Na temelju članka 2., Priloga II., mjere 1., podmjere 1.1. Uredbe o kibernetičkoj sigurnosti („Narodne novine" broj 135/24), a u vezi s člankom 29. stavcima 1. i 2. Zakona o kibernetičkoj sigurnosti („Narodne novine" broj 14/24), te članka 52. stavka 1. točke 23. Statuta Primorsko-goranske županije („Službene novine" broj 23/09, 9/13, 5/18, 2/20 i 4/21) i članka 25. stavka 1. Poslovnika o radu Župana Primorsko-goranske županije („Službene novine" broj 23/14, 16/15, 3/16 i 16/21), župan Primorsko-goranske županije, 26. ožujka 2026. godine, donio je

STRATEGIJU UPRAVLJANJA MJERAMA KIBERNETIČKE SIGURNOSTI PRIMORSKO-GORANSKE ŽUPANIJE

DIO PRVI
OPĆE ODREDBE

Predmet i svrha

Članak 1.

Ovom Strategijom određuje se okvir za primjenu i upravljanje mjerama kibernetičke sigurnosti u Primorsko-goranskoj županiji (dalje u tekstu: Županija) sukladno Zakonu o kibernetičkoj sigurnosti („Narodne novine" br. 14/24) i Uredbi o kibernetičkoj sigurnosti („Narodne novine" br. 135/24, dalje u tekstu zajedno: ZUKS).

Ovom se Strategijom definiraju i opisuju ciljevi kibernetičke sigurnosti Županije, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će Županija primjenjivati, organizacijski sustav, uloge, odgovornosti i obveze te procesi upravljanja kibernetičkom sigurnošću.

Svrha ove Strategije je osigurati visoku razinu kibernetičke sigurnosti mrežnih i informacijskih sustava Županije te njihovu usklađenost s općim poslovnim ciljevima i strateškim prioritetima Županije.

Područje primjene

Članak 2.

Županija je sukladno ZUKS-u kategorizirana kao važan subjekt i obvezna je provoditi mjere kibernetičke sigurnosti napredne razine.

Ova Strategija primjenjuje se na:

1. sva upravna tijela i Ured unutarnje revizije Županije te njihove službenike i namještenike,
2. mrežne i informacijske sustave u nadležnosti Županije,
3. vanjske suradnike, isporučitelje opreme, izvršitelje usluga te ostale treće strane koji imaju pristup mrežnim i informacijskim resursima u nadležnosti Županije.

Načela kibernetičke sigurnosti

Članak 3.

Županija se u upravljanju kibernetičkom sigurnošću vodi sljedećim načelima:

1. Načelo povjerljivosti – pristup podacima imaju samo ovlaštene osobe.
2. Načelo cjelovitosti – zaštita točnosti i kompletnosti informacija i metoda obrade.

3. Načelo dostupnosti – osiguranje pristupa informacijama i uslugama ovlaštenim korisnicima kada je to potrebno.
4. Načelo procjene rizika – sigurnosne mjere temelje se na redovitoj procjeni rizika.
5. Načelo kontinuiranog poboljšanja – primjenjuje se redovita evaluacija i unaprjeđenje sigurnosnih kontrola.

DIO DRUGI
CILJEVI KIBERNETIČKE SIGURNOSTI

Glavni ciljevi

Članak 4.

Glavni ciljevi Županije u području kibernetičke sigurnosti uključuju sljedeća područja:

1. Zaštitu ključne imovine – osiguravanje zaštite osobnih podataka i poslovnih informacija od neovlaštenog pristupa, gubitka ili krađe.
2. Usklađenost s regulativom – potpuna implementacija zahtjeva ZUKS-a za važne subjekte.
3. Otpornost i kontinuitet – minimiziranje prekida u radu ključnih servisa i osiguravanje brzog oporavka u slučaju incidenta.
4. Stvaranje kibernetičke kulture – podizanje svijesti i kompetencija svih službenika i namještenika kroz redovite edukacije i treninge.
5. Osiguranje lanca opskrbe – upravljanje rizicima koji proizlaze iz odnosa s vanjskim dobavljačima i pružateljima usluga.

DIO TREĆI
UPRAVLJANJE KIBERNETIČKIM SIGURNOSNIM RIZICIMA

Mjere upravljanja kibernetičkim sigurnosnim rizicima

Članak 5.

Temeljem ZUKS-a, Županija će provoditi sljedeće mjere upravljanja sigurnosnim rizicima:

1. Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima
2. Upravljanje programskom i sklopovskom imovinom
3. Upravljanje rizicima
4. Sigurnost ljudskih potencijala i digitalnih identiteta
5. Osnovne prakse kibernetičke higijene
6. Osiguravanje kibernetičke sigurnosti mreže
7. Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima
8. Sigurnost lanca opskrbe
9. Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava
10. Kriptografija
11. Postupanje s incidentima
12. Kontinuitet poslovanja i upravljanje kibernetičkim krizama
13. Fizička sigurnost

DIO ČETVRTI
ORGANIZACIJSKI SUSTAV, RASPODJELA ULOGA, ODGOVORNOSTI I OBVEZA

Uloge i odgovornosti

Članak 6.

Organizacijski sustav upravljanja kibernetičkom sigurnošću u Županiji čine:

1. Upravljačko tijelo – Župan koji:
   a) je odgovoran za provedbu i upravljanje mjerama kibernetičke sigurnosti Županije,
   b) odobrava mjere upravljanja kibernetičkim sigurnosnim rizicima koje će Županija primjenjivati i osigurava sve potrebne resurse te nadzire provedbu mjera,
   c) pohađa odgovarajuća osposobljavanja te službenicima i namještenicima Županije omogućava pohađanje odgovarajućih osposobljavanja sukladno ZUKS-u,
   d) donosi odluku o imenovanju osobe operativno odgovorne za kibernetičku sigurnost,
   e) donosi odluku o osnivanju Županijskog tima za zaprimanje prijava i odgovor na incidente (dalje u tekstu: Županijski CERT).

2. Osoba operativno odgovorna za kibernetičku sigurnost koja:
   a) nadgleda i koordinira sve kibernetičke sigurnosne mjere,
   b) koordinira tehničku implementaciju mjera,
   c) koordinira postupanje s incidentima,
   d) jednom godišnje, a po potrebi i češće, izvještava Župana o stanju kibernetičke sigurnosti.

3. Županijski CERT, u koji se obavezno imenuju administratori, korisnici nacionalne platforme i osoba operativno odgovorna za kibernetičku sigurnost, a u okviru kojeg se obavlja:
   a) administriranje računa Županije na nacionalnoj platformi (putem administratora),
   b) analiza i kategorizacija incidenata,
   c) obavještavanje o značajnim incidentima na nacionalnoj platformi (putem korisnika nacionalne platforme),
   d) koordinacija postupanja u slučaju incidenata s vanjskim davateljem usluge,
   e) koordinacija poslova vezanih uz forenziku i oporavak sustava s vanjskim davateljem usluge,
   f) analiza primijenjenih mjera,
   g) izvještavanje Župana o statusu incidenata i poduzetim radnjama,
   h) priprema i podnošenje privremenog izvješća o značajnom incidentu, izvješća o napretku i završnog izvješća o značajnom incidentu nadležnom tijelu sukladno ZUKS-u.

4. Vlasnici poslovnih procesa (pročelnici upravnih tijela i voditelj unutarnje revizije Županije) koji:
   a) sudjeluju u identifikaciji rizika unutar svojih upravnih tijela, odnosno Ureda unutarnje revizije i nadležnosti,

b) su odgovorni za primjenu odredbi ZUKS-a u upravnom tijelu, odnosno Uredu unutarnje revizije kojim rukovode,
c) osiguravaju da se službenici i namještenici u njihovim upravnim tijelima pridržavaju propisanih mjera kibernetičke sigurnosti.

5. Službenici i namještenici Županije, koji su dužni:
   a) pridržavati se propisanih mjera kibernetičke sigurnosti,
   b) najmanje jednom godišnje, a po potrebi i češće, pohađati edukacije,
   c) bez odgode prijaviti svaki sumnjivi događaj ili incident.

DIO PETI
PROCESI UPRAVLJANJA KIBERNETIČKOM SIGURNOŠĆU

Upravljanje rizicima i imovinom

Članak 7.

Županija provodi sustavnu procjenu kibernetičkih rizika najmanje jednom godišnje, a uvijek prilikom značajnih promjena u sustavu ili značajnih incidenata.

Županija vodi i redovito ažurira registar identificiranih kibernetičkih rizika.

Županija vodi i redovito ažurira inventar kritične i ostale programske i sklopovske imovine.

Upravljanje incidentima

Članak 8.

Županijski CERT provodi analizu i kategorizaciju incidenata te sanaciju incidenata u suradnji s vanjskim davateljem usluge.

Svaki službenik i namještenik te vanjski suradnik (izravni dobavljač i pružatelj usluge) dužan je bez odgode prijaviti svaki sumnjivi događaj ili incident.

Značajni incidenti prijavljuju se putem nacionalne platforme nadležnom tijelu sukladno ZUKS-u.

Županija vodi i redovito ažurira evidenciju incidenata.

Kontinuitet poslovanja

Članak 9.

Upravni odjel u čijoj je nadležnosti obavljanje informatičkih poslova izrađuje planove kontinuiteta poslovanja i oporavka za kritične sustave.

Planovi iz stavka 1. ovoga članka testiraju se najmanje jednom godišnje kroz simulacijske vježbe, a sigurnosne kopije se provjeravaju najmanje jednom kvartalno.

Nadzor i revizija

Članak 10.

Županija je dužna kontinuirano provoditi praćenje sigurnosnih metrika.

Županija je dužna najmanje jednom godišnje provesti provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenu njihove djelotvornosti.

Županija je dužna najmanje jednom u dvije godine provesti samoprocjenu kibernetičke sigurnosti.

DIO ŠESTI
ZAVRŠNE ODREDBE

Izvještavanje i ažuriranje

Članak 11.

Osoba operativno odgovorna za kibernetičku sigurnost podnosi Županu godišnje izvješće o stanju kibernetičke sigurnosti najkasnije do 31. ožujka za prethodnu kalendarsku godinu.

Ova Strategija i prateće politike revidirat će se najmanje jednom godišnje ili po potrebi, radi usklađivanja s novim prijetnjama i regulatornim promjenama.

Uspostava evidencija i donošenje planova

Članak 12.

Župan će u roku od 60 dana od dana stupanja na snagu ove Strategije donijeti odluku o imenovanju osobe iz članka 6. točke 2. ove Strategije i odluku o osnivanju tima iz članka 6. točke 3. ove Strategije.

Upravni odjel u čijoj je nadležnosti obavljanje informatičkih poslova će u roku od godine dana od dana stupanja na snagu ove Strategije uspostaviti registar iz članka 7. stavka 2. ove Strategije, inventar iz članka 7. stavka 3. ove Strategije i evidenciju iz članka 8. stavka 4. ove Strategije.

Župan će u roku od godine dana od dana stupanja na snagu ove Strategije donijeti planove iz članka 9. stavka 1. ove Strategije.

Stupanje na snagu i objava

Članak 13.

Ova Strategija stupa na snagu 1. travnja 2026. godine, a objavit će se na mrežnoj stranici Primorsko-goranske županije.

KLASA: 024-01/26-01/13
URBROJ: 2170-01-01/6-26-10
Rijeka, 26. ožujka 2026.

ŽUPAN

Ivica Lukanović, dipl.ing.