					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P18					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, 8	-
NIST SP 800-53 Rev.5	SC-12 až SC-17, SC-28, SC-28(1), SC-12(3)	-
Nariadenie EÚ GDPR	Článok 32, články 33 – 34, odôvodnenie 83	-
Smernica EÚ NIS2	Článok 21(2)(d)	-
Nariadenie EÚ DORA	Články 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Účel

1.1 Táto politika stanovuje záväzné požiadavky na bezpečné a súladné používanie kryptografických kontrol v celej organizácii s cieľom zabezpečiť dôvernosť, integritu a autentickosť citlivých a regulovaných informácií.

1.2 Používanie kryptografie predstavuje základ dôveryhodnosti pri ochrane údajov, podporuje bezpečnú komunikáciu, presadzuje riadenie prístupu a umožňuje súlad s regulačnými požiadavkami prostredníctvom účinného šifrovania a postupov správy kľúčov.

1.3 Táto politika je zosúladená s ISO/IEC 27001:2022, kapitolou 8.1 a prílohou A, kontrolou 8.24, a podporuje zákonné a prevádzkové povinnosti podľa článku 32 GDPR, článku 6(2)(d) nariadenia DORA a článku 21 smernice NIS2. Zároveň podporuje ciele COBIT 2019 v oblasti bezpečnostných služieb a ochrany dátových aktív.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky organizačné jednotky, podnikové funkcie, zamestnancov a poskytovateľov služieb tretích strán zapojených do používania, správy alebo implementácie kryptografických nástrojov a metód.

2.2 Medzi zahrnuté prostredia patria produkčné, vývojové a testovacie prostredia, zálohovacie systémy a prostredia obnovy po havárii, v ktorých sa citlivé údaje prenášajú, spracúvajú alebo uchovávajú.

2.3 Rozsah zahŕňa všetky kryptografické komponenty a prípady použitia vrátane, okrem iného:

2.3.1 Symetrického a asymetrického šifrovania

2.3.2 Digitálnych podpisov a certifikátov

2.3.3 Hašovacích algoritmov

2.3.4 Bezpečného generovania, distribúcie a likvidácie kľúčov

2.3.5 Protokolu Transport Layer Security (TLS), celodiskového šifrovania (FDE) a šifrovania na úrovni API

2.3.6 Bezpečnostných prvkov, ako sú moduly hardvérovej bezpečnosti (HSM), moduly dôveryhodnej platformy (TPM) a systémy správy kľúčov (KMS)

2.4 Táto politika upravuje používanie kryptografie vo vzťahu k:

2.4.1 Údajom klasifikovaným ako Dôverné, Vysoko dôverné alebo Regulované

2.4.2 Autentifikácii a overovaniu digitálnej identity

2.4.3 Bezpečnej komunikácii s externými stranami

2.4.4 Správe kľúčov a mechanizmom dvojitej kontroly

3. Ciele

3.1 Zabezpečiť, aby sa kryptografické technológie vyberali, schvaľovali, implementovali a udržiavali v súlade s podnikovým rizikom, medzinárodnými normami a regulačnými požiadavkami.

3.2 Zaviesť štandardizovaný rámec správy a riadenia kryptografických služieb vrátane jasného priradenia zodpovedností za implementáciu, validáciu a ošetrenie výnimiek.

3.3 Predchádzať neoprávnenému používaniu, chybným konfiguráciám alebo zastaranosti kryptografických algoritmov a kontrol prostredníctvom formálneho procesu schvaľovania a preskúmania.

3.4 Zabezpečiť, aby sa kryptografické kontroly zohľadňovali už vo fáze návrhu systému a pravidelne validovali s cieľom predchádzať vystaveniu údajov, kompromitácii kľúčov alebo oslabeniu protokolov.

3.5 Presadzovať riadenie životného cyklu všetkých kryptografických kľúčov vrátane ich generovania, uchovávania, používania, rotácie, revokácie a bezpečnej likvidácie.

3.6 Zabezpečiť súlad s medzinárodnými a regionálnymi predpismi vyžadujúcimi šifrovanie a bezpečné nakladanie s údajmi vrátane GDPR, DORA, NIS2 a COBIT 2019.

4. Roly a zodpovednosti

4.1 Manažér informačnej bezpečnosti / riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje jej súlad so systémom manažérstva informačnej bezpečnosti (ISMS) a s ISO/IEC 27001, prílohou A, kontrolou 8.24.

4.1.2 Schvaľuje používanie kryptografických algoritmov a kontrol a zabezpečuje ich dodržiavanie v celej organizácii.

4.2 Vedúci kryptografických operácií / bezpečnostný architekt

4.2.1 Riadi každodennú prevádzku a správu kryptografických systémov.

4.2.2 Udržiava Zoznam schválených kryptografických metód (ACML) a register správy kľúčov.

4.2.3 Vykonáva preskúmania kryptografického návrhu (CDR) a posudzuje nové kryptografické technológie.

[... 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 Túto politiku musia každoročne preskúmať manažér informačnej bezpečnosti a vedúci kryptografických operácií.

9.2 Spúšťače preskúmania zahŕňajú:

9.2.1 zistenie kryptografických zraniteľností (napr. zníženie úrovne algoritmu, kvantové útoky)

9.2.2 regulačné zmeny vyžadujúce aktualizované štandardy šifrovania

9.2.3 prevádzkové alebo auditné zistenia odhaľujúce medzery v politike

9.2.4 modernizáciu kryptografických nástrojov alebo architektonické zmeny

9.3 Aktualizácie musia podliehať riadeniu verzií v registri riadenia dokumentov ISMS a musia byť komunikované:

9.3.1 všetkým správcom s prístupovými rolami ku kryptografii

9.3.2 vývojovým tímom a vedúcim DevSecOps

9.3.3 poskytovateľom tretích strán so zmluvnými povinnosťami v oblasti šifrovania

9.4 Tím ISMS musí zabezpečiť archiváciu nahradených verzií a to, aby sa na ne už neodkazovalo v prevádzkových postupoch.

10. Súvisiace politiky a väzby

10.1 P1 - Politika informačnej bezpečnosti. Poskytuje základný rámec správy a riadenia pre všetky bezpečnostné opatrenia vrátane uplatňovania kryptografických kontrol, ochrany aktív a bezpečnej komunikácie.

10.2 P4 - Politika riadenia prístupu. Zabezpečuje, aby bol logický prístup ku kryptografickému materiálu a systémom správy šifrovania prísne obmedzený na základe zásady najmenších oprávnení a oddelenia povinností.

10.3 P6 - Politika riadenia rizík. Podporuje posúdenie rizík kryptografických kontrol a dokumentuje stratégiu ošetrenia rizík pre výnimky, zastaranosť algoritmov alebo scenáre kompromitácie kľúčov.

10.4 P12 - Politika správy aktív. Ukladá klasifikáciu citlivých údajov a hardvérových aktív, ktorá priamo určuje kryptografické požiadavky a povinnosti správy kľúčov.

10.5 P13 - Politika klasifikácie a označovania údajov. Definuje úrovne klasifikácie (napr. Dôverné, Regulované), ktoré vyvolávajú konkrétne požiadavky na šifrovanie pri prenose a v pokoji.

10.6 P14 - Politika uchovávania a likvidácie údajov. Určuje postupy bezpečnej likvidácie šifrovaných úložných médií a materiálu kryptografických kľúčov na konci životnosti.

10.7 P30 - Politika reakcie na incidenty. Stanovuje stratégiu reakcie organizácie na kompromitáciu kľúčov, zneužitie certifikátov alebo podozrenie na algoritmické zraniteľnosti vrátane rýchlej revokácie a oznamovania porušení.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 - Prevádzkové plánovanie a riadenie: Vyžaduje technické bezpečnostné kontroly vrátane kryptografických opatrení ako súčasť prevádzkových ochranných opatrení.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroly 8.24, 8.25, 8: Poskytujú implementačné usmernenia pre ciele kryptografických kontrol, výber algoritmov, uplatňovanie protokolov a riadenie životného cyklu certifikátov.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Zriadenie kryptografických kľúčov: Zabezpečuje bezpečné generovanie a výmenu šifrovacích kľúčov. P18 definuje, ako sa musia symetrické a asymetrické kľúče generovať a vymieňať s použitím schválených algoritmov a protokolov.

11.3.2 SC-13 - Kryptografická ochrana: Vyžaduje používanie kryptografie na ochranu dôvernosti a integrity informácií. P18 presadzuje šifrovanie údajov v pokoji a pri prenose na základe klasifikácie údajov, pričom štandardy algoritmov sú zosúladené s NIST FIPS 140-3.

11.3.3 SC-17 - Certifikáty infraštruktúry verejného kľúča (PKI): Vyžaduje implementáciu PKI na podporu autentifikácie a digitálnych podpisov. P18 vymedzuje používanie PKI na zabezpečenie komunikácie, systémových identít a administratívneho prístupu.

11.3.4 SC-28, SC-28(1) - Ochrana informácií v pokoji a pri prenose: Vyžaduje šifrovanie údajov pri uchovávaní alebo prenose cez nedôveryhodné siete. P18 určuje uplatňovanie TLS, VPN tunelov, celodiskového šifrovania a bezpečných metód uchovávania citlivých údajov.

11.3.5 SC-12(3) - Generovanie symetrických kľúčov na bezpečné uchovávanie a distribúciu: Zameriava sa na bezpečné generovanie a nakladanie so symetrickými kľúčmi. P18 vyžaduje používanie silných generátorov náhodných čísel, pravidiel rotácie kľúčov a bezpečných úložísk kľúčov pre kryptografické operácie.

11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 32 - Bezpečnosť spracúvania: Výslovne odporúča šifrovanie ako opatrenie na znižovanie rizika pre osobné údaje.

11.4.2 Odôvodnenie 83: Zdôrazňuje šifrovanie ako kontrolu na predchádzanie neoprávnenému prístupu k údajom.

11.4.3 Články 33 a 34: Účinné šifrovanie môže organizácie vyňať z povinnosti oznámenia porušenia.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(d): Vyžaduje technické a organizačné opatrenia vrátane kryptografických ochranných opatrení na zachovanie dostupnosti a integrity služieb.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 6(2)(d): Finančné inštitúcie musia chrániť údaje vrátane používania silného šifrovania kritických informácií.

11.6.2 Článok 11(1)(c): Vyžaduje bezpečné kontroly spracúvania údajov pre poskytovateľov služieb tretích strán v oblasti IKT.

11.7 COBIT 2019

11.7.1 DSS05.01 - Chrániť informačné aktíva: Vyžaduje používanie šifrovania a správy kľúčov na ochranu údajov pred neoprávneným prístupom.

11.7.2 DSS06.06 - Riadené bezpečnostné testovanie: Odporúča validáciu súladu kryptografie ako súčasť posúdení zraniteľností.

11.7.3 MEA03 - Monitorovanie, hodnotenie a posudzovanie súladu: Vyžaduje priebežné zabezpečovanie účinnosti kryptografických kontrol.