



ЈАВНА ЗДРАВСТВЕНА УСТАНОВА
ДОМ ЗДРАВЉА
У БАЊОЈ ЛУЦИ

ПОЛИТИКА БЕЗБЈЕДНОСТИ И ЗАШТИТЕ ИНФОРМАЦИЈА

Јавна здравствена установа “Дом здравља” у Бањој Луци (у даљем тексту: Установа) референтна је Установа за примарни ниво здравствене заштите.

У Установи је препознат и признат потенцијални утицај до кога могу да доведу активности у смислу нарушавања, угрожавања и злоупотребе повјерљивости информација, те овим изражавамо спремност и обавезу да безбједност и заштита информација буде саставни дио свих активности у процесу пружања здравствених услуга. Ова спремност се види кроз досљедну примјену Политике безбједности и заштите информација у свим организационим јединицама Установе.

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). Појам безбједности информација не односи се искључиво на техничке мјере заштите (лозинке, заштита компјутерских програма, права приступа и сл.) већ подразумјева и административне (безбједоносне политике, правилнике, процедуре), као и физичке мјере заштите (видео надзор, заштита просторија, физичка контрола приступа, итд.)

Информациона безбједност 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.

Из горе наведеног указује се потреба за имплементацијом система за управљање и безбједност информацијама у Установи.

Намјена оваквог приступа информацијама је да обезбједи и заштити информације и имовину од свих пријетњи, било интерних или екстерних, случајних или намјерних, кроз успостављање, имплементацију, извршавање, надзирање, преиспитивање, одржавање и побољшање система менаџмента безбједности информацијама (ИСМС).

Имплементација ове политике и правила је важна за одржавање интегритета информационог система за пружање услуга.

Политика безбједности и заштите информација обезбеђује и гарантује слиједеће:

- Заштићеност информација од неовлаштеног приступа;
- Одржавање повјерљивости информација;
- Усаглашеност са законима и прописима из ове области;
- Интегритет информација кроз заштиту од неовлаштене измјене;
- Омогућен приступ и измјене информација овлашћеним лицима када је то потребно;
- Подршку политици кроз континуиране пословне планове који ће се одређивати, одржавати и тестирати у сталном практичном раду;
- Обучавање запослених у свим организационим јединицама Установе;
- Разматрање и истраживање свих повреда безбједног управљања информацијама;
- Документовање свих повреда безбједности.

Сви запослени су одговорни за имплементацију политике безбједности и заштите информација и морају да пруже подршку руководству које је прописало политику и циљеве.

Основни циљеви ове политике су:

- Заштита информација Установе;
- Класификација и одређивање степена повјерљивости информација;
- Заштита информација о пацијентима који користе услуге Установе;
- Заштита информационе имовине која припада Установи;
- Пружање поузданих информација запосленима и чување њихове повјерљивости у свим случајевима приступа постојећим информацијама;

Сви запослени у Установи обавезни су да познају Политику и да је примјењују у раду.

Важи од: 31.01.2013.

Издање: друго

ДИРЕКТОРИЦА
Проф.др Гордана Тешановић