POLITIKA INFORMACIJSKE SIGURNOSTI

1. Svrha i područje primjene

Ova politika određuje načela informacijske i kibernetičke sigurnosti u Nastavnom zavodu za javno zdravstvo Splitsko-dalmatinske županije (u nastavku Zavod). Cilj je zaštititi povjerljivost, cjelovitost, dostupnost i autentičnost informacija koje Zavod obrađuje, pohranjuje ili prenosi. To su osobito zdravstveni i osobni podaci pacijenata i korisnika, rezultati ispitivanja te podaci o poslovanju.

Politika se primjenjuje na sve mrežne i informacijske sustave Zavoda, uključujući sustave koje za Zavod vode vanjski davatelji usluga. Obuhvaća sve lokacije i izdvojene odjele, sve djelatnike te vanjske suradnike, servisere i studente koji imaju pristup informacijama ili sustavima Zavoda.

Uprava se obvezuje osigurati resurse i mjere potrebne za provedbu ove politike i njezino stalno poboljšavanje.

2. Zakonski okvir

Politika se temelji na:

- Zakonu o kibernetičkoj sigurnosti (NN 14/2024, u nastavku ZKS);
- Uredbi o kibernetičkoj sigurnosti (NN 135/2024, u nastavku Uredba);
- Općoj uredbi o zaštiti podataka (EU) 2016/679 i Zakonu o provedbi Opće uredbe o zaštiti podataka (NN 42/2018);
- propisima o zdravstvenoj zaštiti i zaštiti podataka o pacijentima;
- zahtjevima normi HRN EN ISO 9001 i HRN EN ISO/IEC 17025 za povjerljivost i zaštitu zapisa.

Zavod je kategoriziran kao važan subject, u srednjoj razini kibernetičkih sigurnosnih rizika prema obavijesti nadležnog tijela od 12.3.2025. Nadležni CSIRT je Nacionalni centar za kibernetičku sigurnost..

3. Odgovornost Uprave

U skladu s čl. 29. ZKS-a, ravnateljica i članovi Uprave:

- odgovaraju za provedbu mjera upravljanja kibernetičkim rizicima;
- odobravaju te mjere i nadziru njihovu provedbu;
- pohađaju osposobljavanje iz kibernetičke sigurnosti i omogućuju redovito osposobljavanje djelatnika;
- osiguravaju resurse za provedbu ove politike;
- odlukom imenuju predstavnike za informacijsku sigurnost.

Uprava preispituje stanje informacijske sigurnosti najmanje jednom godišnje u preispitivanju upravljanja. Pritom razmatra incidente, rezultate provjera i procjenu rizika.

4. Mjere upravljanja kibernetičkim rizicima

Zavod primjenjuje primjerene i razmjerne mjere iz čl. 30. ZKS-a i Uredbe. Detaljno su opisane u postupku za upravljanje informacijskim i komunikacijskim tehnologijama (P-8.5-8 i pripadajući postupak za IT).

Područje	Načelo
Analiza rizika	Rizici za informacijske sustave procjenjuju se najmanje jednom godišnje i nakon svakog značajnog incidenta (O-8-14).
Upravljanje imovinom	Vodi se popis opreme, aplikacija i podataka s odgovornom osobom.
Kontrola pristupa	Prava se dodjeljuju prema matricama ovlaštenja i potrebi posla. Ukidaju se na dan odlaska ili premještaja i provjeravaju najmanje dva puta godišnje.
Autentifikacija	Pristup udaljenim i ključnim sustavima (CEZIH, LIS, Pakel, e-pošta) uz višefaktorsku autentifikaciju gdje je to moguće. Lozinke su osobne.
Zaštita sustava	Softver instalira samo ovlašteno osoblje. Uređaji imaju ažurnu zaštitu od zlonamjernog softvera i sigurnosna ažuriranja, a nepodržani operativni sustavi zamjenjuju se.
Nadzor i bilježenje	Događaji u sustavima bilježe se i nadziru (sigurnosni operativni centar).
Pričuvne kopije i kontinuitet	Kopije baza podataka i mrežnih diskova izrađuju se dnevno, tjedno i mjesečno i čuvaju odvojeno od izvornog sustava. Povrat podataka redovito se provjerava. Za ključne usluge postoji plan kontinuiteta poslovanja i oporavka.
Kriptografija	Osjetljivi podaci šifriraju se pri prijenosu i na prijenosnim medijima.
Lanac opskrbe	Dobavljači programske podrške, servisa i usluga u oblaku ugovorom preuzimaju obveze sigurnosti i povjerljivosti te prijave incidenata. Sigurnost se ocjenjuje pri nabavi i održavanju.
Kadrovska sigurnost	Djelatnici prije pristupa potpisuju izjavu o povjerljivosti i prolaze osnovno osposobljavanje.
Kibernetička higijena	Djelatnici se osposobljavaju najmanje jednom godišnje (npr. prepoznavanje phishinga i sigurno korištenje e-pošte).
Procjena djelotvornosti	Djelotvornost mjera prati se pokazateljima, internim auditom te samoprocjenom ili revizijom prema ZKS-u.

5. Obveze djelatnika i vanjskih suradnika

- Svi djelatnici i vanjski suradnici potpisuju izjavu o povjerljivosti. Službene informacije mogu se iznositi samo uz odobrenje Uprave.
- Korisnički račun i lozinka osobni su. Djelatnik je odgovoran za njihovo čuvanje i ne smije ih dijeliti.
- Djelatnici provode politiku čistog stola i čistog zaslona. Pri napuštanju radnog mjesta povjerljive dokumente spremaju na sigurno mjesto, a računalo zaključavaju ili se odjavljuju.
- Elektronička pošta koristi se isključivo u poslovne svrhe, preko službene adrese. Sumnjive poruke ne otvaraju se, nego se prijavljuju Odjelu za IT.
- Podaci o pacijentima i korisnicima daju se samo ovlaštenim osobama, uz provjeru identiteta tražitelja.
- Informacije dobivene od trećih strana (kupci, dobavljači, partneri) smatraju se povjerljivima i označavaju se na odgovarajući način. Pristup njima imaju samo osobe kojima je to potrebno za posao.
- Privatni uređaji i prijenosni mediji ne spajaju se na mrežu Zavoda bez odobrenja Odjela za IT.
- Informacije i nositelji informacija (diskovi, USB, papir) uklanjaju se na siguran način kad više nisu potrebni.

6. Incidenti i obavještavanje

Svaki djelatnik odmah prijavljuje Odjelu za IT svaki uočeni ili sumnjivi sigurnosni događaj: neobično ponašanje računala, sumnjivu poruku, izgubljen uređaj ili neovlašten pristup.

Odjel za IT i predstavnik za informacijsku sigurnost procjenjuju je li incident značajan prema kriterijima Uredbe i o tome obavještavaju Upravu. Svaki incident se zapisuje i analizira radi uzroka i poboljšanja.

Značajni incident prijavljuje se nadležnom CSIRT-u preko nacionalne platforme PiXi:

Korak	Rok
Rano upozorenje	Bez odgode, najkasnije 24 sata od saznanja
Početna obavijest	Najkasnije 72 sata od saznanja
Privremeno izvješće	Na zahtjev CSIRT-a, u roku koji on odredi
Završno izvješće	Najkasnije 30 dana od početne obavijesti. Ako incident još traje, izvješće o napretku svakih 30 dana

Ako postoji sumnja na kazneno djelo, incident se prijavljuje i policiji (čl. 37. ZKS-a). Ako je došlo do povrede osobnih podataka, službenik za zaštitu podataka obavještava Agenciju za zaštitu osobnih podataka najkasnije 72 sata od saznanja, a po potrebi i ispitanike (čl. 33. i 34. Opće uredbe o zaštiti podataka).

7. Uloge i preispitivanje

Uloga	Odgovornost
Uprava	Odobrava politiku i mjere, nadzire provedbu, osigurava resurse, preispituje stanje jednom godišnje
Predstavnici za informacijsku sigurnost	Koordiniraju mjere, procjenu rizika i obradu incidenata, komuniciraju s nadležnim CSIRT-om, izvještavaju Upravu
Odjel za IT	Provodi tehničke mjere: korisnička prava, ažuriranja, pričuvne kopije, nadzor, prvi odgovor na incident
Službenik za zaštitu podataka	Nadzire obradu osobnih podataka i postupa kod povrede osobnih podataka
Voditelji službi	Traže i odobravaju pristupe za svoje djelatnike, obavještavaju o promjenama osoblja, potvrđuju provjeru prava
Djelatnici i vanjski suradnici	Pridržavaju se politike i prijavljuju sigurnosne događaje

Politika se preispituje najmanje jednom godišnje u preispitivanju upravljanja te pri promjeni propisa, kategorizacije, značajnom incidentu ili većoj promjeni informacijskog sustava. Zavod provodi samoprocjenu ili reviziju kibernetičke sigurnosti kako to propisuje ZKS za njegovu kategoriju. Ključni subjekti imaju reviziju najmanje svake dvije godine (čl. 34.), a važni subjekti samoprocjenu najmanje svake dvije godine (čl. 35.).

Politika je dostupna svim djelatnicima na intranetu i javno na mrežnim stranicama Zavoda.

Split, 22.10.2026.

Ravnateljica:
Doc. prim. dr. sc. Željka Karin, dr. med.