					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P02S					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	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Kapitola 5	
ISO/IEC 27002:2022	Opatření 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
GDPR	Články 5(2), 32	

1. Účel

1.1 Tato politika stanoví způsob přiřazování, delegování a řízení odpovědností v oblasti správy a řízení bezpečnosti informací v organizaci tak, aby byl zajištěn plný soulad s normou ISO/IEC 27001:2022 a dalšími regulatorními povinnostmi.

1.2 Zajišťuje odpovědnost na všech úrovních a podporuje provozní efektivitu tím, že jednoznačně vymezuje, kdo odpovídá za jednotlivé funkce související s bezpečností.

1.3 Tato politika zvyšuje připravenost na audit a posiluje důvěru zákazníků tím, že dokládá formální správu a řízení bezpečnosti i v organizacích s omezenými technickými kapacitami nebo s outsourcovanými IT službami.

2. Rozsah

2.1 Tato politika se vztahuje na všechny osoby, které nakládají se systémy nebo daty organizace, včetně:

2.1.1 vlastníků procesů a vedoucích pracovníků

2.1.2 zaměstnanců a smluvních pracovníků

2.1.3 externích poskytovatelů IT služeb nebo konzultantů

2.2 Vztahuje se na všechny systémy, prostředí a služby používané ke zpracování, přenosu nebo ukládání obchodních informací nebo informací zákazníků, včetně:

2.2.1 kancelářské IT infrastruktury a zařízení pro práci na dálku

2.2.2 cloudových platforem a e-mailových služeb

2.2.3 fyzických záznamů a sdílených úložišť

2.3 Rozsah zahrnuje interní i outsourcované činnosti související se správou a řízením bezpečnosti informací.

3. Cíle

3.1 Stanovit jasnou odpovědnost za všechny povinnosti související s bezpečností, včetně řízení politik, řízení přístupu, zvládání incidentů a monitorování.

3.2 Umožnit účinné oddělení povinností za účelem snížení střetu zájmů nebo rizika podvodu.

3.3 Zajistit, aby bezpečnostní úkoly a role byly jednoznačně zdokumentovány a pravidelně přezkoumávány.

3.4 Umožnit informované rozhodování, eskalaci a dohled nad IT a bezpečnostními riziky.

3.5 Podpořit certifikaci podle ISO/IEC 27001:2022 a posílit důvěru zákazníků, partnerů a auditorů.

4. Role a odpovědnosti

4.1 Vedoucí organizace / vlastník společnosti

4.1.1 Nese plnou odpovědnost za zavedení této politiky a dohled nad jejím uplatňováním.

4.1.2 Schvaluje všechny bezpečnostní role, odpovědnosti a rozhodnutí o delegování.

4.1.3 Sleduje soulad a přijímá konečná rozhodnutí o výjimkách z politiky a eskalacích.

4.2 Určený koordinátor bezpečnosti (je-li jmenován)

4.2.1 Touto osobou může být zaměstnanec nebo důvěryhodný konzultant.

4.2.2 V prostředí mikropodniků může tuto roli vykonávat vedoucí organizace nebo externí poskytovatel.

4.2.3 Podporuje každodenní uplatňování řízení přístupu, reakce na incidenty a základních technických bezpečnostních činností.

4.2.4 O všech bezpečnostních otázkách nebo rizicích informuje přímo vedoucího organizace.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Každoroční přezkum

9.1.1 Tato politika musí být vedoucím organizace přezkoumána každých 12 měsíců, aby bylo zajištěno, že i nadále odpovídá právním povinnostem, provozním potřebám a požadavkům certifikace ISO/IEC 27001.

9.2 Mimořádné přezkumy

9.2.1 Přezkum musí proběhnout také tehdy, pokud:

9.2.1.1 dojde k významným organizačním změnám

9.2.1.2 je zařazen nový poskytovatel

9.2.1.3 dojde k závažnému bezpečnostnímu incidentu

9.2.1.4 jsou aktualizovány předpisy, jako je GDPR, směrnice NIS2 nebo nařízení DORA

9.3 Správa verzí a dokumentace

9.3.1 Každý přezkum musí zahrnovat:

9.3.1.1 datum přezkumu

9.3.1.2 shrnutí všech změn

9.3.1.3 podpis nebo zdokumentované schválení vedoucím organizace

9.3.1.4 archivované předchozí verze pro potřeby auditu

9.4 Komunikace změn

9.4.1 Všechny aktualizace politiky musí být bezodkladně sděleny personálu a poskytovatelům prostřednictvím e-mailu, interních portálů nebo formálních oznámení.

10. Související politiky a vazby

10.1 Tato politika musí být pro zajištění plné účinnosti implementována společně s následujícími SME politikami:

10.1.1 P4S – Politika řízení přístupu: Stanoví, jak je přístup udělován, řízen a odebírán, v přímé vazbě na přiřazené role a dohled.

10.1.2 P8S – Politika bezpečnostního povědomí a školení: Posiluje odpovědnosti a očekávání specifická pro jednotlivé role.

10.1.3 P17S – Politika ochrany osobních údajů a soukromí: Vymezuje právní povinnosti podle GDPR, které jsou přiřazeny rolím definovaným v této politice správy a řízení.

10.1.4 P30S – Politika reakce na incidenty: Vyžaduje jasně definované odpovědnosti za hlášení, eskalaci a řešení incidentů.

10.2 Tyto politiky společně umožňují konzistentní uplatňování, interní odpovědnost a externí soulad.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 5.3 – Organizační role, odpovědnosti a pravomoci: Vyžaduje, aby role byly jednoznačně přiřazeny a podporovány vrcholovým vedením.

11.2 ISO/IEC 27002

11.2.1 Opatření 5.2–5.4: Vyžadují jednoznačnou dokumentaci rolí v oblasti bezpečnosti informací, oddělení povinností a manažerský dohled.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Stanoví zastřešující program bezpečnosti informací s definovanými odpovědnostmi.

11.3.2 PL-1 až PL-4: Vyžadují plánovací opatření, včetně tvorby politik a dokumentovaného přiřazení rolí.

11.3.3 CA-1: Vyžaduje definované role pro hodnocení a autorizaci.

11.3.4 AC-1: Váže řízení přístupu založené na rolích (RBAC) na přiřazené odpovědnosti v oblasti správy a řízení.

11.4 GDPR

11.4.1 Článek 5(2) – Odpovědnost: Vyžaduje, aby organizace byly schopny doložit soulad prostřednictvím rolí a odpovědností.

11.4.2 Článek 32 – Zabezpečení zpracování: Zdůrazňuje jednoznačné přiřazení povinností k ochraně osobních údajů.

11.5 Směrnice EU NIS2

11.5.1 Článek 21(2)(a): Vyžaduje struktury správy a řízení zahrnující formalizované role pro řízení kybernetických rizik a incidentů.

11.6 Nařízení EU DORA

11.6.1 Články 9 a 10: Vyžadují, aby finanční subjekty jednoznačně přiřadily odpovědnosti související s ICT a bezpečností a vykonávaly nad nimi dohled.

11.7 COBIT 2019

11.7.1 EDM03 – Zajištění optimalizace rizik: Vyžaduje dobře definované role a eskalační cesty pro řízení bezpečnostních rizik.

11.7.2 APO13 – Řízení bezpečnosti: Přiřazuje strategické a provozní bezpečnostní povinnosti jednotlivcům a rolím.

11.7.3 DSS05 – Řízení bezpečnostních služeb: Vyžaduje strukturu a dohledatelnost odpovědností za externí i interní bezpečnostní služby.