					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P18S					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	
NIST SP 800-53 Rev. 5	SC-12 do SC-17	
Direktiva EU NIS2	Članci 21(2)(d), 21(2)(e)	
Uredba EU DORA	Članci 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
GDPR EU	Članci 32(1)(a), 34	

1. Svrha

1.1 Ova politika utvrđuje obvezne zahtjeve za primjenu šifriranja i kriptografskih kontrola radi zaštite povjerljivosti, cjelovitosti i autentičnosti poslovnih i osobnih podataka.

1.2 Ovom se politikom osigurava da se kriptografski alati primjenjuju primjereno u sustavima, uređajima i uslugama u oblaku u okruženju malog poduzeća.

1.3 Ova politika izravno podupire certifikaciju prema normi ISO/IEC 27001:2022 te pomaže organizaciji ispuniti pravne obveze koje proizlaze iz GDPR-a EU, Direktive EU NIS2 i Uredbe EU DORA.

1.4 Kriptografske kontrole obuhvaćene ovom politikom uključuju šifriranje podataka, upravljanje certifikatima, sigurno rukovanje ključevima i šifrirane sigurnosne kopije.

2. Područje primjene

2.1 Ova politika primjenjuje se na:

2.1.1 sve zaposlenike, ugovorne izvođače i treće strane koje postupaju s podacima društva

2.1.2 sve poslovne sustave, krajnje uređaje i platforme u oblaku koji se koriste za pohranu, prijenos ili pristup povjerljivim informacijama

2.1.3 sve osobne, financijske, pravne ili osjetljive zapise klasificirane u skladu s politikom klasifikacije podataka organizacije

2.1.4 sve kriptografske kontrole, uključujući metode šifriranja, ključeve, lozinke, certifikate i sigurnosne module

2.2 Ova politika obuhvaća podatke u mirovanju, podatke u prijenosu i podatke u uporabi. Također uređuje šifriranje koje se primjenjuje na sigurnosne kopije, e-poštu, vanjske prijenose podataka i javno dostupne internetske stranice.

3. Ciljevi

3.1 Osigurati da su osjetljivi i regulirani podaci u svakom trenutku zaštićeni odgovarajućim kriptografskim mjerama

3.2 Utvrditi odgovornosti za odabir alata za šifriranje, njihovu konfiguraciju i upravljanje ključevima

3.3 Spriječiti neovlašteni pristup, neovlaštenu izmjenu ili curenje podataka primjenom sigurnih kontrola prijenosa i pohrane

3.4 Ispuniti pravne i regulatorne zahtjeve koji propisuju šifriranje osobnih i poslovnih podataka

3.5 Održavati operativnu sigurnost i dostupnost učinkovitim upravljanjem certifikatima i kriptografskim ključevima

4. Uloge i odgovornosti

4.1 glavni direktor (GM)

4.1.1 odobrava ovu politiku i osigurava provedbu kriptografskih zahtjeva

4.1.2 pregledava iznimke, obavijesti o povredama i usklađenost dobavljača sa zahtjevima šifriranja

4.1.3 provjerava ispunjavaju li eksternalizirane usluge ili usluge u oblaku standarde šifriranja

4.2 pružatelj IT podrške / interni IT administrator

4.2.1 uspostavlja i održava rješenja za šifriranje, primjerice šifriranje cijelog diska, SSL certifikate i VPN veze

4.2.2 upravlja životnim ciklusom kriptografskih ključeva i alatima za sigurnu pohranu

4.2.3 konfigurira i nadzire šifriranje radi zaštite sigurnosnih kopija, internetskih stranica i uređaja

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

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled

9.1.1 Ovu politiku mora pregledati najmanje jednom godišnje glavni direktor u koordinaciji s pružateljem IT podrške i koordinatorom za privatnost.

9.2 Okidači za izvanredni pregled

9.2.1 pregled se mora provesti i ako:

9.2.1.1 dođe do promjene kriptografskih standarda ili protokola, primjerice povlačenja algoritma iz uporabe

9.2.1.2 se uvedu novi sustavi ili usluge u oblaku

9.2.1.3 povreda ili incident uključuje kompromitirani ključ ili certifikat

9.2.1.4 pravna ili regulatorna ažuriranja utječu na zahtjeve za šifriranje

9.3 Upravljanje verzijama i komunikacija

9.3.1 sve promjene politike moraju biti dokumentirane u zapisniku o upravljanju verzijama

9.3.2 osoblje mora biti obaviješteno o ažuriranjima, a prethodne verzije arhivirane

9.3.3 najnovija odobrena verzija mora biti pohranjena u središnjem repozitoriju politika

10. Povezane politike i poveznice

10.1 Ova politika mora se primjenjivati zajedno sa sljedećim SME politikama:

10.1.1 P12S – Politika upravljanja imovinom: osigurava da se šifriranje primjenjuje na klasificiranu imovinu tijekom pohrane, prijenosa i zbrinjavanja.

10.1.2 P14S – Politika zadržavanja i zbrinjavanja podataka: utvrđuje razdoblja čuvanja i zahtijeva šifriranu pohranu podataka do njihova sigurnog brisanja.

10.1.3 P17S – Politika zaštite podataka i privatnosti: usklađuje šifriranje s načelima zaštite podataka i regulatornim zahtjevima iz članka 32. GDPR-a.

10.1.4 P22S – Politika revizijskog zapisivanja i praćenja: zahtijeva bilježenje uporabe ključeva, neuspjeha šifriranja i isteka certifikata za potrebe revizije.

10.1.5 P30S – Politika odgovora na incidente: detaljno uređuje eskalaciju, ograničavanje i postupke obavješćivanja kada šifriranje zakaže ili su ključevi kompromitirani.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8 – zahtijeva provedbu operativnih kontrola, uključujući šifriranje, radi upravljanja sigurnosnim rizicima.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.24 – opisuje zahtjeve za primjenu šifriranja radi osiguranja povjerljivosti i cjelovitosti.

11.2.2 Kontrola 8.25 – utvrđuje zahtjeve za sigurno upravljanje kriptografskim ključevima i certifikatima.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – utvrđuje zahtjeve za uspostavu i provjeru kriptografskih ključeva.

11.3.2 SC-13 – definira standarde za generiranje kriptografskih ključeva.

11.3.3 SC-17 – obuhvaća infrastrukturu javnog ključa (PKI) i upravljanje životnim ciklusom certifikata.

11.3.4 SC-28 – zahtijeva šifriranje podataka u mirovanju.

11.3.5 SC-12 do SC-17 (skupina) – osigurava pravilnu provedbu kriptografskih zaštitnih mjera u svim sustavima.

11.4 GDPR EU

11.4.1 Članak 32(1)(a) – zahtijeva da organizacije provedu tehničke mjere kao što je šifriranje radi osiguranja povjerljivosti podataka.

11.4.2 Članak 34 – propisuje da šifriranje može osloboditi organizaciju obveze obavješćivanja o povredi ako su podaci bili nerazumljivi neovlaštenim osobama.

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(d) – zahtijeva učinkovito šifriranje radi zaštite sustava i komunikacija.

11.5.2 Članak 21(2)(e) – naglašava zaštitu podataka i ublažavanje kibernetičkih prijetnji primjenom šifriranja.

11.6 Uredba EU DORA

11.6.1 Članak 6(2)(d) – zahtijeva da IKT sustavi održavaju sigurne komunikacijske kanale i šifriranje.

11.6.2 Članak 9(2)(f) – obvezuje financijske subjekte na primjenu snažnog šifriranja radi zaštite digitalnih komunikacija i razmjene podataka.

11.7 COBIT 2019

11.7.1 DSS05.01 – nalaže zaštitu osjetljivih informacija primjenom šifriranja i kriptografskih protokola.

11.7.2 APO13.02 – zahtijeva učinkovitu provedbu sigurnosnih kontrola, uključujući kriptografske zaštitne mjere, kao dio planiranja informacijske sigurnosti.