					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P18					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, 8	-
NIST SP 800-53 Rev.5	SC-12 až SC-17, SC-28, SC-28(1), SC-12(3)	-
GDPR	Článek 32, články 33–34, bod odůvodnění 83	-
směrnice NIS2	Článek 21(2)(d)	-
nařízení DORA	Články 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Účel

1.1 Tato politika stanoví závazné požadavky na bezpečné a souladné používání kryptografických opatření v celé organizaci za účelem zajištění důvěrnosti, integrity a autenticity citlivých a regulovaných informací.

1.2 Používání kryptografie je základním předpokladem důvěryhodného zabezpečení dat, podporuje bezpečnou komunikaci, vynucuje řízení přístupu a umožňuje plnění regulačních požadavků prostřednictvím účinného šifrování a správy klíčů.

1.3 Tato politika je v souladu s ISO/IEC 27001:2022, kapitolou 8.1 a přílohou A, opatřením 8.24, a podporuje právní a provozní povinnosti podle článku 32 GDPR, článku 6(2)(d) nařízení DORA a článku 21 směrnice NIS2. Současně podporuje cíle COBIT 2019 v oblasti bezpečnostních služeb a ochrany datových aktiv.

2. Rozsah

2.1 Tato politika se vztahuje na všechny organizační jednotky, podnikové funkce, veškerý personál a poskytovatele služeb třetích stran, kteří se podílejí na používání, správě nebo implementaci kryptografických nástrojů a metod.

2.2 Do rozsahu působnosti spadají produkční, vývojová a testovací prostředí, záložní systémy a prostředí pro obnovu po havárii, v nichž jsou citlivá data přenášena, zpracovávána nebo ukládána.

2.3 Rozsah zahrnuje všechny kryptografické komponenty a případy použití, včetně mimo jiné:

2.3.1 Symetrického a asymetrického šifrování

2.3.2 Digitálních podpisů a certifikátů

2.3.3 Hashovacích algoritmů

2.3.4 Bezpečného generování, distribuce a zničení klíčů

2.3.5 Transport Layer Security (TLS), šifrování celého disku a šifrování na úrovni API

2.3.6 Bezpečných prvků, jako jsou Hardware Security Modules (HSM), Trusted Platform Modules (TPM) a systémy správy klíčů (KMS)

2.4 Tato politika upravuje používání kryptografie ve vztahu k:

2.4.1 Datům klasifikovaným jako Důvěrné, Vysoce důvěrné nebo Regulované

2.4.2 Autentizaci a ověřování digitální identity

2.4.3 Bezpečné komunikaci s externími stranami

2.4.4 Správě úschovy klíčů a mechanismům dvojí kontroly

3. Cíle

3.1 Zajistit, aby kryptografické technologie byly vybírány, schvalovány, implementovány a udržovány v souladu s obchodním rizikem, mezinárodními normami a regulačními požadavky.

3.2 Zavést standardizovaný rámec správy a řízení kryptografických služeb, včetně jasně stanovené odpovědnosti za implementaci, ověřování a řešení výjimek.

3.3 Předcházet neoprávněnému použití, nesprávné konfiguraci nebo zastarání kryptografických algoritmů a opatření prostřednictvím formálního procesu schvalování a přezkumu.

3.4 Zajistit, aby kryptografická opatření byla začleněna již ve fázi návrhu systému a pravidelně ověřována za účelem prevence expozice dat, kompromitace klíčů nebo oslabení protokolů.

3.5 Vynucovat řízení životního cyklu všech kryptografických klíčů, včetně generování, ukládání, používání, rotace, revokace a bezpečného zničení.

3.6 Dodržovat mezinárodní a regionální právní předpisy vyžadující šifrování a bezpečné nakládání s daty, včetně GDPR, nařízení DORA, směrnice NIS2 a COBIT 2019.

4. Role a odpovědnosti

4.1 Manažer informační bezpečnosti / ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za tuto politiku a zajišťuje její soulad se Systémem řízení bezpečnosti informací (ISMS) a přílohou A normy ISO/IEC 27001, opatřením 8.24.

4.1.2 Schvaluje používání kryptografických algoritmů a opatření a zajišťuje jejich dodržování v celé organizaci.

4.2 Vedoucí kryptografických operací / bezpečnostní architekt

4.2.1 Řídí každodenní provoz a správu kryptografických systémů.

4.2.2 Udržuje seznam schválených kryptografických metod (ACML) a registr správy klíčů.

4.2.3 Provádí přezkumy kryptografického návrhu (CDR) a vyhodnocuje nové kryptografické technologie.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být každoročně přezkoumána manažerem informační bezpečnosti a vedoucím kryptografických operací.

9.2 Spouštěče přezkumu zahrnují:

9.2.1 Zjištění kryptografických zranitelností (např. downgrade algoritmu, kvantové útoky)

9.2.2 Regulační změny vyžadující aktualizaci standardů šifrování

9.2.3 Provozní zjištění nebo zjištění auditu odhalující mezery v politice

9.2.4 Aktualizace kryptografických nástrojů nebo architektonické změny

9.3 Aktualizace musí být vedeny v režimu správy verzí v registru řízení dokumentace ISMS a oznámeny:

9.3.1 Všem správcům s rolemi přístupu ke kryptografii

9.3.2 Vývojovým týmům a vedoucím DevSecOps

9.3.3 Poskytovatelům třetích stran se smluvními povinnostmi v oblasti šifrování

9.4 Tým ISMS musí zajistit, aby byly nahrazené verze archivovány a nadále nebyly odkazovány v provozních postupech.

10. Související politiky a vazby

10.1 P1 - Politika informační bezpečnosti. Poskytuje základní rámec správy a řízení pro všechna bezpečnostní opatření, včetně vynucování kryptografických opatření, ochrany aktiv a bezpečné komunikace.

10.2 P4 - Politika řízení přístupu. Zajišťuje, aby logický přístup ke kryptografickému materiálu a systémům správy šifrování byl přísně omezen na základě zásady minimálních oprávnění a oddělení povinností.

10.3 P6 - Politika řízení rizik. Podporuje posuzování rizik kryptografických opatření a dokumentuje strategii ošetření rizik pro výjimky, zastarání algoritmů nebo scénáře kompromitace klíčů.

10.4 P12 - Politika správy aktiv. Stanoví klasifikaci citlivých dat a hardwarových aktiv, která přímo určuje kryptografické požadavky a povinnosti v oblasti úschovy klíčů.

10.5 P13 - Politika klasifikace a označování dat. Definuje úrovně klasifikace (např. Důvěrné, Regulované), které spouštějí konkrétní požadavky na šifrování při přenosu a při uložení.

10.6 P14 - Politika uchovávání údajů. Stanoví postupy pro bezpečnou likvidaci šifrovaných úložných médií a kryptografického klíčového materiálu po ukončení životního cyklu.

10.7 P30 - Politika reakce na incidenty. Popisuje strategii reakce organizace na kompromitaci klíčů, zneužití certifikátů nebo podezření na zranitelnosti algoritmů, včetně rychlé revokace a hlášení porušení zabezpečení.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 - Provozní plánování a řízení: Vyžaduje technická bezpečnostní opatření, včetně kryptografických opatření, jako součást provozních ochranných mechanismů.

11.2 ISO/IEC 27002:2022

11.2.1 Opatření 8.24, 8.25, 8: Poskytují pokyny k implementaci cílů kryptografických opatření, výběru algoritmů, vynucování protokolů a řízení životního cyklu certifikátů.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-12 - Zřízení kryptografických klíčů: Zajišťuje bezpečné generování a výměnu šifrovacích klíčů. P18 stanoví, jak musí být symetrické a asymetrické klíče generovány a vyměňovány s použitím schválených algoritmů a protokolů.

11.3.2 SC-13 - Kryptografická ochrana: Vyžaduje použití kryptografie k ochraně důvěrnosti a integrity informací. P18 vynucuje šifrování při uložení a při přenosu na základě klasifikace dat, se standardy algoritmů sladěnými s NIST FIPS 140-3.

11.3.3 SC-17 - Certifikáty infrastruktury veřejných klíčů (PKI): Vyžaduje implementaci PKI na podporu autentizace a digitálních podpisů. P18 vymezuje použití PKI k zabezpečení komunikace, systémových identit a administrátorského přístupu.

11.3.4 SC-28, SC-28(1) - Ochrana informací při uložení a při přenosu: Vyžaduje šifrování dat při ukládání nebo přenosu přes nedůvěryhodné sítě. P18 stanoví vynucování TLS, tunelů VPN, šifrování celého disku a bezpečných metod ukládání citlivých dat.

11.3.5 SC-12(3) - Generování symetrických klíčů pro bezpečné uložení a distribuci: Zaměřuje se na bezpečné generování a nakládání se symetrickými klíči. P18 vyžaduje použití silných generátorů náhodných čísel, politik rotace klíčů a bezpečných trezorů klíčů pro kryptografické operace.

11.4 GDPR (2016/679)

11.4.1 Článek 32 - Zabezpečení zpracování: Výslovně doporučuje šifrování jako opatření ke snižování rizik pro osobní údaje.

11.4.2 Bod odůvodnění 83: Zdůrazňuje šifrování jako opatření k prevenci neoprávněného přístupu k datům.

11.4.3 Články 33 a 34: Účinné šifrování může organizaci vyjmout z povinnosti oznámit porušení zabezpečení.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21(2)(d): Vyžaduje technická a organizační opatření, včetně kryptografické ochrany, k zajištění dostupnosti a integrity služeb.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 6(2)(d): Finanční instituce musí zabezpečit data mimo jiné prostřednictvím silného šifrování kritických informací.

11.6.2 Článek 11(1)(c): Vyžaduje bezpečné řízení zpracování dat u poskytovatelů služeb třetích stran v oblasti ICT.

11.7 COBIT 2019

11.7.1 DSS05.01 - Chránit informační aktiva: Vyžaduje použití šifrování a správy klíčů k ochraně dat před neoprávněným přístupem.

11.7.2 DSS06.06 - Řízené bezpečnostní testování: Doporučuje validaci souladu kryptografických opatření jako součást hodnocení zranitelností.

11.7.3 MEA03 - Monitorovat, vyhodnocovat a posuzovat soulad: Vyžaduje průběžné zajištění účinnosti kryptografických opatření.