنترل متخصص مرکزی را تضعیف کرده است.

بسیاری از سامانه‌های اطلاعاتی به‌گونه‌ای طراحی نشده‌اند که امن باشند. امنیتی که از طریق وسایل فنی بدست می‌آید، محدود بوده و باید از طریق رویه‌ها و مدیریت مناسب پشتیبانی شود. شناسایی‌کردن کنترل-های مورد استفاده، نیازمند برنامه‌ریزی دقیق و توجه به جزئیات است. مدیریت امنیت اطلاعات، دست‌کم

---

1 - Supporting processes
2 - Defining
3 - Achieving
4 - Maintaining
5 - Cash flow
6 - Profitability
7 - Legal compliance
8 - Commercial image
9 - Computer-assisted fraud
10 - Espionage
11 - Sabotage
12 - Vandalism
13 - Malicious code
14 - Computer hacking
15 - Denial of service attacks
16 - Ambitious
17 - Critical infrastructures
18 - Enabler
19 - Access control
20 - Distributed computing

نیازمند مشارکت تمامی کارمندان در سازمان است. همچنین ممکن است به مشارکت سهامداران[1]، "تامین-کنندگان"[2]، "طرف‌های ثالث"[3]، مشتریان و سایر اشخاص بیرونی نیازمند باشد. دریافت مشاوره از متخصصین خارج از سازمان نیز ممکن است مورد نیاز باشد.

۳-۰ چگونه نیازهای امنیتی را برقرار کنید؟

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

۱- یکی از منابع، از ارزیابی‌کردن ریسک سازمان نتیجه می‌شود، که با درنظرگرفتن اهداف و راهبردهای[4] کلان کسب‌وکار سازمان میسر می‌شود. در طی عملیات "ارزیابی ریسک"[5]، تهدیدات علیه دارایی‌ها شناسایی شده، آسیب‌پذیری و احتمال رخدادن آن ارزیابی شده و میزان پیامد بالقوه حاصل، تخمین زده می‌شود.

۲- منبع دیگر، "محیط فرهنگی-اجتماعی"[6] ، "حقوق مدون"[7]، مقررات[8] و الزامات قراردادی[9] و قانونی[10] است که یک سازمان و شرکای تجاری، پیمانکاران[11] و "ارائه کنندگان سرویس"[12] آن باید رعایت کنند.

۳- منبع دیگر، مجموعه ای خاص از اصول[13]، اهداف[14] و الزامات[15] کسب‌وکار برای پردازش اطلاعات است که سازمان آنها را برای پشتیبانی از عملیات خود، توسعه داده است.

۴-۰ ارزیابی ریسک‌های امنیتی

نیازهای امنیتی از طریق "ارزیابی روش‌مند"[16] ریسک‌های امنیتی، شناسایی می‌شوند. لازم است که هزینه-های صرف شده برای کنترل‌ها، نسبت به هزینه آسیب احتمالی وارد شده به کسب‌وکار که ناشی از خطاهای امنیتی است، متعادل شوند.

نتیجه ارزیابی ریسک به راهنمایی و تعیین "اقدام مدیریتی"[17] مناسب و تعیین اولویت‌ها[18] برای مدیریت ریسک‌های امنیت اطلاعات و پیاده‌سازی کنترل‌های انتخاب شده برای حفاظت در برابر این ریسک‌ها، کمک خواهد کرد.

توصیه می‌شود، ارزیابی ریسک در بازه‌های زمانی تکرار شود تا هر تغییری که ممکن است بر نتایج ارزیابی ریسک تاثیر گذار باشد را نشان دهد.

---

1 - Shareholders
2 - Suppliers
3 - Third parties
4 - Strategy
5 - Risk assessment
6 - Socio-cultural environment
7 - Statutory
8 - Regulatory
9 - Contractual
10 - Legal
11 - Contractors
12 - Service providers
13 - Principles
14 - Objectives
15 - Requirements
16 - Methodical assessment
17 - Management action
18 - Priorities

اطلاعات بیشتر درباره ارزیابی ریسک‌های امنیتی را در بند ۴-۱ ("ارزیابی ریسک‌های امنیت"[1]) از مرجع الزامی این استاندارد می‌توان یافت.

۵-۰ انتخاب کنترل‌ها

پس از اینکه نیازهای امنیتی و ریسک‌ها شناسایی شدند و تصمیم‌ها برای برطرف‌سازی ریسک‌ها اتخاذ شدند، کنترل‌های مناسب باید به‌گونه‌ای انتخاب و به‌کار گرفته شوند که از کاهش ریسک‌ها و رسیدن آنها به "سطح قابل قبول"[2] اطمینان حاصل شود. کنترل‌ها می‌توانند از این استاندارد یا دیگر مجموعه‌های کنترلی، یا از کنترل‌های جدید که به‌گونه‌ای مناسب و به‌منظور برآورده‌کردن نیازهای خاص طراحی شده‌اند، انتخاب شوند. انتخاب کنترل‌های امنیتی، به تصمیمات سازمان که براساس معیار[3] پذیرش ریسک، "گزینه‌های برطرف-سازی ریسک"[4] و رویکرد اتخاذ شده مدیریت ریسک در سازمان و همچنین کلیه "قوانین وضع شده"[5] و مقررات ملی و بین‌المللی که باید مدنظر قرار گیرند، وابسته است.

برخی از کنترل‌ها در این استاندارد می‌توانند به‌عنوان اصول راهنما برای مدیریت امنیت اطلاعات که در بیشتر سازمان‌ها قابل به‌کارگیری هستند، درنظرگرفته شوند. جزئیات بیشتر درباره این کنترل‌ها در ادامه و تحت عنوان "نقطه آغازین امنیت اطلاعات"[6] تشریح شده است.

اطلاعات بیشتر درباره انتخاب کنترل‌ها و سایر گزینه‌های برطرف‌سازی ریسک را می‌توان در بند ۴-۲ ("برطرف‌سازی ریسک‌های امنیت"[7]) از مرجع الزامی این استاندارد یافت.

۶-۰ نقطه آغازین امنیت اطلاعات

تعدادی از کنترل‌ها را می‌توان به عنوان نقطه شروع مناسبی برای پیاده‌سازی امنیت اطلاعات در نظر گرفت. این کنترل‌ها یا براساس الزامات ضروری قوانین وضع شده و یا براساس "تجربه مشترک"[8] در امنیت اطلاعات هستند.

کنترل‌هایی که از منظر قوانین وضع شده - برحسب قابل اجرا بودن این قوانین - برای هر سازمان ضروری فرض می‌شوند، عبارتند از:

الف- حفاظت از داده‌ها و "حریم خصوصی"[9] اطلاعات شخصی (به بند ۱۵-۱-۴ از مرجع الزامی این استاندارد رجوع کنید.)

ب- حفاظت از "سوابق سازمانی"[10] (به بند ۱۵-۱-۳ از مرجع الزامی این استاندارد رجوع کنید.)

پ- "حقوق مالکیت معنوی"[11] (به بند ۱۵-۱-۲ از مرجع الزامی این استاندارد رجوع کنید.)

کنترل‌هایی که حاصل تجربیات مشترک امنیت اطلاعات هستند، عبارتند از:

---

1 - Assessing security risks
2 - Acceptable level
3 - Criteria
4 - Risk treatment options
5 - Legislation
6 - Information security starting point
7 - Treating security risks
8 - Common practice
9 - Privacy
10 - Organizational records
11 - Intellectual property rights

الف- سند خط‌مشی امنیت اطلاعات (به بند ۵-۱-۱ از مرجع الزامی این استاندارد رجوع کنید.)
ب- تخصیص[1] مسوولیت‌های[2] امنیت اطلاعات (به بند ۶-۱-۳ از مرجع الزامی این استاندارد رجوع کنید.)
پ- آگاهی‌رسانی[3]، آموزش[4] و تمرین[5] امنیت اطلاعات (به بند ۸-۲-۲ از مرجع الزامی این استاندارد رجوع کنید.)
ت- پردازش صحیح در برنامه های‌کاربردی (به بند ۱۲-۲ از مرجع الزامی این استاندارد رجوع کنید.)
ث- مدیریت فنی آسیب‌پذیری (رجوع کنید به بند ۱۲-۶ از مرجع الزامی این استاندارد رجوع کنید.)
ج- مدیریت استمرار کسب‌وکار (به بند ۱۴ از مرجع الزامی این استاندارد رجوع کنید.)
چ- مدیریت رخدادهای[6] امنیت اطلاعات و بهینه‌سازی‌ها[7] (به بند ۱۳-۲ از مرجع الزامی این استاندارد رجوع کنید.)
این کنترل‌ها در اکثر سازمان‌ها و محیط‌ها قابل اعمال هستند.
لازم به ذکر است که با وجود اینکه همه کنترل‌های این استاندارد مهم بوده و توصیه می‌شود که درنظر گرفته شوند، ارتباط هر کنترل از لحاظ مواجهه با ریسک‌های مشخص سازمان باید در نظر گرفته شود. بنابراین، هر چند که رویکرد در نظر گرفته شده در بالا نقطه شروع مناسبی است اما نمی‌تواند جایگزین انتخاب کنترل‌ها بر اساس ارزیابی ریسک شود.

۰-۷ عوامل حیاتی موفقیت

تجربه نشان داده است که عوامل زیر معمولاً برای پیاده‌سازی موفقیت‌آمیز امنیت اطلاعات در سازمان، حیاتی[8] هستند:
الف - خط‌مشی امنیت اطلاعات، اهداف و فعالیت‌هایی که منعکس کننده اهداف کسب‌وکار هستند؛
ب - یک رویکرد و چارچوب[9] برای پیاده‌سازی، نگهداری[10]، پایش[11] و بهبود امنیت اطلاعات که با "فرهنگ سازمانی"[12] سازگار است؛
پ - پشتیبانی آشکار[13] و تعهد[14] کلیه سطوح مدیریتی؛
ت - درک مناسب از الزامات امنیت اطلاعات، ارزیابی ریسک و مدیریت ریسک؛
ث - معرفی موثر امنیت اطلاعات برای تمام مدیران، کارکنان و سایر افراد به‌منظور آگاه‌سازی آنها؛

---

1 - Allocation
2 - Responsibilities
3 - Awareness
4 - Education
5 - Training
6 - Incidents
7 - Improvements
8 - Critical
9 - Framework
10 - Maintaining
11 - Monitoring
12 - Organizational culture
13 - Visible
14 - Commitment

ج - توزیع راهنمای خط‌مشی امنیتی و استانداردهای امنیت اطلاعات در بین همه مدیران، کارکنان و سایر افراد؛

چ - تامین منابع مالی برای فعالیت‌های مدیریت امنیت اطلاعات؛

ح - آگاه‌سازی، آموزش و تمرین مناسب؛

خ - برقرارسازی یک فرایند موثر مدیریت رخدادهای امنیت اطلاعات؛

د - پیاده‌سازی یک "سامانه اندازه‌گیری"[1] برای ارزیابی کارایی در مدیریت امنیت اطلاعات و ارایه بازخورد برای بهینه‌سازی.

۰-۸ رهنمودهای خود را توسعه دهید

این آیین‌کار می‌تواند به عنوان یک نقطه شروع برای توسعه رهنمودهای اختصاصی برای سازمان به‌کار گرفته‌شود. ممکن است همه کنترل‌ها و رهنمودهای این آیین‌کار قابل‌اجرا نباشند. همچنین ممکن است رهنمودها و کنترل‌های اضافی که در این استاندارد نیامده‌اند، مورد نیاز باشند. هنگامی که مستندات شامل رهنمودها یا کنترل‌های اضافی توسعه داده می‌شوند، ممکن است "ارجاعات-متقاطع"[2] به بندهای این استاندارد، در موارد مقتضی، جهت سهولت در بررسی انطباق بوسیله ممیزان[3] و شرکای کسب‌وکار، مفید باشد.

1 - Measurement system
2 - Cross-references
3 - Auditors

فن‌آوری اطلاعات - فنون امنیتی - آیین‌کار مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین‌المللی ISO/IEC 17799:2005 + Cor:2007 تدوین شده است.

هدف از تدوین این استاندارد،تعیین نحوه برقراری رهنمودها و اصول کلی برای آغازکردن، پیاده‌سازی، نگهداری و بهبود مدیریت امنیت اطلاعات در یک سازمان است. اهداف ذکر شده در این استاندارد، راهنمایی-هایی عمومی درباره اهداف عموما پذیرفته‌شده مدیریت امنیت اطلاعات را فراهم می‌کنند.

اهداف کنترلی و کنترل‌های این استاندارد به‌منظور برآورده‌کردن الزامات شناسایی شده توسط یک ارزیابی ریسک، پیاده‌سازی می‌شوند. این استاندارد ملی می‌تواند به‌عنوان رهنمود عملی برای توسعه استانداردهای امنیت سازمانی و تجربه‌های موثر مدیریت امنیت، و کمک به ایجاد اطمینان در فعالیت‌های میان سازمانی مورد استفاده قرار گیرد.

۲ واژگان و تعاریف

برای مقاصد این مستند، واژگان 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.

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

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

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

[ISO/IEC Guide 73:2002]

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 مراجع الزامی

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

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

استفاده از مراجع الزامی زیر برای این استاندارد الزامی است:

2.1. ISO/IEC Guide 2:1996, Standardization and related activities – General vocabulary

2.2. ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards

2.3. ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

2.4. ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security

2.5. ISO/IEC 13888-1: 1997, Information technology – Security techniques – Non-repudiation – Part 1: General

2.6. ISO/IEC 11770-1:1996 Information technology – Security techniques – Key management – Part 1: Framework

2.7. ISO/IEC 9796-2:2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

2.8. ISO/IEC 9796-3:2000 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

2.9. ISO/IEC 14888-1:1998 Information technology – Security techniques – Digital signatures with appendix – Part 1: General

2.10. ISO/IEC 15408-1:1999 Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model

2.11. ISO/IEC 14516:2002 Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services

2.12. ISO 15489-1:2001 Information and documentation – Records management – Part 1: General

2.13. ISO 10007:2003 Quality management systems – Guidelines for configuration management

2.14. ISO/IEC 12207:1995 Information technology – Software life cycle processes

2.15. ISO 19011:2002 Guidelines for quality and /or environmental management systems auditing

2.16. OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002

2.17. OECD Guidelines for Cryptography Policy, 1997

2.18. IEEE P1363-2000: Standard Specifications for Public-Key Cryptography

2.19. ISO/IEC 18028-4 Information technology – Security techniques – IT Network security – Part 4: Securing remote access

2.20. ISO/IEC TR 18044 Information technology – Security techniques – Information security incident management

کلیه بندهای استاندارد بین‌المللی ISO/IEC 17799:2005 درمورد این استاندارد، معتبر و الزامی است.