					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P18					Naziv dokumenta: **Politika kriptografskih kontrola**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 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)	-
GDPR EU	Članak 32, članci 33–34, uvodna izjava 83	-
Direktiva EU NIS2	Članak 21(2)(d)	-
Uredba EU DORA	Članci 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA03	-

1. Svrha

1.1 Ova politika utvrđuje obvezne zahtjeve za sigurnu i usklađenu primjenu kriptografskih kontrola u cijeloj organizaciji radi osiguravanja povjerljivosti, cjelovitosti i autentičnosti osjetljivih i reguliranih informacija.

1.2 Primjena kriptografije temelj je povjerenja u operacije zaštite podataka, podupire sigurnu komunikaciju, provodi kontrolu pristupa i omogućuje usklađenost s regulatornim zahtjevima kroz učinkovite prakse šifriranja i upravljanja ključevima.

1.3 Ova je politika usklađena s normom ISO/IEC 27001:2022, točkom 8.1 i kontrolom 8.24 Priloga A te podupire pravne i operativne obveze iz članka 32 GDPR-a, članka 6(2)(d) Uredbe EU DORA i članka 21. Direktive EU NIS2. Također podupire ciljeve okvira COBIT 2019 u području sigurnosnih usluga i zaštite informacijskih resursa.

2. Opseg

2.1 Ova politika primjenjuje se na sve organizacijske jedinice, poslovne funkcije, osoblje i pružatelje usluga trećih strana koji sudjeluju u uporabi, administriranju ili implementaciji kriptografskih alata i metoda.

2.2 Obuhvaćena okruženja uključuju produkcijska, razvojna, testna, sigurnosno-kopijska i sustave za oporavak od katastrofe u kojima se osjetljivi podaci prenose, obrađuju ili pohranjuju.

2.3 Opseg obuhvaća sve kriptografske komponente i slučajeve uporabe, uključujući, ali ne ograničavajući se na:

2.3.1 simetrično i asimetrično šifriranje

2.3.2 digitalne potpise i certifikate

2.3.3 algoritme sažimanja

2.3.4 sigurno generiranje, distribuciju i uništavanje ključeva

2.3.5 Transport Layer Security (TLS), potpuno šifriranje diska i šifriranje na razini API-ja

2.3.6 sigurne elemente kao što su moduli hardverske sigurnosti (HSM), moduli pouzdane platforme (TPM) i sustavi za upravljanje ključevima (KMS)

2.4 Ova politika uređuje uporabu kriptografije u odnosu na:

2.4.1 podatke klasificirane kao Povjerljivo, Visoko povjerljivo ili Regulirano

2.4.2 autentifikaciju i provjeru digitalnog identiteta

2.4.3 sigurnu komunikaciju s vanjskim stranama

2.4.4 skrbništvo nad ključevima i mehanizme dvostruke kontrole

3. Ciljevi

3.1 Osigurati da se kriptografske tehnologije odabiru, odobravaju, implementiraju i održavaju u skladu s poslovnim rizikom, međunarodnim standardima i regulatornim zahtjevima.

3.2 Uspostaviti standardizirani okvir upravljanja kriptografskim uslugama, uključujući jasno utvrđene odgovornosti za implementaciju, provjeru i postupanje s iznimkama.

3.3 Spriječiti neovlaštenu uporabu, pogrešne konfiguracije ili zastarjelost kriptografskih algoritama i kontrola kroz formalni postupak odobravanja i pregleda.

3.4 Osigurati da su kriptografske kontrole ugrađene u fazu projektiranja sustava i da se redovito provjeravaju radi sprječavanja izloženosti podataka, kompromitacije ključeva ili degradacije protokola.

3.5 Osigurati upravljanje životnim ciklusom svih kriptografskih ključeva, uključujući generiranje, pohranu, uporabu, periodičnu zamjenu, opoziv i sigurno uništavanje.

3.6 Osigurati usklađenost s međunarodnim i regionalnim propisima koji zahtijevaju šifriranje i sigurno postupanje s podacima, uključujući GDPR, DORA, NIS2 i COBIT 2019.

4. Uloge i odgovornosti

4.1 Voditelj informacijske sigurnosti / glavni direktor informacijske sigurnosti (CISO)

4.1.1 Vlasnik je ove politike i osigurava njezinu usklađenost sa sustavom upravljanja informacijskom sigurnošću (ISMS) i kontrolom 8.24 Priloga A norme ISO/IEC 27001.

4.1.2 Odobrava uporabu kriptografskih algoritama i kontrola te osigurava poštivanje ove politike u cijeloj organizaciji.

4.2 Voditelj kriptografskih operacija / sigurnosni arhitekt

4.2.1 Upravlja svakodnevnim radom i administriranjem kriptografskih sustava.

4.2.2 Održava Popis odobrenih kriptografskih metoda (ACML) i Registar upravljanja ključevima.

4.2.3 Provodi preglede kriptografskog dizajna (CDR) i ocjenjuje nove kriptografske tehnologije.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ovu politiku moraju godišnje pregledati Voditelj informacijske sigurnosti i Voditelj kriptografskih operacija.

9.2 Okidači pregleda uključuju:

9.2.1 otkrivanje kriptografskih ranjivosti (npr. snižavanje sigurnosne razine algoritma, kvantni napadi)

9.2.2 regulatorne promjene koje zahtijevaju ažurirane standarde šifriranja

9.2.3 operativne nalaze ili nalaze revizije koji upućuju na nedostatke u politici

9.2.4 nadogradnje kriptografskih alata ili arhitekturne promjene

9.3 Ažuriranja moraju biti pod verzijskom kontrolom u Registru upravljanja dokumentima ISMS-a i priopćena:

9.3.1 svim administratorima s ulogama pristupa kriptografskim mehanizmima

9.3.2 razvojnim timovima i voditeljima DevSecOps-a

9.3.3 pružateljima usluga trećih strana koji imaju ugovorne obveze šifriranja

9.4 Tim za ISMS mora osigurati da su zamijenjene verzije arhivirane i da se više ne koriste kao referenca u operativnim postupcima.

10. Povezane politike i poveznice

10.1 P1 - Politika informacijske sigurnosti. Pruža temeljni okvir upravljanja za sve sigurnosne mjere, uključujući provedbu kriptografskih kontrola, zaštitu imovine i sigurnu komunikaciju.

10.2 P4 - Politika kontrole pristupa. Osigurava da je logički pristup kriptografskom materijalu i sustavima za upravljanje šifriranjem strogo ograničen na temelju načela najmanjih ovlasti i razdvajanja dužnosti.

10.3 P6 - Politika upravljanja rizicima. Podupire procjenu rizika kriptografskih kontrola i dokumentira strategiju obrade rizika za iznimke, zastarjelost algoritama ili scenarije kompromitacije ključeva.

10.4 P12 - Politika upravljanja imovinom. Propisuje klasifikaciju osjetljivih podataka i hardverske imovine, što izravno određuje kriptografske zahtjeve i obveze skrbništva nad ključevima.

10.5 P13 - Politika klasifikacije podataka i označavanja. Definira razine klasifikacije (npr. Povjerljivo, Regulirano) koje aktiviraju posebne zahtjeve za šifriranje u prijenosu i u mirovanju.

10.6 P14 - Politika zadržavanja i zbrinjavanja podataka. Utvrđuje postupke za sigurno zbrinjavanje šifriranih medija za pohranu i ključnog kriptografskog materijala na kraju životnog vijeka.

10.7 P30 - Politika odgovora na incidente. Utvrđuje strategiju odgovora organizacije za kompromitaciju ključeva, zlouporabu certifikata ili sumnju na algoritamske ranjivosti, uključujući brzi opoziv i prijavu povrede.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 - Operativno planiranje i kontrola: zahtijeva tehničke sigurnosne kontrole, uključujući kriptografske mjere, kao dio operativnih zaštitnih mjera.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrole 8.24, 8.25, 8: pružaju smjernice za implementaciju ciljeva kriptografskih kontrola, odabir algoritama, provedbu protokola i upravljanje životnim ciklusom certifikata.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 - Uspostava kriptografskih ključeva: osigurava sigurno generiranje i razmjenu ključeva za šifriranje. P18 definira kako se simetrični i asimetrični ključevi moraju generirati i razmjenjivati uporabom odobrenih algoritama i protokola.

11.3.2 SC-13 - Kriptografska zaštita: zahtijeva uporabu kriptografije radi zaštite povjerljivosti i cjelovitosti informacija. P18 propisuje šifriranje podataka u mirovanju i u prijenosu na temelju klasifikacije podataka, uz standarde algoritama usklađene s NIST FIPS 140-3.

11.3.3 SC-17 - Certifikati infrastrukture javnog ključa (PKI): zahtijeva implementaciju PKI-ja radi podrške autentifikaciji i digitalnim potpisima. P18 uređuje uporabu PKI-ja za zaštitu komunikacije, identiteta sustava i administrativnog pristupa.

11.3.4 SC-28, SC-28(1) - Zaštita informacija u mirovanju i u prijenosu: zahtijeva šifriranje podataka kada su pohranjeni ili se prenose preko nepouzdanih mreža. P18 propisuje provedbu TLS-a, VPN tunela, potpunog šifriranja diska i sigurnih metoda pohrane za osjetljive podatke.

11.3.5 SC-12(3) - Generiranje simetričnih ključeva za sigurnu pohranu i distribuciju: usmjereno je na sigurno generiranje i rukovanje simetričnim ključevima. P18 zahtijeva uporabu snažnih generatora slučajnih brojeva, politike periodične zamjene ključeva i sigurna spremišta ključeva za kriptografske operacije.

11.4 GDPR EU (2016/679)

11.4.1 Članak 32 - Sigurnost obrade: izričito preporučuje šifriranje kao mjeru za smanjenje rizika za osobne podatke.

11.4.2 Uvodna izjava 83: naglašava šifriranje kao kontrolu za sprječavanje neovlaštenog pristupa podacima.

11.4.3 Članci 33 i 34: šifriranje može osloboditi organizacije od obveze prijave povrede ako je učinkovito.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(d): zahtijeva tehničke i organizacijske mjere, uključujući kriptografsku zaštitu, radi održavanja dostupnosti i cjelovitosti usluga.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 6(2)(d): financijske institucije moraju osigurati zaštitu podataka, uključujući primjenu snažnog šifriranja kritičnih informacija.

11.6.2 Članak 11(1)(c): zahtijeva sigurne kontrole obrade podataka za pružatelje IKT usluga trećih strana.

11.7 COBIT 2019

11.7.1 DSS05.01 - Zaštita informacijskih resursa: zahtijeva uporabu šifriranja i upravljanja ključevima radi zaštite podataka od neovlaštenog pristupa.

11.7.2 DSS06.06 - Upravljano sigurnosno testiranje: preporučuje provjeru usklađenosti kriptografije kao dio procjena ranjivosti.

11.7.3 MEA03 - Praćenje, vrednovanje i procjena usklađenosti: zahtijeva kontinuirano osiguranje djelotvornosti kriptografskih kontrola.