					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P02					Název dokumentu: **Politika rolí a odpovědností v oblasti správy a řízení**						
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	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 5.3; Příloha A, opatření 5	
ISO/IEC 27002:2022	Opatření 5	
NIST SP 800-53 Rev.5	PL-1 až PL-4, PM-1 až PM-13	
GDPR	Články 5(1)(f), 24, 37	
směrnice NIS2	Článek 21(2)(a)	
nařízení DORA	Článek 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Účel

1.1 Tato politika stanoví model správy a řízení, organizační role a odpovědnosti nezbytné pro provoz účinného Systému řízení bezpečnosti informací (ISMS).

1.2 Zavádí jasné linie odpovědnosti, rozhodovacích pravomocí a eskalačních postupů tak, aby byla bezpečnost informací začleněna do všech úrovní organizace a sladěna se strategickými obchodními cíli.

1.3 Tato politika implementuje požadavky ISO/IEC 27001:2022, kapitoly 5.3 a opatření A.5.2, a zajišťuje, že odpovědnosti za činnosti související s bezpečností jsou jednoznačně přiřazeny, zdokumentovány, komunikovány a pravidelně přezkoumávány.

1.4 Tato politika rovněž vytváří základ pro integrovanou správu a řízení s dalšími oblastmi, jako jsou řízení rizik, compliance, IT provoz a právní agenda.

2. Rozsah

2.1 Tato politika se vztahuje na všechny osoby a subjekty zapojené do správy, provozu a dohledu nad bezpečností informací v rámci rozsahu ISMS. To zahrnuje zejména:

2.1.1 výkonné vedení, vrcholové vedení a členy správních orgánů

2.1.2 manažery ISMS, ředitele informační bezpečnosti (CISO) a vlastníky kontrol

2.1.3 vlastníky procesů a aktiv

2.1.4 dodavatele a poskytovatele služeb třetích stran s delegovanými odpovědnostmi v oblasti bezpečnosti

2.2 Vztahuje se na interně zajišťované i externě poskytované funkce (např. outsourcing SOC nebo správce cloudové platformy), pokud jsou role v rámci správy a řízení formálně přiřazeny nebo smluvně vymezeny.

2.3 Tato politika se rovněž vztahuje na organizační jednotky, oddělení a projektové týmy, které spravují nebo ovlivňují aktiva, systémy nebo služby relevantní z hlediska bezpečnosti.

3. Cíle

3.1 Zajistit, aby role a odpovědnosti v oblasti bezpečnosti informací byly formálně definovány, přiřazeny, komunikovány a zdokumentovány.

3.2 Udržovat model správy a řízení, který prosazuje oddělení povinností, eliminuje střety zájmů a umožňuje eskalaci nevyřešených bezpečnostních otázek.

3.3 Zajistit, aby odpovědnost a pravomoc při bezpečnostních rozhodnutích byly rozděleny v souladu s dopadem na obchodní činnost a organizační strukturou.

3.4 Zavést rámec pro řízení delegování, změn rolí a přezkumu přiřazených odpovědností.

3.5 Poskytnout zainteresovaným stranám, včetně regulačních orgánů, auditorů a klientů, jistotu, že bezpečnost informací je řízena účinně a v souladu s příslušnými normami.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Zajišťuje strategický dohled, přiděluje zdroje a zajišťuje soulad mezi cíli ISMS a obchodními cíli.

4.1.2 Schvaluje klíčovou dokumentaci ISMS, včetně Politiky informační bezpečnosti, plánů ošetření rizik a rozhodnutí o nápravných opatřeních z auditů.

4.1.3 Účastní se přezkoumání ISMS vedením a eskaluje rozhodnutí vyžadující schválení na úrovni správního orgánu.

4.1.4 Podporuje kulturu bezpečnosti a prosazuje dodržování principů správy a řízení bezpečnosti v celé organizaci.

4.2 Řídicí výbor pro bezpečnost informací (ISSC)

4.2.1 Působí jako mezioborový řídicí orgán pro dohled nad ISMS.

4.2.2 Přezkoumává rizikový profil, účinnost kontrol, zjištění z auditů a strategické bezpečnostní iniciativy.

4.2.3 Zajišťuje koordinaci mezi útvary (např. IT, právní a compliance, HR, řízení rizik, compliance, provoz).

4.2.4 Schvaluje eskalační prahy, přidělení rozpočtu a změny politik vyžadující vstup výkonného vedení.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Harmonogram přezkumu

9.1.1 Tato politika musí být přezkoumána nejméně jednou ročně nebo při vzniku některé z následujících skutečností:

9.1.1.1 změny organizační struktury nebo složení výkonného vedení

9.1.1.2 rozšíření nebo nového vymezení rozsahu ISMS

9.1.1.3 změny právních předpisů ovlivňující přiřazení rolí nebo dohled

9.1.1.4 významná zjištění z auditu nebo incidenty zahrnující selhání správy a řízení

9.2 Proces přezkumu a schválení

9.2.1 Manažer ISMS zahajuje a vede proces přezkumu, včetně shromáždění podnětů od zainteresovaných stran a zpětné vazby z auditů.

9.2.2 Navrhované aktualizace musí být přezkoumány ISSC a formálně schváleny vrcholovým vedením.

9.2.3 Každá verze musí být sledována v registru dokumentů ISMS a musí obsahovat následující metadata:

9.2.3.1 identifikátor politiky a název

9.2.3.2 číslo verze a shrnutí změn

9.2.3.3 datum účinnosti a datum příštího přezkumu

9.2.3.4 vlastník politiky a schvalovatel

9.2.3.5 úroveň klasifikace dokumentu

9.2.3.6 historie uchovávání a archivace

10. Související politiky a vazby

10.1 Tato politika musí být vykládána ve spojení s následujícími politikami:

10.1.1 P1 – Politika informační bezpečnosti: Stanoví celkový bezpečnostní program a vymezuje odpovědnosti vedení za schválení politiky a strategický dohled.

10.1.2 P5 – Politika řízení změn: Zajišťuje, aby změny struktur správy a řízení, rolí nebo odpovědností podléhaly dokumentovanému schválení a přezkumu rizik.

10.1.3 P6 – Politika řízení rizik: Identifikuje a ošetřuje rizika správy a řízení vznikající z konfliktů rolí, nepřiřazených povinností nebo chybějící eskalace.

10.1.4 P7 – Politika nástupu a ukončení: Prosazuje procesy přiřazení kontrol a odebrání při změnách v životním cyklu personálu.

10.1.5 P33 – Politika monitorování auditů a souladu: Podporuje nezávislý přezkum účinnosti správy a řízení a prosazuje nápravná opatření při nesouladu.

10.2 Tyto politiky společně podporují jednotný a vymahatelný rámec správy a řízení ISMS.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s celosvětově uznávanými normami a rámci pro správu a řízení bezpečnosti informací a odpovědnost za role. Zajišťuje dohledatelnost vůči regulatorním a certifikačním požadavkům a podporuje obhajitelnou strukturu ISMS.

11.2 ISO/IEC 27001

11.2.1 Kapitola 5.3 – Organizační role, odpovědnosti a pravomoci: Tato politika naplňuje požadavek, aby role relevantní pro bezpečnost informací byly jednoznačně přiřazeny, komunikovány a dokumentovány.

11.2.2 Kapitola 9.3 – Přezkoumání vedením: Tato politika prosazuje dohled výkonného vedení nad rolemi ISMS a správou a řízením prostřednictvím čtvrtletních a ročních přezkumů.

11.2.3 Příloha A, opatření 5.2 – Role a odpovědnosti v oblasti bezpečnosti informací: Definuje role na technické, provozní a strategické úrovni tak, aby bylo zajištěno oddělení povinností, vlastnictví rizik a dohledatelná odpovědnost.

11.3 ISO/IEC 27002:2022 – Opatření 5

11.3.1 Poskytuje návod k implementaci přiřazování odpovědností v oblasti bezpečnosti informací v celé organizaci. Tato politika tento návod přebírá definováním typů rolí, pravidel delegování, eskalačních postupů a mechanismů přezkumu.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 až PL-4: Prosazují potřebu formální plánovací dokumentace, včetně politik, které vymezují správu a řízení a přiřazují bezpečnostní odpovědnosti.

11.4.2 PM-1 (plán programu bezpečnosti informací) a PM-2 (vedoucí pracovník pro bezpečnost informací): V této politice jsou promítnuty prostřednictvím přiřazení role CISO/manažera ISMS a formálních rolí správy a řízení.

11.4.3 PM-5 až PM-13: Tato politika naplňuje požadavky na dokumentaci rolí, role řízení rizik v celé organizaci, dohled nad řízením konfigurace a integraci s klíčovými funkcemi organizace a podnikání.

11.5 GDPR (2016/679)

11.5.1 Článek 5(1)(f): Vyžaduje, aby osobní údaje byly chráněny před neoprávněným nebo protiprávním zpracováním. Tato politika zajišťuje, že osoby odpovědné za ochranu osobních údajů jsou jednoznačně určeny a podléhají dohledu.

11.5.2 Článek 24: Vyžaduje přijetí vhodných organizačních opatření, včetně struktur správy a řízení.

11.5.3 Článek 37: Vyžaduje jmenování pověřence pro ochranu osobních údajů (DPO), které musí být promítnuto do rámce správy a řízení organizace a registru odpovědností.

11.6 směrnice NIS2 (2022/2555)

11.6.1 Článek 21(2)(a): Ukládá subjektům zavést politiky pro analýzu rizik a bezpečnost informačních systémů, včetně odpovědností specifických pro role. Tato politika takové role a jejich mechanismy správy a řízení definuje.

11.7 nařízení DORA (2022/2554)

11.7.1 Článek 5 – rámec správy a řízení a vnitřní kontroly: Vyžaduje formální přiřazení odpovědností za řízení ICT rizik, rozhodovacích rolí a reportingových kanálů. Tato politika poskytuje základ pro správu a řízení rolí souvisejících s bezpečností v prostředích ICT.

11.8 COBIT 2019

11.8.1 EDM01 – Nastavení rámce správy a řízení: Tato politika zajišťuje, že ISMS má jasně definovanou strukturu správy a řízení sladěnou s potřebami podniku.

11.8.2 EDM02 – Zajištění přínosů: Slaďuje bezpečnostní činnosti založené na rolích se strategickými a provozními cíli a zajišťuje odpovědnost a měřitelné výstupy.

11.8.3 APO01 – Řízený rámec řízení I&T a APO12 – Řízené riziko: Tato politika podporuje strukturované řízení rolí v oblasti bezpečnosti informací v rámci širšího rámce správy IT a řízení rizik.

11.8.4 MEA01 – Monitorování, vyhodnocování a posuzování výkonnosti: Zavádí mechanismy přezkumu pro ověřování, že role v oblasti správy a řízení jsou účinné, aktuální a uplatňované.