Политике безбедности информација

(ISO/IEC 27001:2022)

Информације су витална вредност ЈКП Шумадија Крагујевац и захтевају одговарајућу заштиту поверљивости, интегритета и доступности.

Ово правило управљања информационом сигурношћу пружа смер и подршку за управљање информационом сигурношћу у складу са пословним захтевима ЈКП Шумадија Крагујевац и релевантним законским прописима. Она прописује захтеве за успостављање информационе сигурности и праксе у свакодневном коришћењу информационих система ЈКП Шумадија Крагујевац.

Ова политика састоји се од скупа политика који одражава преданост ЈКП Шумадија Крагујевац сигурности података и континуираном побољшању.

Обавезе и деловања руководства у погледу сигурности информација дефинисане су овом Политиком, Одлуком директора о успостављању система менаџмента безбедношћу информација, именовању Представника руководста за ИМС, дефинисању надлежности Тима за безбедност информација, као и Одлуком директора о именовању Менаџера за безбедност информација и осталом документацијом ИМС.

Наведеним документима раздвојене су дужности и подручје одговорности учесника у обезбеђењу безбедности информација, тако да су смањене могућности за неовлашћену или ненамерну модификацију или злоупотребу имовине Предузећа.

За одржавање контакта са релевантним овлашћеним телима, заинтересованим странама, меродавним специјалистичким форумима и професионалним удружењима из домена безбедности, надлежни су Представник руководства за ИСМС, Менаџер за безбедност информација и остали чланови Тима за безбедност информација.

Елементи безбедности информација су укључени у управљање свим делатностима ЈКП Шумадија Крагујевац.

Ова Политика се односи на све запослене у ЈКП Шумадија Крагујевац и особе које раде под њеним именом. Тим за безбедност информација одговоран је за преглед и ажурирање ове Политике у редовним интервалима или ако се догодила значајна промена.

Корисници информационог система ЈКП Шумадија Крагујевац су одговорни за заштиту података које обрађују, допуњују или дистрибуирају.

Свако кршење правила у области безбедности информација ће бити истражено, а ако је узрок пронађен, због намерног занемаривања или немара, биће третиран као дисциплински прекршај.

Копија: _____	Израдио	Контролисао	Одобрио
Име и презиме	Марина Милосављевић	Горан Стојковић	Марко Вујновић
Потпис			
Број страна: 5		Издање: друго	Датум: 01.04.2024.г

Листа измена документа

Број измене	**Датум измене**	**Промењене стране**	**Број измене**	**Датум измене**	**Промењене стране**

Политика мобилних уређаја

Документом ИУ.25.01 - Безбедност преносивих компјутера и телефона утврђене су одговарајуће мере безбедности за заштиту од ризика при раду са преносивим рачунарима и телефонима.

Сигурносним мерама ИСМС дефинисани су оперативни планови и процедуре за активности при раду са удаљености.

Политика управљања безбедности људских ресурса

Овом политиком ЈКП Шумадија Крагујевац осигурава да запослени, добављачи и трећа лица, разумеју своје одговорности. Служи за одређивање улога и за смањење ризика од људске грешке, крађе, преваре или злоупотребе.

Сигурносне улоге и одговорности су описане у Пословнику ИМС.

Сви запослени ће добити одговарајућу обуку и бити редовно обавештавани у вези са политиком и процедурама ЈКП Шумадија Крагујевац, као и са релевантним информацијама за њихов посао и функцију. Ове обуке и тренинзи су у вези сигурносним захтевима, правном одговорности и пословном контролом. Такође представљу и обуку о правилној употреби информација као и многе друге аспекте који ће помоћи како би се смањили могући сигурносни ризици.

Сви запослени, сарадници и треће стране ће вратити сву организацијску имовину у свом поседу по престанку њиховог запослења, уговора или споразума, и њихова права приступа ће бити уклоњена или прилагођена промени.

Детаљи у вези организације и обезбеђења обука наведени су у ИП.12.02 – Менаџмент кадровским пословима

Политика управљања вредностима Предузећа (средствима)

Евидентирање имовине битне за безбедност информација, њихова класификација и вредновање са аспекта поверљивости, интегритета и расположивости врши се у складу са ИП.25.01 – Менаџмент безбедношћу информација, и ИП.25.02 Класификовање и означавање информација.

Правила за прихватљиво коришћење информационе имовине су дефинсана и у осталим докумената ISMS.

Политика управљања контролом приступа

Кроз ову политику ЈКП Шумадија Крагујевац осигурава да контрола приступа информацијама у информационом систему, унутар ЈКП Шумадија Крагујевац, буде на одговарајући начин дефинисана. Приступ информационом систему ЈКП Шумадија Крагујевац контролише се кроз дефинисање и редован преглед права приступа за различите кориснике и регистрацију корисника са одговарајућим лозинкама за све оперативне системе и апликације.

На запосленима је одговорност за памћење шифара, које ће држати само за себе.

Сви запослени ће имати као праксу ‘clear desk’ и ‘clear screen policy’, што значи да ће после радног времена или кад нису поред рачунара држати чист десктоп од отворених

докумената које садрже информације и да ће користи ‘screen saver’ са шифром.

Детаљи везани за обезбеђење контроле приступа дефинисани су у ИУ.25.04 Формирање лозинке, ИУ.25.05 Одобравање права приступа базама података и ИУ.25.06 Ризици којим организацију могу изложити трећа лица.

Политика управљања физичким обезбеђењем и обезбеђењем од спољашњих утицаја и управљања опремом

Ова политика осигурава да се уведу одговарајуће физичке контоле ради смањења ризика по безбедност информација и информационог система. У ЈКП Шумадија Крагујевац у складу са ИУ.25.05 Одобравање права приступа базама података и ИУ.25.06 Ризици којим организацију могу изложити трећа лица, дефинисане су контроле да би се осигурали објекти и опрема у њима од неовлашћеног физичког приступа, манипулације и крађе.

Физички приступ је на локацији ЈКП Шумадија Крагујевац контролисан за овлашћене особе. Посетиоци се примају и упућују до одредишта на контролисан начин. Врата остају закључана након радног времена или када у канцеларијама нема никога дуже време.

Објекти и канцеларије ЈКП Шумадија Крагујевац су заштићене против-пожарним системом.

Само запослени овлашћен од стране руководства може поставити/инсталирати или однети нешто од опреме, података и софтвера ван канцеларија.

Зона безбедности у којој се налазе осетљиве или критичне информације и опрема за обраду информација (сервери) је канцеларија сустем администратора, обезбеђена је кључем и под видео надзором је.

Политика управљања комуникацијама и операцијама

Ова политика наводи одговорности запослених у осигурању исправног и сигурног функционисања информационог система ЈКП Шумадија Крагујевац.

Све промене у информационом систему морају бити одобрене од стране руководећег кадра. Детаљи о управљању променама дати су у ИП.25.03 Управљање променама и капацитетима.

Заштита интегритета софтвера и информације од ‘злонамерног кода' реализује се у складу са ИУ.25.11 Контроле против злонамерног софтвера.

Сигурносна копија информација формира се у складу са ИУ.25.03 Складиштење података.

Поступци и одговорности за активности надгледања система у циљу откривања неовлашћених активности обраде информација наведени су у ИП.25.04 Евидентирање и праћење догађаја.

Поступци и одговорности за управљање инсталацијом софтвера у оперативном систему са циљем обезбеђења сигурности системских датотека дефинисани су у ИУ.25.08 Инсталација софтвера у оперативном систему.

Поступци и одговорности за управљање системом безбедности информација са циљем смањења ризика од искоришћавања јавно објављених техничких рањивости и разматрање провера дефинисани су у ИУ.25.09 Менаџмент техничким рањивостима и разматрање провера.

Комуницирање унутар предузећа и са окружењем и обезбеђење заштите информација у мрежама дефинисани су у ИП.25.05 Безбедност комуникација и ИУ.25.10 Обезбеђивање услуга на јавним мрежама.

Политика набавке, развоја и одржавања софтвера и односа са добављачима

ЈКП Шумадија Крагујевац настоји да безбедност сврста као интегрисани део свих информационих система у свом саставу било да су они купљени или интерно развијени. У том циљу, информациони системи се анализирају, тестирају и, уколико је потребно, имплементира се контрола путем енкрипције.

Одговарајући уговор, споразум о обради података морају бити успостављени и примењиви пре него што се ангажује добављач услуга у облику да обрађује, чува или преноси поверљиве или личне податке.

Више о овим детаљима, може се пронаћи у ИУ.25.08 Инсталација софтвера у оперативном систему и ИУ.25.10 Обезбеђивање услуга на јавним мрежама.

Политика управљања безбедносним инцидентима

У ЈКП Шумадија Крагујевац имплементиран је систем за управљање инцидентима, да би осигурао лакши приступ информацијама, решио безбедносне слабости, као и друге инциденте и штетне догађаје.

Дефиниције горе поменутих категорија:

- **Слабост:** грешка или слаба тачка у управљању информационим системом
- **Догађај:** идентификована ситуација у систему, сервису или мрежном стању које указује на могућу провалу политике информационог система, неисправно обезбеђење или претходно непознату ситуацију која може бити у вези са безбедношћу
- **Инцидент:** серија непожељних и неочекиваних догађаја, која има велику вероватноћу да компромитује посао и запрети информационом систему

Сви корисници информационог система ЈКП Шумадија Крагујевац су одговорни за брзо извештавање о свакој сигурносној слабости, догађају и инциденту који се јавља током дневне оперативне активности.

Систем администратор процесира извештаје о инцидентима и решава их на основу приоритета и доступности ресурса.

Детаљи о управљању безбедносним инцидентима наведени су у ИП.25.04 Евидентирање и праћење догађаја и ИУ.25.09 Менаџмент техничким рањивостима и разматрање провера.

Политика управљања континуираним пословањем

Дугорочни циљ политике је да осигура јасан смер за подршку управљању континуитетом пословања и пружа основу за планирање како би се осигурала непосредна реакција организације након штетног догађаја.

Систем за континуирано пословање, се редовно проверава и по потреби ажурира.

У ИП.25.06 План пословног континуитета је установљен поступак који би ЈКП Шумадија Крагујевац морала да предузме да би наставила пословне процесе упркос евентуалној ванредној ситуацији (у области безбедности информација).

Политика управљања усклађеношћу система менаџмента безбедношћу информација

Циљ ове политике је да се избегне било какво одступање (неусклађеност) са утврђеним обавезама за усклађеност.
Сва интерна и екстерна документа (укључује све обавезе за усклађеност) су заштићена и њима се управља на начин дефинисан у ИП.00.02 - Управљање документима и записима.