					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P06S					Název dokumentu: **Politika řízení rizik**						
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:						
X	Politika		Standard		Postup		Formulář		Registr		Jiné

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma/právní předpis	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Články 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 až RA-7, PM-9	
směrnice NIS2	Článek 21 odst. 2 písm. a) až d)	
nařízení DORA	Článek 5	
COBIT 2019	APO12, MEA01	

1. Účel

1.1 Tato politika stanoví, jak organizace identifikuje, vyhodnocuje a řídí rizika související s bezpečností informací, provozem, technologiemi a službami třetích stran.

1.2 Zajišťuje, aby řízení rizik bylo aktivní součástí plánování, realizace projektů, výběru dodavatelů a reakce na incidenty v souladu s ISO 27001, ISO 31000 a regulatorními požadavky.

1.3 Tato politika podporuje informované rozhodování, ochranu informačních aktiv a odolnost klíčových obchodních činností.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechna oddělení, systémy a uživatele v rámci organizace,

2.1.2 veškeré informace, služby a aktiva spravované interně nebo prostřednictvím třetích stran,

2.1.3 činnosti související s riziky, včetně přezkumů projektů, modernizací systémů, outsourcingu a souladu s právními předpisy.

2.2 Zahrnuje všechny typy rizik, například:

2.2.1 kybernetické hrozby a zranitelnosti systémů,

2.2.2 provozní narušení a výpadky služeb,

2.2.3 právní rizika, rizika nesouladu nebo poškození dobré pověsti,

2.2.4 rizika třetích stran a dodavatelského řetězce.

2.3 Veškerý personál, smluvní pracovníci a poskytovatelé služeb musí tuto politiku dodržovat při identifikaci nebo hlášení rizik.

3. Cíle

3.1 Začlenit jednoduché a opakovatelné postupy hodnocení rizik do běžného provozu organizace.

3.2 Identifikovat a prioritizovat rizika, která by mohla ovlivnit důvěrnost, integritu, dostupnost nebo právní soulad.

3.3 Přidělit vlastnictví a definovat opatření k ošetření rizik pro všechna významná rizika.

3.4 Udržovat přesný a aktuální registr rizik na podporu připravenosti na audit a monitorování rizik.

3.5 Zajistit zapojení vedení do schvalování ochoty podstupovat riziko a hlavních plánů ošetření rizik.

4. Role a odpovědnosti

4.1 Generální ředitel

4.1.1 Stanovuje ochotu organizace podstupovat riziko a schvaluje rámec řízení rizik.

4.1.2 Schvaluje zásadní rozhodnutí o ošetření rizik a související zdroje.

4.1.3 Čtvrtletně přezkoumává nejvýznamnější rizika s koordinátorem rizik.

4.2 Koordinátor rizik (nebo vlastník ISMS)

4.2.1 Zajišťuje provádění hodnocení rizik a spravuje registr rizik.

4.2.2 Zajišťuje, aby skórování rizik, vlastnictví a činnosti v rámci ošetření rizik byly zdokumentovány.

4.2.3 Organizuje nejméně jeden formální přezkum rizik ročně.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Každoroční přezkum politiky

9.1.1 Tato politika musí být alespoň jednou ročně přezkoumána generálním ředitelem a koordinátorem rizik, aby byla zajištěna její relevance a úplnost.

9.2 Spouštěče aktualizace

9.2.1 Předčasný přezkum a aktualizace musí proběhnout, pokud:

9.2.1.1 významný incident nebo zjištění auditu odhalí nedostatky v řízení rizik,

9.2.1.2 jsou zavedeny nové obchodní jednotky, technologie nebo partnerství,

9.2.1.3 dojde ke změně regulatorního nebo smluvního požadavku.

9.3 Řízení verzí

9.3.1 Všechny aktualizace této politiky musí být vedeny s následujícími metadaty:

9.3.1.1 číslo verze a datum účinnosti,

9.3.1.2 shrnutí změn,

9.3.1.3 schvalovatel (generální ředitel),

9.3.1.4 archivované předchozí verze pro účely auditu.

9.4 Komunikace a povědomí

9.4.1 Aktualizované verze politiky a hlavní plány ošetření rizik musí být komunikovány dotčeným pracovníkům. Každoroční opakovací školení musí zahrnovat základní principy povědomí o rizicích.

10. Související politiky a návaznosti

10.1 Tato politika funguje v koordinaci s několika dalšími dokumenty, aby bylo zajištěno komplexní řízení bezpečnosti:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Definuje, kdo odpovídá za vlastnictví rizik a rozhodování.

10.1.2 P5S – Politika řízení změn: Vyžaduje hodnocení rizik před implementací technických nebo procesních změn.

10.1.3 P17S – Politika ochrany dat a soukromí: Řeší regulatorní rizika spojená se zpracováním osobních údajů.

10.1.4 P30S – Politika reakce na incidenty: Zajišťuje, že ošetření rizik pokračuje během bezpečnostních incidentů i po nich.

10.1.5 P33S – Politika kontinuity činností: Identifikuje zbytková rizika a opatření obnovy pro kritické služby.

11. Referenční normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Článek 6.1 – Stanoví formální proces řízení rizik a plánování ošetření rizik.

11.1.2 Článek 6.1.3 – Vyžaduje, aby organizace uchovávaly zdokumentované plány ošetření a schválení.

11.2 ISO/IEC 27002:

11.2.1 Opatření 5.4, 5.25 – Poskytují pokyny k implementaci pro vlastnictví rizik, stanovení priorit a řízení životního cyklu.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 až RA-7 – Definují hodnocení rizik, strategie reakce, dokumentaci a mechanismy přezkumu.

11.4 PM-9 – Vyžaduje konzistentní dohled nad organizačními riziky na úrovni vedení.

11.5 Směrnice NIS2

11.5.1 Článek 21 odst. 2 písm. a) až d) – Ukládá základním a důležitým subjektům povinné hodnocení rizik, zmírňování rizik a opatření správy a řízení.

11.6 Nařízení DORA

11.6.1 Článek 5 – Vyžaduje, aby regulované subjekty definovaly a řídily rámce řízení ICT rizik, včetně identifikace, klasifikace a reakce.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: Začleňuje rizika do strategického a provozního plánování.

11.7.2 MEA01 – Monitor, Evaluate, and Assess: Zajišťuje účinnost a soulad procesů a opatření v oblasti rizik.