На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, broj 6/2016,94/2017 и 77/2019), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Службени гласник РС“, бр. 94/2016) и члана 54. Статута ЈП Кикинда 03.05.2019. године, директор Данило С. Фурунџић дана 5.5.2020. године донео је

ЈАВНО ПРЕДУЗЕЋЕ ЗА КОМУНАЛНУ ИНФРАСТРУКТУРУ И УСЛУГЕ "КИКИНДА"
KIKINDA KOMMUNÁLIS INFRASTRUKTÚRA ÉS SZOLGÁLTATÓ KŐZVÁLLALAT
БРОЈ: 4936
ДАТУМ: 05. 05 2020.

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ЈП КИКИНДА

I Опште одредбе

Члан 1.

Правилником о безбедности информационо- комуникационог система ЈП Кикинде (у даљем тексту: Правилник) уређују се ближи садржај акта о безбедности информационо-комуникационих система од посебног значаја, начин провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја, утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система, (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система ЈП „Кикинда“ (у даљем тексту: Оператор).

Члан 2.

Информациона добра Оператора су сви ресурси који садрже пословне информације Оператора, односно сви ресурси путем којих се врши израда, обрада, чување, пренос, брисање и уништвање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и сл.

О информационим добрима води се евиденција послова на посебном обрасцу.

Евиденцију из става 2. овог члана води запослени у складу са важећом систематизацијом радних места (у даљем тексту: надлежни субјект ИКТ система).

Члан 3.

Мере прописане овим правилником се односе на све организационе јединице Оператора, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Оператора.

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса Оператора.

За праћење примене овог правилника обавезује се надлежни субјект ИКТ система.

Члан 4.

Под пословима из области безбедности ИКТ система сматрају се:

- послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност,
- послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности
- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Оператора, као и приступ, измена или коришћење средстава без овлашћења и без евиденције о томе.
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу.
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

II Мере заштите

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Оператора

Члан 5.

ИКТ системом управља надлежни субјект ИКТ система.

Надлежни субјект ИКТ система је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Оператора, да га обучи за коришћење ресурса ИКТ система, да по завршетку обуке од запосленог узме изјаву о обучености за коришћење ИКТ ресурса и да о истима води евиденцију.

Члан 6.

Сваки запослени-корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности.

Контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и над обављањем послова из области

безбедности целокупног ИКТ система Оператора обавља надлежни субјект ИКТ система у складу са систематизацијом радних места у Оператору.

У случају инцидента надлежни субјект ИКТ система, обавештава непосредног руководиоца/извршне директоре, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Нерегистровани корисници, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ Интернету али не и деловима мреже кроз коју се обавља службена комуникација.

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву Оператора, и који су подешени од стране надлежног субјекта ИКТ система да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности (електронска пошта).

Приступ ресурсима ИКТ система Оператора са удаљених локација, од стране запослених-корисника, у циљу обављања радних задатака, омогућен је путем заштићене VPN/интернет конекције.

Запосленом-кориснику, забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.)

Надлежни субјекат ИКТ система, контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава непосредног руководиоца, а та MAC адреса се уноси у «block" листу софтвера који се користи за контролу приступа.

Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен, осим ако је уређај у власништву ЈП Кикинда , оштећен и није обезбеђена замена.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води Надлежни субјекат ИКТ система, а по одобрењу непосредног руководиоца.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране Надлежни субјекат ИКТ система, могу се користити само за обављање послова у надлежности корисника-запосленог и то само у периоду када није могуће користити уређај у власништву Оператора.

Надлежни субјекат ИКТ система је дужан да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради backup података који се налазе у мобилном уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати податке у мобилни уређај.

3. Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места.

Надлежни субјект ИКТ система, је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса

Оператора, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденцију о изјавама новозапослених – корисника да су упознати са правилима коришћења ИКТ ресурса.

Свако коришћење ИКТ Оператора од стране запосленог-корисника, ван додељених овлашћење, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

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

Члан 7.

У случају промене радног места, односно надлежности корисника-запосленог надлежни субјект ИКТ система ће извршити промену права у коришћењу ИКТ система које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева непосредног руководиоца.

Члан 8.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида.

Корисник ИКТ ресурса, коме је престало радно ангажовање по било ком основу код Оператера, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 9.

Информациона добра Оператора су сви ресурси који садрже пословне информације Оператора, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем и сл.

Евиденцију о информационим добрима води Надлежни субјект ИКТ система, у папирној или електронској форми.

Предмет заштите ИКТ система су:

- хардверске и софтверске компоненте ИКТ система
- подаци који се обрађују или чувају на компонентама ИКТ система
- кориснички налози и други подаци о корисницима иноформатичких ресурса ИКТ система

Члан 10.

Мере прописане овим актом се односе на све организационе јединице ИКТ система Оператора, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Оператора.

Члан 11.

Мерама заштите ИКТ система Оператора обезбеђује се превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Ради заштите тајности, аутентичности и интегритета података, Оператор може да размотри коришћење одговарајућих мера криптозаштите.

Члан 12.

За обављање послова из области безбедности ИКТ система Оператора надлежан је референт за одржавање ИТ .

6. Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебним прописима.

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. Гласник РС", бр. 53/2011).

7. Заштита носача података

Надлежни субјект ИКТ система ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да:

- подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено одлуком генералног директора .
- подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника Надлежни субјект ИКТ система уз сагласност непосредног руководиоца /извршних директора.

Евиденцију носача на којима су снимљени подаци, води Надлежни субјект ИКТ система и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, генерални директор/извршни директор ће одредити одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на медијима, подаци морају бити неповратно обрисани, а ако то није могуће, такви медији морају бити физички оштећени, односно уништени.

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

Право приступа ИКТ систему имају само запослени, односни корисници који имају администраторске и корисничке налоге.

Администраторски налог је јединствен налог којим је омогућен приступ и администрација свих ресурса ИКТ система, само са једним корисничким налогом, као и отварање нових и измена постојећих налога, може да користи само запослени који је распоређен на послове и радне задатке администратора.

Кориснички налог је налог који садржи корисничко име и лозинку, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу којих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налог додељује администратор, на основу захтева шефа службе за кадровске и опште правне послове и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима - КАД. На основу послова и радних задатака запосленог, администратор одређује права приступа у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева шефа службе за кадровске и опште правне послове, односно непосредног руководиоца у организационим јединицима Оператера.

Члан 14.

Запослени у Оператеру је дужан да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система:

1. да користи информатичке ресурсе искључиво у пословне сврхе;
2. да прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Оператора и да могу бити предмет надгледања и прегледања;
3. да поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. да безбедно чува своје лозинке у односу на друга лица;

5. да мења лозинке сагласно утврђеним правилима;
6. да се, пре сваког удаљавања од радне станице, одјави са система, односно закључа радну станицу;
7. да захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8. да обезбеди сигурност података у складу са важећим прописима;
9. да приступа информатичким ресурсима само на основу изричито додељених корисничких права од стране надлежног субјекта;
10. да не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11. да не сме да на радној станици складишти садржај који не служи у пословне сврхе;
12. да израђује заштитне копије (backup) података у складу са прописаним процедурама;
13. да користи Intrnet и Intrnet e-mail сервис Оператора у складу са прописаним процедурама;
14. да прихвати да се одређене врсте информатичких интервенција обављају у утврђено време;
15. да прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
16. да прихвати инсталацију техника и програма у циљу сигурности ИКТ система.
17. да не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 15.

Приступ ресурсима ИКТ система одређен је врстом налога који запослени има.

Запослени који има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Запослени може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, сем администратору за подешавање корисничког профила и радне станице.

Запослени који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу кога/јих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налог додељује администратор, на основу захтева шефа службе за кадровске и опште правне послове у сарадњи са непосредним руководиоцем и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима - КАД,

а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева шефа службе за кадровске и опште правне послове, односно непосредног руководиоца.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира по матрици име.презиме, латиничним писмом без употребе слова ђ, ж ,љ, њ, ћ, ч, џ, ш. Уместо ових слова користе се слова из следеће табеле:

Ћирилична слова	Латинична слова
ђ	dj
ж	z
љ	lj
њ	nj
ћ, ч	c
ш	s
џ	dz

Лозинка мора да садржи минимум осам карактера латиничног писма комбинованих од малих и великих слова, цифара и специјалних знакова.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке.

Ако запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Запослени-корисник дужан је да мења лозинку најмање једном у периоду од годину дана.

Кориснички налог може да се се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр. лична карта са чипом и уписаним сертификатом).

Пријављивање у ИКТ систем Оператора се врши убацивањем медија са електронским сертификатом у читач картица.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 16.

Запослени-корисници користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама.

Запослени на пословима ИКТ су задужени за инсталацију потребног софтвера и хардвера за коришћење сертификата.

Запослени-корисници су дужни да чувају своје квалификоване електронске сертификате како не би дошли у посед других лица.

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

Члан 17.

Простор у коме се налазе рачунари за вођење база података и централни рачунар (сервер), мрежна или комуникациона опрема ИКТ система, организује са као административна просторија.

Административна просторија се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом.

13. Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем

Члан 18.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система.

Осим администратора система, приступ административној просторији могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу генералног директора или извршног/их директора.

Просторија из става 1. овог члана мора бити климатизована 24 сата дневно 7 дана у недељи са максималном температуром од 20 °C ± 2°C.

Просторија из става 1. овог члана мора бити видљиво обележена и у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима.

Прозори и врата на овој просторији из става 1. овог члана морају увек бити затворени.

Сервери и активна мрежна опрема (switch, modem, router, firewal), морају стално бити прикључени на уређаје за непрекидно напајање – UPS.

У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, овлашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.

У случају изношења опреме из просторије из става 1. овог члана ради селидбе, или сервисирања, неопходно је одобрење генералног директора или извршног/их директора који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења генералног директора или извршног/их директора, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрењагенералног директора или извршног/их директора.

Уговором са сервисером обавезно се дефинише обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Оператера.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим, планирају, односно предлажу непосредном руководиоцу одговарајуће мере.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери који су намењени тестирању и развоју. Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података.

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије врши се по завршетку радног времена, како не би био заустављен оперативни рад запослених-корисника.

15. Заштита података и средства за обраду података од злонамерног софтвера

Члан 20.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, е-маил-ом, зараженим преносним медијима (УСБ меморија, ЦД и тд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару се инсталира антивирусни програм.

Свакодневно се аутоматски у тачно одређено време врши допуна антивирусних дефиниција.

Сваког последњег радног дана у недељи је потребно оставити укључене и закључане рачунаре ради скенирања на вирусе.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером.

Ризик од евентуалног губитка података приликом чишћења медија од вируса сноси доносилац медија.

Заштита при коришћењу интернета

Члан 21.

У циљу заштите, односно упада у ИКТ систем Опертара са интернета, надлежни субјект ИКТ система је дужан да одржава систем за спречавање упада.

Руководиоци организационих јединица Оператора одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Запослени којима је одобрено коришћење интернета и електронске поште дужни су да приликом коришћења истог поступају по међународним конвенцијама и правилима понашања.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључење на интернет, односно прикључење преко сопственог модема.

Надлежни субјект ИКТ система може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система којима је одобрено коришћење интернета дужни су да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени-корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши надлежни субјект ИКТ система.

Приликом коришћења интернета корисник ИКТ система коме је одобрено коришћење интерента дужан је избегавати сумњиве WEB странице, у циљу спречавања инсталирања програма који могу нанети штету ИКТ систему.

У случају да корисник примети необично понашање рачунара, ту појаву је дужан да без одлагања да пријави надлежном субјекту ИКТ система.

Члан 22.

Кориснику ИКТ система коме је дозвољено коришћење инернета је забрањено гледање филмова и играње игрица на рачунарима и претраживање WEБ страница које садрже порнографски и остали недоличан садржај, као и самовољно преузимање истих са интернета.

Члан 23.

Недозвољена употреба интернета обухвата и:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;

- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;

- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друга врста недозвољених софтвера);

- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено одлуком надлежног органа Оператора;

- преузимање података у количини која проузрокује велико оптерећење на мрежи;

- преузимање материјала заштићених ауторским правима;

- коришћење линкова који нису у вези са послом;

- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

Члан 24.

Базе података обавезно се архивирају на преносиве медије (DWD, STRIMER TRAKA, EKSTERNI HDD) или мрежни диск, најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

Остали фајлови-документи се архивирају најмање једном недељно, месечно и годишње.

Подаци о запосленима-корисницима, архивирају се најмање једном месечно.

Члан 25.

Дневно копирање-архивирање врши се за сваки радни дан у седмици, од 20:00 часа сваког радног дана.

Недељно копирање-архивирање врши се последњег радног дана у недељи, од 20:00 часа, у онолико недељних примерака колико има последњих радних дана у месецу.

Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно, од 20:00 часа.

Годишње копирање-архивирање врши се последњег радног дана у години.

Члан 26.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан важећим Правилником о канцеларијском пословању и архивској грађи.

Дневне, недељне и месечне копије-архиве се чувају у просторији која је физички и у складу са мерама заштите од пожара обезбеђена.

Годишње копије-архиве се израђују у два примерка, од којих се један чува у просторији у којој се чувају дневне, недељне и месечне копије-архиве а други примерак у посебном објекту који је најмање 1 км удаљен од зграде управе.

Одлуку о посебном објекту у коме ће се чувати други примерак годишње копије – архиве доноси генерални директор/извршни директор посебним решењем.

Члан 27.

Исправност копија-архива проверава се најмање на шест месеци и то тако што се врши враћање база података које се налазе на медију, при чему подаци после враћања треба да буду исправни и спремни за употребу.

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

Члан 28.

О активностима администратора и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др).

Сваког последњег радног дана у недељи датотеке у којима се налази дневник активности се архивирају по процедури за израду копија-архива осталих података у ИКТ систему, у складу са чл. 20 овог правилника.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и другим могућим проблемима у ИКТ систему, мора бити подешен тако да одмах обавештава администратора о свим нерегуларним активностима запослених-корисника, покушајима упада и упадима у систем.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 29.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Оператора, односно Freeware и Open source верзије.

Инсталацију и подешавање софтвера може да врши само надлежни субјект ИКТ система, односно запослени-корисник који има овлашћење за то.

Инсталацију и подешавање софтвера може да изврши и треће лице, у случају да је софтвер набављен у поступку јавне набавке, а на начин дефинисан са Уговором о набавци, односно одржавања софтвера.

Треће лице може да изврши Инсталацију и подешавање софтвера када је између Оператора и њега уговорено одржавање софтвера у одређеном временском периоду.

Члан 30.

Пре сваке инсталације нове верзије софтвера, односно подешавања, неопходно је направити копију постојећег,како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

19. Заштита од злоупотребе безбедносних слабости ИКТ система

Члан 31.

Надлежни субјект ИКТ система најмање једном месечно, а по потреби и чешће врши анализу активности ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система надлежни субјект ИКТ система је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

Надлежни субјект ИКТ система, дужан је да подешавањем корисничких полиса, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

20. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Члан 32.

Ревизија ИКТ система се мора вршити тако да не омета пословне процесе корисника-запослених.

Надлежни субјект ИКТ система одредиће време обављања ревизије, у зависности од врсте послова и радних задатака запослених – корисника у Оператору.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 33.

Комуникациони каблови и каблови за напајање морају бити постављени у зид или каналнице, тако да се онемогући неовлашћен приступ, односно да се изврши изолација.

Мрежна опрема (switch, router, firewall) морају се налазити у rack орману, закључани.

Надлежни субјект ИКТ система је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коју могу да користе посетиоци објеката у надлежности Оператора, мора бити одвојена од интерне мреже коју користе корисници запослени у Оператору и кроз коју се врши размена службених података.

Та мрежа треба да буде означена (ССИД) по моделу јпкикинда_гост.

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

Члан 34.

Размена података који су означени ознаком тајности са другим органима, организацијама или правни лицима врши се у складу са потписаним актом о размени података.

Акт из става 1 овог члана садржи податке о овлашћеним лицима за размену података, начину размене података, правни оквир за такву врсту размене, као и правни оквир којим се дефинише заштита података који се размењују.

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

Члан 35.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Оператору биће дефинисан уговором који ће бити склопљен са тим лицима.

Надлежни субјект ИКТ система је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система Надлежни субјект ИКТ система води документацију.

Документација из претходног става мора да садржи описе свих процедура а посебно процедура које се односе на безбедност ИКТ система.

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

Члан 36.

За потребе тестирања ИКТ система, односно делова система надлежни субјект ИКТ систма може да користи податке који нису означени ознаком тајности односно службености, који нису осетљиви и који се штите, чувају и контролишу на одговарајући начин.

25. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 37.

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји Уговором дефинисан приступ.

Надлежни субјект ИКТ система је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог Правилника којима су такве активности дефинисане.

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

Члан 38.

Надлежни субјект ИКТ система је одговоран за надзор над поштовањем уговорених обавеза од стране трећих лица-пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система.

У случају непоштовања уговорених обавеза надлежни субјект ИКТ система је дужан да одмах обавести непосредног руководиоца , ради предузимања мера у циљу отклањања неправилности.

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

Члан 39.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести надлежниог субјекта ИКТ система.

По пријему пријаве става 1. овог члана надлежни субјект ИКТ система је дужан да одмах обавести непосредног руководиоца и предузме мере у циљу заштите ресурса ИКТ система.

Члан 40.

Уколико се ради о инциденту који је дефинисан у Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Сл. Гласник РС", бр, 94/2016), надлежни субјект ИКТ је дужан да поред непосредног руководиоца или извршног директора обавести и надлежни орган дефинисан наведеном Уредбом.

Надлежни субјект ИКТ система води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са Уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 41.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде управе, надлежни субјект ИКТ система је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује надлежни субјект ИКТ система, у три примерка, од којих се један налази код њега, други код запосленог у служби ИМС, а трећи примерак код генералног директора/извршног директора.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди генерални директор/ извршни директор.

Складиштење делова ИКТ система који нису неопходни врши се на начин да опрема буде безбедна и обележена.

III Провера ИКТ система

Члан 42.

Проверу ИКТ система врши надлежни субјект ИКТ система.

Члан 43.

Провера ИКТ система се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и акта на који се врши упућивање, са прописаним условима, односно проверава да ли су Правилником адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;

2) проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама интервјуа, симулације, посматрања, увида у предвиђене евиденције и другу документацију;

3) врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења,техничке конфигурације, техничке податке о статусима, записе о догађајима (логове), као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

О извршеној провери сачињава се извештај, који се доставља непосредном руководиоцу.

Члан 44.

Извештај из члана 44. овог Правилника садржи:

1) назив Оператора;

2) време провере;

3) подаци о лицима која су вршила проверу;

4) извештај о спроведеним радњама провере;

5) закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;

6) закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;

7) закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система;

8) оцена укупног нивоа информационе безбедности;

9) предлог евентуалних корективних мера;

10) потпис одговорног лица које је спровело проверу ИКТ система.

IV Измена Правилника

Члан 45.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност надлежни субјект ИКТ система је дужан да обавести непосредног руководиоца, како би он могао да приступи измени овог Правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивања овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

V Прелазне и завршне одредбе

Члан 46.

Овај правилник ступа на снагу осам дана од дана објављивања на огласној табли ЈП Кикинда.

Ступањем на снагу овог правилника престаје да важи Правилник о безбедности информационо-комуникционог система ЈП Кикинда од 20.02.2017. године.

ЈАВНО ПРЕДУЗЕЋЕ ЗА КОМУНАЛНУ ИНФРАСТРУКТУРУ И УСЛУГЕ „КИКИНДА" • KÖZÜZEMI SZOLGÁLTATÓ KFT. KIKINDA • KOMMUNALISTRUKTURA

ДИРЕКТОР
Данило С.Фурунџић