					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P18					Naslov dokumenta: **Politika kriptografskih kontrol**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	-
ISO/IEC 27002:2022	Kontrole 8.24, 8.25, 8	-
NIST SP 800-53 Rev. 5	SC-12 do SC-17, SC-28, SC-28(1), SC-12(3)	-
Uredba EU GDPR	Člen 32, člena 33–34, uvodna izjava 83	-
Direktiva EU NIS2	Člen 21(2)(d)	-
Uredba EU DORA	Člena 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA03	-

1. Namen

1.1 Ta politika določa obvezne zahteve za varno in skladno uporabo kriptografskih kontrol v celotni organizaciji, da se zagotovi zaupnost, celovitost in avtentičnost občutljivih in reguliranih informacij.

1.2 Uporaba kriptografije podpira zaupanje v postopke varovanja podatkov, omogoča varne komunikacije, uveljavlja nadzor dostopa ter podpira skladnost z regulativnimi zahtevami z učinkovitim šifriranjem in upravljanjem ključev.

1.3 Ta politika je usklajena z ISO/IEC 27001:2022, klavzulo 8.1, in Prilogo A, kontrolo 8.24, ter podpira pravne in operativne obveznosti iz člena 32 GDPR, člena 6(2)(d) Uredbe EU DORA in člena 21 Direktive EU NIS2. Podpira tudi cilje okvira COBIT 2019 na področju varnostnih storitev in zaščite informacijskih sredstev.

2. Področje uporabe

2.1 Ta politika velja za vse organizacijske enote, poslovne funkcije, zaposlene in ponudnike storitev tretjih oseb, ki sodelujejo pri uporabi, upravljanju ali uvedbi kriptografskih orodij in metod.

2.2 Zajeta okolja vključujejo produkcijska, razvojna, preizkusna okolja, sisteme za varnostno kopiranje in okolja za obnovitev po nesreči, v katerih se občutljivi podatki prenašajo, obdelujejo ali hranijo.

2.3 Področje uporabe vključuje vse kriptografske komponente in primere uporabe, vključno z, vendar ne omejeno na:

2.3.1 simetrično in asimetrično šifriranje

2.3.2 digitalne podpise in digitalna potrdila

2.3.3 algoritme zgoščevanja

2.3.4 varno generiranje, distribucijo in uničenje ključev

2.3.5 protokol Transport Layer Security (TLS), šifriranje celotnega diska in šifriranje na ravni API

2.3.6 varne komponente, kot so strojni varnostni moduli (HSM), moduli zaupanja vredne platforme (TPM) in sistemi za upravljanje ključev (KMS)

2.4 Ta politika ureja uporabo kriptografije v povezavi z:

2.4.1 podatki, razvrščenimi kot zaupni, strogo zaupni ali regulirani

2.4.2 avtentikacijo in preverjanjem digitalne identitete

2.4.3 varnimi komunikacijami z zunanjimi stranmi

2.4.4 skrbništvom nad ključi in mehanizmi dvojne kontrole

3. Cilji

3.1 Zagotoviti, da so kriptografske tehnologije izbrane, odobrene, uvedene in vzdrževane v skladu s poslovnimi tveganji, mednarodnimi standardi in regulativnimi zahtevami.

3.2 Vzpostaviti standardiziran okvir upravljanja kriptografskih storitev, vključno z jasno odgovornostjo za uvedbo, preverjanje in obravnavo izjem.

3.3 Preprečiti nepooblaščeno uporabo, napačno konfiguracijo ali zastarelost kriptografskih algoritmov in kontrol s formalnim postopkom odobritve in pregleda.

3.4 Zagotoviti, da so kriptografske kontrole vključene v fazo zasnove sistema in redno preverjane, da se preprečijo izpostavljenost podatkov, kompromitacija ključev ali degradacija protokolov.

3.5 Uveljaviti upravljanje življenjskega cikla dostopa za vse kriptografske ključe, vključno z generiranjem, hrambo, uporabo, menjavo, preklicem in varnim uničenjem.

3.6 Zagotoviti skladnost z mednarodnimi in regionalnimi predpisi, ki zahtevajo šifriranje in varno ravnanje s podatki, vključno z GDPR, DORA, NIS2 in COBIT 2019.

4. Vloge in odgovornosti

4.1 vodja informacijske varnosti

4.1.1 Je lastnik te politike in zagotavlja njeno usklajenost z ISMS in Prilogo A standarda ISO/IEC 27001, kontrolo 8.24.

4.1.2 Odobrava uporabo kriptografskih algoritmov in kontrol ter zagotavlja skladnost v celotni organizaciji.

4.2 vodja kriptografskih operacij / varnostni arhitekt

4.2.1 Upravlja dnevno delovanje in administriranje kriptografskih sistemov.

4.2.2 Vzdržuje seznam odobrenih kriptografskih metod (ACML) in register upravljanja ključev.

4.2.3 Izvaja preglede kriptografske zasnove (CDR) in ocenjuje nove kriptografske tehnologije.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 To politiko morata letno pregledati vodja informacijske varnosti in vodja kriptografskih operacij.

9.2 Povodi za pregled vključujejo:

9.2.1 odkritje kriptografskih ranljivosti (npr. znižanje ravni algoritma, kvantni napadi)

9.2.2 regulativne spremembe, ki zahtevajo posodobljene standarde šifriranja

9.2.3 operativne ugotovitve ali ugotovitve presoj, ki razkrivajo vrzeli v politiki

9.2.4 nadgradnje kriptografskih orodij ali arhitekturne spremembe

9.3 Posodobitve morajo biti vodene po različicah v registru nadzora dokumentov ISMS in sporočene:

9.3.1 vsem skrbnikom z vlogami dostopa do kriptografskih funkcij

9.3.2 razvojnim ekipam in vodjem DevSecOps

9.3.3 ponudnikom tretjih oseb s pogodbenimi obveznostmi glede šifriranja

9.4 Ekipa ISMS mora zagotoviti, da so nadomeščene različice arhivirane in da se nanje v operativnih postopkih ne sklicuje več.

10. Povezane politike in povezave

10.1 P1 - Politika informacijske varnosti. Določa temeljni okvir upravljanja za vse varnostne ukrepe, vključno z uveljavljanjem kriptografskih kontrol, zaščito sredstev in varnimi komunikacijami.

10.2 P4 - Politika nadzora dostopa. Zagotavlja, da je logični dostop do kriptografskega gradiva in sistemov za upravljanje šifriranja strogo omejen na podlagi načela najmanjših privilegijev in ločevanja dolžnosti (SoD).

10.3 P6 - Politika upravljanja tveganj. Podpira ocenjevanje tveganj kriptografskih kontrol in dokumentira strategijo obravnave tveganj za izjeme, zastarelost algoritmov ali scenarije kompromitacije ključev.

10.4 P12 - Politika upravljanja sredstev. Zahteva razvrščanje občutljivih podatkov in strojnih sredstev, kar neposredno določa kriptografske zahteve in obveznosti skrbništva nad ključi.

10.5 P13 - Politika razvrščanja in označevanja podatkov. Določa ravni razvrščanja (npr. zaupno, regulirano), ki sprožijo posebne zahteve za šifriranje med prenosom in pri hrambi.

10.6 P14 - Politika hrambe in odstranjevanja podatkov. Določa postopke za varno odstranjevanje šifriranih medijev za shranjevanje in kriptografskega ključnega materiala ob koncu življenjske dobe.

10.7 P30 - Politika odzivanja na incidente. Opredeljuje strategijo odziva organizacije na kompromitacijo ključev, neustrezno uporabo digitalnih potrdil ali sum na algoritemske ranljivosti, vključno s hitrim preklicem in poročanjem o kršitvah.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 - Operativno načrtovanje in kontrola: zahteva tehnične varnostne kontrole, vključno s kriptografskimi ukrepi, kot del operativnih varnostnih ukrepov.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrole 8.24, 8.25, 8: podajajo usmeritve za uvedbo ciljev kriptografskih kontrol, izbiro algoritmov, uveljavljanje protokolov in upravljanje življenjskega cikla digitalnih potrdil.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 - Vzpostavitev kriptografskih ključev: zagotavlja varno generiranje in izmenjavo ključev za šifriranje. P18 določa, kako morajo biti simetrični in asimetrični ključi generirani in izmenjani z uporabo odobrenih algoritmov in protokolov.

11.3.2 SC-13 - Kriptografska zaščita: zahteva uporabo kriptografije za zaščito zaupnosti in celovitosti informacij. P18 uveljavlja šifriranje pri hrambi in med prenosom na podlagi razvrstitve podatkov, pri čemer so standardi algoritmov usklajeni z NIST FIPS 140-3.

11.3.3 SC-17 - Digitalna potrdila infrastrukture javnih ključev (PKI): zahteva uvedbo PKI za podporo avtentikaciji in digitalnim podpisom. P18 opredeljuje uporabo PKI za varovanje komunikacij, sistemskih identitet in administrativnega dostopa.

11.3.4 SC-28, SC-28(1) - Zaščita informacij pri hrambi in med prenosom: zahteva šifriranje podatkov, ko so shranjeni ali preneseni prek nezaupanja vrednih omrežij. P18 določa uveljavljanje TLS, tunelov VPN, šifriranja celotnega diska in varnih načinov hrambe za občutljive podatke.

11.3.5 SC-12(3) - Generiranje simetričnih ključev za varno hrambo in distribucijo: osredotoča se na varno generiranje in ravnanje s simetričnimi ključi. P18 zahteva uporabo močnih generatorjev naključnih števil, politik menjave ključev in varnih repozitorijev ključev za kriptografske operacije.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 32 - Varnost obdelave: izrecno priporoča šifriranje kot ukrep za zmanjševanje tveganj za osebne podatke.

11.4.2 Uvodna izjava 83: poudarja šifriranje kot kontrolo za preprečevanje nepooblaščenega dostopa do podatkov.

11.4.3 Člena 33 in 34: učinkovito šifriranje lahko organizacijo izvzame iz obveznega prijavljanja kršitev.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(d): zahteva tehnične in organizacijske ukrepe, vključno s kriptografskimi zaščitami, za ohranjanje razpoložljivosti in celovitosti storitev.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 6(2)(d): finančni subjekti morajo zavarovati podatke, tudi z močno šifrirno zaščito kritičnih informacij.

11.6.2 Člen 11(1)(c): zahteva varne kontrole obdelave podatkov za ponudnike storitev tretjih oseb na področju IKT.

11.7 COBIT 2019

11.7.1 DSS05.01 - Zaščita informacijskih sredstev: zahteva uporabo šifriranja in upravljanja ključev za zaščito podatkov pred nepooblaščenim dostopom.

11.7.2 DSS06.06 - Upravljano varnostno testiranje: priporoča preverjanje skladnosti kriptografije kot del ocen ranljivosti.

11.7.3 MEA03 - Spremljanje, vrednotenje in presoja skladnosti: zahteva stalno zagotavljanje učinkovitosti kriptografskih kontrol.