Temeljem Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/2018) i čl. 30. Statuta Zavoda za javno zdravstvo Međimurske županije, uz prethodno savjetovanje s Radničkim vijećem, ravnateljica prim. Marina Payerl-Pal, dr.med.spec. dana 10.06.2025.g. donosi sljedeći:

PRAVILNIK O SUSTAVU INFORMACIJSKE SIGURNOSTI

1. Svrha

Ovim pravilnikom o sustavu informacijske sigurnosti **(„Pravilnik")** uređuju se mjere i postupci koji služe za prevenciju od gubitka ili neovlaštenog otkrivanja osobnih podataka. Uređuje se otkrivanje i otklanjanje posljedica u slučaju gubitka ili neovlaštenog otkrivanja osobnih podataka koje obrađuje voditelj obrade („**u daljnjem tekstu Zavod**"), kao i službenih podataka Zavoda.

2. Definicije

Pojmovi navedeni u ovom Pravilniku imaju sljedeće značenje:

Službeni podatak: dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za Zavod, a osobito poslovne tajne i Osobni podaci, podaci o sklopljenim ugovorima i bitnim sastojcima ugovora, o uvjetima pružanja usluga od strane Zavoda i sl.

Informacijski sustav: računalni, komunikacijski ili drugi elektronički sustav u kojem se Službeni podaci obrađuju, pohranjuju ili prenose tako da budu dostupni i uporabljivi za radnike, a koji obuhvaća tehničku infrastrukturu Zavoda, osobe i postupke kojima se podaci obrađuju, pohranjuju ili prenose.

Pristup: svaka radnja koja uključuje mogućnost uvida, preuzimanja, otkrivanja, izmjene ili brisanja podataka.

Mjere sigurnosti: skup mjera i postupaka, na tehničkoj i organizacijskoj razini, čijom se primjenom postiže i održava prihvatljiva razina zaštite sigurnosti Informacijskog sustava.

Sigurnosni incident: događaj koji ugrožava povjerljivost, integritet i dostupnost Službenih podataka, integritet i sigurnost Informacijskog sustava ili ukazuje na neovlašteni pristup Informacijskom sustavu.

3. Primjena Pravilnika

Ovaj Pravilnik obvezuje sve radnike i vanjske suradnike Zavoda kojima je dozvoljen pristup Informacijskom sustavu.

Vanjskim suradnicima Zavoda, po potrebi, se mogu dodijeliti prava radnika, s tim da se i u odnosu na njih primjenjuju odredbe ovog Pravilnika.

Kršenje odredbi ovog Pravilnika od strane radnika može dovesti do povrede radne obveze te izvanrednog otkaza ugovora o radu pod uvjetima propisanim Zakonom o radu, a u slučaju kršenja od strane Vanjskih suradnika Zavoda do raskida ugovornog odnosa.

4. Prava i obveze Ovlaštenih osoba

Ovlaštenu osobu za koordinaciju, savjetovanje i kontakt glede Informacijskog sustava određuje ravnatelj. Radnicima se s obzirom na radno mjesto i sukladno poslovnim procesima koje obavljaju određuje i opseg ovlasti za pristup Informacijskom sustavu u skladu s potrebama njihovog radnog mjesta.

Radnici su dužni pridržavati se odredbi ovog Pravilnika radi osiguranja pravilnog rada i zaštite sigurnosti Informacijskog sustava te sprječavanja Sigurnosnih incidenata.

Radnici su dužni poduzimati sve mjere sigurnosti propisane ovim Pravilnikom kao i druge razumne mjere sigurnosti radi osiguranja pravilnog rada i zaštite sigurnosti Informacijskog sustava i sprječavanja Sigurnosnih incidenata odnosno njihova otklanjanja.

5. Zaštita Informacijskog sustava

5.1. Kontrola i zaštita pristupa

Voditelj djelatnosti dodjeljuje prava za pristup Informacijskom sustavu radnicima svoje djelatnosti, sukladno potrebama njihovog radnog mjesta i to u najmanjoj mjeri potrebnoj za obavljanje radnih zadataka u okviru redovitog poslovnog procesa.

Voditelj djelatnosti vodi evidenciju odobrenja pristupa te istu evidenciju i dodijeljene ovlasti revidira uslijed svake značajnije promjene u sustavu, a najmanje jednom godišnje.

Radnici se prilikom pristupa Informacijskom sustavu identificiraju korištenjem korisničkog imena i lozinke, te su odgovorni za izbor i čuvanje tajnosti lozinki koje koriste.

5.2. Pravila korištenja opreme

Oprema Zavoda smije se koristiti isključivo u poslovne svrhe, a sva oprema mora biti evidentirana i svi korisnici opreme zabilježeni.

Oprema Zavoda ne smije se koristiti u privatne svrhe, osim uz izričito dopuštenje Zavoda.

Korištenje opreme Zavoda, odnosno osobne opreme koja se koristi u poslovne svrhe, mora biti u skladu sa zakonom, internim aktima Zavoda i licencnim pravima.

Oprema Zavoda mora biti zaštićena na adekvatan način, primjeren određenoj vrsti opreme Zavoda.

Radnici su odgovorni za profesionalno, etično i zakonito korištenje opreme Zavoda i osobne opreme kada se koristi za poslovne svrhe.

Radnici su dužni poduzeti sve potrebne Mjere sigurnosti kako bi spriječili otuđenje opreme, odnosno osobne opreme koja se koristi u poslovne svrhe.

Radnici ne smiju davati opremu Zavoda na uporabu trećim osobama, a u slučaju davanja osobne opreme koja se koristi u poslovne svrhe moraju poduzeti sve razumne Mjere sigurnosti kako bi spriječili nastanak Sigurnosnog incidenta.

5.3. Pravila korištenja osobne opreme

Korištenje osobne opreme u poslovne svrhe predstavlja rizik za poslovanje, u najvećoj mjeri prisutan kao rizik od neovlaštenog pristupa, krađe i gubitka podataka.

Dozvoljeno je spajanje vlastitih uređaja za pohranu podataka (npr. eksterni diskovi) na opremi Zavoda u svrhu izrade sigurnosnih kopija podataka, te prijenosa podataka u slučaju da to nije moguće ili nije dovoljno praktično odraditi preko Informacijskog sustava. Prije korištenja vlastitog uređaja za pohranu podataka potrebno je provjeriti uređaj i njegov sadržaj antivirusnim alatom. Nije dozvoljeno spajanje i korištenje uređaja koji su zaraženi virusima ili drugim zlonamjernim programima. Ako se uređaj za pohranu podataka iznosi izvan prostorija Zavoda, Službeni i Osobni podaci na uređaju moraju biti šifrirani, te dodatno zaštićeni lozinkom za pristup uređaju, ako uređaj ima tu mogućnost. Kada više nisu potrebni svi podaci moraju biti obrisani na siguran način.

Nije dozvoljeno kopiranje i spremanje internih i povjerljivih podataka na vlastite uređaje bez prethodnog odobrenja Zavoda. Na vlastite uređaje i medije za pohranu podataka nije dozvoljeno kopiranje i spremanje podataka koji su označeni kao poslovna tajna, čak niti u šifriranom obliku.

5.4. Korištenje službenih Informacijskih sustava i elektroničke pošte

Radnici su dužni koristiti službene Informacijske sustave Zavoda i službenu elektroničku poštu Zavoda na takav način kojim se izbjegava nanošenje štete Zavodu te nastanak Sigurnosnog incidenta.

Korištenje elektroničke pošte definirano je Pravilnikom o korištenju pošte i elektroničke pošte Zavoda.

5.5. Pristup internetu i korištenje internetskih usluga

Internet se može koristiti isključivo za poslovnu namjenu, informiranje i edukaciju.

Zavod će poduzeti odgovarajuće Mjere sigurnosti kojima se onemogućuje neovlašten pristup Informacijskom sustavu Zavoda putem interneta, a osobito mjere zaštite od virusa i drugih destruktivnih programa, uključujući instalaciju i pokretanje programa koji služe za zaštitu od virusa na opremi (uređajima) koja se koristi za pristup internetu.

Programi koji služe za zaštitu od virusa moraju biti redovito ažurirani, a radnici ne smiju isključivati ili onemogućavati takva ažuriranja i programe.

Radnici su dužni izbjegavati internetske aktivnosti koje bi mogle ugroziti sigurnost njihovih računala i Informacijskog sustava Zavoda te prilikom korištenja interneta smiju posjećivati samo stranice koje su neophodne za obavljanje posla.

5.6. Dodatne mjere zaštite

U cilju zaštite Informacijskog sustava, Zavod provodi i sljedeće mjere zaštite:
Mjere zaštite za sprječavanje neovlaštenih osoba od korištenja Informacijskog sustava:

- postavljanje lozinki i prava pristupa podacima, programima i opremi
- zaštita Internet usmjerivača i vatrozida od neovlaštenog pristupa
- zaštita pristupa mrežnoj infrastrukturi i opremi
- fizička zaštita pristupa IT opremi
- zaštita od neovlaštenog pristupa s udaljenih lokacija uvođenjem MFA autentifikacije

Mjere kojima se osigurava da se podaci sadržani u Informacijskom sustavu ne mogu čitati, kopirati, mijenjati ili ukloniti bez odgovarajućeg ovlaštenja tijekom postupka elektroničkog prijenosa, prijevoza ili pohranjivanja na podatkovne medije, te da postoji mogućnost provjere i identifikacije primatelja na koje se žele prenijeti osobni podaci kroz sustave za obradu podataka:

- Zaštita podataka od neovlaštenog pristupa uvođenjem autentifikacije i autorizacije korisnika pomoću lozinki te kartica s čipom

Mjere kojima se osigurava da su podaci sadržani u Informacijskom sustavu zaštićeni od slučajnog uništenja ili gubitka:

- poslovanje migrirano u „Državni oblak" (CDU)
- pohranjivanje podataka na sigurnoj eksternoj lokaciji (CDU)

6. Prijava Sigurnosnog incidenta

Radnici i vanjski suradnici kojima su dodijeljena ovlaštenja Ovlaštenih osoba, dužni su, bez odgađanja, obavijestiti ravnatelja Zavoda ili Ovlaštenu osobu sukladno smjernicama o korištenju poslovnih računala i mobilnih uređaja (SOP – SIGURNOST) ako saznaju za bilo kakav Sigurnosni incident i za bilo kakvo kršenje odredbi ovog Pravilnika, odnosno ako uoče bilo kakav nedostatak u radu Informacijskog sustava, a osobito u mjerama sigurnosti Informacijskog sustava.

7. Završne odredbe

Prilikom prestanka ugovora o radu ili ugovornog odnosa, radnici su dužni vratiti opremu Zavoda, kao i svu ostalu imovinu koja im je dodijeljena na korištenje. Također, radnici su dužni predati svu dokumentaciju te sve podatke u vlasništvu Zavoda. Nije dozvoljeno kopiranje i iznošenje Službenih i Osobnih podataka koji su radnicima bili povjereni.

Ovaj Pravilnik stupa na snagu osam dana od dana objave na oglasnim pločama Zavoda.

Ravnateljica
prim. Marina Payerl-Pal, dr.med.spec.

Ovaj Pravilnik objavljen je na oglasnoj ploči dana 11.06.2025.g., te stupa na snagu dana 20.6.2025.g..

Ravnateljica
prim. Marina Payerl-Pal, dr.med.spec.

Klasa: 030-05/25-06/1
Urbroj: 2109-70-03-25/1