به نام خدا

سیستم مدیریت امنیت اطلاعات (ISMS)

کلیات استاندارد ISO/IEC 17799

حیات و دوام سازمانها در دنیای پیچیده امروز بـه عوامـل مختلفـی بـستگی دارد. یکـی از ایـن عوامل تأمین حفاظ برای کلیه سرمایه های سازمان می باشد. هدف امنیـت اطلاعـات ایجـاد حفـاظ برای سرمایه های سازمان است به طوریکه سرعت عمل و انعطـاف پـذیری سـازمان را دچـار ضـعف نسازد. تدوین استانداردهای جهانی، تصویب قوانین حقوقی و کیفری به منظور حفاظـت از سـرمایه ها در حال رشد می باشد. ISO / IEC ۱۷۷۹۹ یکی از این استانداردها ست.

این استاندارد که مشابه بخش ۱ استاندارد BS۷۷۹۹ می باشد روش استقرار امنیت اطلاعات را در سازمان ارائه می نماید. این استاندارد شامل ۱۰ مرحله است که تعریف هر مرحله به طور خلاصه در زیر آمده است.

۱- سیاست امنیت اطلاعات

ایجاد دیدگاه و جلب پشتیبانی مدیریت برای امنیت اطلاعات و جلـب مـشارکت در تـدوین سند امنیت اطلاعات با محتوی (اهداف، محدوده عملکرد، سیاستها، مفاهیم، استانداردها، قوانین موضوعه، مسئولیتهای کلان مدیریت امنیت اطلاعـات، ارزیـابی مخـاطرات، آسـیب پـذیری هـا، تعهدات و وقایع) و بازبینی آن بـا تغییـر در زیـر سـاختهای سـازمان یـا بـروز وقـایع و آسـیب پذیریهای جدید

۲ - امنیت سازمانی

مدیریت امنیت اطلاعات در سازمان با تدوین چارچوب امنیت، تشکیل انجمن مدیریت امنیت اطلاعات هدایت و اداره کردن استقرار امنیت اطلاعات، تعیین مسئولیتها در حفاظت از سرمایه ها اعم از مشهود و نامشهود

۳ - کنترل و دسته بندی سرمایه

برقراری حفاظت مناسب از سرمایه های سازمان با شناسائی سرمایه ها و تعیین متولی برای آنها در سه جنبه سرمایه های اطلاعاتی، نرم افزاری و فیزیکی

۴ - امنیت پرسنل

شناسائی اطلاعات در حوزه های فردی و نحوه ایمن سازی آنها، آموزش پرسنل، تدوین،پذیرش و امضاء توافقنامه های حفظ محرمانگی اطلاعات

۵ - امنیت محیطی و فیزیکی

جلوگیری از دسترسی افراد غیر مجاز، پیشگیری از خرابی، تأثیر مخرب بر روی اطلاعات سازمان، سازماندهی تجهیزات پردازش اطلاعات در محلهای امن و ایجاد کنترلهای لازم.

۶ - مدیریت عملیات و ارتباطات

حصول اطمینان از عملکرد درست و ایمن تجهیزات پردازش اطلاعات، شناخت روالها و مسئولیتها به منظورمدیریت و عملکرد کلیه تجهیزات پردازش اطلاعات، از نحوه عملکرد کاربر تا سرویسها و تجهیزات ارتباطی، اطمینان از صحت و در دسترس بودن تجهیزات و برنامه ریزی

برای جایگزینی، ارتقاء و استفاده از سیستم جدید،ایمن سازی تبادلات الکترونیکی (تبادل اطلاعات،تجارت الکترونیک،پست الکترونیک).

۷- کنترل دسترسی

تدوین، استقرار و مدیریت قوانین و کنترلهای لازم جهت دسترسی کاربران به منابع و سرمایه های سازمان اعم از سیستم های اطلاعاتی، شبکه و کامپیوترها.

۸- امنیت سیستمهای اطلاعاتی

اطمینان از وجود کنترلهای امنیتی در سیستمهای اطلاعاتی، زیر ساختها و نرم افزارهای کاربردی تولید شده توسط کاربران.

شناسایی اطلاعات در حوزه های فردی و نحوه ایمن سازی آنها، آموزش پرسنل تدوین توافقنامه های حفظ محرمانگی اطلاعات

۹ - مدیریت دوام (حیات) سازمان

کاهش و پیشگیری از وقفه در فعالیتهای سازمان و حفاظت از فرایندهای حیاتی سازمان در مقابل خطاها و توقفات (ناشی از حوادث قهریه، خطای تجهیزات ، اتفاقات و فعالیتهای عمومی) استقرارفرایند تدوام سازمان سبب کاهش خرابی از طریق اقدامهای بازدارنده و کنترلهای بازیابی خواهد شد.

کلیه مشکلات اعم از خطاهای امنیتی، نقص در سرویسها و حتی نتایج خرابیها باید تحلیل شود.

برنامه پیشامدهای احتمالی به منظور بازیابی فرایندهای سازمانی باید ایجاد و استقرار یابد این طرحها باید چنان اجراء شوند که بخشی از دیگر فرایندهای مدیریتی گردند.

مدیریت تدوام سازمان باید شامل کنترلهای تعریف و کاهش خطاها، محدود سازی نتایج اتفاقات مخرب و تأمین کننده اطمینان از بازیابی فرایندهای اصلی باشد.

۱۰ - سازگاری

سازگاری با شرایط قانونی به منظور پیشگیری از تخطی از قوانین حقوقی و کشوری و رعایت کلیه حقوق معنوی و حق تألیف و تکثیر در سیستمهای سازمان طراحی، عمل، مدیریت و استفاده از سیستم های اطلاعاتی باید از شرایط امنیتی قانونی، قراردادی و حقوقی متابعت نماید. حدود قانونی که باید رعایت شود را از سازمانهای مشاور حقوقی یا وکلای حقوقی تأیید صلاحیت شده باید جویا شد. شرایط قانونی در هر کشور متفاوت بوده و این شرایط بر اطلاعاتی که از کشوری به کشور دیگر منتقل می شود نیز حاکم خواهد بود.