



JAVNA ZDRAVSTVENA USTANOVA
DOM ZDRAVLJA
U BANJOJ LUCI

Sime Matavulja bb, Banja Luka, tel: 051/ 230-200, fax: 051/216-813, e mail: domzdravlja-bl@teol.net
www.domzdravljabanjaluka.com JIB:4400802010004, PIB 400802010004, Matični broj:1212761 Žiro račun: 571-010-00000792-16

POLITIKA BEZBJEDNOSTI I ZAŠTITA INFORMACIJA

1. UVOD

Javna zdravstvena ustanova „Dom zdravlja“ u Banjoj Luci u svom radu prikuplja, obrađuje, koristi i čuva značajnu količinu informacija, uključujući medicinske podatke o pacijentima, podatke o zaposlenima, poslovne, finansijske i druge povjerljive informacije.

S obzirom na prirodu zdravstvene djelatnosti, ovi podaci imaju poseban stepen osjetljivosti i njihova zaštita predstavlja zakonsku, profesionalnu i etičku obavezu Ustanove.

Politika bezbjednosti i zaštite informacija ima za cilj uspostavljanje sistemskog okvira za zaštitu povjerljivosti, integriteta i dostupnosti informacija kojima JZU „Dom zdravlja“ u Banjoj Luci raspolaže, bez obzira na oblik u kojem se nalaze (elektrosni, pisani ili usmeni).

Ova politika definiše osnovna pravila, principe i odgovornosti u vezi sa upravljanjem informacionom bezbjednošću u skladu sa relevantnim zakonima.

2. OPŠTE ODREDBE

Politika bezbjednosti i zaštite informacija (u daljem tekstu: „Politika“) je temeljni akt kojim se u Ustanovi uspostavlja okvir za bezbjednu i zakonitu obradu, zaštitu, čuvanje i pristup informacijama i ličnim podacima, u skladu sa Zakonom o zaštiti ličnih podataka Bosne i Hercegovine (Sl. glasnik BiH, br. 12/25), Zakonom o zdravstvenoj zaštiti Republike Srpske (Sl. Glasnik RS, 27/22 i 62/25) i drugim relevantnim zakonskim i podzakonskim aktima.

Primjena ove politike doprinosi sprječavanju neovlaštenog pristupa, gubitka, zloupotrebe ili oštećenja podataka, obezbjeđuje kontinuitet poslovanja Ustanove, kao i očuvanje povjerenja pacijenata, zaposlenih i drugih zainteresovanih strana.

Politika je obavezujuća za sve zaposlene, saradnike i treća lica koja na bilo koji način imaju pristup informacijama i informacionim sistemima Ustanove.

3. SVRHA I CILJEVI

Svrha i ciljevi ove Politike su:

- Osigurati visoku razinu bezbjednosti informacija i ličnih podataka korisnika, zaposlenih i drugih subjekata,
- Uskladiti poslovne procese i informacione sisteme sa Zakonom o zaštiti ličnih podataka
- Uspostaviti jasne obaveze i odgovornost svih zaposlenih u pogledu zaštite informacija,
- Minimizirati rizike nenamjerne ili namjerne povrede podataka

4. PODRUČJE PRIMJENE

Politika se primjenjuje na sve informacione i komunikacione sisteme Ustanove, fizičke i digitalne podatke, uključujući lične podatke pacijenata, zaposlenih, dobavljača i drugih lica, bez obzira na medij obrade (papir, server, cloud, mobilni uređaj, itd.)

5. OSNOVNI PRINCIPI ZAŠTITE INFORMACIJA I LIČNIH PODATAKA

U cilju bezbjednosti i zaštite informacija, Ustanova obezbjeđuje i garantuje sljedeće:

5.1. Pravna i legitimna obrada podataka

Obrada ličnih podataka mora biti zasnovana na jasnoj pravnoj osnovi (npr. saglasnost, ugovorna ili zakonska obaveza) i u skladu sa svrhom i namjenom zbog koje su prikupljeni.

5.2. Transparentnost i jasna obavještenja

Ustanova jasno i razumljivo informiše sve nosioce podataka o tome koje podatke prikuplja, te u koju svrhu.

5.3. Prava nosilaca podataka

Osiguravaju se prava nosilaca podataka, uključujući:

- Pravo na pristup
- Pravo na ispravku,
- Pravo na brisanje („zaborav“)
- Pravo na ograničenje obrade
- Pravo na prenosivost ličnog podatka
- Pravo na prigovor

5.4. Minimalna obrada

Obraduju se samo podaci koji su nužni za ostvarivanje konkretne svrhe i ciljeva Ustanove (princip minimizacije)

5.5. Obavještanje o povredi ličnih podataka

Svaka povreda sigurnosti koja može ugroziti prava i slobode pojedinaca mora se prijaviti Agenciji za zaštitu ličnih podataka u roku od 72 časa od nastale povrede.

6. INFORMACIONA BEZBJEDNOST I TEHNIČKE MJERE

6.1. Fizička sigurnost

Zaštita servera i infrastrukture obezbjeđuje se kontrolom pristupa objektima, nadzornim sistemima i uputstvima za korištenje informacionog sistema.

6.2. Sigurnosni sistemi

Ustanova koristi antivirusnu zaštitu, ažurirane software pakete i firewall-e kako bi spriječila neovlašten pristup.

6.3. Enkripcija i rezervne kopije

Podaci moraju biti zaštićeni enkripcijom u prenosu i mirovanju, uz redovno pravljenje rezervnih kopija radi oporavka u slučaju incidenta.

7. ODGOVORNOST

Nepoštovanje ove Politike i zakonskih propisa može rezultovati disciplinskim i drugim pravnim posljedicama prema internim aktima Ustanove i važećim zakonskim propisima.

8. STAPANJE NA SNAGU

Ova Politika stupa na snagu danom donošenja.

Broj:01.013/50-406/26

Datum: 02.02.2026. godine



DIREKTORICA
Prof. dr. sci. med. Nevena Todorović
spec. porodične medicine,
supspecijalista angiologije

A handwritten signature in blue ink, written over the official stamp and text.