استاندارد ایران-
ایزو- آی ای سی۲۷۰۰۳
چاپ اول

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان استاندارد و تحقیقات صنعتی ایران

Institute of Standards and Industrial Research of Iran

ISIRI- ISO/IEC 27003

1st. Edition

Identical with ISO/IEC 27003: 2010

فناوری اطلاعات ـ فنون امنیتی ـ راهنمای اجرای سامانه مدیریت امنیت اطلاعات

Information technology–Security techniques- Information security management system implementation guidance

ICS:35.040

به‌نام خدا

آشنایی با سازمان استاندارد و تحقیقات صنعتی ایران

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

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند 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 بین المللی 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 کشور و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان 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 سازمانها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، مؤسسهٔ استاندارد این گونه سازمان‌ها 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.

---

* سازمان 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

« فناوری اطلاعات ـ فنون امنیتی ـ راهنمای اجرای سامانه مدیریت امنیت اطلاعات»

رئیس	**سمت/ نمایندگی**
آستانی، مهبد (لیسانس مهندسی کامپیوتر)	مدیر انفورماتیک شرکت بازرسی مهندسی ایران (IEI)
دبیر	
محرابی، سروناز (لیسانس مدیریت صنعتی)	متخصص تضمین کیفیت کانال فروش شرکت ام تی ان ایرانسل
اعضاء (اسامی به ترتیب حروف الفباء)	
آستانی،مهبد (لیسانس مهندسی کامپیوتر)	مدیر انفورماتیک شرکت بازرسی مهندسی ایران
اکرام نصرتیان، بهرنگ (لیسانس مکانیک)	مدیر پروژه شرکت بازرسی مهندسی ایران
باقرتبریزی، بابک (لیسانس مهندسی صنایع)	مدیر تضمین کیفیت و بازرگانی شرکت بازرسی مهندسی ایران
موفقی، سولماز (فوق لیسانس مهندسی مکانیک)	مدیرپروژه و کارشناس فنی شرکت بازرسی مهندسی ایران
نامغ، ساناز (فوق لیسانس مهندسی پزشکی)	کارشناس فنی و بازرگانی شرکت بازرسی مهندسی ایران

فهرست مندرجات

پیش گفتار

استاندارد "فناوری اطلاعات- فنون امنیتی – راهنمای اجرای سامانه مدیریت امنیت اطلاعات" که پیش نویس آن در کمیسیون فنی مربوط ،توسط .....سازمان استاندارد، بر مبنای روش تنفیذ مورد اشاره در راهنمای ISO/IEC Guide21-1 (پذیرش منطقه ای یا ملی استاندارد های " بین المللی/ منطقه ای" و دیگر مدارک استاندارد) به عنوان استاندارد ملی ایران ، تهیه شده ودر یک صد و سی هفتمین اجلاسیه کمیته ملی استانداردرایانه و فر آوری داده.مورخ .۱۳۸۹/۱۲/۲۴.مورد تصویب قرارگرفته است اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱،به عنوان استانداردملی ایران منتشر می گردد.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفتهای ملی و جهانی در زمینه صنایع ،علوم وخدمات ،استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهدشدو هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود،در هنگام تجدیدنظردرکمیسیون فنی مربوط،موردتوجه قرارخواهدگرفت.بنابراین همواره از آخرین تجدیدنظرآنها استفاده خواهدشد.

این استاندارد ملی بر اساس پذیرش استاندارد" بین المللی " به شرح زیر است:

ISO/IEC 27003: 2010, Information technology – security techniques – information security management implementation guidance

فناوری اطلاعات ـ فنون امنیتی ـ راهنمای اجرای سامانه مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین المللی ISO/IEC 27003:2010 تدوین شده است.

هدف از تدوین این استانداردتمرکز بر روی جنبه های حیاتی مورد نیاز برای طراحی و اجرای یک سامانه مدیریت امنیت اطلاعاتی۱ (ISMS) هماهنگ با استاندارد ملی ایران – ایزو آی ای سی ۲۷۰۰۱ : سال ۸۷ است.

این استاندارد فرآیند ویژگی سیستم مدیریت امنیت اطلاعات و طراحی آن از ابتدا تا تولید طرحهای اجرایی را توصیف می کند. این استاندارد فرآیند دستیابی به تایید مدیریت جهت اجرای سیستم مدیریت امنیت اطلاعات، معرف پروژه ای جهت اجرای سامانه مدیریت امنیت اطلاعات (که در این استاندارد ملی به عنوان پروژه ISMS بیان شده است.) و راهنمایی جهت طرح ریزی پروژه ISMS فراهم می کند که منجر به طرح نهایی اجرای پروژه ISMS می شود.

این استاندارد ملی مخصوص در سازمان های اجرا کننده ISMS است. این استاندارد قابلیت کاربرد برای تمام انواع سازمان ها در تمامی ابعاد را دارا می باشد (برای مثال بنگاههای اقتصادی تجاری ، ارگان های دولتی،سازمان های غیرانتفاعی) . پیچیدگی هر سازمان و ریسک هایش منحصر بفرد می باشد و الزامات ویژه آن منجر به اجرای ISMS می شود. سازمانهای کوچکتر فعالیتهای ذکرشده در این استاندارد ملی را برای خود، کاربردی میدانند و میتوانند آن را ساده سازی کنند. سازمانهای با مقیاس بزرگترو پیچیده متوجه می شوند که سازمان با لایه های ساختاری یا سامانه مدیریت ، برای مدیریت فعالیتهای این استاندارد ملی به صورت اثر بخش مورد نیاز می باشد. اگرچه، در دو حالت ذکرشده ، میتوانند فعالیتهای مرتبطی برای کاربرد این استاندارد ملی طرح ریزی شود.

این استاندارد ملی توضیحات و توصیه هایی ارائه می دهد که تعیین کننده هیچ گونه الزاماتی نمی باشد . این استاندارد به منظور استفاده مقارن با استاندارد ملی ایران–ایزو آی ای سی ۲۷۰۰۲ : سال ۸۷ ایجاد شده است ، اما قصد اصلاح و/یا کم کردن الزامات مشخص شده در استاندارد ملی ایران– ایزو آی ای سی ۲۷۰۰۱ و یا توصیه های فراهم شده در استاندارد ملی ایران– ایزو آی ای سی ۲۷۰۰۲ : سال ۸۷ را ندارد . ادعای تطابق با این استاندارد ملی صحیح نمی باشد .

۲ مراجع الزامی

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

در صورتی که با مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه هـا و تجدیـد نظرهـای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی بدون ذکر تـاریخ انتشـار بـه آن هـا ارجاع داده شده است،همواره آخرین تاریخ تجدید نظر و اصلاحیه های بعدی آن ها مورد نظر است . استفاده از مراجع زیر برای این استاندارد الزامی است :

2-1 ISO/IEC 27000:2009 Information technology – security techniques – information security management system – overview and vocabulary

۲-۲ استاندارد ملی ایران – ایزو آی ای سی ۲۷۰۰۱ : سال ۸۷، فن آوری اطلاعات ،فنون امنیتی – سیستم های مدیریت امنیت اطلاعات – الزامات

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف تعریف شده در استاندارد ایران– ایزو آی ای سی ۲۷۰۰۱ : سال ۸۷ و استاندارد ISO/IEC 27000:2009 کاربرد دارد .

کلیه بندهای استاندارد بین المللی ISO/IEC 27003: 2010 در مورد این استاندارد معتبر و الزامی است.