به نام خدا

عنوان سند:

Statement of Applicability – SOA

بیانیه کاربردپذیری

۱- هدف (Purpose)

این بیانیه کاربردپذیری (SoA) به‌منظور مشخص نمودن کنترل‌های امنیت اطلاعات قابل اعمال، غیرقابل اعمال و یا اعمال‌شده در سیستم مدیریت امنیت اطلاعات (ISMS) شرکت «فین‌تک نوآور» تدوین گردیده است. این سند ارتباط مستقیم بین نتایج ارزیابی ریسک، برنامه درمان ریسک و کنترل‌های Annex A استاندارد ISO/IEC ۲۷۰۰۱:۲۰۲۲ را نشان می‌دهد.

۲- دامنه کاربرد(Scope)

این SoA کلیه کنترل‌های امنیت اطلاعات مندرج در Annex A استاندارد ISO/IEC ۲۷۰۰۱:۲۰۲۲ را در محدوده دامنه تعریف‌شده ISMS پوشش می‌دهد و برای تصمیم‌گیری مدیریت، ممیزی داخلی و ممیزی صدور/مراقبتی مورد استفاده قرار می‌گیرد.

۳- مبنای انتخاب کنترل‌ها

کنترل‌های انتخاب‌شده در این SoA بر اساس موارد زیر تعیین گردیده‌اند:

- نتایج فرآیند ارزیابی ریسک امنیت اطلاعات
- معیار پذیرش ریسک سازمان
- الزامات قانونی و نظارتی (بانک مرکزی، شاپرک، پلیس فتا)
- نیازهای کسب‌وکار و الزامات ذی‌نفعان

۴- وضعیت کنترل های Annex A

- Applicable قابل اعمال
- Not Applicable غیرقابل اعمال
- Implementedاجرا شده / در حال اجرا

۵- جدول بیانیه کاربردپذیری

Domain	Control ID	Control Description	Applicability	Implementation Status	Justification / Link to Risk
Organizational	A.5.1	Policies for information security	Applicable	Implemented	کاهش ریسک نبود حاکمیت امنیت اطلاعات
Organizational	A.5.7	Threat intelligence	Applicable	Partially Implemented	ریسک تهدیدات فیشینگ و حملات سایبری
Organizational	A.5.23	Information security for use of cloud services	Applicable	Planned	ریسک وابستگی به سرویس‌دهنده ابری
People	A.6.3	Information security awareness, education and training	Applicable	Implemented	ریسک خطای انسانی و فیشینگ
People	A.6.6	Confidentiality or non-disclosure agreements	Applicable	Implemented	ریسک افشای اطلاعات توسط کارکنان
Physical	A.7.4	Physical security monitoring	Applicable	Partially Implemented	ریسک دسترسی فیزیکی غیرمجاز
Physical	A.7.10	Storage media	Applicable	Planned	ریسک نشت اطلاعات از رسانه‌ها
Technological	A.8.2	Privileged access rights	Applicable	Implemented	ریسک سوءاستفاده از دسترسی سطح بالا
Technological	A.8.7	Protection against malware	Applicable	Implemented	ریسک آلودگی بدافزاری
Technological	A.8.9	Configuration management	Applicable	Planned	ریسک پیکربندی ناامن سیستم‌ها
Technological	A.8.12	Data leakage prevention	Applicable	Planned	ریسک نشت اطلاعات مشتریان
Technological	A.8.16	Cryptographic controls	Applicable	Implemented	ریسک افشای داده‌های تراکنشی
Technological	A.8.23	Web filtering	Applicable	Partially Implemented	ریسک دسترسی به سایت‌های مخرب
Technological	A.8.25	Secure development lifecycle	Applicable	Planned	ریسک آسیب‌پذیری نرم‌افزار
Technological	A.8.28	Secure coding	Applicable	Partially Implemented	ریسک نقص‌های امنیتی کد
Technological	A.8.31	Logging	Applicable	Implemented	ریسک عدم کشف حوادث
Technological	A.8.32	Monitoring activities	Applicable	Implemented	ریسک عدم تشخیص به‌موقع حملات

۶- ارتباط میان Statement of Applicability و Risk Treatment Plan

کنترل‌های درج‌شده در این SoA مستقیماً از برنامه درمان ریسک استخراج شده‌اند و اجرای آن‌ها منجر به کاهش ریسک‌های شناسایی‌شده تا سطح قابل پذیرش سازمان می‌گردد.

۷- پایش و بازبینی

این بیانیه حداقل سالی یک‌بار و همچنین در صورت تغییرات در نتایج ارزیابی ریسک، دامنه ISMS یا الزامات قانونی بازبینی و به‌روزرسانی می‌شود.

تصویب‌کننده :مدیریت ارشد شرکت
تاریخ اجرا
نسخه