ИНСТИТУТ ЗА ЈАВНО ЗДРАВЉЕ- Н И Ш
Телефон 4226-448, 4226-384; Телефакс 4225-974; Пошт.фах 39
Булевар др Зорана Ђинђића 50, 18000 Ниш, Србија

Број : 07/1-570
14.12. 2023. године

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16 и 94/17 и 77/2019), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС”, број 94/16), и овлашћења из чл 20. Статута Института за јавно здравље Ниш (у даљем тексту: Институт), Управни одбор Института, на седници од 14.12.2023. године доноси

Правилник о безбедности информационо-комуникационог система Института за јавно здравље Ниш

I ОСНОВНЕ ОДРЕДБЕ

Предмет Правилника

Члан 1.

Правилником о безбедности информационо-комуникационог система Института за јавно здравље Ниш (у даљем тексту: Правилник) у складу са Законом о информационој безбедности (у даљем тексту: Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система Института (у даљем тексту: ИКТ систем).

Циљеви Правилника о безбедности

Члан 2.

Циљеви доношења Правилника о безбедности ИКТ система су:

1. дефинисање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2. спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
3. подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4. прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
5. свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Правилника о безбедности

Члан 3.

Мере заштите ИКТ система које су ближе уређене овим Правилником служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за све запослене.

Запослени Института_морају бити упознати са садржином Правилника о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

Администратор ИКТ система, помоћници директора и начелници центара одговорни су за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност запослених

Члан 4.

Запослени Института су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице (администратора ИКТ система) о свим сигурносним инцидентима и проблемима.

Непоштовање одредби Правилника о безбедности, као и свако угрожавање или нарушавање информационе безбедности, повлачи одговорност за повреду радне обавезе запосленог.

Предмет заштите

Члан 5.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски код, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

II МЕРЕ ЗАШТИТЕ

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

Члан 6.

Интерни акти којима ће бити уређене обавезе и одговорности запослених у вези са управљањем информационом безбедношћу између осталих су:

- Правилник о унутрашњој организацији и систематизацији радних места;
- Уговори о раду;
- Изјаве о поверљивости;
- Уговори о чувању поверљивости са правним лицима;
- Процедура о приступу посебно осетљивим подацима и информацијама у ИКТ систему.

Институт ће донети појединачни акт, у складу са актом о систематизацији, којим одређује одговорна лица за обезбеђивање и праћење безбедности информационог система. Сви запослени морају бити упознати са процедуром заштите безбедности ИКТ система.

Институт утврђује начин доделе овлашћења за приступ ИКТ систему, степен обуке и квалификацију запослених, начин одобравања приступа запосленима од стране руководиоца, односно непосредно надређеног лица. У случају непоштовања одредби које уређују информациону безбедност, запослени подлежу дисциплинској одговорности, у складу са општим актима Института.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 7.

Институт дозвољава рад на даљину и употребу мобилних уређаја од стране запослених, уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја.

Коришћење мобилних уређаја

Мобилни уређаји подразумевају све преносне електронске уређаје намењене за комуникацију на даљину.

У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони, PDA и сви други мобилни уређаји који садржи податке и имају могућност повезивања на мрежу.

У случају коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који обављају и у потпуности разумеју своју одговорност

Члан 8.

Институт ће се старати да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају. Њихове одговорности су утврђене уговором о раду или о ангажовању за рад ван радног односа и интерним актом.

Провера кандидата и услови запошљавања

Институт спроводи радње у циљу провере испуњености услова сваког појединачног кандидата за запослење, у складу са одговарајућим прописима и етичким правилима, сразмерно пословним захтевима, класификацији информација којима ће имати приступ и сагледаним ризицима.

Сви запослени и радно ангажовани појединци по другом основу којима је додељен приступ поверљивим информацијама, морају штитити поверљивост и старати се о заштити података и информација од трећих лица.

Обавезе у току запослења

Руководство Института је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и касније усвојеним процедурама.

Институт у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

-Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;

-Штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама;

-Спроводи програме заштите на конзистентан и уједначен начин у свим организационим јединицама;

-Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

Запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура континуирано се обучавају у циљу унапређења техничког и технолошког знања и предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Поступак против запослених у случају повреде радне обавезе

Институт ће спроводити поступак због повреде радне обавезе против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и процедура које се примењују ради заштите безбедности информација.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Члан 9.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања.

Ова мера је ближе одређена:

-Процедуром о правима приступа информационом систему

-Уговором о раду

-Уговором о ангажовању лица ван радног односа.

За поступања приликом престанка запослења или ангажовања задужен је надређени руководилац који предузима следеће активности:

-проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату,

- прегледа све налоге и приступе систему који су били доступни запосленом,
- преузима од запосленог електронске и друге мобилне уређаје,
- утврђује начин контакта са бившим запосленим након одласка,
- проверава враћене мобилне уређаје и уређаје за преношење података,
- даје налог за укидање налога електронске поште и свих других права приступа систему Института на дан престанка радног односа или другог основа ангажовања бившег запосленог,
- прегледа све налоге за приступ одлазећег запосленог и прикупља приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
- преузима картице и друге уређаје којима се омогућава приступ пословним просторијама и опреми Института.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Пописивање имовине

Институт врши идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација.

Евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води администратор ИКТ система.

Надзор над имовином, прихватљиво коришћење имовине и њен повраћај

Запослени и друга лица, којима је дата одговорност за контролисање имовине дужни су да правилно управљају имовином.

Институт уређује правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација.

Запослени и екстерни корисници су обавезни да врате сву имовину Института коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком

Члан 11.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем за Институт.

Институт означава типове и локације података као поверљиве, интерне или јавне.

Имовина се означава уз помоћ идентификационих налепница које носе одговарајућу класификациону ознаку.

Институт класификациону шему поверљивости информација базира на четири нивоа:

- откривање не изазива никакву штету;
- откривање изазива мању непријатност или мању штету;
- откривање има значајан краткорочни утицај на пословање или тактичке циљеве;
- откривање има озбиљан утицај на дугорочне стратешке циљеве или угрожава опстанак.

Институт врши класификацију ради јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење;

- Подизања свести о вредности информације или документа;
- Заштите садржаја.

Заштита носача података

Члан 12.

Институт обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података.

Расходовање носача података (медијума)

Када више нису потребни, медијуми су расходују на безбедан начин, применом Процедуре за безбедно расходовање медијума.

Расходовање медијума на безбедан начин Институт врши свођењем на минимум ризика од могућег преузимања осељивих података од стране неовлашћених особа.

Процедуром за безбедно расходовање медијума који садрже поверљиве податке утврђују се различити начини процеса расходовања, а у складу са осетљивошћу података.

Ограничење приступа подацима и средствима за обраду података

Члан 13.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности података.

Корисницима је дозвољен приступ само мрежи и мрежним услугама за чије коришћење су овлашћени.

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Члан 14.

Институт управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

Управљање корисничким идентификаторима врши се уз поштовање следећих принципа:

- кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење;
- корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;
- периодично идентификовање и уклањање или онемогућавање вишеструких корисничких идентификатора;
- вишеструки идентификатори неког корисника се не издају другим корисницима.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

Шифре за приступ општим корисничким идентификаторима администратора се мењају променом корисника.

Запосленима и другим радно ангажованим корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.

Утврђивање одговорности корисника за заштиту сопствених средстава заутентификацију

Члан 15.

Аутентификације корисника којима је одобрен приступ систему врши се путем јединственог корисничког имена и шифре.

Сви корисници Института су дужни да:

- корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
- избегавају чување корисничког имена и шифре у писаном облику;
- промене шифру када примете да постоји било какав наговештај могућег компромитовања.

Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Члан 16.

У циљу заштите података Институт на основу процене ризика може да развија и имплементира политику коришћења криптографских контрола, и успоставља механизме и систем за управљање кључевима.

Криптозаштита обезбеђује:

Аутентификацију (идентификацију корисника и других системских ентитета који захтевају приступ или одобрење акције корисника);

Непорецивост (примена криптографских техника, најчешће дигиталног потписа, како би се добила потврда о извршавању или неизвршавању неке акције од стране појединачног корисника);

Поверљивост (применом шифровања врши се заштита осетљивих или критичних информација које се складиште или преносе);

Интегритет (непроменљивост података који се преносе).

Поступак криптографске контроле обухватиће:

- анализу и процене потреба примене криптографије у пословним процесима укључујући опште принципе према којима би пословне информације требало да се штите;
- ниво заштите се одређује узимањем у обзир типа алгоритма за криптовање података, јачине и квалитета криптографског алгоритма;
- примену шифровања за заштиту осетљивих података приликом преноса мобилним или другим медијумима, уређајима или преко комуникационих водова;
- управљање кључевима (заштита криптографских кључева, повраћај шифрованих података у случају губљења, компромитовања или оштећења кључева).

Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему

Члан 17.

Институт је дужан да предузме мере ради спречавања неовлашћеног физичког приступа објекту-просторијама у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација.

Опрема за обраду информација се штити закључавањем просторија у којима се налази.

Заштита канцеларија, просторија, средстава, као и заштита од претњи екстерних фактора из окружења

Институт обезбеђује и примењује одговарајућу контролу приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава. Такође, безбедним конфигурисањем се онемогућава приступ кључној опреми а у циљу спречавања видљивости поверљивих информација, активностима споља. Физичка заштита се планира и за случајеве природних катастрофа, непријатељских напада или несрећа.

Члан 18.

Постављање и заштита опреме

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа.

Опрема се поставља на месту које се може обезбедити од неовлашћеног приступа;

Опрема за обраду информација која служи за приступ и коришћење осетљивих података се поставља не места која нису видљива неовлашћеним особама;

Врши се редовна контрола система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, гас, електронске комуникације;

• Просторије са опремом треба редовно чистити од прашине;

• Забрањено је конзумирање хране и пића и пушење близини опреме за обраду информација;

• Опрема мора бити заштићена од атмосферских падавина.

Помоћне функције за подршку

Опрема се штити од прекида напајања, тако што се:

- помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
- капацитет помоћне опреме редовно процењује;
- редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова;
- обезбеђује вишеструко напајање са различитих траса.

Безбедносни елементи приликом постављања каблова

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од ометања или оштећења на следећи начин:

- водови напајања и телекомуникациони водови који улазе у просторије за обраду информација су подземни, онда када је то могуће, или имају адекватну алтернативну заштиту;
- каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње;
-за осетљиве или критичне системе се постављају оклопљени водови, користе се закључане просторије или кутије и примењује се електромагнетско оклапање ради заштите каблова.

Одржавање опреме

Опрема се одржава како би се осигурала њена непрекидна расположивост и неповредивост, и то на следећи начин:

- опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;
- поправке и сервисирање опреме обавља само особље овлашћено за одржавање;
- о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;
- осетљиве информације треба избрисати из опреме;
- пре враћања опреме у рад након одржавања, потребно је прегледати како би проверили да није неовлашћено коришћена или оштећена.

Опрема, информације или софтвер се измештају само уз одобрење одговорног лица.

Безбедност измештене опреме и имовине

На измештену опрему примењују се безбедносни механизми заштите, узимајући у обзир различите ризике приликом рада изван просторија.

Безбедно расходовање или поновно коришћење опреме

Сви делови опреме који садрже медијуме за чување података се верификују да би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњени.

Безбедност опреме корисника без надзора

Корисници треба да обезбеде да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.

Остављање осетљивих и поверљивих докумената и материјала

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

Запослени се обавезују на следеће активности:

1. Све осетљиве и поверљиве информације у штампаном или електронском облику запослени морају одложити на сигурно место на крају радног дана или када нису присутни на свом радном месту.
2. Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана.
3. Ормари и фиоке у којима се чувају поверљиви подаци морају бити закључани када се не користе, а кључеви не смеју бити остављени на приступачном месту без надзора.
4. Лаптопови морају бити везани уз помоћ одговарајуће опреме или закључани у фиоци. Таблети и остали преносни уређаји морају бити закључани у фиоци.
5. Носачи података као што су дискови и flash меморија морају бити одложени и закључани.
6. Шифре за приступ не смеју бити написане и остављене на приступачном месту.
7. Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, дефинишу се процедуре за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевивма измештања делова ИКТ система.

Члан 20.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен или неумрежен рачунар. Заштита од злонамерног софтвера се заснива на софтверу за откривање злонамерног софтвера и отклањање штете, на познавањуинформационе безбедности, као и на одговарајућим контролама приступа систему и управљању захтеваним и потребним променама.

Поступак контроле и предузимање мера против злонамерног софтвера

Институт кроз Процедуре одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Институт ће успоставити и процедуру о антивирусној заштити и процедуру о подизању свести запослених о информационој безбедности. У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави дипл. инг електронике.

У циљу заштите одупада у ИКТ систем, дипл. инг електронике је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета дипл. инг електронике може укинути приступ.

Заштита од губитка података

Члан 21.

Институт врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација и података

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих и log фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије омогућавају брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и израђују се у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

За чување заштитних копија користе се екстерни хард дискови.

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Члан 22.

У ИКТ систему Института формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Записивање догађаја

Институт прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са информационом безбедношћу, који се морају чувати и редовно преиспитивати, а посебно подаци о активирању и деактивирању система заштите, као што су антивирусни системи и системи за откривање упада.

Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

Институт спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за контролу промена и инсталацију софтвера.

Инсталацију и подешавање софтвера може да врши само односно запослени који има овлашћење за то.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

Институт врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

Ограничења у погледу инсталације софтвера

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедносним ризицима.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 25.

У циљу заштите података у комуникационим мрежама, уређајима и водовима врши се њихова контрола и заштита од неовлашћеног приступа.

Безбедност података који се преносе унутар Института, као и између оператора ИКТ система и лица ван оператора ИКТ система

Члан 26.

Заштита података који се преносе комуникационим средствима унутар Института између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са успостављеним процедурама и адекватним контролама над спровођењем истих. Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

Правила коришћења Интернета

Приступ садржајима на Интернету је дозвољен искључиво за пословне намене. На мрежи је омогућено надгледање, односно користи се поступак периодичне ревизије и контролисања логовања, како на пријему тако и на слању.

Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намену коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 27.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, Институт је у обавези да обезбеди информациону безбедност у свакој фази.

Анализа и спецификација захтева за информациону безбедност

У захтеве за нове информационе системе или за побољшање постојећих информационих система морају бити укључени захтеви који се односе на информациону безбедност и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Захтеви за информациону безбедност укључују:

Проверу идентитета корисника;

Доступност, поверљивост, непорецивост и интегритет података и имовине;

Надгледање пословних процеса;

Омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке кориснике.

Спецификација захтева обухвата аутоматску контролу која ће бити уведена у информациони систем, као и потребу да постоји и ручна контрола, која мора бити примењена при вредновању развијених или купљених пакета софтвера, намењених за пословне апликације.

Формално тестирање и процес имплементације ће се примењивати за све купљене производе.

У уговору са извођачем, односно испоручиоцем купљених производа, посебно се дефинишу захтеви за информациону безбедност.

У случају да безбедносна функционалност предложеног производа не задовољава одређен захтев, ризик и повезане контроле ће бити преиспитане пре куповине производа.

Заштита података који се користе за потребе тестирања ИКТ система односно делова система

Члан 28.

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера наведених у овом члану.

За потребе испитивања и тестирања ИКТ система, односно делова система, Институт ће избегавати коришћење оперативних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачног добављача, купца, запосленог или др. Уколико се за сврху испитивања користе лични подаци или неке друге поверљиве информације, онда се сви осетљиви подаци и информације пре коришћења штите анонимизацијом личних података, уклањањем садржаја или изменом текста садржаја у предметном делу.

За податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су подаци о личности коришћени приликом тестирања система, одговорни су запослени који обрађују те податке, у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 29.

Политика безбедности размене информација у пословним односима са пружаоцима услуга и између независних пружалаца услуга

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација Института, морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

Пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са Институтом.

Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга

Члан 30.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, Институт успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама

Члан 31.

Одговорност појединаца и поступак одговора на инциденте

У случају инцидента- нарушавања информационе безбедности одређује се особа овлашћена за контакт у случајевима нарушавања безбедности, као и контакт са надлежним органима.

Институт одређује администратора чији је задатак да придржавајући се процедура одређених овим чланом, планирају, детектују, анализирају и информишу надлежне у току и након инцидента.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени је дужан да о томе одмах обавести руководиоца, односно администратора.

Извештавање о догађајима у вези са безбедношћу информација

Сви запослени морају бити упознати са обавезом и Процедуром извештавања о догађајима у вези са информационом безбедношћу.

Извештавање о утврђеним слабостима система заштите

Сви запослени су у обавези да о уоченим и утврђеним слабостима ИКТ система известеадминистратора ИКТ система, у што краћем року, како би се инциденти нарушавања информационе безбедности спречили и спречио настанак штете.

Члан 32.

Институт примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

III ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Института

Члан 33.

Посебна обавеза Института је:

- да најмање једном годишње изврши проверу ИКТ система и
- по потреби изврши евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Института.

У случају елементарних и других већих непогода и ванредних околности, примењују се мере заштите ИКТ система у складу са Акционим планом Института за јавно здравље Ниш за поступање у елементарним и другим већим непогодама и ванредним приликама.

Ступање на снагу Акта о безбедности

Члан 34.

Овај Акт о безбедности ступа на снагу осмог дана од дана објављивања на огласној табли Института.

Ступањем на снагу овог правилника престаје да важи Правилник о безбедности информација -ИКТ безбедности у Институту за јавно здравље Ниш, број 07/1-389 од 09.08.2023. године.

Председник Управног одбора
Проф. др Саша Станковић

Овај Правилник је објављен на огласној табли Института дана 19.12.2023. године