					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P01S					Názov dokumentu: **Politika informačnej bezpečnosti**							
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	Kapitoly 5.1, 5.2, 5.3, 6.1, 8	Stanovuje záväzok vedenia, požiadavky na politiku, priradenie rolí, posúdenie rizík a prevádzkové bezpečnostné opatrenia
ISO/IEC 27002:2022	Opatrenia 5.1–5.5	Stanovuje vypracovanie zdokumentovaných politík informačnej bezpečnosti, priradenie rolí, oddelenie povinností a zodpovednosti vedenia
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Stanovuje požiadavky na plán programu informačnej bezpečnosti, politiku bezpečnostného plánovania, posudzovanie a autorizáciu a riadenie prístupu
Nariadenie (EÚ) 2016/679 (GDPR)	Článok 5 ods. 2, článok 32	Upravuje zásadu zodpovednosti a opatrenia na bezpečnosť spracúvania, najmä vo vzťahu k zdokumentovaným roliam
Smernica (EÚ) 2022/2555 (NIS2)	Článok 21 ods. 2 písm. a)	Vyžaduje opatrenia na riadenie rizík, roly a zodpovednosti v oblasti kybernetických rizík
Nariadenie (EÚ) 2022/2554 (DORA)	Článok 9, článok 10	Vyžaduje priradenie rolí pre riadenie IKT rizík a zabezpečenie kontinuity činností
COBIT 2019	EDM03, APO13, DSS05	Podporuje optimalizáciu rizík, riadenie bezpečnosti a riadenie bezpečnostných služieb prostredníctvom jasného priradenia rolí

1. Účel

1.1 Táto politika vyjadruje záväzok organizácie chrániť informácie zákazníkov a interné informácie prostredníctvom jasného vymedzenia zodpovedností a primeraných bezpečnostných opatrení, vhodných aj pre organizácie bez vyhradeného IT tímu.

1.2 Zabezpečuje, aby všetci zamestnanci, zmluvní dodávatelia a poskytovatelia služieb dodržiavali záväzné pravidlá, a tým umožňuje plný súlad s požiadavkami certifikácie podľa ISO/IEC 27001.

1.3 Táto politika umožňuje organizácii budovať dôveru zákazníkov tým, že jednoznačne preukazuje, ako chránime ich informácie prostredníctvom definovaných zodpovedností, štruktúrovaných procesov a jasne priradenej zodpovednosti.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky osoby, ktoré pristupujú k údajom a systémom organizácie alebo ich spravujú, vrátane:

2.1.1 vlastníkov spoločnosti a generálnych manažérov

2.1.2 zamestnancov, zmluvných pracovníkov a stážistov

2.1.3 externých poskytovateľov IT služieb alebo konzultantov

2.2 Zahŕňa všetky typy informácií, systémov a služieb vrátane:

2.2.1 obchodných záznamov, zákazníckych údajov, hesiel a e-mailov

2.2.2 IT hardvéru, ako sú notebooky a mobilné telefóny

2.2.3 cloudových služieb používaných na ukladanie súborov, komunikáciu alebo finančné činnosti

2.2.4 fyzických dokumentov uchovávaných v kancelárskych priestoroch

2.3 Politika sa uplatňuje vo všetkých pracovných prostrediach — v kancelárii, pri práci na diaľku aj v cloudovom prostredí — a vzťahuje sa na všetky zariadenia a softvér používané na spracúvanie alebo uchovávanie interných informácií.

3. Ciele

3.1 Jasné priradenie zodpovednosti: Zabezpečiť, aby za informačnú bezpečnosť vždy zodpovedala konkrétna osoba. Spravidla ide o generálneho manažéra (GM) alebo osobu, ktorú na to formálne poverí.

3.2 Ochrana informácií zákazníkov a organizácie: Zaviesť spoľahlivé a konzistentné bezpečnostné opatrenia na predchádzanie zneužitiu, strate alebo odcudzeniu citlivých údajov vrátane zákazníckych a finančných záznamov.

3.3 Podpora certifikácie podľa ISO/IEC 27001: Umožniť organizácii preukázať plný súlad s požiadavkami normy ISO/IEC 27001, dosiahnuť pripravenosť na audit a spôsobilosť na certifikáciu bez potreby komplexnej infraštruktúry.

3.4 Začlenenie bezpečnosti do prevádzky organizácie: Integrovať informačnú bezpečnosť do každodenných činností a rozhodovania v celej organizácii.

3.5 Budovanie bezpečnostného povedomia a kultúry: Zabezpečiť, aby každý zamestnanec rozumel bezpečnostným postupom a dodržiaval ich, napríklad používaním silných hesiel a nahlasovaním podozrivej činnosti.

4. Roly a zodpovednosti

4.1 Generálny manažér alebo vlastník spoločnosti

4.1.1 Nesie celkovú zodpovednosť za informačnú bezpečnosť.

4.1.2 Schvaľuje túto politiku a zabezpečuje jej udržiavanie.

4.1.3 Zabezpečuje, aby všetky kľúčové bezpečnostné úlohy boli vykonávané priamo alebo delegované písomne.

4.1.4 Overuje, že všetky delegované bezpečnostné úlohy (napríklad riadenie prístupu alebo riešenie incidentov) sa vykonávajú účinne.

4.1.5 Pôsobí ako hlavná kontaktná osoba pre všetky interné a externé bezpečnostné záležitosti vrátane auditov a otázok zákazníkov.

4.1.6 Počas ročného preskúmania monitoruje plnenie týchto cieľov. Ciele majú byť podľa možností merateľné (napr. % preškolených zamestnancov, počet nahlásených incidentov a pod.) a majú sa revidovať na základe bezpečnostných zistení a zmien rizík.

4.2 Určený zamestnanec (ak je to relevantné)

4.2.1 Môže pomáhať generálnemu manažérovi pri riadení každodenných úloh, ako je vytváranie používateľských účtov, odoberanie prístupových práv pri odchode zamestnancov alebo koordinácia s poskytovateľom IT služieb.

4.2.2 Musí byť formálne poverený a musí mať dostatočné právomoci a nástroje na vykonávanie týchto úloh.

4.2.3 Oznamuje všetky problémy 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 (GM) preskúmať najmenej raz ročne, aby sa zabezpečil trvalý súlad s požiadavkami certifikácie ISO/IEC 27001, zmenami právnych predpisov (ako napríklad nariadenie GDPR, smernica NIS2 a nariadenie DORA) a meniacimi sa potrebami organizácie.

9.2 Mimoriadne preskúmania

9.2.1 Dodatočné preskúmania sa musia vykonať vždy, keď dôjde k významným zmenám, napríklad:

9.2.1.1 závažné bezpečnostné incidenty alebo porušenia ochrany osobných údajov

9.2.1.2 zavedenie nových podnikových procesov alebo technológií (napr. nový softvér, platformy na prácu na diaľku alebo cloudové služby)

9.2.1.3 zmeny právnych alebo regulačných požiadaviek, ktoré ovplyvňujú nakladanie s informáciami

9.3 Dokumentovanie zmien

9.3.1 Všetky preskúmania politiky a všetky zmeny musia byť formálne zdokumentované s jasným uvedením dátumu, povahy zmien a schválenia GM.

9.3.2 Historický záznam verzií politiky sa musí bezpečne uchovávať s cieľom preukázať vývoj politiky a súlad počas auditov.

9.4 Oboznámenie s aktualizáciami

9.4.1 Každá zmena tejto politiky musí byť bezodkladne oznámená všetkým zamestnancom, zmluvným pracovníkom a relevantným tretím stranám.

9.4.2 Aktualizované verzie politiky musia byť ľahko dostupné všetkým dotknutým osobám (napr. elektronicky zdieľané alebo fyzicky sprístupnené na pracovisku).

10. Súvisiace politiky a väzby

10.1 Táto politika úzko súvisí s ďalšími politikami v súbore SME politík organizácie, konkrétne:

10.1.1 P2S – Politika rolí a zodpovedností riadenia: Spresňuje priradenie bezpečnostných úloh a zodpovedností.

10.1.2 P4S – Politika riadenia prístupu: Definuje bezpečné riadenie prístupu k informáciám spoločnosti.

10.1.3 P8S – Politika povedomia a školení v oblasti informačnej bezpečnosti: Poskytuje základné usmernenia pre školenie a budovanie povedomia zamestnancov.

10.1.4 P17S – Politika ochrany údajov a súkromia: Zabezpečuje súlad s GDPR a ďalšími právnymi predpismi na ochranu údajov.

10.1.5 P30S – Politika reakcie na incidenty: Opisuje podrobné opatrenia vyžadované pri reakcii na bezpečnostné incidenty.

10.2 Tieto súvisiace politiky poskytujú jasné prevádzkové usmernenia a musia sa implementovať spoločne na dosiahnutie plného súladu s požiadavkami certifikácie ISO/IEC 27001.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 5.1 – Vedenie a záväzok: Vyžaduje záväzok vrcholového vedenia a zodpovednosť za účinnosť informačnej bezpečnosti v organizácii.

11.1.2 Kapitola 5.2 – Politika informačnej bezpečnosti: Vyžaduje jasné, zdokumentované politiky zosúladené so stratégiou organizácie a požiadavkami na súlad.

11.1.3 Kapitola 5.3 – Organizačné roly a zodpovednosti: Definuje jasné priradenie zodpovedností za informačnú bezpečnosť v celej organizácii, čo je nevyhnutné pre účinné riadenie a auditovateľný súlad.

11.1.4 Kapitola 6.1 – Opatrenia na riešenie rizík a príležitostí: Zabezpečuje, aby riziká informačnej bezpečnosti boli systematicky identifikované, vyhodnocované a ošetrované.

11.1.5 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: Vyžaduje, aby organizácia plánovala a implementovala procesy potrebné na plnenie cieľov informačnej bezpečnosti a účinne riadila súvisiace riziká.

11.2 ISO/IEC 27002:2022 Opatrenia 5.1–5.5

11.2.1 Príloha A, opatrenie 5.1 – Politiky informačnej bezpečnosti: Stanovuje vypracovanie a komunikovanie zdokumentovaných politík informačnej bezpečnosti.

11.2.2 Príloha A, opatrenie 5.2 – Roly informačnej bezpečnosti: Spresňuje a formálne priraďuje roly a zodpovednosti informačnej bezpečnosti príslušným stranám.

11.2.3 Príloha A, opatrenie 5.3 – Oddelenie povinností: Vyžaduje jasné oddelenie povinností s cieľom znížiť konflikty záujmov a riziká podvodu pri správe citlivých informácií.

11.2.4 Príloha A, opatrenie 5.4 – Zodpovednosti vedenia: Vyžaduje, aby vedenie preukazovalo záväzok k informačnej bezpečnosti prostredníctvom aktívneho dohľadu a prideľovania zdrojov.

11.2.5 Posilňuje nevyhnutnosť jasne zdokumentovaných politík informačnej bezpečnosti, rolí, zodpovedností a štruktúr riadenia, čím zabezpečuje konzistentné riadenie a auditnú sledovateľnosť v celej organizácii.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plán programu informačnej bezpečnosti: Vyžaduje zdokumentované stratégie a politiky riadenia informačnej bezpečnosti, ktoré poskytujú rámec na konzistentnú implementáciu a riadenie.

11.3.2 PL-1 – Politika bezpečnostného plánovania: Vyžaduje celopodnikovú politiku bezpečnostného plánovania na usmernenie bezpečnej prevádzky a strategického zosúladenia činností informačnej bezpečnosti.

11.3.3 CA-1 – Politika posudzovania a autorizácie bezpečnosti: Vyžaduje jasne definované roly pre posudzovanie a autorizáciu s cieľom zabezpečiť priebežnú účinnosť a súlad s požiadavkami informačnej bezpečnosti.

11.3.4 AC-1 – Politika riadenia prístupu: Vyžaduje, aby organizácie jasne definovali, dokumentovali a uplatňovali postupy a zodpovednosti pri správe prístupu.

11.4 Nariadenie (EÚ) 2016/679 (GDPR)

11.4.1 Článok 5 ods. 2 – Zásada zodpovednosti: Vyžaduje, aby organizácie preukázali súlad so zásadami ochrany údajov vrátane zdokumentovaných rolí a politík pre zodpovednosti v oblasti ochrany údajov.

11.4.2 Článok 32 – Bezpečnosť spracúvania: Vyžaduje implementáciu primeraných technických a organizačných opatrení vrátane jasných bezpečnostných zodpovedností na ochranu osobných údajov pred porušeniami a neoprávneným prístupom.

11.5 Smernica (EÚ) 2022/2555 (NIS2)

11.5.1 Článok 21 ods. 2 písm. a) – Opatrenia na riadenie rizík: Vyžaduje jasné opatrenia riadenia vrátane definovaných rolí a zodpovedností za informačnú bezpečnosť, ktoré sú nevyhnutné na účinné riadenie kybernetických rizík.

11.6 Nariadenie (EÚ) 2022/2554 (DORA)

11.6.1 Článok 9 – Riadenie IKT rizík: Vyžaduje, aby organizácie jasne priraďovali roly a zodpovednosti súvisiace s riadením IKT rizík, čím sa zvyšuje odolnosť a pripravenosť na kontinuitu činností.

11.6.2 Článok 10 – Kontinuita činností IKT: Vyžaduje jasnú zodpovednosť a štruktúrované roly na udržiavanie odolnosti a kontinuity IKT, aby organizácie dokázali spoľahlivo reagovať na narušenia.

11.7 COBIT 2019

11.7.1 EDM03 – Zabezpečenie optimalizácie rizík: Zdôrazňuje jasne definovanú zodpovednosť a roly pri riadení rizík organizácie, čím podporuje silné riadenie a účinný dohľad nad rizikami informačnej bezpečnosti.

11.7.2 APO13 – Riadenie bezpečnosti: Vyžaduje, aby organizácie jasne stanovili a komunikovali zodpovednosti za riadenie bezpečnosti, čím sa zabezpečí súlad s cieľmi organizácie a regulačnými požiadavkami.

11.7.3 DSS05 – Riadenie bezpečnostných služieb: Vyžaduje štruktúrované roly a jasné zodpovednosti pri riadení bezpečnostných služieb, čím umožňuje konzistentnú implementáciu a overovanie súladu.