					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P18S					Názov dokumentu: **Politika kryptografických kontrol**							
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 8	
ISO/IEC 27002:2022	Kontroly 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 až SC-17	
Smernica EÚ NIS2	Články 21(2)(d), 21(2)(e)	
Nariadenie EÚ DORA	Články 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
Nariadenie EÚ GDPR	Články 32(1)(a), 34	

1. Účel

1.1 Táto politika stanovuje záväzné požiadavky na používanie šifrovania a kryptografických kontrol na ochranu dôvernosti, integrity a autentickosti údajov organizácie a osobných údajov.

1.2 Zabezpečuje primerané používanie kryptografických nástrojov v systémoch, zariadeniach a cloudových službách v prostredí malej organizácie.

1.3 Táto politika priamo podporuje certifikáciu podľa ISO/IEC 27001:2022 a pomáha organizácii plniť zákonné povinnosti podľa nariadenia EÚ GDPR, smernice EÚ NIS2 a nariadenia EÚ DORA.

1.4 Kryptografické kontroly, na ktoré sa táto politika vzťahuje, zahŕňajú šifrovanie údajov, správu certifikátov, bezpečné nakladanie s kľúčmi a šifrované zálohy.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých zamestnancov, zmluvných dodávateľov a tretie strany, ktoré nakladajú s údajmi spoločnosti,

2.1.2 všetky podnikové systémy, koncové zariadenia a cloudové platformy používané na ukladanie, prenos alebo prístup k dôverným informáciám,

2.1.3 všetky osobné, finančné, právne alebo citlivé záznamy klasifikované podľa politiky klasifikácie údajov organizácie,

2.1.4 akékoľvek kryptografické kontroly vrátane metód šifrovania, kľúčov, hesiel, certifikátov a hardvérových bezpečnostných modulov.

2.2 Táto politika sa vzťahuje na údaje v pokoji, údaje pri prenose a údaje počas používania. Zároveň upravuje šifrovanie používané pre zálohy, e-mail, externé prenosy údajov a verejne dostupné webové sídla.

3. Ciele

3.1 Zabezpečiť, aby citlivé údaje a údaje podliehajúce regulácii boli nepretržite chránené primeranými kryptografickými opatreniami.

3.2 Určiť zodpovednosti za výber nástrojov na šifrovanie, ich konfiguráciu a správu kľúčov.

3.3 Predchádzať neoprávnenému prístupu, manipulácii alebo úniku údajov uplatňovaním kontrol bezpečného prenosu a uchovávania.

3.4 Dodržiavať zákonné a regulačné požiadavky, ktoré vyžadujú šifrovanie osobných údajov a údajov organizácie.

3.5 Udržiavať prevádzkovú bezpečnosť a dostupnosť prostredníctvom účinnej správy certifikátov a kryptografických kľúčov.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 schvaľuje túto politiku a zabezpečuje uplatňovanie kryptografických požiadaviek,

4.1.2 preskúmava výnimky, oznámenia o porušení ochrany a súlad dodávateľov s požiadavkami na šifrovanie,

4.1.3 overuje, že outsourcované služby alebo služby prevádzkované v cloudovom prostredí spĺňajú štandardy šifrovania.

4.2 Externý poskytovateľ IT podpory / interný IT administrátor

4.2.1 implementuje a udržiava riešenia šifrovania (napr. celodiskové šifrovanie, certifikáty SSL/TLS, VPN),

4.2.2 riadi životný cyklus kryptografických kľúčov a nástroje na ich bezpečné uchovávanie,

4.2.3 konfiguruje a monitoruje šifrovanie na ochranu záloh, webových sídiel a zariadení.

[... 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 najmenej raz ročne preskúmať generálny manažér v koordinácii s externým poskytovateľom IT podpory a koordinátorom ochrany údajov.

9.2 Spúšťače priebežného preskúmania

9.2.1 Preskúmanie sa musí vykonať aj vtedy, ak:

9.2.1.1 sa zmenia kryptografické štandardy alebo protokoly (napr. vyradenie algoritmu),

9.2.1.2 sa zavedú nové systémy alebo cloudové služby,

9.2.1.3 porušenie ochrany alebo incident zahŕňa kompromitovaný kľúč alebo certifikát,

9.2.1.4 zmeny právnych alebo regulačných požiadaviek ovplyvnia požiadavky na šifrovanie.

9.3 Riadenie verzií a komunikácia

9.3.1 Všetky zmeny politiky musia byť zdokumentované v evidencii verzií.

9.3.2 Zamestnanci musia byť o aktualizáciách informovaní a predchádzajúce verzie musia byť archivované.

9.3.3 Najnovšia schválená verzia musí byť uložená v centrálnom úložisku politík.

10. Súvisiace politiky a väzby

10.1 Táto politika sa musí uplatňovať spolu s nasledujúcimi politikami MSP:

10.1.1 P12S – Politika správy aktív: Zabezpečuje, aby sa šifrovanie uplatňovalo na klasifikované aktíva počas uchovávania, prenosu a likvidácie.

10.1.2 P14S – Politika uchovávania a likvidácie údajov: Vymedzuje lehoty uchovávania a vyžaduje šifrované uchovávanie údajov až do ich bezpečného vymazania.

10.1.3 P17S – Politika ochrany údajov a súkromia: Zosúlaďuje šifrovanie so zásadami ochrany údajov a regulačnými očakávaniami podľa článku 32 GDPR.

10.1.4 P22S – Politika logovania a monitorovania: Vyžaduje logovanie používania kľúčov, zlyhaní šifrovania a exspirácie certifikátov na účely auditu.

10.1.5 P30S – Politika reakcie na incidenty: Upravuje eskalačné, obmedzujúce a oznamovacie postupy pri zlyhaní šifrovania alebo kompromitácii kľúčov.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8 – Vyžaduje implementáciu prevádzkových kontrol vrátane šifrovania na riadenie bezpečnostných rizík.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.24 – Opisuje požiadavky na uplatňovanie šifrovania na zabezpečenie dôvernosti a integrity.

11.2.2 Kontrola 8.25 – Vymedzuje bezpečnú správu kryptografických kľúčov a certifikátov.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Stanovuje požiadavky na zavedenie a validáciu kryptografických kľúčov.

11.3.2 SC-13 – Definuje štandardy pre generovanie kryptografických kľúčov.

11.3.3 SC-17 – Pokrýva infraštruktúru verejného kľúča (PKI) a riadenie životného cyklu certifikátov.

11.3.4 SC-28 – Vyžaduje šifrovanie údajov v pokoji.

11.3.5 SC-12 až SC-17 (skupina) – Zabezpečuje správnu implementáciu kryptografických ochranných opatrení naprieč systémami.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 32(1)(a) – Vyžaduje, aby organizácie zaviedli technické opatrenia, ako je šifrovanie, na zabezpečenie dôvernosti údajov.

11.4.2 Článok 34 – Uvádza, že šifrovanie môže organizáciu oslobodiť od oznamovania porušenia ochrany, ak boli údaje nezrozumiteľné pre neoprávnené osoby.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(d) – Vyžaduje účinné šifrovanie na zabezpečenie systémov a komunikácie.

11.5.2 Článok 21(2)(e) – Zdôrazňuje ochranu údajov a zmierňovanie kybernetických hrozieb prostredníctvom šifrovania.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 6(2)(d) – Vyžaduje, aby systémy IKT udržiavali bezpečné komunikačné kanály a šifrovanie.

11.6.2 Článok 9(2)(f) – Ukladá finančným subjektom používať silné šifrovanie na ochranu digitálnej komunikácie a výmeny údajov.

11.7 COBIT 2019

11.7.1 DSS05.01 – Vyžaduje ochranu citlivých informácií prostredníctvom šifrovania a kryptografických protokolov.

11.7.2 APO13.02 – Vyžaduje účinnú implementáciu bezpečnostných kontrol vrátane kryptografických ochranných opatrení ako súčasti plánovania informačnej bezpečnosti.