					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P06					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**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.1, 8.32, 10	Základ identifikácie a riadenia rizík, integrácia do riadenia zmien, nepretržité zlepšovanie
ISO/IEC 27005:2024	Úplná metodika životného cyklu rizík	Úplný proces riadenia rizík v súlade s normou
ISO 31000:2018	Princípy a rámec riadenia rizík	Princípy riadenia rizík prevzaté do rámca
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Usmernenia a štruktúra pre posudzovanie rizík, viacúrovňová správa a riadenie rizík
Nariadenie EÚ GDPR	Články 24, 25, 32	Procesy a kontroly rizík v oblasti ochrany osobných údajov
Smernica EÚ NIS2	Článok 21(2)(a–d)	Povinnosti v oblasti posudzovania rizík a bezpečnosti
Nariadenie EÚ DORA	Články 5, 6	Riadenie rizík IKT a prevádzková odolnosť
COBIT 2019	APO12, MEA	Štruktúra a dohľad nad riadením rizík

1. Účel

1.1 Táto politika stanovuje jednotný a formalizovaný rámec na identifikáciu, analýzu, hodnotenie, ošetrenie, monitorovanie a preskúmavanie rizík informačnej bezpečnosti v celej organizácii.

1.2 Zabezpečuje konzistentné uplatňovanie princípov založených na riziku, ktoré chránia dôvernosť, integritu a dostupnosť informačných aktív v súlade s kapitolou 6.1 normy ISO/IEC 27001:2022 a normou ISO 31000:2018.

1.3 Táto politika začleňuje riadenie rizík informačnej bezpečnosti do rozhodovacích procesov organizácie s cieľom plniť interné strategické ciele a externé regulačné požiadavky.

2. Rozsah pôsobnosti

2.1 Táto politika sa vzťahuje na všetky organizačné jednotky, podnikové procesy, systémy, personál a vzťahy s tretími stranami zapojené do nakladania s informačnými aktívami, ich vývoja, uchovávania alebo správy.

2.2 Rozsah zahŕňa fyzické, digitálne a cloudové aktíva vrátane štruktúrovaných a neštruktúrovaných údajov, aplikácií, infraštruktúry, sietí a služieb.

2.3 Zahŕňa riziká informačnej bezpečnosti na strategickej, prevádzkovej, projektovej a technickej úrovni a je záväzná pre všetkých zamestnancov, zmluvných pracovníkov a poskytovateľov služieb zapojených do činností ISMS.

2.4 Riadenie rizík sa musí uplatňovať najmä v týchto situáciách:

2.4.1 implementácia nového projektu alebo systému

2.4.1.1 významné zmeny (napr. architektúry, vlastníctva, procesov)

2.4.1.2 zapojenie dodávateľa a uzatvorenie dohôd s tretími stranami

2.4.1.3 reakcia na incidenty a následné poincidentné preskúmania

2.4.1.4 pravidelné organizačné preskúmania rizík alebo audity

3. Ciele

3.1 Zaviesť a prevádzkovať opakovateľný proces riadenia rizík v celej organizácii založený na metodikách ISO/IEC 27005 a ISO 31000.

3.2 Zabezpečiť, aby boli riziká identifikované, analyzované, hodnotené a ošetrované pomocou štruktúrovaných a sledovateľných metód vrátane priradenia vlastníctva rizík a väzieb na kontroly.

3.3 Udržiavať centralizovaný register rizík a plán ošetrenia rizík s riadením verzií, ktoré odrážajú aktuálny stav rizík, pokrytie kontrolami a priebeh zmierňovania.

3.4 Zosúladiť rozhodnutia o rizikách so zdokumentovaným apetítom na riziko a úrovňami tolerancie a umožniť informované rozhodovanie v oblasti správy a riadenia o akceptácii rizika, zmierňovaní rizika, prenose alebo vyhýbaní sa riziku.

3.5 Nepretržite monitorovať trendy rizík a zabezpečovať účinnosť ošetrenia rizík pri súčasnom umožnení proaktívnych úprav na základe vývoja hrozieb alebo zmien v organizácii.

4. Roly a zodpovednosti

4.1 vrcholový manažment / predstavenstvo

4.1.1 Schvaľuje rámec riadenia rizík a určuje prijateľný apetít na riziko a prahové hodnoty tolerancie.

4.1.2 Schvaľuje stratégie ošetrenia rizík pre reziduálne riziká presahujúce toleranciu.

4.1.3 Prideľuje zdroje a vykonáva dohľad nad účinným fungovaním programu riadenia rizík.

4.2 manažér ISMS / manažér rizík

4.2.1 Je vlastníkom tejto politiky a zabezpečuje jej súlad s normami ISO/IEC 27001 a ISO/IEC 27005.

4.2.2 Vedie proces podnikového posudzovania rizík a spravuje register rizík a plán ošetrenia rizík.

4.2.3 Zabezpečuje pravidelné preskúmania a eskaláciu kľúčových rizík vrcholovému manažmentu alebo Riadiacemu výboru pre ISMS.

[... 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 Táto politika a súvisiaci rámec sa musia preskúmavať každoročne alebo:

9.1.1 po významnej rizikovej udalosti alebo bezpečnostnom incidente

9.1.2 po významnej organizačnej alebo technickej zmene

9.1.3 v reakcii na auditné zistenia alebo nové regulačné požiadavky

9.2 Manažér ISMS, manažér rizík a funkcia compliance spoločne zodpovedajú za:

9.2.1 začatie cyklu preskúmania

9.2.2 zber vstupov od organizačných jednotiek

9.2.3 revíziu postupov a prahových hodnôt podľa potreby

9.3 Všetky revízie musia byť:

9.3.1 predmetom riadenia verzií a zaznamenané

9.3.2 schválené vrcholovým manažmentom

9.3.3 oznámené zainteresovaným stranám

9.3.4 uchovávané v auditnom úložisku najmenej 5 rokov

10. Súvisiace politiky a väzby

10.1 Táto politika je vzájomne previazaná s nasledujúcimi politikami informačnej bezpečnosti:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje celkový model správy a riadenia bezpečnosti, v rámci ktorého sa táto politika riadenia rizík uplatňuje.

10.1.2 P2 – Politika rolí a zodpovedností v oblasti správy a riadenia: definuje zodpovedných vlastníkov a úrovne správy a riadenia, na ktoré odkazuje matica eskalácie rizík.

10.1.3 P5 – Politika riadenia zmien: vyvoláva prehodnotenie rizík pri zmenách infraštruktúry a organizačných zmenách.

10.1.4 P13 – Politika klasifikácie a označovania údajov: podporuje posúdenie dopadu počas identifikácie rizík.

10.1.5 P33 – Politika monitorovania auditu a súladu: overuje dodržiavanie politiky vrátane úplnosti registra rizík a dôkazov o ošetrení rizík.

11. Referenčné normy a rámce

11.1 Táto politika je výslovne zosúladená s nasledujúcimi normami a rámcami, aby spĺňala medzinárodne uznávané osvedčené postupy a regulačné očakávania v oblasti riadenia rizík informačnej bezpečnosti:

11.2 ISO/IEC 27001:

11.2.1 Kapitola 6.1: stanovuje požiadavky na identifikáciu rizík a príležitostí vrátane celého životného cyklu posudzovania a ošetrenia rizík informačnej bezpečnosti. Táto politika prevádza požiadavky kapitol 6.1 a 6.1.2 do praxe prostredníctvom štruktúrovaného rámca, ktorý vyžaduje zdokumentovanú identifikáciu, analýzu, hodnotenie a ošetrenie rizík, ako aj protokoly akceptácie reziduálneho rizika.

11.2.2 Kapitola 8.32: integrácia prístupu založeného na riziku do procesov riadenia zmien zabezpečuje, že všetky významné organizačné zmeny vyvolajú formálne prehodnotenie rizík.

11.2.3 Kapitola 10: nepretržité zlepšovanie je zabezpečené prostredníctvom pravidelných preskúmaní politiky, analýzy trendov rizík a aktualizácií SoA vychádzajúcich z poznatkov o rizikách.

11.3 ISO/IEC 27005:

11.3.1 Poskytuje špecializované a podrobné usmernenia pre riadenie rizík informačnej bezpečnosti. Táto politika implementuje úplný model procesu rizík podľa ISO/IEC 27005: stanovenie kontextu, identifikácia rizík, analýza rizík, hodnotenie rizík, ošetrenie rizík, akceptácia rizika, komunikácia o rizikách, monitorovanie rizík a preskúmanie.

11.4 ISO 31000:

11.4.1 Táto politika integruje princípy ISO 31000, ako sú záväzok vedenia, integrácia do rozhodovania a nepretržité zlepšovanie. Zabezpečuje, aby bolo riadenie rizík začlenené do kultúry a prevádzky organizácie.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Je zosúladená s príručkou NIST pre vykonávanie posúdení rizík vrátane identifikácie hrozieb, analýzy zraniteľností, odhadu pravdepodobnosti a určenia dopadu. Štruktúra tejto politiky odráža kroky posudzovania rizík definované v NIST a prispôsobuje ich technickým aj podnikovým procesom.

11.6 NIST SP 800-39:

11.6.1 Podporuje správu a riadenie rizík na podnikovej úrovni so zdôraznením viacúrovňového riadenia rizík na úrovni organizácie, poslania/podnikových procesov a informačných systémov. Politika zabezpečuje, aby bolo vlastníctvo rizík jednoznačne určené na všetkých úrovniach, a zahŕňa stratégie ošetrenia na úrovni organizácie.

11.7 Nariadenie EÚ GDPR:

11.7.1 Článok 24: vyžaduje zavedenie primeraných technických a organizačných opatrení na zabezpečenie riadneho riadenia rizík ochrany osobných údajov, čo je riešené prostredníctvom štruktúrovaného procesu riadenia rizík podľa tejto politiky.

11.7.2 Článok 25: zásada „ochrany údajov už pri návrhu a štandardne“ je v súlade so začlenením ošetrenia rizík do návrhu systémov a procesov.

11.7.3 Článok 32: vyžaduje prístup k bezpečnostným opatreniam založený na riziku, ktorý sa napĺňa prostredníctvom hodnotenia rizík na základe dopadu a výberu kontrol na základe rizika.

11.8 Smernica EÚ NIS2:

11.8.1 Článok 21(2)(a–d): vyžaduje, aby subjekty vykonávali posúdenia rizík, zavádzali politiky analýzy rizík a zabezpečovali primerané bezpečnostné opatrenia. Táto politika tieto povinnosti napĺňa prostredníctvom nepretržitého uplatňovania životného cyklu rizík a zdokumentovanej správy a riadenia.

11.9 Nariadenie EÚ DORA:

11.9.1 Článok 5: vyžaduje zdokumentovaný rámec riadenia rizík IKT, ktorý je touto politikou plne pokrytý vrátane mapovania na SoA a KRI.

11.9.2 Článok 6: vyžaduje integráciu riadenia rizík do stratégií prevádzkovej odolnosti, čo je riešené prostredníctvom matíc eskalácie a sledovania kritických aktív.

11.10 COBIT 2019:

11.10.1 APO12 – Riadenie rizík: priamo sa mapuje na zavedenie štruktúrovaného prístupu k riadeniu rizík v organizácii, priradenie rolí, sledovanie ošetrenia rizík a zabezpečenie zodpovednosti na úrovni predstavenstva.

11.10.2 MEA01 – Monitorovanie, hodnotenie a posudzovanie výkonnosti a súladu: odráža sa v zameraní tejto politiky na analýzu trendov, monitorovanie KRI a integráciu spätnej väzby z auditov do cyklov nepretržitého zlepšovania.