

Temeljem Priloga II. mjera 1. podmjera 1.1. Uredbe o kibernetičkoj sigurnosti ("Narodne novine" broj 135/24.), a u svezi članka 29. stavci 1. i 2. Zakona o kibernetičkoj sigurnosti ("Narodne novine" broj 14/24.) i članka 55a. stavak 2. točka 7. Statuta Osječko-baranjske županije ("Županijski glasnik" broj 2/95., 2/97., 3/99., 3/01., 8/01., 9/03., 13/05., 2/06., 5/09., 16/09., 2/13., 4/18., 2/20., 2/21. i 2/25.), Županica Osječko-baranjske županije donijela je 14. srpnja 2026. godine

PLAN

upravljanja mjerama kibernetičke sigurnosti Osječko-baranjske županije

DIO PRVI

OPĆE ODREDBE

Članak 1.

Ovim Planom određuje se okvir za primjenu i upravljanje mjerama kibernetičke sigurnosti u Osječko-baranjskoj županiji (u daljnjem tekstu: Županija) sukladno Zakonu o kibernetičkoj sigurnosti (u daljnjem tekstu: Zakon) i Uredbi o kibernetičkoj sigurnosti (u daljnjem tekstu: Uredba).

Ovim se Planom 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 ovoga Plana je osigurati visoku razinu kibernetičke sigurnosti mrežnih i informacijskih sustava Županije te njihovu usklađenost s općim poslovnim ciljevima i strateškim prioritetima Županije.

Članak 2.

Izrazi koji se u ovom Planu koriste za osobe u muškom rodu, neutralni su i odnose se na muške i ženske osobe.

Članak 3.

Županija je sukladno Zakonu i Uredbi kategorizirana kao važan subjekt i obvezna je provoditi naprednu razinu mjera kibernetičke sigurnosti.

Ovaj Plan primjenjuje se na:

1. sva upravna tijela 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.

Članak 4.

Županija se u upravljanju kibernetičkom sigurnošću vodi sljedećim načelima:

1. Načelo povjerljivosti - pristup podacima imaju samo ovlaštene osobe.
2. Načelo cjelovitosti - zaštita točnosti i potpunosti 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

Članak 5.

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 Zakona i Uredbe 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

Članak 6.

Temeljem Zakona i Uredbe, 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**

Članak 7.

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 Zakonu i Uredbi,
 - d) donosi rješenje o imenovanju osobe operativno odgovorne za kibernetičku sigurnost,
 - e) donosi rješenje o osnivanju Tima za kibernetičku sigurnost Osječko-baranjske županije.
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. Tim za kibernetičku sigurnost Osječko-baranjske županije, 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) obavještanje 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 i implementacija 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 Zakonu i Uredbi.
4. Vlasnici poslovnih procesa (pročelnici upravnih tijela Županije) koji:
 - a) sudjeluju u identifikaciji rizika unutar svojih upravnih tijela, odgovorni su za primjenu odredbi Zakona i Uredbe u upravnom tijelu kojim rukovode,
 - b) 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 SIGURNOSTI

Članak 8.

Tim za kibernetičku sigurnost Osječko-baranjske županije provodi sustavnu procjenu kibernetičkih rizika najmanje jednom godišnje, a uvijek prilikom značajnih promjena u sustavu ili značajnih incidenata.

Tim za kibernetičku sigurnost Osječko-baranjske županije vodi i redovito ažurira registar identificiranih kibernetičkih rizika.

Tim za kibernetičku sigurnost Osječko-baranjske županije vodi i redovito ažurira inventar kritične i ostale programske i sklopovske imovine.

Članak 9.

Tim za kibernetičku sigurnost Osječko-baranjske županije provodi analizu i kategorizaciju incidenata te sanaciju incidenata, po potrebi, i 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 Zakonu i Uredbi.

Županija vodi i redovito ažurira evidenciju incidenata.

Članak 10.

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.

Članak 11.

Tim za kibernetičku sigurnost Osječko-baranjske županije je dužan kontinuirano provoditi praćenje sigurnosnih metrika.

Tim za kibernetičku sigurnost Osječko-baranjske županije je dužan najmanje jednom godišnje provesti provjeru uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i procjenu njihove djelotvornosti.

Tim za kibernetičku sigurnost Osječko-baranjske županije je dužan najmanje jednom u dvije godine provesti samoprocjenu kibernetičke sigurnosti.

DIO ŠESTI
ZAVRŠNE ODREDBE

Članak 12.

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

Ovaj Plan revidirat će se po potrebi, radi usklađivanja s novim prijetnjama i regulatornim promjenama.

Članak 13.

Župan će u roku od 30 dana od dana stupanja na snagu ovoga Plana donijeti rješenje o imenovanju osobe iz članka 7. točke 2. ovoga Plana i rješenje o osnivanju tima iz članka 7. točke 3. ovoga Plana.

Tim za kibernetičku sigurnost Osječko-baranjske županije će u roku od godine dana od dana stupanja na snagu ovoga Plana uspostaviti registar identificiranih kibernetičkih rizika iz članka 8. stavka 2. ovoga Plana, inventar kritične i ostale programske i sklopovske imovine iz članka 8. stavka 3. ovoga Plana i evidenciju incidenata iz članka 9. stavka 4. ovoga Plana.

Upravni odjel u čijoj je nadležnosti obavljanje informatičkih poslova će u roku od godine dana od dana stupanja na snagu ovoga Plana donijeti planove kontinuiteta poslovanja i oporavka za kritične sustave iz članka 10. stavka 1. ovoga Plana.

Članak 14.

Ovaj Plan stupa na snagu osmog dana od dana objave u "Županijskom glasniku".

KLASA: 650-03/26-01/5
URBROJ: 2158-02-26-2
Osijek, 14. srpnja 2026.

ŽUPANICA
Nataša Tramišak, mag. iur.