ГРАДСКИ ЗАВОД ЗА ЈАВНО ЗДРАВЉЕ, БЕОГРАД

ИЗЈАВА О ПРИМЕНИ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИНФОРМАЦИЈА

Руководство Градског завода за јавно здравље Београд (у даљем тексту Завод), својом Политиком безбедности информација одређује и дефинише оквир за постављање циљева безбедности информација, укључује посвећеност задовољењу применљивих захтева који су у вези са безбедношћу информација и сталном побољшавању система менаџмента безбедношћу информација.

Општи циљ менаџмента безбедношћу информација је да обезбеди и заштити информације и имовину од свих претњи, било интерних или екстерних, случајних или намерних кроз успостављање, одржавање, надзор, преиспитивање, и стално побољшавање система менаџмента безбедношћу информација (ИСМС - *Information security management system*).

ИСМС обухвата управљање безбедношћу информација свих пословних процеса Завода, као и процеса имплементације, техничке подршке, едукације и услуге у области ИКТ.

Руководство Завода у континуитету прати и подржава нова технолошка достигнућа у области ИКТ технологије, као и свим областима којима се бави и у складу са друштвено – економским условима обезбеђује њихову примену. Оваква пословна политика нам је осигурала статус поузданог партнера и колектива посвећеног делатностима широког спектра. ИКТ систем представља подршку комплетном пословању Завода и чини основ свих пословних процеса. Дигитализација здравственог система Србије нам је додатни мотив у процесу стандардизације и имплементације SRPS ISO/IEC 27001:2014.

Имплементиране стандарде квалитета услуга Завода смо унапредили применом SRPS ISO/IEC 27001:2014, који се системски прожима кроз све пословне процесе Завода.

На овај начин осигуравамо ниво квалитета услуга, гарантујемо континуитет у квалитету и боримо се за статус лидера у својој области.

Опсег тј. обим ИСМС-а је успостављен на основу:

- анализе интерних и екстерних фактора у вези са безбедношћу информација,
- захтева заинтересованих страна и повезаности између активности које реализује Завод и
- активности које се изводе од стране других организација / сарадника.

Имплементација ове политике и правила је важна за одржавање интегритета информационих система, база података и свих других података који настају кроз процесе пружања услуга корисницима и другим заинтересованим странама.

Политика ИКТ безбедности примењује се у свим организационим деловима и има намену да:

- Дефинише предмет и подручје примене Система менаџмента безбедношћу информација Завода;
- Успостави јасан правац деловања руководства у складу са пословним циљевима и да руководство искаже своју подршку и привржености систему безбедности информација;
- Дефинише циљеве и мере ИКТ заштите сагласно најбољој пракси дефинисаној у SRPS ISO/IEC 27001:2014
- Промовише начело да су ИКТ, укључујући и податке које се на њима обрађују, преносе и чувају у надлежности Завода;
- Укаже да запослени у Заводу, корисници ИКТ система наше установе, прихватају обавезу да неће кршити имплементирана и дефинисана правила понашања са аспекта безбедности података;

ГРАДСКИ ЗАВОД ЗА ЈАВНО ЗДРАВЉЕ, БЕОГРАД

ИЗЈАВА О ПРИМЕНИ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИНФОРМАЦИЈА

- Укаже да су сви корисници ИКТ система Завода лично одговорни за ИКТ ресурсе из свог поља рада и да ће се лично старати о инфомрационо технолошкој безбедности;
- Осигура да корисник прихвата обавезу да ИКТ систему Завода приступа само у сврху обављања посла за потребе установе;
- Промовише принцип да Завод надзире употребу ИКТ система из безбедносних разлога;
- Дефинише опште и посебне обавезе за управљање заштитом инфомрација, укључујући извештавање о инцидентима нарушавања безбедности;
- Дефинише и објашњава, предочава нашу безбедносну политику, принципе, критеријуме и захтеве за усаглашеност са посебним значајем за нашу установу;
- Дефинише последице кршења политике кроз имплементирање интерне документе и правилнике;;
- Документовано опише кључне процесе и њихово међусобно деловање у ИСМС;
- Обухвати документоване процедуре које се примењују у ИСМС и да се позове на процедуре дефинисане у оквиру интегрисаног система менаџмента имплементираног у Заводу;
- Служи као стални, основни документ за управљање безбедношћу информација, његову ефикасну примену и одржавање
- Служи као основ за стална побољшања Система управљања безбедношћу информација обезбеђењем потребних услова у оквиру ИКТ система које захтева поступак испитивања, доказе и извештаје о провери и тестирању ИКТ ресурса, квалитетну и адекватну опрему која омогућава процесе заштите података / информација;
- Континуираним надзором над радом особља и поступком испитивања;
- Едукацијом особља овлашћеног за имплементацију, мониторинг, извештавање, унапређење SRPS ISO/IEC 27001:2014.

У складу са усвојеном Политиком менаџмента безбедношћу информација уз постојеће имплементиране стандарде квалитета, одржавамо висок квалитет својих услуга, дигитализацијом постојећих података пратимо техничко технолошке иновације и максимално штитимо интерес појединца и заједнице, побољшавамо своје инфраструктурне и људске ресурсе, уводимо нове технике и вештине у у пословне процесе.

Обавезујем се да ћу у оквиру својих овлашћења, а у складу са расположивим ресурсима, обезбедити спровођење Политике безбедности података, кроз непристрасност и поверљивост, као и стално унапређење ефективности система менаџмента безбедношћу информација. Све ово ће бити могуће континуираним преиспитивањем оперативних процедура, коришћењем креираних политика, реализацијом свеукупних циљева, као и детаљном анализом резултата провера, применом корективних мера, преиспитивањем од стране руководства, оцењивањем ризика, анализом података и резултата испитивања оспособљености.

Београд, 07.12.2020. године

ДИРЕКТОР

Проф.др Душанка Матијевић