					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P18S					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	Kontroli 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 do SC-17	
Direktiva EU NIS2	Člena 21(2)(d), 21(2)(e)	
Uredba EU DORA	Člena 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
Uredba EU GDPR	Člena 32(1)(a), 34	

1. Namen

1.1 Ta politika določa obvezne zahteve za uporabo šifriranja in kriptografskih kontrol za varovanje zaupnosti, celovitosti in avtentičnosti poslovnih podatkov in osebnih podatkov.

1.2 Zagotavlja, da se kriptografska orodja ustrezno uporabljajo v sistemih, napravah in oblačnih storitvah v okolju malega podjetja.

1.3 Ta politika neposredno podpira certificiranje po standardu ISO/IEC 27001:2022 ter organizaciji pomaga izpolnjevati pravne obveznosti iz Uredbe EU GDPR, Direktive EU NIS2 in Uredbe EU DORA.

1.4 Kriptografske kontrole, ki jih zajema ta politika, vključujejo šifriranje podatkov, upravljanje digitalnih potrdil, varno ravnanje s ključi in šifrirane varnostne kopije.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse zaposlene, pogodbene izvajalce in tretje osebe, ki obdelujejo podatke podjetja,

2.1.2 vse poslovne sisteme, končne naprave in oblačne platforme, ki se uporabljajo za hrambo, prenos ali dostop do zaupnih informacij,

2.1.3 vse osebne, finančne, pravne ali občutljive evidence, razvrščene v skladu s politiko razvrščanja podatkov organizacije,

2.1.4 vse kriptografske kontrole, vključno z metodami šifriranja, ključi, gesli, digitalnimi potrdili in varnostnimi moduli.

2.2 Politika zajema podatke v mirovanju, podatke med prenosom in podatke med uporabo. Ureja tudi šifriranje, ki se uporablja za varnostne kopije, elektronsko pošto, zunanje prenose podatkov in javno dostopna spletna mesta.

3. Cilji

3.1 Zagotoviti, da so občutljivi in regulirani podatki ves čas zaščiteni z ustreznimi kriptografskimi ukrepi.

3.2 Opredeliti odgovornosti za izbor orodij za šifriranje, njihovo konfiguracijo in upravljanje ključev.

3.3 Preprečiti nepooblaščen dostop, posege v podatke ali uhajanje podatkov z uvedbo ustreznih kontrol prenosa in hrambe.

3.4 Zagotoviti skladnost s pravnimi in regulativnimi zahtevami, ki zahtevajo šifriranje osebnih in poslovnih podatkov.

3.5 Ohranjati operativno varnost in razpoložljivost z učinkovitim upravljanjem digitalnih potrdil in kriptografskih ključev.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 odobri to politiko in zagotovi izvajanje kriptografskih zahtev,

4.1.2 pregleduje izjeme, obvestila o kršitvah in skladnost dobaviteljev s pogodbenimi določili o šifriranju,

4.1.3 zagotovi, da zunanje izvajane storitve ali oblačne storitve izpolnjujejo zahteve glede šifriranja.

4.2 Zunanji izvajalec IT-podpore / notranji skrbnik IT

4.2.1 uvede in vzdržuje rešitve za šifriranje (npr. šifriranje celotnega diska, potrdila SSL/TLS, VPN),

4.2.2 upravlja življenjski cikel kriptografskih ključev in orodja za varno hrambo,

4.2.3 konfigurira in spremlja šifriranje za zaščito varnostnih kopij, spletnih mest in naprav.

[... 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 Letni pregled

9.1.1 To politiko mora najmanj enkrat letno pregledati generalni direktor v sodelovanju z zunanjim izvajalcem IT-podpore in koordinatorjem za zasebnost.

9.2 Sprožilci za vmesni pregled

9.2.1 Pregledi se morajo izvesti tudi, če:

9.2.1.1 se spremenijo kriptografski standardi ali protokoli (npr. opustitev algoritma),

9.2.1.2 se uvedejo novi sistemi ali oblačne storitve,

9.2.1.3 kršitev ali incident vključuje kompromitiran ključ ali digitalno potrdilo,

9.2.1.4 pravne ali regulativne spremembe vplivajo na zahteve glede šifriranja.

9.3 Nadzor različic in obveščanje

9.3.1 Vse spremembe politike morajo biti dokumentirane v evidenci nadzora različic.

9.3.2 Zaposlene je treba obvestiti o posodobitvah, prejšnje različice pa arhivirati.

9.3.3 Zadnja odobrena različica mora biti shranjena v osrednjem repozitoriju politik.

10. Povezane politike in povezave

10.1 Ta politika se mora uporabljati skupaj z naslednjimi SME-politikami:

10.1.1 P12S – Politika upravljanja sredstev: zagotavlja, da se šifriranje uporablja za razvrščena sredstva med hrambo, prenosom in odstranjevanjem.

10.1.2 P14S – Politika hrambe podatkov: določa obdobja hrambe in zahteva šifrirano hrambo podatkov do njihovega varnega izbrisa.

10.1.3 P17S – Politika varstva podatkov in zasebnosti: usklajuje šifriranje z načeli varstva podatkov in regulativnimi pričakovanji po členu 32 Uredbe EU GDPR.

10.1.4 P22S – Politika beleženja dnevnikov in spremljanja: zahteva beleženje uporabe ključev, odpovedi šifriranja in poteka veljavnosti digitalnih potrdil za namene presoje.

10.1.5 P30S – Politika odzivanja na incidente: podrobno določa postopke eskalacije, zajezitve in obveščanja, ko šifriranje odpove ali so ključi kompromitirani.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – Zahteva uvedbo operativnih kontrol, vključno s šifriranjem, za obvladovanje varnostnih tveganj.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.24 – Opisuje zahteve za uporabo šifriranja za zagotavljanje zaupnosti in celovitosti.

11.2.2 Kontrola 8.25 – Določa varno upravljanje kriptografskih ključev in digitalnih potrdil.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Določa zahteve za vzpostavitev in preverjanje kriptografskih ključev.

11.3.2 SC-13 – Opredeljuje standarde za generiranje kriptografskih ključev.

11.3.3 SC-17 – Obravnava infrastrukturo javnih ključev (PKI) in upravljanje življenjskega cikla digitalnih potrdil.

11.3.4 SC-28 – Zahteva šifriranje podatkov v mirovanju.

11.3.5 SC-12 do SC-17 (družina kontrol) – Zagotavlja, da so kriptografske zaščite ustrezno uvedene v vseh sistemih.

11.4 Uredba EU GDPR

11.4.1 Člen 32(1)(a) – Zahteva, da organizacije uvedejo tehnične ukrepe, kot je šifriranje, za zagotavljanje zaupnosti podatkov.

11.4.2 Člen 34 – Določa, da so organizacije lahko oproščene obveščanja o kršitvi, če so bili podatki za nepooblaščene osebe nerazumljivi.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(d) – Zahteva učinkovito šifriranje za zaščito sistemov in komunikacij.

11.5.2 Člen 21(2)(e) – Poudarja varstvo podatkov in zmanjševanje kibernetskih groženj s šifriranjem.

11.6 Uredba EU DORA

11.6.1 Člen 6(2)(d) – Zahteva, da sistemi IKT vzdržujejo varne komunikacijske kanale in šifriranje.

11.6.2 Člen 9(2)(f) – Finančnim subjektom nalaga uporabo močnega šifriranja za zaščito digitalnih komunikacij in izmenjave podatkov.

11.7 COBIT 2019

11.7.1 DSS05.01 – Zahteva zaščito občutljivih informacij s šifriranjem in kriptografskimi protokoli.

11.7.2 APO13.02 – Zahteva učinkovito uvedbo varnostnih kontrol, vključno s kriptografskimi zaščitnimi ukrepi, kot del politike varnostnega načrtovanja.