Јавна здравствена установа
Институт за физикалну медицину,
рехабилитацију и ортопедску хирургију
"Др Мирослав Зотовић" Бања Лука

П О Л И Т И К А
БЕЗБЈЕДНОСТИ И ЗАШТИТЕ ИНФОРМАЦИЈА

Бања Лука, септембар 2025. године

САДРЖАЈ

1 ПРЕДМЕТ И ПОДРУЧЈЕ ПРИМЈЕНЕ

1.1 Предмет документа

Политиком безбједности и заштите информација (у даљем тексту: Политика) се дефинишу основни принципи обезбјеђења безбједности и заштите информација у Јавној здравственој установи Институт за физикалну медицину, рехабилитацију и ортопедску хирургију „Др Мирослав Зотовић“ Бања Лука (у даљем тексту: Институт).

Овом Политиком дефинишу се основни принципи безбједности информација са циљем несметаног пословања, заштите повјерљивих информација и даљег успјешног пословања Института, као и постизања задовољства корисника квалитетом пружених услуга.

1.2 Подручје примјене

Политика се примјењује на нивоу Института и сви запослени дужни су се придржавати ове Политике.

За обезбјеђење примјене ове Политике и надзор над примјеном надлежан је помоћник директора за техничке послове и инфраструктуру, руководилац Службе за информационо-комуникационе технологије, шеф Одсјека за информациону безбједност и ИТ безбједност администратор.

2 ВЕЗА СА ДРУГИМ ДОКУМЕНТИМА

- Закон о здравственој заштити („Службени гласник Републике Српске“, број 57/22 и 62/25)
- Закон о заштити личних података БиХ („Службени гласник БиХ“, број 12/25)
- Стандарди за акредитацију и сертификацију болница у Републици Српској
- Стандарди за управљање безбједношћу информација (ISO 27001)

3 СКРАЋЕНИЦЕ И ДЕФИНИЦИЈЕ

Скраћеница/Дефиниција	Значење
Институт	Јавна здравствена установа Институт за физикалну медицину, рехабилитацију и ортопедску хирургију „Др Мирослав Зотовић“ Бања Лука

4 ОСНОВНИ ЦИЉЕВИ

Политика обезбјеђује и гарантује сљедеће:

- заштиту информација и интегритета информација од неовлаштеног приступа и/или измјене;
- одржавање повјерљивости информација;
- усаглашеност са законима и прописима из ове области;
- подршку политици кроз континуиране пословне планове који ће се одређивати, одржавати и тестирати у сталном практичном раду;
- едукацију запослених у свим организационим јединицама Института;

– документовање и истраживање свих повреда безбједног руковања информацијама.

Основни циљеви Политике су:

– стварање оквира који је неопходан за безбједни системски приступ идентификовању и борби против читавог низа потенцијалних ризика којима су изложене информације;

– класификација и одређивање степена повјерљивости информација;

– заштита информација о пацијентима који користе услуге Института;

– заштита информационе имовине која припада Институту;

– пружање поузданих информација запосленима и чување њихове повјерљивости у свим случајевима приступа постојећим информацијама.

5 ОСНОВНИ ПРИНЦИПИ

Руководство и запослени у Институту су свјесни потенцијалног утицаја до кога могу да доведу активности Института у смислу нарушавања, угрожавања и злоупотребе повјерљивих информација те изјавом кроз Политику безбједности и заштите информација изражавају спремност и обавезу да безбједност и заштита информација буду саставни дио свих активности у процесу пружања здравствених услуга.

Ову спремност Институт потврђује кроз примјену свих активности на безбједности и заштити информација које се одвијају у складу са важећим законским прописима и системом управљања безбједношћу информација.

У складу са овом спремношћу и препознавањем властите дужности, Институт успјешност цјелокупног система безбједности и заштите информација остварује кроз реализацију сљедећих принципа:

– дефинисање и успостављање интерних процедура и упутстава у складу са овом Политиком, важећим законима, прописима и контролама безбједности информација;

– поштовање, спровођење и усклађивање система безбједности и заштите информација са законским прописима, статутарним или уговорним обавезама, као и другим захтјевима у овој области;

– унапређење процеса и организације рада и континуирано унапређење ефективности и ефикасности система безбједности и заштите информација;

– одговорно управљање и прихватљиво коришћење информационе имовине кроз додјелу власништва и класификовање информација према дефинисаним критеријумима, у циљу осигурања одговарајућег нивоа заштите информација;

– детектовање циљева и успостављање процеса безбједности људских ресурса кроз дефинисање система правила понашања која обавезују запослене да разумију и прихвате своју одговорност и улогу у вези безбједности и заштите информација у свим фазама прије, у току и код престанка или промјене радног ангажмана у Институту;

– управљање физичком безбједношћу имовине и опреме ради спречавања прекида пословања Института, тј. спречавање неовлашћеног приступа, губитка, оштећења, крађе и слично;

– успостављање управљања резервним копијама почев од одређивања информација које се чувају, дефинисања учесталости израде у зависности од класификације информација,

тестирања, рестаурације информација до исправне манипулације медијумима за чување резервних копија;

- успостављање система правила понашања и контрола за размјену датотека и софтвера преко спољне мреже с циљем уклањања ризика изложености уноса малициозног и неауторизованог софтвера;
- прописивање обима коришћења и размјене информација кроз дефинисање ауторизованих корисника за коришћење одређене групе или цијеле класе информација, и упознавање запослених о правима власништва над информацијама Института;
- дефинисање правила о забрани инсталације и коришћења неауторизованог софтвера на уређајима који приступају ИТ инфраструктури Института, независно да ли су уређаји у власништву Института или не;
- управљање ризицима од неауторизованог приступа и посљедично нарушавање интегритета и повјерљивости информација кроз систем контролних механизама, којима се врши верификација корисника на систему, ауторизација за обављање одређених задатака и преузимање одговорности за изршену акцију над информационом имовином;
- успостављање разгранате контроле приступа по свим нивоима ИТ инфраструктуре, од пословних апликација, алата, оперативних система и другог системског софтвера, мреже и мрежних ресурса, све до посебно осјетљивих мобилних уређаја и мобилне инфраструктуре и рада на даљину;
- заштита и тајност информација примјеном безбједносних принципа укључујући понашање, организационе поступке и примјењене технолошке методе у складу са дефинисаном безбједносном категоријом којој информација припада, а у циљу спречавања ризика од неауторизованог објављивања, обраде или приступа подацима;
- управљање инцидентима нарушавања безбједности информација са становишта препознавања инцидената и успостављања поступака за благовремени и адекватан одговор на инциденте, планови за њихово отклањање, извјештавање о догађајима у вези са безбједношћу информација и слабостима, предузете акције праћења инцидената и побољшања;
- управљање континуитетом пословања као мјери одговора у случају катастрофе, уз дефинисање плана опоравка од катастрофе, активности са дефинисаним тимом и одговорностима за инцидентне ситуације и обавезама тестирања и предузимања акција послије сваког нежељеног догађаја са интегрисаним поступцима за очување безбједности информација у непредвиђеним околностима;
- редовно оспособљавање и мотивисање запослених за квалитетно обављање послова из домена безбједности информација и подизање свијести и охрабривање запослених са циљем да превентивно дјелују, мјењају навике и укључе се у настојање Института да побољша своје пословање;
- периодично преиспитивање система безбједности и заштите информација у сврху процјене да ли се примјењују у потпуности и да ли су погодни за остваривање политика, циљева и стратегија из ових области са циљем остварења одрживог пословања.

6 ПОЈАМ И ЗНАЧАЈ

6.1 Појам информација

Информација је податак са одређеним значењем, који има употребну вриједност односно сазнање које се може пренијети у било којем облику (писаном, аудио, визуелном, електронском или неком другом). Да би се информацијама могло квалитетно управљати потребно је информације на адекватан начин класификовати, прецизно им одредити сврху, вриједност, доступност као и остале параметре.

Савремено пословање карактерише проток великог броја информација које су потенцијално изложене бројним пријетњама и злоупотребама. Власништво над информацијама и њихова употреба постали су кључни за функционисање државних, привредних и јавних субјеката. Из тога разлога намеће се потреба за контролу пријема, преноса, чувања, обраде, дистрибуције те заштите информација.

6.2 Појам безбједности информација

Информације и њима припадајући подаци, затим процеси и системи (хардверски, софтверски, мрежни итд.) који се користе за њихово генерисање, обраду, пренос, меморисање као и приступ представљају важан дио пословне имовине Института коју је потребно адекватно заштитити ако се жели нормално пословање које ће обезбједити опстанак и развој.

Безбједност информација у савременим условима постала је један од кључних фактора развоја, због чега се успостављају бројни стандарди који укључују најбољу праксу и препоруке о безбједном управљању информацијама.

Појам безбједности информација односи се на:

- информатички аспект, гдје се анализирају и дефинишу перформансе ИТ опреме, права приступа, криптовања, лозинке, протоколи, политике са аспекта појаве ризика по сигурност података и информација;
- административни аспект, гдје се дефинишу јасна упутства, политике и процедуре за генерисање информација, њихову дистрибуцију, чување (складиштење);
- физички аспект, гдје се утврђује физичка контрола приступа, евиденција запослених, видео надзор, заштита радних просторија и слично.

Информациони ресурси могу да буду угрожени дјеловањем различитих фактора. Претње могу долазити од: запослених, ниске свијести о потреби заштите информација, пораста умрежености и дистрибуиране обраде података, пораста сложености и ефективности хакерских алата и вируса, e-mail-ова, пожара, поплава, земљотреса итд.

Без обзира на извор претње, основни циљеви заштите информација су: обезбјеђивање континуитета пословања и минимизација ризика од потенцијалних штета (хаварија). Ово се постиже, прије свега, превенцијом штетних догађаја и смањењем њиховог потенцијалног утицаја.

Из горе наведеног указује се потреба за имплементацијом адекватног система за заштиту и безбједност информација у Институту.

Сврха оваквог приступа информацијама је да обезбједи и заштити информације и имовину Института од свих пријетњи, било интерних или екстерних, случајних или намјерних а кроз успостављање, имплементацију, извршавање, контролу, преиспитивање, одржавање и побољшање система управљања безбједношћу информација.

7 МЈЕРЕ БЕЗБЈЕДНОСТИ ИНФОРМАЦИЈА

Безбједност информација обезбјеђује се примјеном мјера у циљу заштите повјерљивости, цјеловитости и доступност информација и заштите од sajber пријетњи и инцидената мрежних и информационих система.

7.1 Заштита информација

Повјерљивост информација подразумјева да је информација доступна само лицима која су овлашћена да остваре приступ или поступе са том информацијом.

Цјеловитост информација подразумјева очување постојања, тачности и комплетности информација, као и заштиту процеса или програма који спречавају неовлаштено мијењање информација.

Доступност информација подразумјева да овлаштени корисници могу да приступе информацији увијек када за тим имају потребу.

Заштита информација обухвата превенцију и отклањање штете од губитака, откривања или неовлашћене измјене информације. Заштита информација односи се на:

- правила за поступање са информацијама;
- садржај и начин вођења евиденције о извршеним приступима информацијама;
- надзор безбједности информација.

Заштита од sajber пријетњи и инцидената мрежних и информационих система подразумјева:

- физичку заштиту – обухвата заштиту објеката, простора и уређаја у којем се налазе информације и мрежни и иформациони системи;
- заштиту мрежних и информационих система – обухвата заштиту информација које се обрађују, складиште или преносе у мрежном и информационом систему, као и заштиту повјерљивости и доступности мрежног и информационог система у процесу планирања, пројектовања, изградње, употребе, одржавања и престанка рада тог система;
- управљање sajber безбједносним ризицима – односи се на примјену мјера којима се обезбјеђује заштита од sajber пријетњи и инцидената мрежних и информационих система, корисника тих система и других лица на које оне утичу.

8 ПЛАН ОПОРАВКА У СЛУЧАЈУ НЕЖЕЉЕНИХ ИКТ ДОГАЂАЈА

План опоравка у случају нежељених ИКТ догађаја (енгл. Disaster Recovery Plan) је документ који садржи детаљна упутства о поступцима у случају критичних догађаја као што су sajber напади, природне катастрофе, неисправна опрема и слично. План се састоји од стратегија за минимизирање негативних учинака критичних догађаја како би Институт могао брзо наставити са радом.

Прекиди у пословања Института у случају критичних догађаја могу довести до незадовољства корисника услуга, губитка прихода и штете Институту. Што је процес опоравка дужи то је негативни утицај на пословање већи. Стога би добро осмишљен План опоравка у случају нежељених ИКТ догађаја требао гарантовати брзи опоравак од прекида и поремећаја, без обзира на њихов извор.

Сигурносне копије или репликације података су облици рјешења за опоравак од катастрофе и саставни су дио Плана опоравка у случају нежељених ИКТ догађаја. Осигуравање заштите

података и одржавање могућности поврата услуга и апликација у случају опоравка од катастрофе континуиран је, оперативни процес.

Опоравак од катастрофе зависи од дуплирања података и рачунарске обраде на секундарну локацију на коју катастрофални догађај не утиче. У случају губитка података због sajber напада, природне катастрофе, неиправне опреме и слично, врши се поврат изгубљених података са секундарне локације на којој су подаци спремљени.

За израду и редовно ревидирање Плана опоравка у случају нежељених ИКТ догађаја надлежна је Служба за информационо-комуникационе технологије.

9 ПРИЛОЗИ И ОБРАСЦИ

9.1 Прилози

Нема прилога.

9.2 Обрасци

Нема образаца.

10 ТАБЕЛА ИСТОРИЈЕ ИЗМЈЕНЕ ДОКУМЕНТА

Назив документа	Број документа	Издање	Власник документа	Важи од	Важи до
Политика безбједности и заштите информација у Заводу	-	2		29.01.2014. године	28.05.2024. године
Политика безбједности и заштите електронских информација у Заводу	-	1		23.04.2015. године	28.05.2024. године
Ова два документа су спојена у ову Политику					
Политика безбједности и заштите информација	ОА-35-01	1	Служба за информационо-комуникационе технологије	28.05.2024. године	28.07.2025. године
Политика безбједности и заштите информација	ОА-35-01	2	Служба за информационо-комуникационе технологије	28.07.2025. године	15.09.2025. године
Политика безбједности и заштите информација	ОА-35-01	3	Служба за информационо-комуникационе технологије	15.09.2025. године	-

11 ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Измјене и допуне ове Политике врше се на начин и по поступку који је прописан за њено доношење.

Ова Политика ступа на снагу дана 15.09.2025. године, од када се и примјењује. Ступањем на снагу ове Политике престаје да важи Политика безбједности и заштите информација ОА-35-01 издање 2 од 28.07.2025. године.

Број: 03-01-21271/25

Датум: 10. 09. 2025

ДИРЕКТОР
ИНСТИТУТА

Проф. др Горан Талић прим. др мед.
специјалиста ортопедије са
трауматологијом