استاندارد بین‌المللی ISO/IEC 27001

امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی

سیستم‌های مدیریت امنیت اطلاعات - الزامات

ویرایش سوم ۲۰۲۲-۱۰

سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC)

شماره مرجع

ISO/IEC 27001 :2022

مترجم:

« مهندس علی پولادی »

دارای پروانه صلاحیت نظارت و مشاوره فناوری اطلاعات و ارتباطات (فاوا)

رشته « شبکه و اینترنت » و « سخت افزار و زیرساخت »

فهرست مطالب

فهرست مطالب

۱. کلیات

این سند برای ارائه الزامات مربوط به ایجاد، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات تهیه شده است. استقرار سیستم مدیریت امنیت اطلاعات یک تصمیم راهبردی برای سازمان محسوب می‌شود. ایجاد و پیاده‌سازی این سیستم تحت تأثیر نیازها و اهداف سازمان، الزامات امنیتی، فرآیندهای سازمانی و همچنین اندازه و ساختار سازمان قرار دارد. همه این عوامل تأثیرگذار به مرور زمان تغییر خواهند کرد.

سیستم مدیریت امنیت اطلاعات با به‌کارگیری فرآیند مدیریت ریسک، محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات را حفظ می‌کند و به ذینفعان اطمینان می‌دهد که ریسک‌ها به‌صورت مناسب مدیریت می‌شوند. مهم است که سیستم مدیریت امنیت اطلاعات به‌عنوان بخشی از فرآیندها و ساختار کلی مدیریت سازمان در نظر گرفته شود و در طراحی فرآیندها، سیستم‌های اطلاعاتی و کنترل‌ها، امنیت اطلاعات مدنظر قرار گیرد. انتظار می‌رود پیاده‌سازی سیستم مدیریت امنیت اطلاعات متناسب با نیازهای سازمان مقیاس‌بندی شود.

این سند می‌تواند توسط طرف‌های داخلی و خارجی برای ارزیابی توانایی سازمان در برآورده‌سازی الزامات امنیت اطلاعات خود مورد استفاده قرار گیرد. ترتیب ارائه الزامات در این سند نشان‌دهنده اهمیت آن‌ها یا ترتیب اجرا نیست و شماره‌گذاری موارد صرفاً برای سهولت ارجاع انجام شده است.

استاندارد ISO/IEC 27000 به توصیف کلیات و واژگان سیستم‌های مدیریت امنیت اطلاعات می‌پردازد و با اشاره به خانواده استانداردهای سیستم مدیریت امنیت اطلاعات (از جمله ISO/IEC 27003، ISO/IEC 27004 و ISO/IEC 27005)، اصطلاحات و تعاریف مرتبط را ارائه می‌کند.

۲. سازگاری با سایر استانداردهای سیستم مدیریت

این سند از ساختار سطح بالا، عناوین یکسان زیربندها، متن مشترک، اصطلاحات یکسان و تعاریف اصلی مندرج در پیوست SL از دستورالعمل‌های ISO/IEC (بخش ۱، الحاقیه تجمیع‌شده ISO) پیروی می‌کند و بنابراین با سایر

بخش دوم

امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی - سیستم‌های مدیریت امنیت اطلاعات - الزامات

۴ چارچوب سازمان

۱٫۴ درک سازمان و چارچوب آن

سازمان باید مسائل خارجی و داخلی مرتبط با اهداف خود را که بر توانایی آن در دستیابی به نتایج مورد نظر سیستم مدیریت امنیت اطلاعات تأثیر می‌گذارند، تعیین کند.

❖ تذکر: تعیین این مسائل به معنای ایجاد چارچوب خارجی و داخلی سازمان است که در بند ۱.۴.۵ ISO 31000:2018 [۵] مورد توجه قرار گرفته است.

۲٫۴ درک نیازها و انتظارات ذینفعان

سازمان باید موارد زیر را تعیین کند:

الف) ذینفعان مرتبط با سیستم مدیریت امنیت اطلاعات؛

ب) الزامات مرتبط این ذینفعان؛

پ) کدام یک از این الزامات از طریق سیستم مدیریت امنیت اطلاعات مورد توجه قرار خواهند گرفت.

❖ تذکر: الزامات ذینفعان می‌تواند شامل الزامات قانونی، مقرراتی و تعهدات قراردادی باشد.

۳٫۴ تعیین محدوده سیستم مدیریت امنیت اطلاعات

سازمان باید حدود و قابلیت اعمال سیستم مدیریت امنیت اطلاعات را بهمنظور تعیین محدوده آن مشخص کند.

هنگام تعیین این محدوده، سازمان باید موارد زیر را در نظر بگیرد:

الف) مسائل خارجی و داخلی اشارهشده در بند ۱٫۴؛

ب) الزامات اشارهشده در بند ۲٫۴؛

ج) رابطها و وابستگیهای بین فعالیتهای انجامشده توسط سازمان و فعالیتهایی که توسط سازمانهای دیگر انجام میشوند.

محدوده تعیی نشده باید به عنوان اطلاعات مستند در دسترس باشد.

۴٫۴ سیستم مدیریت امنیت اطلاعات

سازمان باید یک سیستم مدیریت امنیت اطلاعات را مطابق با الزامات این استاندارد ایجاد، پیادهسازی، نگهداری و بهبود مستمر کند. این سیستم شامل فرآیندهای مورد نیاز و تعاملات بین آنها است.

۵ رهبری

۱٫۵ رهبری و تعهد

مدیریت ارشد باید رهبری و تعهد خود را نسبت به سیستم مدیریت امنیت اطلاعات از طریق موارد زیر نشان دهد: