					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P02					Názov dokumentu: **Politika rolí a zodpovedností v oblasti správy a riadenia**							
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	Kapitola 5.3; Príloha A, kontrola 5	
ISO/IEC 27002:2022	Kontrola 5	
NIST SP 800-53 Rev.5	PL-1 až PL-4, PM-1 až PM-13	
Nariadenie EÚ GDPR	Články 5(1)(f), 24, 37	
Smernica EÚ NIS2	Článok 21(2)(a)	
Nariadenie EÚ DORA	Článok 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Účel

1.1 Táto politika definuje model správy a riadenia, organizačné roly a zodpovednosti potrebné na prevádzku účinného systému manažérstva informačnej bezpečnosti (ISMS).

1.2 Stanovuje jasné línie zodpovednosti, rozhodovacie právomoci a eskalačné postupy s cieľom zabezpečiť, aby bola informačná bezpečnosť začlenená na všetkých úrovniach organizácie a zosúladená so strategickými cieľmi organizácie.

1.3 Táto politika zavádza požiadavky ISO/IEC 27001:2022, kapitoly 5.3 a kontroly A.5.2, a zabezpečuje, aby zodpovednosti za činnosti súvisiace s bezpečnosťou boli jednoznačne pridelené, zdokumentované, oznámené a pravidelne preskúmavané.

1.4 Táto politika zároveň vytvára základ pre integrovanú správu a riadenie s ďalšími oblasťami, ako sú riadenie rizík, compliance, IT prevádzka a právne záležitosti.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky osoby a subjekty zapojené do správy a riadenia, prevádzky a dohľadu nad informačnou bezpečnosťou v rozsahu ISMS. Zahŕňa najmä:

2.1.1 výkonné vedenie, vrcholový manažment a členov predstavenstva,

2.1.2 manažérov ISMS, riaditeľa informačnej bezpečnosti (CISO) a vlastníkov kontrol,

2.1.3 vlastníkov procesov a aktív,

2.1.4 zmluvných dodávateľov a poskytovateľov služieb tretích strán s delegovanými bezpečnostnými zodpovednosťami.

2.2 Vzťahuje sa na interné aj externe zabezpečované funkcie (napr. outsourcované SOC, správcov cloudových platforiem), ak sú roly správy a riadenia formálne pridelené alebo zmluvne definované.

2.3 Politika sa vzťahuje aj na organizačné jednotky, oddelenia a projektové tímy, ktoré riadia alebo ovplyvňujú bezpečnostne relevantné aktíva, systémy alebo služby.

3. Ciele

3.1 Zabezpečiť, aby boli roly a zodpovednosti v oblasti informačnej bezpečnosti formálne definované, pridelené, komunikované a zdokumentované.

3.2 Udržiavať model správy a riadenia, ktorý zabezpečuje oddelenie povinností, odstraňuje konflikty záujmov a umožňuje eskaláciu nevyriešených bezpečnostných otázok.

3.3 Zabezpečiť, aby zodpovednosť a právomoci pri bezpečnostných rozhodnutiach boli rozdelené v súlade s dopadom na organizáciu a jej organizačnou štruktúrou.

3.4 Vytvoriť rámec na riadenie delegovania, zmien rolí a preskúmavania pridelených zodpovedností.

3.5 Poskytnúť zainteresovaným stranám vrátane regulátorov, audítorov a klientov uistenie, že informačná bezpečnosť je riadená účinne a v súlade s uplatniteľnými normami.

4. Roly a zodpovednosti

4.1 Výkonné vedenie (vrcholový manažment)

4.1.1 Zabezpečuje strategický dohľad, prideľuje zdroje a zabezpečuje zosúladenie medzi cieľmi ISMS a cieľmi organizácie.

4.1.2 Schvaľuje kľúčovú dokumentáciu ISMS vrátane Politiky informačnej bezpečnosti, plánov ošetrenia rizík a rozhodnutí o nápravných opatreniach z auditov.

4.1.3 Zúčastňuje sa na preskúmaniach ISMS manažmentom a eskaluje rozhodnutia vyžadujúce schválenie na úrovni predstavenstva.

4.1.4 Podporuje kultúru bezpečnosti a presadzuje dodržiavanie princípov správy a riadenia bezpečnosti v celej organizácii.

4.2 Riadiaci výbor pre informačnú bezpečnosť (ISSC)

4.2.1 Pôsobí ako medziodborový orgán správy a riadenia pre dohľad nad ISMS.

4.2.2 Preskúmava stav rizík, výkonnosť kontrol, auditné zistenia a strategické bezpečnostné iniciatívy.

4.2.3 Zabezpečuje koordináciu medzi oddeleniami (napr. IT, právne záležitosti a compliance, ľudské zdroje, riadenie rizík, prevádzka).

4.2.4 Schvaľuje prahové hodnoty eskalácie, rozpočtové alokácie a zmeny politík vyžadujúce vstup výkonného vedenia.

[... 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 Harmonogram preskúmania

9.1.1 Táto politika sa musí preskúmať najmenej raz ročne alebo pri výskyte:

9.1.1.1 zmien organizačnej štruktúry alebo výkonného tímu,

9.1.1.2 rozšírenia alebo predefinovania rozsahu ISMS,

9.1.1.3 regulačných zmien ovplyvňujúcich pridelenie rolí alebo dohľad,

9.1.1.4 významných auditných zistení alebo incidentov zahŕňajúcich zlyhanie správy a riadenia.

9.2 Proces preskúmania a schválenia

9.2.1 Manažér ISMS musí iniciovať a viesť proces preskúmania vrátane zberu vstupov od zainteresovaných strán a spätnej väzby z auditov.

9.2.2 Navrhované aktualizácie musia byť preskúmané ISSC a formálne schválené výkonným vedením.

9.2.3 Každá verzia musí byť evidovaná v Registri dokumentov ISMS a musí obsahovať tieto metadáta:

9.2.3.1 identifikátor a názov politiky,

9.2.3.2 číslo verzie a súhrn zmien,

9.2.3.3 dátum účinnosti a dátum nasledujúceho preskúmania,

9.2.3.4 vlastníka politiky a schvaľovateľa,

9.2.3.5 úroveň klasifikácie dokumentu,

9.2.3.6 históriu uchovávania a archivácie.

10. Súvisiace politiky a väzby

10.1 Táto politika sa má vykladať v spojení s týmito politikami:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje celkový bezpečnostný program a vymedzuje zodpovednosti vedenia za schválenie politiky a strategický dohľad.

10.1.2 P5 – Politika riadenia zmien: zabezpečuje, aby zmeny štruktúr správy a riadenia, rolí alebo zodpovedností podliehali zdokumentovanému schváleniu a preskúmaniu rizík.

10.1.3 P6 – Politika riadenia rizík: identifikuje a ošetruje riziká správy a riadenia vyplývajúce z konfliktov rolí, nepridelených povinností alebo nedostatočnej eskalácie.

10.1.4 P7 – Politika nástupu a ukončenia pracovného pomeru: zabezpečuje procesy prideľovania kontrol a odoberania prístupových práv počas zmien v životnom cykle personálu.

10.1.5 P33 – Politika monitorovania auditu a compliance: podporuje nezávislé preskúmanie účinnosti správy a riadenia a vyžaduje nápravné opatrenia pri nesúlade.

10.2 Tieto politiky spoločne podporujú jednotný a uplatniteľný rámec správy a riadenia ISMS.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými normami a rámcami pre správu a riadenie informačnej bezpečnosti a zodpovednosti rolí. Zabezpečuje sledovateľnosť voči regulačným a certifikačným požiadavkám a podporuje obhájiteľnú štruktúru ISMS.

11.2 ISO/IEC 27001

11.2.1 Kapitola 5.3 – Organizačné roly, zodpovednosti a právomoci: Táto politika plní požiadavku, aby roly relevantné pre informačnú bezpečnosť boli jednoznačne pridelené, komunikované a zdokumentované.

11.2.2 Kapitola 9.3 – Preskúmanie manažmentom: Táto politika vyžaduje dohľad výkonného vedenia nad rolami ISMS a správou a riadením prostredníctvom štvrťročných a ročných preskúmaní.

11.2.3 Príloha A, kontrola 5.2 – Roly a zodpovednosti v oblasti informačnej bezpečnosti: Definuje roly na technickej, prevádzkovej a strategickej úrovni s cieľom zabezpečiť oddelenie povinností, vlastníctvo rizík a sledovateľnú zodpovednosť.

11.3 ISO/IEC 27002:2022 – Kontrola 5

11.3.1 Poskytuje usmernenie k implementácii prideľovania zodpovedností za informačnú bezpečnosť v rámci organizácie. Táto politika preberá toto usmernenie tým, že definuje typy rolí, pravidlá delegovania, eskalačné postupy a mechanizmy preskúmania.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 až PL-4: Vyžadujú formálnu plánovaciu dokumentáciu vrátane politík, ktoré definujú správu a riadenie a prideľujú bezpečnostné zodpovednosti.

11.4.2 PM-1 (plán programu informačnej bezpečnosti) a PM-2 (vedúci pracovník informačnej bezpečnosti): V tejto politike sú zohľadnené prostredníctvom pridelenia roly CISO/manažéra ISMS a formálnych rolí správy a riadenia.

11.4.3 PM-5 až PM-13: Táto politika spĺňa požiadavky na dokumentáciu rolí, podnikové roly v oblasti rizík, dohľad nad riadením konfigurácie a integráciu s kľúčovými funkciami organizácie.

11.5 Nariadenie EÚ GDPR (2016/679)

11.5.1 Článok 5(1)(f): Vyžaduje, aby osobné údaje boli chránené pred neoprávneným alebo nezákonným spracúvaním. Táto politika zabezpečuje, že osoby zodpovedné za ochranu údajov sú jasne určené a monitorované.

11.5.2 Článok 24: Vyžaduje primerané organizačné opatrenia vrátane štruktúr správy a riadenia.

11.5.3 Článok 37: Vyžaduje určenie zodpovednej osoby pre ochranu osobných údajov (DPO), čo musí byť zohľadnené v rámci správy a riadenia organizácie a v registri zodpovedností.

11.6 Smernica EÚ NIS2 (2022/2555)

11.6.1 Článok 21(2)(a): Ukladá subjektom povinnosť zaviesť politiky pre analýzu rizík a bezpečnosť informačných systémov vrátane zodpovedností špecifických pre jednotlivé roly. Táto politika takéto roly a ich mechanizmy správy a riadenia definuje.

11.7 Nariadenie EÚ DORA (2022/2554)

11.7.1 Článok 5 – Rámec správy a riadenia a vnútornej kontroly: Vyžaduje formálne pridelenie zodpovedností za riadenie IKT rizík, rozhodovacích rolí a reportovacích kanálov. Táto politika vytvára základ pre správu a riadenie rolí súvisiacich s bezpečnosťou v prostrediach IKT.

11.8 COBIT 2019

11.8.1 EDM01 – Zavedenie rámca správy a riadenia: Táto politika zabezpečuje, aby ISMS mal jednoznačne definovanú štruktúru správy a riadenia zosúladenú s potrebami organizácie.

11.8.2 EDM02 – Zabezpečenie prínosov: Zosúlaďuje bezpečnostné činnosti podľa rolí so strategickými a prevádzkovými cieľmi a zabezpečuje zodpovednosť a merateľné výstupy.

11.8.3 APO01 – Riadený rámec riadenia I&T a APO12 – Riadené riziko: Táto politika podporuje štruktúrované riadenie rolí informačnej bezpečnosti v širšom rámci IT správy a riadenia a riadenia rizík.

11.8.4 MEA01 – Monitorovanie, hodnotenie a posudzovanie výkonnosti: Zavádza mechanizmy preskúmania na overenie, že roly správy a riadenia sú účinné, aktuálne a uplatňované.