					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P06S					Názov dokumentu: **Politika riadenia rizík**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 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	
Smernica EÚ NIS2	Článok 21(2)(a–d)	
Nariadenie EÚ DORA	Článok 5	
COBIT 2019	APO12, MEA	

1. Účel

1.1 Táto politika stanovuje, ako organizácia identifikuje, vyhodnocuje a riadi riziká súvisiace s informačnou bezpečnosťou, prevádzkou, technológiami a službami tretích strán.

1.2 Zabezpečuje, aby rámec riadenia rizík tvoril aktívnu súčasť plánovania, realizácie projektov, výberu dodávateľov a reakcie na incidenty v súlade s ISO 27001, ISO 31000 a regulačnými požiadavkami.

1.3 Táto politika podporuje informované rozhodovanie, ochranu informačných aktív a odolnosť kľúčových prevádzkových činností organizácie.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky oddelenia, systémy a používateľov v rámci organizácie,

2.1.2 všetky informácie, služby a aktíva spravované interne alebo prostredníctvom tretích strán,

2.1.3 činnosti súvisiace s rizikami vrátane preskúmaní projektov, modernizácie systémov, outsourcingu a dodržiavania predpisov.

2.2 Zahŕňa všetky typy rizík, najmä:

2.2.1 hrozby kybernetickej bezpečnosti a zraniteľnosti systémov,

2.2.2 prevádzkové narušenia a výpadky služieb,

2.2.3 právne, súladové a reputačné riziká,

2.2.4 riziká tretích strán a dodávateľského reťazca.

2.3 Všetci zamestnanci, zmluvní pracovníci a poskytovatelia služieb musia túto politiku dodržiavať pri identifikácii a nahlasovaní rizík.

3. Ciele

3.1 Zaviesť jednoduché a opakovateľné postupy posudzovania rizík do bežnej prevádzky organizácie.

3.2 Identifikovať a prioritizovať riziká, ktoré by mohli ovplyvniť dôvernosť, integritu, dostupnosť alebo súlad s právnymi požiadavkami.

3.3 Priradiť vlastníctvo a definovať opatrenia na ošetrenie rizík pre všetky významné riziká.

3.4 Udržiavať presný a aktuálny register rizík na podporu auditnej pripravenosti a monitorovania rizík.

3.5 Zabezpečiť zapojenie vedenia do schvaľovania tolerancie rizika a hlavných plánov ošetrenia rizík.

4. Roly a zodpovednosti

4.1 Generálny riaditeľ

4.1.1 Určuje apetít organizácie na riziko a schvaľuje rámec riadenia rizík.

4.1.2 Schvaľuje zásadné rozhodnutia o ošetrení rizík a potrebné zdroje.

4.1.3 Štvrťročne preskúmava najvýznamnejšie riziká spolu s koordinátorom rizík.

4.2 Koordinátor rizík (alebo vlastník ISMS)

4.2.1 Zabezpečuje vykonávanie posúdení rizík a udržiava register rizík.

4.2.2 Zabezpečuje, aby skórovanie rizík, vlastníctvo rizík a opatrenia na ošetrenie rizík boli zdokumentované.

4.2.3 Organizuje najmenej jedno formálne preskúmanie rizík ročne.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Ročné preskúmanie politiky

9.1.1 Túto politiku musia Generálny riaditeľ a koordinátor rizík preskúmať najmenej raz ročne, aby zabezpečili jej relevantnosť a úplnosť.

9.2 Spúšťače aktualizácie

9.2.1 Mimoriadne preskúmanie a aktualizácia sa musia vykonať, ak:

9.2.1.1 významný incident alebo zistenia z auditu odhalia nedostatky v kontrolách riadenia rizík,

9.2.1.2 sa zavedú nové organizačné jednotky, technológie alebo partnerstvá,

9.2.1.3 sa zmení regulačná alebo zmluvná požiadavka.

9.3 Riadenie verzií

9.3.1 Všetky aktualizácie tejto politiky musia byť verzované s týmito metadátami:

9.3.1.1 číslo verzie a dátum účinnosti,

9.3.1.2 súhrn zmien,

9.3.1.3 schvaľovateľ (Generálny riaditeľ),

9.3.1.4 archivované predchádzajúce verzie na účely auditu.

9.4 Komunikácia a zvyšovanie povedomia

9.4.1 Aktualizované verzie politiky a hlavné plány ošetrenia rizík musia byť oznámené dotknutým pracovníkom. Ročné školenie zvyšovania povedomia musí zahŕňať základné princípy riadenia rizík.

10. Súvisiace politiky a väzby

10.1 Táto politika sa uplatňuje v koordinácii s ďalšími politikami s cieľom zabezpečiť komplexnú správu a riadenie bezpečnosti:

10.1.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: vymedzuje, kto nesie zodpovednosť za vlastníctvo rizík a rozhodovanie.

10.1.2 P5S – Politika riadenia zmien: vyžaduje posúdenie rizík pred implementáciou technických alebo procesných zmien.

10.1.3 P17S – Politika ochrany údajov a súkromia: rieši regulačné riziká spojené so spracúvaním osobných údajov.

10.1.4 P30S – Politika reakcie na incidenty: zabezpečuje, aby ošetrenie rizík pokračovalo počas bezpečnostných incidentov aj po ich ukončení.

10.1.5 P33S – Politika kontinuity činností: identifikuje reziduálne riziká a opatrenia obnovy pre kritické služby.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Kapitola 6.1 – stanovuje formálny proces riadenia rizík a plánovanie ošetrenia rizík.

11.1.2 Kapitola 6.1.3 – vyžaduje, aby organizácie uchovávali zdokumentované plány ošetrenia rizík a schválenia.

11.2 ISO/IEC 27002:

11.2.1 Kontroly 5.4, 5.25 – poskytujú implementačné usmernenia pre vlastníctvo rizík, prioritizáciu a riadenie životného cyklu.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 až RA-7 – definujú posudzovanie rizík, stratégie reakcie, dokumentáciu a mechanizmy preskúmania.

11.4 PM-9 – vyžaduje konzistentný dohľad nad organizačnými rizikami na úrovni vedenia.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(a–d) – ukladá základným a dôležitým subjektom povinné kontroly posudzovania rizík, zmierňovania rizík a správy a riadenia.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 5 – vyžaduje, aby regulované subjekty definovali a riadili rámce riadenia IKT rizík vrátane identifikácie, klasifikácie a reakcie.

11.7 COBIT 2019

11.7.1 APO12 – Riadenie rizík: integruje riziká do strategického a prevádzkového plánovania.

11.7.2 MEA01 – Monitorovanie, hodnotenie a posudzovanie: zabezpečuje účinnosť a súlad procesov a opatrení riadenia rizík.