					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P02S					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	
ISO/IEC 27002:2022	Opatrenia: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev. 5	PM-1, PL-1, PL-4, CA-1, AC-1	
Nariadenie EÚ GDPR	Články 5 ods. 2, 32	

1. Účel

1.1 Táto politika stanovuje spôsob prideľovania, delegovania a riadenia zodpovedností v oblasti správy a riadenia informačnej bezpečnosti v organizácii s cieľom zabezpečiť úplný súlad s normou ISO/IEC 27001:2022 a ďalšími regulačnými povinnosťami.

1.2 Zabezpečuje preukázateľnú zodpovednosť na každej úrovni a podporuje prevádzkovú efektívnosť tým, že jednoznačne určuje, kto zodpovedá za jednotlivé funkcie súvisiace s bezpečnosťou.

1.3 Táto politika posilňuje pripravenosť na audit a buduje dôveru zákazníkov tým, že preukazuje formálnu správu a riadenie bezpečnosti aj v organizáciách s obmedzenými internými technickými kapacitami alebo s outsourcovanými IT službami.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky osoby, ktoré pracujú so systémami alebo údajmi organizácie, vrátane:

2.1.1 vlastníkov procesov a generálnych manažérov

2.1.2 zamestnancov a zmluvných pracovníkov

2.1.3 externých poskytovateľov IT služieb alebo konzultantov

2.2 Zahŕňa všetky systémy, prostredia a služby používané na spracúvanie, prenos alebo uchovávanie informácií organizácie alebo informácií zákazníkov, vrátane:

2.2.1 kancelárskej IT infraštruktúry a zariadení používaných na prácu na diaľku

2.2.2 cloudových platforiem a služieb elektronickej pošty

2.2.3 fyzických záznamov a zdieľaných úložísk

2.3 Rozsah zahŕňa interné aj outsourcované činnosti súvisiace so správou a riadením informačnej bezpečnosti.

3. Ciele

3.1 Zaviesť jednoznačnú a preukázateľnú zodpovednosť za všetky povinnosti súvisiace s bezpečnosťou vrátane riadenia politík, riadenia prístupov, riešenia incidentov a monitorovania.

3.2 Umožniť účinné oddelenie povinností s cieľom znížiť konflikty záujmov alebo riziko podvodu.

3.3 Zabezpečiť, aby bezpečnostné úlohy a roly boli jednoznačne zdokumentované a pravidelne preskúmavané.

3.4 Umožniť informované rozhodovanie, eskaláciu a dohľad nad IT a bezpečnostnými rizikami.

3.5 Podporiť certifikáciu podľa ISO/IEC 27001:2022 a posilniť dôveru zákazníkov, partnerov a audítorov.

4. Roly a zodpovednosti

4.1 Generálny manažér / vlastník organizácie

4.1.1 Nesie celkovú zodpovednosť za implementáciu tejto politiky a dohľad nad jej uplatňovaním.

4.1.2 Schvaľuje všetky bezpečnostné roly, zodpovednosti a rozhodnutia o delegovaní.

4.1.3 Monitoruje súlad a prijíma konečné rozhodnutia o výnimkách z politík a eskaláciách.

4.2 Určený koordinátor bezpečnosti (ak je ustanovený)

4.2.1 Túto rolu môže vykonávať zamestnanec alebo dôveryhodný konzultant.

4.2.2 V prostredí mikropodnikov môže túto rolu vykonávať generálny manažér alebo externý poskytovateľ.

4.2.3 Podporuje každodenné uplatňovanie riadenia prístupov, reakcie na incidenty a základných technických bezpečnostných úloh.

4.2.4 O všetkých bezpečnostných otázkach alebo rizikách podáva správu priamo generálnemu manažérovi.

[... 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 Ročné preskúmanie

9.1.1 Túto politiku musí generálny manažér preskúmať každých 12 mesiacov, aby sa zabezpečilo, že naďalej odráža zákonné povinnosti, prevádzkové potreby a požiadavky certifikácie ISO/IEC 27001.

9.2 Mimoriadne preskúmania

9.2.1 Preskúmanie sa musí vykonať aj vtedy, keď:

9.2.1.1 dôjde k významným organizačným zmenám

9.2.1.2 je zavedený nový poskytovateľ

9.2.1.3 dôjde k závažnému bezpečnostnému incidentu

9.2.1.4 sa aktualizujú predpisy, ako sú GDPR, smernica EÚ NIS2 alebo nariadenie EÚ DORA

9.3 Riadenie verzií a dokumentácia

9.3.1 Každé preskúmanie musí zahŕňať:

9.3.1.1 dátum preskúmania

9.3.1.2 súhrn všetkých zmien

9.3.1.3 podpis alebo zdokumentované schválenie generálnym manažérom

9.3.1.4 archivované predchádzajúce verzie na účely auditu

9.4 Oznámenie zmien

9.4.1 Všetky aktualizácie politiky musia byť bezodkladne oznámené zamestnancom a poskytovateľom e-mailom, prostredníctvom interných portálov alebo formálnych oznámení.

10. Súvisiace politiky a prepojenia

10.1 Táto politika sa má uplatňovať spolu s nasledujúcimi SME politikami, aby sa zabezpečila jej plná účinnosť:

10.1.1 P4S – Politika riadenia prístupu: Definuje, ako sa prístup udeľuje, riadi a odoberá, v priamej väzbe na pridelené roly a dohľad.

10.1.2 P8S – Politika povedomia a školení v oblasti informačnej bezpečnosti: Posilňuje zodpovednosti a očakávania špecifické pre jednotlivé roly.

10.1.3 P17S – Politika ochrany údajov a súkromia: Uvádza zákonné povinnosti podľa GDPR, ktoré sú pridelené rolám definovaným v tejto politike správy a riadenia.

10.1.4 P30S – Politika reakcie na incidenty: Vyžaduje definované zodpovednosti za nahlasovanie, eskaláciu a riešenie incidentov.

10.2 Tieto politiky spoločne umožňujú konzistentné uplatňovanie, internú zodpovednosť a externý súlad.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 5.3 – Organizačné roly, zodpovednosti a právomoci: Vyžaduje, aby boli roly jednoznačne pridelené a podporované vrcholovým manažmentom.

11.2 ISO/IEC 27002

11.2.1 Opatrenia 5.2–5.4: Vyžadujú jednoznačnú dokumentáciu rolí v oblasti informačnej bezpečnosti, oddelenie povinností a manažérsky dohľad.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PM-1: Zavádza zastrešujúci program informačnej bezpečnosti s definovanými zodpovednosťami.

11.3.2 PL-1 až PL-4: Vyžadujú plánovacie opatrenia vrátane tvorby politík a zdokumentovaného priradenia rolí.

11.3.3 CA-1: Vyžaduje definované roly pre posudzovanie a autorizáciu.

11.3.4 AC-1: Prepája riadenie prístupu na základe rolí (RBAC) s pridelenými zodpovednosťami správy a riadenia.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 5 ods. 2 – Zodpovednosť: Vyžaduje, aby organizácie preukázali súlad prostredníctvom rolí a zodpovedností.

11.4.2 Článok 32 – Bezpečnosť spracúvania: Zdôrazňuje jednoznačné pridelenie povinností na ochranu osobných údajov.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21 ods. 2 písm. a): Vyžaduje štruktúry správy a riadenia, ktoré zahŕňajú formalizované roly na riadenie kybernetických rizík a incidentov.

11.6 Nariadenie EÚ DORA

11.6.1 Články 9 a 10: Vyžadujú, aby finančné subjekty jednoznačne pridelili a vykonávali dohľad nad zodpovednosťami súvisiacimi s IKT a bezpečnosťou.

11.7 COBIT 2019

11.7.1 EDM03 – Zabezpečenie optimalizácie rizík: Vyžaduje dobre definované roly a eskalačné postupy na riadenie bezpečnostných rizík.

11.7.2 APO13 – Riadenie bezpečnosti: Prideľuje strategické a prevádzkové bezpečnostné povinnosti jednotlivcom a rolám.

11.7.3 DSS05 – Riadenie bezpečnostných služieb: Vyžaduje štruktúru a sledovateľnosť zodpovedností za externé a interné bezpečnostné služby.