Na temelju Zakona o kibernetičkoj sigurnosti ("Narodne novine" br. 14/24), Uredbe o kibernetičkoj sigurnosti ("Narodne novine" br. 135/24), članka 84. Zakona o zdravstvenoj zaštiti ("Narodne novine" br. 102/25), te članka 16. Statuta Nastavnog zavoda za javno zdravstvo Primorsko-goranske županije, Upravno vijeće Nastavnog zavoda za javno zdravstvo Primorsko-goranske županije na 06. sjednici održanoj dana 25.03.2026. donosi sljedeći:

STRATEŠKI AKT O KIBERNETIČKOJ SIGURNOSNOJ POLITICI

I. OPĆE ODREDBE

Članak 1.

(1) Ovim Strateškim aktom o kibernetičkoj sigurnosnoj politici (u daljnjem tekstu: Akt) definira se okvir za upravljanje kibernetičkom sigurnošću u Nastavnom zavodu za javno zdravstvo Primorsko-goranske županije (u daljnjem tekstu: Zavod).

Akt definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima, organizacijski sustav i raspodjelu uloga, odgovornosti i obveze, te procese upravljanja kibernetičkom sigurnošću s ciljem očuvanja povjerljivosti, integriteta i dostupnosti podataka, kao i osiguravanja neprekidnog rada u Zavodu.

Svrha ovoga Akta jest osigurati zaštitu informacijskih sustava, informacijske imovine, podataka, digitalnih usluga i infrastrukture subjekta od kibernetičkih prijetnji i rizika, u skladu sa važećim izdanjem Zakona i Uredbe o kibernetičkoj sigurnosti, te ostalim mjerodavnim zakonskim i regulatornim zahtjevima.

(2) Strateški akt se primjenjuje na sve zaposlenike, vanjske suradnike i druge dionike koji imaju pristup informacijskoj imovini i mogu ugroziti kibernetičku sigurnost Zavoda; sve informacijske sustave i digitalne usluge subjekta; te sve aktivnosti koje uključuju obradu, prijenos i pohranu podataka u digitalnom i fizičkom obliku.

(3) Izrazi koji se koriste u ovom Strateški aktu, a koji imaju rodno značenje, bez obzira jesu li korišteni u muškom ili ženskom rodu, koriste se neutralno i odnose se jednako na muški i ženski rod odnosno, obuhvaćaju na jednak način muški i ženski rod.

Članak 2.

(1) U upravljanju kibernetičkom sigurnošću Zavod primjenjuje sljedeća načela:

- **Ugrađena sigurnost**
  Kibernetička sigurnost integrira se u planiranje, razvoj, nabavu i uporabu informacijskih sustava i digitalnih rješenja od početnih faza njihova životnog ciklusa.

- **Razmjernost zaštite**
  Opseg i intenzitet sigurnosnih mjera određuju se u skladu s razinom kibernetičkih rizika i značajem za poslovne procese Zavoda.

- **Kontinuirano unaprjeđenje**
  Učinkovitost mjera kibernetičke sigurnosti redovito se preispituje te se, prema potrebi, prilagođava i unaprjeđuje.

- **Dodijeljena odgovornost**
  Odgovornosti za upravljanje, provedbu i nadzor mjera kibernetičke sigurnosti jasno su definirane i dodijeljene.

- **Normativna usklađenost**
  Upravljanje kibernetičkom sigurnošću provodi se u skladu s važećim zakonskim, regulatornim i drugim primjenjivim zahtjevima.

Načela iz ovoga članka primjenjuju se razmjerno ulozi i značaju informacijskih sustava Zavoda.

II. CILJEVI KIBERNETIČKE SIGURNOSTI

Članak 3.

Ciljevi kibernetičke sigurnosti Zavoda uključuju:

1. **Osiguranje povjerljivosti, cjelovitosti i dostupnosti informacija**
   Zaštititi informacijske sustave, podatke i digitalne usluge Zavoda od neovlaštenog pristupa, gubitka i narušavanja.
2. **Upravljanje kibernetičkim rizicima**
   Sustavno identificirati, procjenjivati, pratiti i smanjivati kibernetičke sigurnosne rizike.
3. **Jačanje sposobnosti za odgovor na kibernetičke incidente**
   Unaprijediti spremnost Zavoda za pravodobno otkrivanje, prijavu i učinkovito upravljanje kibernetičkim incidentima.
4. **Osiguranje otpornosti i oporavka**
   Održavati otpornost informacijskih sustava te osigurati učinkovit oporavak nakon kibernetičkih sigurnosnih incidenata.
5. **Razvoj svijesti i kompetencija zaposlenika**
   Povećavati razinu znanja, svijesti i odgovornosti zaposlenika u području kibernetičke sigurnosti.
6. **Učinkovita komunikacija u slučaju incidenata**
   Osigurati jasnu i učinkovitu (internu i eksternu) komunikaciju u slučaju kibernetičkih sigurnosnih incidenata.

III. MJERE ZA OSIGURANJE KIBERNETIČKE SIGURNOSTI

Članak 4.

(1) Zavod provodi mjere kibernetičke sigurnosti u skladu sa strateškim ciljevima i razmjerno identificiranim kibernetičkim rizicima. Mjere uključuju upravljanje rizicima, tehničke, organizacijske i operativne aktivnosti, kontinuirano praćenje, edukaciju zaposlenika te učinkovitu komunikaciju u slučaju incidenata:

I. Upravljanje kibernetičkim sigurnosnim rizicima

Zavod primjenjuje sustavan pristup upravljanju rizicima koji uključuje:

- identifikaciju i procjenu prijetnji i ranjivosti sustava
- primjenu mjera za smanjenje rizika
- kontinuirano praćenje i evaluaciju djelotvornosti mjera
- prilagodbu resursa, uloga i odgovornosti prema značaju sustava
- izvještavanje upravljačkog tijela i zaposlenika o stanju kibernetičke sigurnosti

II. Tehničke mjere

- Primjena sigurnosnih alata i tehnologija (firewall, antivirus, backup, autentikacija)
- Održavanje otpornosti mrežnih i informacijskih sustava
- Sigurnost medicinske opreme i IoT sustava

III. Organizacijske mjere

- Definiranje i dodjela uloga i odgovornosti u kibernetičkoj sigurnosti
- Uspostava kontrola pristupa i procedura zaštite podataka
- Razdvajanje uloga radi izbjegavanja sukoba interesa
- Planovi kontinuiteta poslovanja i sigurnosne politike
- Edukacija i podizanje svijesti zaposlenika (radionice, seminari, kontinuirano informiranje)
- Upravljanje incidentima i komunikacija s unutarnjim i vanjskim dionicima

IV. Operativne mjere

- Redovita procjena i praćenje sigurnosnih rizika
- Redovito ažuriranje softvera i sustava radi ispravljanja ranjivosti i održavanja sigurnosti
- Testiranje otpornosti sustava i sustava nadzora (npr. alarmi, dashboardi)
- Pravodobno otkrivanje i odgovor na incidente
- Redovita edukacija i podizanje svijesti zaposlenika
- Praćenje i izvještavanje o ključnim sigurnosnim metrikama (broj incidenata, vrijeme reakcije, usklađenost)

IV. ORGANIZACIJSKI SUSTAV I ODGOVORNOSTI

Članak 5.

(1) Za osiguranje učinkovite primjene mjera kibernetičke sigurnosti, organizacijski sustav i raspodjela odgovornosti unutar Zavoda definirani su kako slijedi:

Upravno vijeće odgovorno je za donošenje i nadzor provedbe Akta, odobravanje proračuna i strateških inicijativa te nadzor usklađenosti sa zakonima, uredbama i standardima.

Uprava je odgovorna za definiranje strateških ciljeva i smjernica kibernetičke sigurnosti, osiguranje resursa i podrške za operativnu provedbu mjera te praćenje učinkovitosti provedenih mjera kibernetičke sigurnosti na strateškoj razini.

Tim za kibernetičku sigurnost odgovoran je za operativnu provedbu mjera i politike kibernetičke sigurnosti, redovitu procjenu rizika i prijetnji, razvoj i održavanje planova kontinuiteta i oporavka, usklađivanje sigurnosnih mjera s poslovnim potrebama, izradu sigurnosnih izvještaja za Upravu te provedbu samoprocjene.

Voditelj odsjeka za informatiku odgovoran je za koordinaciju dnevnih aktivnosti, nadgledanje provedbe sigurnosnih mjera, savjetovanje i koordinaciju aktivnosti zaštite, izradu sigurnosnih izvještaja za Upravno vijeće u koordinaciji s Timom za kibernetičku sigurnost, prijavu sigurnosnih incidenata te praćenje rada informatičkog sustava i mreža.

Zaposlenici odsjeka za informatiku odgovorni su za održavanje stabilnog i sigurnog rada informatičkog sustava i mrežnih infrastruktura, provedbu tehničkih mjera zaštite, uključujući nadzor sustava i servera,

zaštitu podataka i provođenje sigurnosnih politika, pravovremeno otklanjanje tehničkih problema i analizu sigurnosnih incidenata, održavanje i ažuriranje softvera i sustava, tehničku podršku zaposlenicima i dokumentiranje IT procedura, podršku u provođenju digitalne transformacije i modernizacije te sudjelovanje u edukaciji zaposlenika o kibernetičkoj sigurnosti.

Zaposlenici odnosno korisnici sustava i vanjski suradnici odgovorni su za pridržavanje sigurnosnih politika i procedura, sigurno korištenje informacijskih sustava, odgovorno rukovanje povjerljivim informacijama, prepoznavanje i pravovremenu prijavu sumnjivih aktivnosti te sudjelovanje u obveznim edukacijama.

(2) Pružatelji IKT usluga odgovorni su za odgovorni su za pravovremeno obavještavanje Zavoda o svim sigurnosnim incidentima koji utječu na sustave i usluge koje pružaju. Pružatelji usluga dužni su uskladiti svoje aktivnosti s važećim zakonima i Uredbom o kibernetičkoj sigurnosti, kao i s politikama i internim pravilima Zavoda.

V. PROCESI UPRAVLJANJA KIBERNETIČKOM SIGURNOŠĆU

Članak 6.

(1) Procesi upravljanja kibernetičkom sigurnošću unutar Zavoda definiraju se s ciljem usklađivanja sa Zakonom i Uredbom o kibernetičkoj sigurnosti, te u svrhu uspostave sustava koji osigurava učinkovito upravljanje sigurnosnim rizicima i zaštitu povjerljivih informacija.

(2) Zavod provodi upravljanje kibernetičkom sigurnošću kroz ključne procese koji osiguravaju zaštitu informacijskih sustava, podataka i digitalnih usluga, kontinuiranu prilagodbu sigurnosnih mjera te pravovremenu reakciju na prijetnje.

(3) Ključni procesi uključuju:

a) Reagiranje na kibernetičke incidente – pravovremena prijava, analiza, klasifikacija i sanacija sigurnosnih događaja te dokumentiranje i učenje iz incidenata;
b) Sigurnosne provjere i auditi – redovite interne i vanjske revizije, procjena učinkovitosti mjera i ažuriranje politika i procedura;
c) Kontinuirano poboljšanje sigurnosnih mjera – praćenje novih prijetnji, prilagodba strategija i sudjelovanje u nacionalnim i međunarodnim inicijativama za kibernetičku sigurnost.

(4) Uz ključne procese, Zavod provodi i upravljanje kibernetičkim rizicima, upravljanje pristupima i autorizacijom, te planiranje kontinuiteta poslovanja i oporavka sustava, a sve s ciljem osiguravanja cjelovite i učinkovite zaštite informacijskih sustava i podataka.

VI. ZAVRŠNE ODREDBE

Članak 7.

(1) Ovaj Strateški akt stupa na snagu osmog dana od dana objave na oglasnoj ploči Zavoda i službenim internetskim stranicama Zavoda, u skladu s načelom transparentnosti iz Opće uredbe o zaštiti podataka.

(2) Zavod je dužan osigurati da je Strateški akt uvijek dostupan zaposlenicima i ispitanicima, te se svaka promjena ili dopuna Strateški akta mora javno objaviti na isti način kako bi se ispitanici pravovremeno informirali o pravima i obvezama u vezi s obradom njihovih osobnih podataka.

(3) Svi zaposlenici i vanjski suradnici obvezni su pridržavati se mjera definiranih ovim Aktom. Nepoštivanje odredbi ovog Strateškog akta predstavlja povredu radne obveze i može rezultirati disciplinskim mjerama u skladu s važećim propisima o radu i internim aktima Zavoda.

Rijeka, 25.03.2026. godine.

Broj: 700-15/01-26

PREDSJEDNICA UPRAVNOG VIJEĆA

Nastavni zavod za javno zdravstvo Primorsko-goranske županije Rijeka, Krešimirova 52/a 101

Aleksandra Vio, mag. oec.

Utvrđuje se da je ovaj Strateški akt objavljen na oglasnoj ploči Zavoda dana 26.03. 2026. godine i da je stupio na snagu dana 03.04. 2026. godine.

RAVNATELJ

izv. prof. dr. sc. Željko Linšak, dipl. sanit. ing.

Nastavni zavod za javno zdravstvo Primorsko-goranske županije Rijeka, Krešimirova 52/a 101