



POLITIKA INFORMACIJSKE SIGURNOSTI I KIBERNETIČKE OTPORNOSTI

Koprivničko-križevačka županija, kao javnopravno tijelo, u svom svakodnevnom radu koristi informacijske sustave i tehnologije za pružanje usluga građanima, gospodarstvu i institucijama. Sigurnost informacija i kibernetička otpornost predstavljaju ključne elemente povjerenja u sustav javne uprave te preduvjet za kontinuirano i učinkovito djelovanje.

Ova politika definira temeljna načela i smjernice za uspostavu, primjenu i održavanje sustava informacijske sigurnosti i kibernetičke otpornosti, u skladu sa zahtjevima:

- ISO/IEC 27001:2022 – Sustav upravljanja informacijskom sigurnošću
- Direktiva (EU) 2022/2555 (NIS2)
- Zakon o kibernetičkoj sigurnosti Republike Hrvatske.

Svrha politike:

Svrha ove politike je uspostaviti jedinstveni okvir za upravljanje informacijskom sigurnošću i kibernetičkom otpornošću u Koprivničko-križevačkoj županiji.

Ciljevi ove politike su:

- Osigurati da su informacije pod nadzorom Županije zaštićene od neovlaštenog pristupa, izmjena, gubitka ili uništenja
- Upravlјati informacijskim i kibernetičkim rizicima na strukturiran i sustavan način
- Uspostaviti okvir za upravljanje sigurnosnim incidentima i kibernetičkim prijetnjama
- Osigurati usklađenost sa zakonskim i regulatornim zahtjevima, uključujući NIS2
- Ojačati otpornost informacijskih sustava i digitalnih usluga koje pruža Županija
- Povećati razinu znanja i svijesti svih dionika, osobito upravljačke strukture
- Osigurati usklađenost s preporukama ENISA-e i smjernicama Nacionalnog centra za kibernetičku sigurnost.

Područje primjene:

Ova politika primjenjuje se na sve zaposlenike, vanjske suradnike, ugovorne partnere i druge osobe koje koriste ili imaju pristup informacijskim resursima Županije. Obuhvaća sve informacijske sustave, podatke, aplikacije, mrežnu i komunikacijsku infrastrukturu pod upravom Županije.

Načela informacijske sigurnosti:

Županija se obvezuje provoditi sljedeća načela:

- **Povjerljivost** – Informacije su dostupne isključivo ovlaštenim osobama
- **Cjelovitost** – Informacije su točne i zaštićene od neovlaštene izmjene
- **Dostupnost** – Informacije i usluge dostupne su u potrebnom trenutku
- **Autentičnost** – Identitet korisnika i izvora informacija mora biti potvrđen
- **Neporecivost** – Moguće je dokazati tko je pristupio informacijama ili ih mijenjao
- **Minimizacija podataka** – Obrada podataka ograničava se na ono što je nužno
- **Privatnost po dizajnu i po zadanom** – Zaštita je osigurana tehničkim i organizacijskim mjerama od samog početka dizajna sustava.

Obveze i odgovornosti:

- **Izvršna vlast:** Odgovorna za donošenje, preispitivanje i podršku provedbi ove politike, te osiguravanje potrebnih resursa.
- **Službenik za informacijsku sigurnost (CISO):** Koordinira provedbu sigurnosnih mjera, izvještava o statusu sigurnosti, vodi procjene rizika i planira odgovore na incidente.
Ime i prezime: Verica Ujlaki
- **Osoba zadužena za NIS2 usklađenost:** Nadgleda primjenu specifičnih NIS2 zahtjeva, komunicira s nadležnim tijelima i koordinira izvještavanje.
Ime i prezime: Nino Šegerc
- **Zaposlenici:** Obvezni su se pridržavati politike, sudjelovati u edukaciji te odmah prijaviti sve sumnjive aktivnosti ili incidente.
- **Vanjski suradnici i dobavljači:** Obavezni su poštivati uvjete iz ugovora i internih procedura u pogledu sigurnosti te prijavljivati incidente.

Upravljanje rizicima i sigurnosni incidenti:

Županija kontinuirano provodi procjenu kibernetičkih i informacijskih rizika te određuje mjere zaštite prema načelima upravljanja rizicima.

Svi sigurnosni incidenti (npr. napadi, gubitak podataka, kompromitacije sustava) moraju se odmah prijaviti CISO-u. Incidenti se obrađuju u skladu s rokovima propisanim NIS2 direktivom::

- **Preliminarna prijava** – unutar 24 sata
- **Detaljna prijava** – unutar 72 sata

- **Konačno izvješće** – unutar 1 mjeseca.

Kontinuitet poslovanja i oporavak od katastrofe

Razvijaju se i redovito testiraju planovi kontinuiteta poslovanja i oporavka od katastrofa, s ciljem održavanja pružanja ključnih usluga u slučaju incidenata.

Edukacija i podizanje svijesti:

Redovito će se provoditi programi edukacije i osvještavanja zaposlenika i vanjskih suradnika s naglaskom na kibernetičke prijetnje, odgovornosti i postupanje u kriznim situacijama. Poseban fokus stavlja se na edukaciju upravljačke strukture.

Praćenje, evaluacija i poboljšavanje:

Učinkovitost ove politike nadzire se kroz:

- interne i vanjske audite
- ocjene izvršne vlasti
- nadzor nad rizicima i incidentima
- pokazatelje učinka sigurnosnih mjera

Politika se redovito preispituje i poboljšava na temelju promjena u prijetnjama, zakonodavstvu i organizacijskim ciljevima.

KLASA: 650-01/25-01/3

URBROJ: 2137-08/02-26-43

Koprivnica, 8. srpnja 2026.

ŽUPAN
Tomislav Golubić

