	Broj dokumenta	JU ZAVOD ZA ZDRAVSTVENU ZAŠTITU ŽENA I MATERINSTVA KANTONA SARAJEVO ЈУ ЗАВОД ЗА ЗДРАВСТВЕНУ ЗАШТИТУ ЖЕНА И МАТЕРИНСТВА КАНТОНА САРАЈЕВО	Komisija za kvalitet
	10-1332-01/21		
	Datum odobrenja/ usvajanja	UPRAVLJANJE INFORMACIJAMA I INFORMACIJSKE TEHNOLOGIJE Kriterij: S-9.8 A - 9.1	Revizija se vrši svake 3 godine ili po potrebi ranije
	08.07.2021.		

POLITIKA I STRATEGIJA INFORMACIJSKOG SISTEMA ZDRAVSTVENE USTANOVE I UPRAVLJANJA INFORMACIJAMA I INFORMACIJSKIM TEHNOLOGIJAMA UNUTAR USTANOVE	Verzija:
	Ukupno str. 4

1. OPŠTA IZJAVA O POLITICI

Svrha politike je da definira prihvatljive i neprihvatljive načine ponašanja, da jasno raspodijeli zadatke i odgovornosti te da propiše sankcije u slučaju nepridržavanja.

Sigurnosna politika vrijedi za svu računarsku opremu koja se nalazi u prostorima Zavoda, administratore informacionih sistema, korisnike (radnike i vanjske suradnike), organizacije koje rade na održavanju opreme ili softvera.

Sigurnosna politika informacionih tehnologija je usko vezana za Strategiju upravljanja informacijama i informacijskim tehnologijama zdravstvene ustanove.

Ova politika se odnosi na standardne i sigurnosne procedure koje se odnose na zaštitu ličnih podataka pacijenata, korisnika usluga te podataka koji se odnose na podatke potrebne za upravljanje Ustanovom.

Sigurnosno politika je dokument koji definira skup pravila, smjernica i prijedloga o ponašanju prilikom rukovanja informacijskim sistemom u bolnici i mjerama koje je potrebno poduzeti u konkretnim situacijama. Te se mjere u najvećem procentu odnose na program upravljanja medicinskom dokumentacijom (AIS, eDoktor), koji postoji u Zavodu.

Informacijski sistemi i podaci koji su sadržani u njima, često su vrlo bitni za poslovanje Zavoda. Povećanjem upotrebe elektroničkih informacija u poslovanju, povećava se i zabrinutost za sigurnost sistema i podataka koji su u njemu pohranjeni. Da bi se podaci i informacijski sistemi kvalitetno zaštitili, važno je osmisliti i provesti politiku sigurnosti.

Razmjena informacija igra ključnu ulogu u procesu rada, kako medicinskog tako i nemedicinskog osoblja. Svaki dan se unutar Zavoda generira velika količina informacija o pacijentima, tretmanima i slično, a one se pohranjuju na vanjske servere koje održava Zavod zdravstvenog osiguranja Kantona Sarajevo.

2. POVJERLJIVOST

Povjerljivost je zaštita podataka koje sadrži sistem od neovlaštenog pristupa. Ključni aspekt povjerljivosti je identifikacija korisnika i provjera autentičnosti.

Identifikacija je proces prijave korisnika na sistem, pri čemu sistem zna da takav korisnik postoji. Provjera autentičnosti je proces kojim sistem želi biti siguran da je korisnik koji se prijavljuje pod određenim imenom, upravo ta osoba.

Postoji više načina provjere autentičnosti, a najrašireniji je unoz lozinke, ali se i sve više razvija tehnička oprema koja jedinstvene ljudske osobine, poput otiska prsta ili mrežnice oka pretvara u digitalne signale koji služe za autentifikaciju.

Povjerljivost može biti narušena na nekoliko načina, a najčešće prijetnje povjerljivosti su:

- Hakeri,
- Lažno predstavljanje,
- Neovlaštena aktivnost,
- Nezaštićeno preuzimanje podataka,
- Lokalna mreža,
- Trojanski konji.

3. SIGURNOST INFORMACIJSKIH SISTEMA

Sigurnost IT sistema Ustanove može biti ugrožena izvana ili iznutra. Da bi se spriječila mogućnost obavljanja ovakvih neželjenih radnji, potrebno je uvesti odgovarajuće mjere.

Mjerama poput educiranja radnika, smanjuje se vjerovatnost njihove pogreške kojima bi mogli ugroziti integritet i sigurnost sistema.

Smještajem opreme na kojima se čuvaju podaci u posebnu prostoriju, određivanjem ko joj smije pristupiti, kontroliranjem uvjeta u takvoj prostoriji (temperatura i vlaga), postižemo duži radni vijek opreme, a time i pouzdaniji rad sistema.

Napadi na IT sistem izvana, čiji je cilj pribavljanje informacija, njihovo mijenjanje ili uništavanje, se odbijaju na način kontrole prometa s interneta prema sistemu i obratno, sprečavanjem instaliranja programa u operacijski sistem ili kriptiranjem podataka. Uvođenjem ovakvih mjera u informaciji sistem, podiže se stepen sigurnosti, a mogućnost obavljanja neželjenih radnji se svodi na minimum. Najveće prijetnje IT sistemima su ljudi koji s njim imaju vezu, kroz svakodnevni rad ili kroz povremeno održavanje.

Neke osobe nisu dovoljno kvalificirane za određeni postao te se može dogoditi da takva osoba slučajno uništi podatke te ugrozi IT sistem.

4. SIGURNOST KOMUNIKACIJE

Komunikacija između računala doprinosi povećanju snage sistema, brzini obrade podataka, dostupnosti, ali što više računala komunicira s drugim računalima, to je organizacija u kojoj se ona nalaze ranjivija.

Komunikaciju mrežom možemo učiniti sigurnoijom kontrolom pristupa, kriptiranjem podataka koji putuju mrežom, zaštitom vatrenim zidovima (firewall) i ostalim mjerama fizičke zaštite.

5. INSTALIRANJE I LICENCIRANJE PROGRAMSKE PODRŠKE

Korištenje ilegalne programske podrške nezakonito je i predstavlja povredu autorskih prava. Kako bi se Ustanova zaštitila od štete nastale korištenjem ilegalne programske podrške, potrebno je provoditi kontrolu da li su instalirani programi na računalima sistema licencirani.
Sve korisnike je potrebno obavezati na pridržavanje autorskih prava.

Odgovornost direktora je da obezbijedi da su softverske aplikacije uredno licencirane.

6. PREVENTIVNE SIGURNOSNE MJERE

Pravila sigurnosti za elektroničku poštu su sljedeća:

- Niti jedan program, datoteka ili dokument koji bi mogao narušiti sigurnosnu politiku, zakon, licencu, prava ili dozvole kopiranje, ne smije se slati elektroničkom poštom,
- Članovi Zavoda su odgovorni za svaku datoteku primljenu putem mail-a,
- Primljena pošta koja krši politiku sigurnosti mora se prijaviti Stručnom saradniku za IS,
- Prilozi koji se šalju, ne smiju sadržavati autorski zaštićene informacije.

6.1 Antivirusna zaštita

Zaštita od virusa je obavezna i treba da se provodi na nekoliko nivoa:

- Na poslužiteljima elektroničke pošte,
- Na internim poslužiteljima, gdje se stavlja centralna instalacija,
- Na svakom osobnom računalu korisnika.

Članovi osoblja ne smiju samovoljno isključiti protivvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti program, korisnici moraju prethodno obavijestiti osobu zaduženu za održavanje IT sistema u Zavoda (Stručni saradnik za IS).

7. RASPODJELA ZADATAKA

Zadaci iz ove Politike se raspoređuju na sljedeći način:

Stručni saradnik za IS preuzima prijave o mogućem kršenju smjernica i pravila iz ove Procedure, zatim, redovito održavaju dijelove IT sistema i o provedenim aktivnostima izvještavaju Upravu Zavoda.

Uposleni Zavoda preuzimaju odgovornost prijave mogućeg kršenja smjernica i pravila ove Procedure.

Stručni saradnik za IS prati provođenje iste, učestvuje u procesu davanja ovlasti za pristup informacijskom sistemu, ostvaruje kontakte sa odgovornim osobama društva za održavanje IT sistema, ukoliko je potrebno da se novom radniku dodijele ovlasti vezane za pristup programu za vođenje medicinske dokumentacije i sl.

Medicinske sestre su obavezne prijavljiati incidente na proceduralno propisan način, a dužni su i upozoriti druge osobe koje se nalaze u Zavodu, ako primijete da ugrožavaju sigurnost IT sistema.

8. PRIHVATLJIVA I NEPRIHVATLJIVA PONAŠANJA

Svaka zloupotreba dostupnih ifnormacija ili nepridržavanje ovoj Proceduri spada u neprihvatljivo ponašanje i bit će sankcionisana na odgovarajući način, pokretanjem disciplinskog postupka protiv uposlenika ili drugim načinima (akcijskim planom, ocjenom izvedbe rada i dr).

9. STRATEŠKI CILJEVI USTANOVE I REVIZIJA DOKUMENTA

Dugoročni ciljevi o upravljanju informacijama i o informacijskim tehnologijama zdravstvene ustanove, u narednim periodima će biti:

1. Održavanje i unapređenje informaciong sistema u Zavodu,

2. Unifikacija podataka (historije) i dosljednost podataka,
3. Uspostava i vođenje elektronske baze radnika (matične evidencije),
4. Korištenje usluga državnih organa, a koje omogućavaju elektronsko podnošenje, preuzimanje i razmjenu podataka,
5. Upravljanje kvalitetom, sigurnosti i rizikom na nivou Zavoda tako da se putem integracije podataka IT koristi za kontrolu i poboljšanje kvaliteta,
6. Edukacija i obuka uposlenih,
7. Uspostava procesa prikupljanja općih podataka i protokom informacija između institucija zdravstvenih vlasti, zdravstvenih ustanova, socijalnih službi i dobrovoljnih organizacija.

Za resurse i nabavku informacijskih tehnologija koje su u skladu sa dugoročnim ciljevima, direktno je odgovoran Direktor Zavoda.

Revizija ovog dokumenta u dijelu dugoročnih ciljeva se vrši svake treće godine.

Izradio/la	Saglasnost I	Saglasnost II	Odobrenje	Revizija	
stručni saradnik za IS	rukovodilac APS	Koordinator-menadžer kvaliteta	Direktor	Datum odobrenja/ usvajanja	Br. Revizije
Damir Rahmanović, dipl.ecc.	Akir Šišić, dipl.pravnik	Akir Šišić, dipl.pravnik	Mr.sci.med.dr. Enis Hasanović		