به نام خدا

عنوان سند:

Risk Register & Risk Treatment Plan

ارزیابی ریسک و برنامه مقابله با ریسک

۱- هدف (Purpose)

هدف از این سند، ثبت، مدیریت و پایش ریسک‌های امنیت اطلاعات شناسایی‌شده در چارچوب سیستم مدیریت امنیت اطلاعات (ISMS) شرکت «فین‌تک نوآور» و تعیین اقدامات درمان ریسک به‌منظور کاهش ریسک‌ها تا سطح قابل پذیرش سازمان می‌باشد. این سند مطابق با الزامات (Clause ۶.۱) ISO/IEC ۲۷۰۰۱:۲۰۲۲ تدوین شده است.

۲- دامنه کاربرد(Scope)

این سند کلیه ریسک‌های مرتبط با دارایی‌های اطلاعاتی، فرآیندها، سیستم‌ها، کارکنان و اشخاص ثالث تعریف‌شده در دامنه ISMS را پوشش می‌دهد و ورودی اصلی برای Statement of Applicability (SoA) محسوب می‌شود.

۳- تعاریف کلیدی(Definitions)

- **Risk Register**: مخزن رسمی ثبت ریسک‌های شناسایی‌شده
- **Risk Treatment Plan**: برنامه اقدام جهت حذف، کاهش، انتقال یا پذیرش ریسک
- **Risk Owner**: مسئول تصمیم‌گیری و پیگیری درمان ریسک

۴- معیار امتیاز دهی ریسک

سطح ریسک بر اساس فرمول زیر محاسبه می‌شود:

Risk Level = Likelihood × Impact

سطوح ریسک:

- Low (1–5)
- Medium (6–12)
- High (15–25)

۵- جدول ارزیابی ریسک (Risk Register)

Risk ID	Asset	Threat	Vulnerability	Likelihood	Impact	Risk Level	Risk Owner
R-01	Database مشتریان	Phishing	آگاهی پایین کاربران	4	5	20 (High)	مدیر امنیت اطلاعات
R-02	سامانه کیف پول	Access Abuse	دسترسی بیش‌ازحد ادمین	3	5	15 (High)	مدیر IT
R-03	سرورهای عملیاتی	Malware	کامل EDR نبود	3	4	12 (Medium)	مدیر زیرساخت
R-04	کد منبع نرم‌افزار	Secure Coding Flaw	Code نبود رسمی Review	3	4	12 (Medium)	مدیر DevOps
R-05	حساب‌های کاربری کارکنان	Credential Theft	رمز عبور ضعیف	4	4	16 (High)	مدیر IT
R-06	لاگ‌های امنیتی	Incident Blindness	مانیتورینگ ناکافی	3	4	12 (Medium)	SOC Manager
R-07	اطلاعات HR	Data Leakage	کنترل دسترسی ناکافی	2	4	8 (Medium)	HR Manager
R-08	سرویس ابری	Third-Party Risk	امنیتی SLA نبود	3	5	15 (High)	مدیر فناوری
R-09	تجهیزات فیزیکی	Physical Access	کنترل فیزیکی ضعیف	2	4	8 (Medium)	Facility Manager
R-10	فرآیند Incident Response	Delayed Response	نبود تمرین سناریو	3	4	12 (Medium)	ISMS Manager

۶- برنامه درمان ریسک ها (Risk Treatment Plan)

Risk ID	Treatment Option	Treatment Action	Annex A Control	Responsible	Target Date	Residual Risk
R-01	Reduce	آموزش آگاهی فیشینگ و شبیه‌سازی حمله	A.6.3	HR / Security	3ماه	Medium
R-02	Reduce	بازبینی دسترسی‌های سطح بالا	A.8.2	IT Manager	2ماه	Medium
R-03	Reduce	پیاده‌سازی EDR و Anti-Malware	A.8.7	Infra Manager	3ماه	Low
R-04	Reduce	تعریف Secure Code و SDLC Review	A.8.25	DevOps Manager	4ماه	Medium
R-05	Reduce	سیاست رمز عبور و MFA	A.8.5 / A.8.2	IT Manager	2ماه	Low
R-06	Reduce	بهبود لاگینگ و مانیتورینگ	A.8.31 / A.8.32	SOC Manager	3ماه	Medium
R-07	Reduce	محدودسازی دسترسی به اطلاعات HR	A.6.6	HR Manager	2ماه	Low
R-08	Reduce	تعریف SLA و ارزیابی ریسک طرف ثالث	A.5.23	CIO	4ماه	Medium
R-09	Reduce	کنترل دسترسی فیزیکی و CCTV	A.7.1	Facility Manager	3ماه	Low
R-10	Reduce	تمرین سناریو Incident Response	A.5.24	ISMS Manager	6ماه	Medium

۷- پذیرش ریسک (Risk Acceptance)

ریسک‌های باقی‌مانده (Residual Risks) که در سطح Low یا Medium قرار دارند، با تأیید مدیریت ارشد قابل پذیرش خواهند بود. پذیرش ریسک‌ها مستندسازی می‌گردد.

۸- پایش و بازبینی

این سند حداقل سالی یک‌بار و یا در صورت بروز تغییرات اساسی در دارایی‌ها، تهدیدات یا نتایج ممیزی بازبینی و به‌روزرسانی می‌شود.

تصویب‌کننده :مدیریت ارشد شرکت
تاریخ اجرا
نسخه