به نام خدا

عنوان سند:

High-Level Information Security Policy

سیاست کلی امنیت اطلاعات

۱- هدف (Purpose)

هدف از این سند، تعیین چارچوب کلی امنیت اطلاعات در شرکت و اطمینان از حفاظت مناسب از اطلاعات، دارایی‌های اطلاعاتی و سیستم‌های مرتبط در برابر تهدیدات داخلی و خارجی است. این سیاست در راستای پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) و همسو با استاندارد ISO/IEC ۲۷۰۰۱ ، چارچوب NIST Cybersecurity Framework و اصول حاکمیت فناوری اطلاعات COBIT تدوین شده است.

۲- دامنه کاربرد(Scope)

این سیاست برای کلیه کارکنان، مدیران، پیمانکاران، مشاوران و اشخاص ثالثی که به اطلاعات، سیستم‌ها یا دارایی‌های اطلاعاتی شرکت دسترسی دارند، الزامی است. دامنه این سیاست شامل کلیه اطلاعات دیجیتال، فیزیکی و کاغذی شرکت می‌باشد.

۳- تعاریف (Definitions)

- ISMS: سیستم مدیریت امنیت اطلاعات مبتنی بر ISO/IEC ۲۷۰۰۱
- NIST CSF: چارچوب امنیت سایبری موسسه ملی استاندارد و فناوری
- COBIT: چارچوب حاکمیت و مدیریت فناوری اطلاعات
- دارایی اطلاعاتی: هر نوع داده، سیستم، نرم‌افزار، سخت‌افزار یا دانش سازمانی

۴- اصول کلی امنیت اطلاعات(Information Security Principles)

سیاست امنیت اطلاعات شرکت بر اساس اصول زیر بنا شده است:

- محرمانگی :(Confidentiality) جلوگیری از دسترسی غیرمجاز به اطلاعات
- یکپارچگی :(Integrity) حفظ صحت و کامل بودن اطلاعات
- دسترس‌پذیری :(Availability) اطمینان از در دسترس بودن اطلاعات برای کاربران مجاز در زمان نیاز

۵- حاکمیت و مسئولیت‌ها(Governance & Responsibilities)

مدیریت ارشد

- حمایت و تعهد به اجرایISMS
- تأمین منابع لازم برای امنیت اطلاعات
- بازبینی دوره‌ای وضعیت امنیت اطلاعات

مسئول امنیت اطلاعاتISMS Officer

- پیاده‌سازی و نگهداریISMS
- انجام ارزیابی ریسک‌های امنیت اطلاعات
- نظارت بر اجرای کنترل‌های امنیتی

کارکنان و کاربران

- رعایت سیاست‌ها و رویه‌های امنیت اطلاعات
- گزارش فوری حوادث و ضعف‌های امنیتی

۶- مدیریت ریسک امنیت اطلاعات (Information Security Risk Management)

شرکت متعهد است ریسک‌های امنیت اطلاعات را شناسایی، تحلیل، ارزیابی و درمان نماید. این فرآیند مطابق با الزامات ISO/IEC ۲۷۰۰۱و همسو با NIST CSF (Identify & Protect) انجام می‌شود. نتایج ارزیابی ریسک در قالب **Risk Register**مستندسازی و به‌صورت دوره‌ای بازبینی می‌گردد.

۷- کنترل‌های امنیتی(Security Controls)

کنترل‌های امنیتی مناسب بر اساس نتایج ارزیابی ریسک انتخاب و در قالب Statement of Applicability (SoA) مستندسازی می‌شوند. این کنترل‌ها حوزه‌های زیر را پوشش می‌دهند:

- کنترل دسترسی
- امنیت منابع انسانی
- امنیت فیزیکی و محیطی
- امنیت عملیات و شبکه
- مدیریت حوادث امنیت اطلاعات

۸- مدیریت حوادث امنیت اطلاعات(Incident Management)

شرکت فرآیند مشخصی برای شناسایی، گزارش‌دهی، پاسخ و درس‌آموخته‌های حوادث امنیت اطلاعات دارد. کلیه کارکنان موظف‌اند هرگونه حادثه یا ضعف امنیتی را در اسرع وقت گزارش نمایند. این بخش همسو با بخش Respond و Recover در NIST CSF می‌باشد.

۹- انطباق و الزامات قانونی(Compliance)

شرکت متعهد است کلیه قوانین، مقررات و الزامات مرتبط با امنیت اطلاعات در جمهوری اسلامی ایران (از جمله الزامات افتا در صورت کاربرد) و تعهدات قراردادی را رعایت نماید.

۱۰- آموزش و آگاهی امنیت اطلاعات(Awareness & Training)

برنامه‌های آموزش و آگاهی امنیت اطلاعات به‌صورت دوره‌ای برای کارکنان اجرا می‌شود تا سطح آگاهی نسبت به تهدیدات امنیتی، مسئولیت‌ها و رویه‌های امنیتی افزایش یابد.

۱۱- پایش، ممیزی و بهبود مستمر(Monitoring & Continuous Improvement)

عملکرد ISMS از طریق شاخص‌های کلیدی عملکرد(KPIs) ، ممیزی‌های داخلی و بازبینی مدیریت پایش می‌شود. شرکت متعهد به بهبود مستمر سیستم مدیریت امنیت اطلاعات بر اساس چرخه Plan-Do-Check-Act (PDCA)است.

۱۲- تصویب و بازبینی سیاست(Approval & Review)

این سیاست توسط مدیریت ارشد تصویب شده و حداقل سالی یک‌بار یا در صورت بروز تغییرات اساسی در کسب‌وکار، فناوری یا تهدیدات امنیتی بازبینی می‌گردد.

تصویب‌کننده :مدیریت ارشد شرکت
تاریخ اجرا
نسخه