

0. Povijest promjena dokumenta

Verzija	Datum	Točka	Opis promjene
1.0	30.04.2025.		Inicijalni dokument

1. Uvod

Ova politika osigurava jasne smjernice za sigurno korištenje kriptografskih kontrola u poduzeću, što je ključno za zaštitu osjetljivih informacija od neovlaštenog pristupa i manipulacije.

2. Namjena

Ova politika definira smjernice za uporabu kriptografskih kontrola u poduzeću kako bi se osigurala zaštita povjerljivosti, integriteta i dostupnosti osjetljivih informacija te zaštitili informacijski sustavi od neovlaštenog pristupa i napada.

3. Područje primjene

Ova politika se primjenjuje na sve informacijske sustave, aplikacije i procese koji koriste kriptografske algoritme i mehanizme unutar poduzeća.

Odgovornost za provedbu ove politike leži na svim zaposlenicima koji koriste kriptografske kontrole u okviru svojih radnih aktivnosti.

Grupa za sistemsku administraciju ima posebnu odgovornost za upravljanje kriptografskim ključevima, certifikatima i infrastrukturom.

4. Politika

4.1. Opći principi

4.1.1. Primjena kriptografije

- Kriptografija se primjenjuje tamo gdje je to potrebno za zaštitu osjetljivih podataka u prijenosu ili pohrani.
- Kriptografski algoritmi i protokoli moraju biti odabrani i implementirani u skladu s najboljim praksama i standardima.

4.1.2. Upravljanje ključevima

- Ključevi moraju biti generirani, pohranjeni, upravljani i distribuirani na siguran način.
- Pristup kriptografskim ključevima ograničen je samo na ovlaštene osobe.

4.1.3. Certifikati

- Certifikati se koriste za potvrdu identiteta entiteta i osiguranje povjerenja u komunikaciji.
- Certifikati moraju biti izdani od pouzdanih autoriteta za izdavanje certifikata (CA).

4.1.4. Redovito ažuriranje

- Kriptografske kontrole, algoritmi i ključevi redovito se ažuriraju i revidiraju u skladu s promjenama tehnologije i sigurnosnih standarda

5. Korištenje kriptografije

Kriptografija se primjenjuje prilikom prijenosa osjetljivih informacija preko nezaštićenih mreža, kao i za šifriranje pohranjenih podataka na mobilnim uređajima, serverima i drugim medijima.

6. Obuka

Svi zaposlenici moraju biti obučeni o pravilnoj uporabi kriptografskih alata i tehnika. Redovito se provode edukacije o sigurnosti informacija kako bi se osigurala svijest o važnosti kriptografije i njezine uloge u zaštiti podataka.

7. Kontrola

Svi kriptografski algoritmi i mehanizmi moraju biti podvrgnuti redovitim sigurnosnim revizijama i provjerama kako bi se osigurala njihova sigurnost i pouzdanost.

8. Praćenje i pregled

Implementacija ove politike redovito će se pratiti, pregledavati i ažurirati kako bi se osigurala usklađenost s najnovijim sigurnosnim standardima i praksama.

9. Poštivanje politike

Za kršenje ove politike primjenjuju se disciplinske mjere propisane internim aktima.

	Ime i prezime:	Funkcija:	Datum:	Potpis:
Odobrio:	Luka Šikić	Direktor	30.04.2025.	<i>Luka Šikić</i>