					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P18S					Název dokumentu: **Politika kryptografických opatření**							
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 8	
ISO/IEC 27002:2022	Opatření 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 až SC-17	
směrnice NIS2	Články 21 odst. 2 písm. d), 21 odst. 2 písm. e)	
nařízení DORA	Články 6 odst. 2 písm. d), 9 odst. 2 písm. f)	
COBIT 2019	DSS05.01, APO13	
GDPR	Články 32 odst. 1 písm. a), 34	

1. Účel

1.1 Tato politika stanoví závazné požadavky na používání šifrování a kryptografických opatření k ochraně důvěrnosti, integrity a autenticity podnikových a osobních údajů.

1.2 Zajišťuje, aby byly kryptografické nástroje v přiměřeném rozsahu používány napříč systémy, zařízeními a cloudovými službami v prostředí malého podniku.

1.3 Tato politika přímo podporuje certifikaci podle ISO/IEC 27001:2022 a napomáhá organizaci plnit právní povinnosti vyplývající z GDPR, směrnice NIS2 a nařízení DORA.

1.4 Kryptografická opatření upravená touto politikou zahrnují šifrování dat, správu certifikátů, bezpečné nakládání s klíči a šifrované zálohy.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny zaměstnance, smluvní pracovníky a třetí strany, které nakládají s údaji organizace,

2.1.2 všechny podnikové systémy, koncová zařízení a cloudové platformy používané k ukládání, přenosu nebo zpřístupnění důvěrných informací,

2.1.3 všechny osobní, finanční, právní nebo jiné citlivé záznamy klasifikované podle politiky klasifikace dat organizace,

2.1.4 veškerá kryptografická opatření, včetně metod šifrování, klíčů, hesel, certifikátů a bezpečnostních modulů.

2.2 Tato politika se vztahuje na data v klidu, data při přenosu i data při používání. Současně upravuje šifrování používané pro zálohy, e-mail, externí přenosy dat a veřejně dostupné webové stránky.

3. Cíle

3.1 Zajistit, aby citlivá a regulovaná data byla vždy chráněna odpovídajícími kryptografickými opatřeními.

3.2 Vymezit odpovědnost za výběr nástrojů pro šifrování, jejich konfiguraci a správu klíčů.

3.3 Předcházet neoprávněnému přístupu, manipulaci s daty nebo úniku dat prostřednictvím zajištění bezpečného přenosu a bezpečného ukládání dat.

3.4 Zajistit soulad s právními a regulačními požadavky, které vyžadují šifrování osobních a podnikových údajů.

3.5 Udržovat provozní bezpečnost a dostupnost prostřednictvím účinné správy certifikátů a kryptografických klíčů.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 schvaluje tuto politiku a zajišťuje uplatňování kryptografických požadavků,

4.1.2 přezkoumává výjimky, oznámení o porušení zabezpečení a soulad dodavatelů se smluvními požadavky na šifrování,

4.1.3 ověřuje, že outsourcingové a cloudové služby splňují požadované standardy šifrování.

4.2 poskytovatel IT podpory / interní správce IT

4.2.1 implementuje a udržuje řešení šifrování (např. šifrování celého disku, certifikáty SSL/TLS, VPN),

4.2.2 spravuje životní cyklus kryptografických klíčů a nástroje pro jejich bezpečné ukládání,

4.2.3 konfiguruje a monitoruje šifrování pro ochranu záloh, webových stránek a zařízení.

[... 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 přezkoumána nejméně jednou ročně generálním ředitelem ve spolupráci s poskytovatelem IT podpory a koordinátorem ochrany soukromí.

9.2 Spouštěče mimořádného přezkumu

9.2.1 Přezkum musí být proveden také v případě, že:

9.2.1.1 dojde ke změně kryptografických standardů nebo protokolů (např. vyřazení algoritmu),

9.2.1.2 jsou zavedeny nové systémy nebo cloudové služby,

9.2.1.3 porušení zabezpečení nebo incident souvisí s kompromitovaným klíčem nebo certifikátem,

9.2.1.4 změny právních nebo regulačních požadavků mají dopad na požadavky na šifrování.

9.3 Řízení verzí a komunikace

9.3.1 Všechny změny politiky musí být zdokumentovány v evidenci verzí.

9.3.2 Personál musí být o aktualizacích informován a předchozí verze musí být archivovány.

9.3.3 Nejnovější schválená verze musí být uložena v centrálním repozitáři politik.

10. Související politiky a vazby

10.1 Tato politika musí být uplatňována společně s následujícími politikami SME:

10.1.1 P12S – Politika správy aktiv: Zajišťuje, aby bylo šifrování použito na klasifikovaná aktiva při ukládání, přenosu a likvidaci.

10.1.2 P14S – Politika uchovávání údajů: Definuje doby uchovávání a vyžaduje šifrované ukládání dat až do jejich bezpečného výmazu.

10.1.3 P17S – Politika ochrany dat a soukromí: Uvádí šifrování do souladu se zásadami ochrany údajů a regulatorními očekáváními podle článku 32 GDPR.

10.1.4 P22S – Politika protokolování a monitorování: Vyžaduje protokolování používání klíčů, selhání šifrování a ukončení platnosti certifikátů pro účely auditu.

10.1.5 P30S – Politika reakce na incidenty: Stanoví eskalaci, zamezení šíření a oznamovací postupy v případě selhání šifrování nebo kompromitace klíčů.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Vyžaduje zavedení provozních opatření, včetně šifrování, k řízení bezpečnostních rizik.

11.2 ISO/IEC 27002

11.2.1 Opatření 8.24 – Popisuje požadavky na použití šifrování k zajištění důvěrnosti a integrity.

11.2.2 Opatření 8.25 – Stanoví požadavky na bezpečnou správu kryptografických klíčů a certifikátů.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Stanoví požadavky na zavedení a ověřování kryptografických klíčů.

11.3.2 SC-13 – Definuje standardy pro generování kryptografických klíčů.

11.3.3 SC-17 – Pokrývá infrastrukturu veřejných klíčů (PKI) a správu životního cyklu certifikátů.

11.3.4 SC-28 – Vyžaduje šifrování dat v klidu.

11.3.5 SC-12 až SC-17 (skupina) – Zajišťuje řádnou implementaci kryptografické ochrany napříč systémy.

11.4 GDPR

11.4.1 Článek 32 odst. 1 písm. a) – Vyžaduje, aby organizace zavedly technická opatření, jako je šifrování, k zajištění důvěrnosti údajů.

11.4.2 Článek 34 – Stanoví, že šifrování může organizaci zprostit oznamovací povinnosti při porušení zabezpečení, pokud byly údaje pro neoprávněné osoby nečitelné.

11.5 směrnice NIS2

11.5.1 Článek 21 odst. 2 písm. d) – Vyžaduje účinné šifrování pro zabezpečení systémů a komunikace.

11.5.2 Článek 21 odst. 2 písm. e) – Zdůrazňuje ochranu dat a zmírňování kybernetických hrozeb prostřednictvím šifrování.

11.6 nařízení DORA

11.6.1 Článek 6 odst. 2 písm. d) – Vyžaduje, aby systémy ICT udržovaly zabezpečené komunikační kanály a šifrování.

11.6.2 Článek 9 odst. 2 písm. f) – Ukládá finančním subjektům používat silné šifrování k ochraně digitální komunikace a výměny dat.

11.7 COBIT 2019

11.7.1 DSS05.01 – Vyžaduje ochranu citlivých informací prostřednictvím šifrování a kryptografických protokolů.

11.7.2 APO13.02 – Vyžaduje účinnou implementaci bezpečnostních opatření, včetně kryptografických opatření, jako součásti plánování bezpečnosti informací.