					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P06					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**

Soulad s normami a právními předpisy

Norma/právní předpis	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Články 6.1, 8.32, 10	Základ pro identifikaci a řízení rizik, začlenění do řízení změn, neustálé zlepšování
ISO/IEC 27005:2024	Úplná metodika životního cyklu rizik	Komplexní proces řízení rizik v souladu s normou
ISO 31000:2018	Zásady a rámec řízení rizik	Zásady řízení rizik převzaté do rámce
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Pokyny a struktura pro hodnocení rizik, víceúrovňová správa rizik
GDPR	Články 24, 25, 32	Procesy a opatření pro rizika v oblasti ochrany osobních údajů
směrnice NIS2	Článek 21(2)(a–d)	Povinnosti v oblasti hodnocení rizik a bezpečnosti
nařízení DORA	Články 5, 6	Řízení ICT rizik a provozní odolnost
COBIT 2019	APO12, MEA	Struktura řízení rizik a dohled

1. Účel

1.1 Tato politika stanoví jednotný a formalizovaný rámec pro identifikaci, analýzu, vyhodnocení, ošetření, monitorování a přezkum rizik informační bezpečnosti v celé organizaci.

1.2 Zajišťuje konzistentní uplatňování principů založených na rizicích, které chrání důvěrnost, integritu a dostupnost informačních aktiv, v souladu s článkem 6.1 normy ISO/IEC 27001:2022 a normou ISO 31000:2018.

1.3 Tato politika začleňuje řízení rizik informační bezpečnosti do rozhodovacích procesů organizace tak, aby byly naplněny interní strategické cíle i externí regulatorní požadavky.

2. Rozsah

2.1 Tato politika se vztahuje na všechny organizační jednotky, podnikové procesy, systémy, veškerý personál a zapojení třetích stran, které se podílejí na nakládání s informačními aktivy, jejich vývoji, ukládání nebo správě.

2.2 Rozsah zahrnuje fyzická, digitální a cloudová aktiva, včetně strukturovaných i nestrukturovaných dat, aplikací, infrastruktury, sítí a služeb.

2.3 Pokrývá rizika informační bezpečnosti na strategické, provozní, projektové a technické úrovni a je závazná pro všechny zaměstnance, smluvní pracovníky a poskytovatele služeb zapojené do činností ISMS.

2.4 Řízení rizik musí být uplatněno zejména v následujících situacích:

2.4.1 Implementace nového projektu nebo systému

2.4.1.1 Významné změny (např. architektury, vlastnictví, procesů)

2.4.1.2 Zavedení dodavatele a smluvní vztahy s třetími stranami

2.4.1.3 Reakce na incidenty a přezkum po incidentu

2.4.1.4 Pravidelné organizační přezkumy rizik nebo audity

3. Cíle

3.1 Zavést a provozně uplatňovat opakovatelný proces řízení rizik v celé organizaci na základě metodik ISO/IEC 27005 a ISO 31000.

3.2 Zajistit, aby rizika byla identifikována, analyzována, vyhodnocována a ošetřována pomocí strukturovaných a dohledatelných metod, včetně přiřazení vlastnictví rizik a vazeb na opatření.

3.3 Udržovat centralizovaný Registr rizik a Plán ošetření rizik, vedené v režimu správy verzí, které odrážejí aktuální stav rizik, pokrytí opatřeními a průběh zmírňování rizik.

3.4 Slaďovat rozhodnutí o rizicích se zdokumentovanou ochotou podstupovat riziko a úrovněmi tolerance rizika a umožnit informovaná rozhodnutí v oblasti správy a řízení týkající se přijetí rizika, zmírnění rizika, přenosu rizika nebo vyhnutí se riziku.

3.5 Průběžně sledovat trendy rizik a zajišťovat účinnost ošetření rizik při současném umožnění proaktivních úprav na základě vývoje hrozeb nebo změn v podnikání.

4. Role a odpovědnosti

4.1 Vrcholové vedení / správní rada

4.1.1 Schvaluje rámec řízení rizik a stanoví přijatelnou ochotu podstupovat riziko a prahové hodnoty tolerance rizika.

4.1.2 Schvaluje strategie ošetření rizik pro zbytková rizika překračující toleranci.

4.1.3 Přiděluje zdroje a zajišťuje dohled nad účinným fungováním programu řízení rizik.

4.2 Manažer ISMS / manažer rizik

4.2.1 Odpovídá za tuto politiku a udržuje její soulad s normami ISO/IEC 27001 a ISO/IEC 27005.

4.2.2 Řídí podnikový proces hodnocení rizik a spravuje Registr rizik a Plán ošetření rizik.

4.2.3 Zajišťuje pravidelné přezkumy a eskalaci klíčových rizik vrcholovému vedení nebo Řídicímu výboru pro informační bezpečnost.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika a související rámec musí být přezkoumávány každoročně, nebo:

9.1.1 Po závažné rizikové události nebo bezpečnostním incidentu

9.1.2 Po významné organizační nebo technické změně

9.1.3 V reakci na zjištění auditu nebo nové regulatorní požadavky

9.2 Manažer ISMS, manažer rizik a tým compliance společně odpovídají za:

9.2.1 Zahájení cyklu přezkumu

9.2.2 Shromáždění vstupů od organizačních útvarů

9.2.3 Úpravu postupů a prahových hodnot podle potřeby

9.3 Všechny změny musí být:

9.3.1 Vedeny v režimu správy verzí a zaznamenány

9.3.2 Schváleny vrcholovým vedením

9.3.3 Oznámeny zainteresovaným stranám

9.3.4 Uchovávány v auditním repozitáři po dobu nejméně 5 let

10. Související politiky a vazby

10.1 Tato politika je provázána s následujícími politikami informační bezpečnosti:

10.1.1 P1 – Politika informační bezpečnosti: Stanoví celkový model správy a řízení bezpečnosti, v jehož rámci je tato politika rizik uplatňována.

10.1.2 P2 – Politika rolí a odpovědností v oblasti správy a řízení: Vymezuje odpovědné vlastníky a úrovně správy a řízení uvedené v matici eskalace rizik.

10.1.3 P5 – Politika řízení změn: Vyvolává opětovné posouzení rizik při změnách infrastruktury a organizace.

10.1.4 P13 – Politika klasifikace a označování dat: Podporuje posouzení dopadů při identifikaci rizik.

10.1.5 P33 – Politika monitorování auditu a souladu: Ověřuje dodržování politiky, včetně úplnosti Registru rizik a důkazů o ošetření rizik.

11. Referenční normy a rámce

11.1 Tato politika je výslovně sladěna s následujícími normami a rámci, aby splňovala mezinárodně uznávané osvědčené postupy a regulatorní očekávání pro řízení rizik informační bezpečnosti:

11.2 ISO/IEC 27001:

11.2.1 Článek 6.1: Stanoví požadavky na identifikaci rizik a příležitostí, včetně celého životního cyklu hodnocení a ošetření rizik informační bezpečnosti. Tato politika uvádí do praxe články 6.1.2 a 6.1 prostřednictvím strukturovaného rámce, který vyžaduje zdokumentovanou identifikaci, analýzu, vyhodnocení a ošetření rizik a postupy pro přijetí zbytkového rizika.

11.2.2 Článek 8.32: Začlenění přístupu založeného na rizicích do procesů řízení změn zajišťuje, že všechny významné organizační změny vyvolají formální opětovné posouzení rizik.

11.2.3 Článek 10: Neustálé zlepšování je zajištěno prostřednictvím pravidelných přezkumů politiky, analýzy trendů rizik a aktualizací SoA vycházejících z poznatků o rizicích.

11.3 ISO/IEC 27005:

11.3.1 Poskytuje specializované a podrobné pokyny pro řízení rizik informační bezpečnosti. Tato politika implementuje úplný procesní model ISO/IEC 27005 pro rizika: stanovení kontextu, identifikaci rizik, analýzu rizik, vyhodnocení rizik, ošetření rizik, přijetí rizika, komunikaci rizik a monitorování a přezkum rizik.

11.4 ISO 31000:

11.4.1 Tato politika začleňuje zásady normy ISO 31000, jako jsou závazek vedení, integrace do rozhodování a neustálé zlepšování. Zajišťuje, aby bylo řízení rizik zakotveno v kultuře a provozu organizace.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Je v souladu s metodikou NIST pro provádění hodnocení rizik, včetně identifikace hrozeb, analýzy zranitelností, odhadu pravděpodobnosti a určení dopadů. Struktura této politiky odpovídá krokům hodnocení rizik definovaným NIST a přizpůsobuje je technickým i podnikovým procesům.

11.6 NIST SP 800-39:

11.6.1 Podporuje správu rizik na úrovni podniku a zdůrazňuje víceúrovňové řízení rizik na úrovni organizace, poslání/podnikových procesů a informačních systémů. Tato politika zajišťuje, že vlastnictví rizik je jasně definováno na všech úrovních a zahrnuje i strategie ošetření na úrovni organizace.

11.7 GDPR:

11.7.1 Článek 24: Vyžaduje zavedení vhodných technických a organizačních opatření k zajištění řádného řízení rizik v oblasti ochrany osobních údajů — tato politika to řeší prostřednictvím strukturovaného procesu řízení rizik.

11.7.2 Článek 25: „Ochrana osobních údajů již od návrhu a standardně“ odpovídá začlenění ošetření rizik do návrhu systémů a procesů.

11.7.3 Článek 32: Vyžaduje přístup k bezpečnostním opatřením založený na rizicích — tento požadavek je naplněn prostřednictvím vyhodnocení rizik na základě dopadů a výběru bezpečnostních opatření na základě rizika.

11.8 směrnice NIS2:

11.8.1 Článek 21(2)(a–d): Vyžaduje, aby subjekty prováděly hodnocení rizik, zaváděly politiky pro analýzu rizik a zajišťovaly přiměřená bezpečnostní opatření. Tato politika tyto povinnosti naplňuje prostřednictvím průběžného uplatňování životního cyklu rizik a zdokumentované správy a řízení.

11.9 nařízení DORA:

11.9.1 Článek 5: Vyžaduje zdokumentovaný rámec řízení ICT rizik — tato politika jej plně pokrývá, včetně mapování na SoA a KRI.

11.9.2 Článek 6: Vyžaduje začlenění řízení rizik do strategií provozní odolnosti, což je řešeno prostřednictvím matic eskalace a sledování kritických aktiv.

11.10 COBIT 2019:

11.10.1 APO12 – Manage Risk: Přímo odpovídá zavedení strukturovaného přístupu k řízení rizik v organizaci, přiřazení rolí, sledování ošetření rizik a zajištění odpovědnosti na úrovni správní rady.

11.10.2 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Odráží se v důrazu této politiky na analýzu trendů, monitorování KRI a začlenění zpětné vazby z auditů do cyklů neustálého zlepšování.