ناوک هوشمند پویان

Edge Intelligent Enterprise

ISO 27001

www.navak-ai.ir

ISO-27001

ISO 27001 یک استاندارد بین‌المللی برای مدیریت امنیت اطلاعات است که توسط سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC) منتشر شده است. این استاندارد چارچوبی را برای ایجاد، پیاده‌سازی، نگهداری و بهبود مداوم سیستم مدیریت امنیت اطلاعات (ISMS) فراهم میکند. هدف اصلی ISO 27001 این است که اطمینان حاصل شود که سازمانها به طور موثر امنیت اطلاعات خود را مدیریت میکنند و از داده‌های حساس محافظت میکنند.

برخی از نکات کلیدی ISO 27001 عبارتند از:

ارزیابی ریسک: شناسایی، تحلیل و ارزیابی ریسک‌های امنیتی.

کنترل‌ها: پیاده‌سازی مجموعه‌ای از کنترل‌های امنیتی برای مدیریت و کاهش ریسک‌ها.

خط مشی‌ها و رویه‌ها: ایجاد و مستندسازی خطمشی‌ها و رویه‌های مرتبط با امنیت اطلاعات.

آموزش و آگاهی‌بخشی: اطمینان از اینکه کارکنان از اهمیت امنیت اطلاعات آگاه هستند و آموزش‌های لازم را دریافت میکنند.

نظارت و بازنگری: مانیتورینگ مداوم عملکرد ISMS و انجام بازنگری‌های منظم برای اطمینان از اثربخشی آن.

بهبود مستمر: شناسایی فرصت‌های بهبود و اجرای تغییرات لازم برای بهبود مستمرISMS .

سازمانهایی که استاندارد ISO 27001 را پیاده‌سازی و از آن پیروی میکنند، می‌توانند از مزایای مختلفی نظیر افزایش اعتماد مشتریان، بهبود مدیریت ریسک، و ارتقاء امنیت اطلاعات برخوردار شوند. همچنین، این استاندارد میتواند به سازمان‌ها در برآورده کردن الزامات قانونی و قراردادی مرتبط با امنیت اطلاعات کمک کند.

021-88109330
0933-6889690
www.navak-ai.ir
info@navak-ai.ir

ISO-27001

الزامات استقرار ISO 27001 شامل مجموعه‌ای از فرآیندها، سیاست‌ها، رویه‌ها و کنترل‌هایی است که سازمان باید به منظور ایجاد، پیاده‌سازی، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات (ISMS) خود دنبال کند. این الزامات در استاندارد ISO 27001 مشخص شده‌اند و به سه بخش اصلی تقسیم میشوند:

الزامات مدیریت سیستم امنیت اطلاعات

محدوده ISMS : تعیین و مستندسازی محدوده ISMS که شامل فرآیندها، سیستمها، مکانها و اطلاعاتی است که تحت پوشش قرار میگیرند.

خط مشی امنیت اطلاعات: تدوین و تصویب یک خط‌مشی امنیت اطلاعات که راهنمایی‌های لازم برای پیاده‌سازی و مدیریت ISMS را ارائه میدهد.

تعهد مدیریت: تعهد مدیریت ارشد به حمایت از ISMS و تخصیص منابع کافی برای پیاده‌سازی و نگهداری آن.

برنامه‌ریزی ISMS :تدوین برنامه‌ای برای پیاده‌سازی ISMS که شامل اهداف امنیت اطلاعات و فرآیندهای لازم برای دستیابی به آنها است.

ارزیابی و مدیریت ریسک

شناسایی ریسک‌ها: شناسایی دارایی‌های اطلاعاتی، تهدیدها، آسیب‌پذیری‌ها و ریسک‌های مرتبط با آنها.

ارزیابی ریسک: تحلیل و ارزیابی ریسک‌های شناسایی شده بر اساس تأثیر و احتمال وقوع آنها.

مدیریت ریسک: تعیین استراتژی‌های مدیریت ریسک شامل پذیرش، انتقال، کاهش یا حذف ریسک‌ها و انتخاب کنترل‌های مناسب برای مدیریت آنها.

بیانیه کاربردی بودن (SoA) :تدوین یک بیانیه کاربردی بودن که نشان میدهد کدام کنترل‌ها انتخاب شده‌اند و چرا.

021-88109330
0933-6889690
www.navak-ai.ir
info@navak-ai.ir

ISO-27001

کنترل‌ها و سیاست‌ها

کنترل‌های امنیت اطلاعات: پیاده‌سازی مجموعه‌ای از کنترل‌های امنیت اطلاعات بر اساس نیازها و ریسک‌های شناسایی شده. این کنترل‌ها در پیوست A استاندارد ISO 27001 ذکر شده‌اند و شامل موارد زیر هستند:

سیاست‌های امنیت اطلاعات: سیاست‌ها و استانداردهای مرتبط با امنیت اطلاعات.

سازمان امنیت اطلاعات: ساختار سازمانی و نقش‌ها و مسئولیت‌ها.

امنیت منابع انسانی: فرآیندهای مربوط به استخدام، آموزش و مدیریت کارکنان.

مدیریت دارایی‌ها: شناسایی و مدیریت دارایی‌های اطلاعاتی.

کنترل‌های دسترسی: کنترل دسترسی به اطلاعات و سیستم‌ها.

رمزنگاری: استفاده از تکنیک‌های رمزنگاری برای حفاظت از اطلاعات حساس.

امنیت فیزیکی و محیطی: حفاظت فیزیکی از اطلاعات و تجهیزات.

امنیت عملیات: مدیریت عملیات امنیت اطلاعات شامل پشتیبان‌گیری، مانیتورینگ و نگهداری سیستم‌ها.

امنیت ارتباطات: حفاظت از اطلاعات در حین انتقال.

مدیریت دسترسی تأمین‌کنندگان: مدیریت دسترسی و روابط با تأمین‌کنندگان و شرکای تجاری.

مدیریت حوادث امنیتی: شناسایی، گزارش‌دهی و پاسخ به حوادث امنیتی.

استمراری کسب و کار: برنامه‌ریزی برای حفظ استمراری کسب و کار در مواجهه با وقایع مخرب.

انطباق: اطمینان از انطباق با قوانین، مقررات و الزامات قراردادی.

021-88109330
0933-6889690
www.navak-ai.ir
info@navak-ai.ir

ISO-27001

نظارت، بازنگری و بهبود مستمر

نظارت و اندازه‌گیری: مانیتورینگ مداوم و اندازه‌گیری عملکرد ISMS و کنترل‌های امنیتی.

ممیزی داخلی: انجام ممیزی‌های داخلی برای ارزیابی عملکرد ISMS و شناسایی نقاط ضعف و نیازهای بهبود.

بازنگری مدیریت: برگزاری جلسات بازنگری مدیریت برای ارزیابی عملکرد ISMS و تصمیم‌گیری درباره اقدامات اصلاحی و بهبود.

اقدامات اصلاحی و پیشگیرانه: شناسایی و اجرای اقدامات اصلاحی و پیشگیرانه برای رفع نواقص و بهبود عملکرد ISMS

بهبود مستمر: شناسایی فرصت‌های بهبود و اجرای تغییرات لازم برای بهبود مستمر ISMS

با پیروی از این الزامات، سازمان‌ها میتوانند اطمینان حاصل کنند که سیستم مدیریت امنیت اطلاعات آنها مطابق با استاندارد ISO 27001 است و به طور مؤثر از اطلاعات حساس خود محافظت میکنند.

نکات ویژه برای استقرار استاندارد ISO-27001 در ایران

انتخاب مشاور داخلی :استفاده از مشاوران داخلی که با شرایط و الزامات بومی ایران آشنا هستند، میتواند کمک بزرگی باشد.

رعایت مقررات ملی :اطمینان حاصل کنید که پیاده‌سازی ISMS با قوانین و مقررات ملی ایران، از جمله مقررات مرتبط با حفاظت از اطلاعات و حریم خصوصی، همخوانی دارد.

آموزش محلی :فراهم کردن آموزش‌های مناسب و بومی‌سازی شده برای کارکنان میتواند به بهبود آگاهی و کارایی پیاده‌سازی کمک کند.

021-88109330
0933-6889690
www.navak-ai.ir
info@navak-ai.ir