На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16, 94/2017 и 77/2019), члана 2. Уредбе о ближем садржају Правилника 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 („Сл. гласник РС“, бр. 94/2016) и члана 54. Статута Града Ниша („Сл. лист Града Ниша”, бр. 88/08, 143/16 и 18/2019),

Градоначелница Града Ниша, донела је

Правилник о безбедности информационо-комуникационог система града Ниша

Правилник је објављен у "Службеном листу града Ниша", бр. 84/2022 од 1.9.2022. године, а ступио је на снагу 9.9.2022.

Уводне одредбе

Члан 1.

Овим правилником, утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система града Ниша (у даљем тексту: ИКТ систем).

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог – корисника информатичких ресурса Града Ниша.

За реализацију и праћење примене овог правилника задужује се управа надлежна за послове ИКТ система града Ниша (у даљем тексту: Управа за послове ИКТ система).

Члан 2.

Мере прописане овим правилником се односе на све организационе јединице Града Ниша (градске управе, Канцеларија за локални економски развој, Правобранилаштво Града Ниша и други органи или организациони облици Града Ниша), на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Града Ниша.

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

1) *информационо-комуникациони систем (ИКТ систем)* је технолошко-организациона целина која обухвата:

(1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;

(2) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;

(3) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

(4) организациону структуру путем које се управља ИКТ системом;

2) *информациона безбедност* представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

3) *тајност* је својство које значи да податак није доступан неовлашћеним лицима;

4) *интегритет* значи очуваност изворног садржаја и комплетности податка;

5) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) *аутентичност* је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

7) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

8) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

9) *управљање ризиком* је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

10) *инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

11) *мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ

система;

12) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

13) *ИКТ систем* за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

14) *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

15) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

16) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

17) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;

18) *криптоматеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

19) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

20) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

21) VPN (Virtual Private Network)-је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;

22) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;

23) Backup је резервна копија података;

24) Download је трансфер података са централног рачунара или web презентације на локални рачунар;

25) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;

26) Freeware је бесплатан софтвер;

27) Opensource софтвер отвореног кода;

28) Firewall је „заштитни зид" односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

29) USB или флеш меморија је спољашњи медијум за складиштење података;

30) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;

31) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података.

I. Мере заштите

Члан 4.

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 Града Ниша

Члан 5.

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 за обављање послова из области безбедности целокупног ИКТ система града Ниша врши Управа за послове ИКТ система.

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност

- послови управљање 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 града Ниша, као и приступ, измене 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.

У случају инцидента руководилац унутрашње организационе јединице надлежне за послове ИКТ система обавештава свог начелника управе који, у складу са важећим прописима, обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву града Ниша, и који су подешени од стране Ресорне ОЈ, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности (примера ради електронска пошта), а на основу захтева корисника и сагласности руководиоца Службе за ИКТ.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

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

Забрањено је давање мобилних уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.). Запосленом – кориснику, забрањена је самостална инсталација софтвера и подешавање преносног рачунара. Запослени – корисник се обавезује да ће телефон, односно таблет користити савесно, и да сходно томе одлучује о врсти и намени апликација које ће инсталирати, као и да је свестан одговорности својих поступака.

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

Управа за послове ИКТ система је дужна 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

Члан 8.

Сви запослени и радно ангажовани појединци по другом основу, којима је додељен приступ поверљивим информацијама, морају потписати споразум о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Члан 9.

Запослени и друга радно – ангажована лица дужни се да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

У циљу развоја, имплементације и одржавања система заштите и безбедности података, Град Ниш преко Управе за послове ИКТ система обезбеђује услове за интеграцију контролних механизама тако што:

- Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и и у континуитету;
- Штити информације и податке са сличним профилом осетљивости и карактеристика 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.

Члан 10.

Сви корисници ИКТ система Града Ниша су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању на радном месту.

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

Члан 11.

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.

Дужности и обавезе које остају важеће и после престанка запослења треба да буду садржане у тексту решења о заснивању радног односа за службенике односно у уговору о раду за намештенике.

Члан 12.

За поступања приликом престанка запослења или ангажовања задужена је Управа за послове ИКТ система.

Унутрашња организациона јединица надлежна за послове радних односа дужна је да обавести унутрашњу организациону јединицу надлежну за послове ИКТ система о престанку радног односа или престанку ангажовања по другом основу неког лица у року од једног дана како би управа из става 1. овог члана предузела следеће активности:

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском облику,
- прегледа све налоге и приступе систему који су били доступни запосленом,
- преузима од запосленог електронске и друге мобилне уређаје,
- утврдила начин контакта са бившим запосленим након одласка,
- проверава враћене мобилне уређаје и уређаје за преношење података,
- издала налог за укидање налога електронске поште и свих других права приступа систему Града Ниша на дан престанка радног односа или другог основа ангажовања бившег запосленог,
- преглед свих налога за приступ одлазећег запосленог и прикупљање приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
- преузела картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Града Ниша.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 13.

Информациона добра Града Ниша су сви ресурси који садрже пословне информације Града Ниша, 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 и сл.

За идентификацију опреме и одређивање лица одговорног за наведену опрему користи се апликација за евиденцију опреме.

Евиденцију о информационим добрима води службеник задужен за послове евиденције опреме и софтвера, у папирној или електронској форми.

Члан 14.

Појединци којима је дата одговорност за контролисање животног циклуса имовине дужни су да правилно управљају имовином током целог животног циклуса.

Управа за послове ИКТ система у оквиру документа под називом реверс уређује правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација.

Током отказног рока запослених, након добијених информација из области радних односа, унутрашња организациона јединица надлежна за послове ИКТ система надлежне управе контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

Запослени и екстерни корисници су обавезни да врате сву опрему Управи за послове ИКТ система коју поседују након престанка њиховог запослења, истека уговора или другог правног основа по коме су били ангажовани за обављање одређених послова и задатака.

Раздужење опреме се врши потписивањем реверса који издаје Управа за послове ИКТ система.

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

Члан 15.

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

Свака организациона јединица у оквиру Града Ниша означава типове и локације података као јавне, интерне, поверљиве и строго поверљиве.

Класификациона шема поверљивости информација базира се на четири нивоа:

Јавни подаци (Информације које могу да се дистрибуирају без штете за њене запослене и заинтересоване стране). Ови документи могу бити откривени или прослеђени особама изван организације.

Интерни подаци (Информације чије неовлашћено обелодањивање би било непримерено и неугодно). Обелодањивање ван органа и организационих јединица Града Ниша захтева одобрење руководиоца органа, односно организационе јединице Града Ниша.

Поверљиви подаци (Високо осетљиве или вредне информације). Не смеју се објављивати изван органа, односно организационе јединице Града Ниша без изричите дозволе Градоначелника.

Строго поверљиви подаци (Информације чије откривање има озбиљан утицај на дугорочне стратешке циљеве или угрожава опстанак).

Град Ниша врши класификацију ради:

- Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и буду свесни одговорности за неовлашћено коришћење или преношење;

- Подизања свести о вредности информације или документа;

7. Заштита носача података

Члан 16.

Управа за послове 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 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 сходно радном месту и врсти посла којим се запослени бави. Право приступа додељује администратор.

- 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, на радном месту администратора.

Снимање и евиденција тонских записа врши се по одређеној процедури, медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, начелници управа и руководиоци других организационих јединица 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 17.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има.

Администраторска права разврстана су на одређене нивое и носе различите привилегије сходно својој намени.

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

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

Члан 18.

Запослени-корисник дужан је да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система, и то да:

1) користи информатичке ресурсе искључиво у пословне сврхе;

2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво града Ниша и да могу бити предмет надгледања и прегледања;

3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;

4) безбедно чува своје лозинке, односно да их не одаје другим лицима;

5) мења лозинке сагласно утврђеним правилима правилника

6) пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу

7) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;

8) обезбеди сигурност података у складу са важећим прописима;

9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;

10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;

11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;

12) израђује заштитне копије (backup) података у складу са прописаним процедурама;

13) користи интернет и електронску пошту Града Ниша у складу са прописаним процедурама;

14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;

15) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;

16) прихвати да технике сигурности (антивирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему.

17) 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 19.

Право приступа ИКТ систему Града Ниша имају само запослени/корисници који имају администраторске или корисничке налоге.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Администраторски налог за управљање доменом може/могу да користе само запослени на пословима систем инжењера.

Адинистраторски налог за управљање базом података може/могу да користе само запослени на пословима управљања базама података и систем инжењера.

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 непосредног руководиоца запосленог, који упућује Управа за послове ИКТ система, 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, надлежног руководиоца у оквиру чије организационе јединице је запослени-корисник.

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.

Додељивање привилегованих (администраторских) права на приступ врши начелник Управе за послове ИКТ система.

Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

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

Једном годишње врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење,

разрешење и крај запослења).

Запосленим лицима и екстерним корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 20.

Кориснички налог се састоји од корисничког имена и лозинке.

(Пример: Корисничко име се креира по матрици име.презиме, латиничним писмом без употребе слова ђ, ж, љ, њ, ћ, ч, џ, ш.

(Препорука: Уместо ових слова користити слова из 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 комбинованих од малих и великих слова, цифара и специјалних знакова.

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 6 месеци.

Иста лозинка се не сме понављати у временском периоду од годину дана.

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

У том случају, пријављивање у ИКТ систем града Ниша се може вршити и 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 21.

Запослени-корисници користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама, као и за приступ екстерним националним порталима Е-управе.

Електронски сертификати који се користе могу бити издати од овлашћеног националног сертификационог тела, или имплементирани у лична документа издата од МУП-а Републике Србије.

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. Забрањено је давање и пријављивање на портале и сервисе туђим електронским сертификатом, као и давање својих електронских сертификата другим лицима.

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

Члан 22.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује са као административна зона.

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

Простор мора да буде обезбеђен од пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор).

Право улаза у ову административну зону имају лица која се налазе на Листи овлашћених лица за улаз у сервер салу, као и трећа лица ангажована у циљу инсталације и сервисирања одређених ресурса ИКТ система, расхладног и система напајања, уз обавезно присуство овлашћеног лица Управе за послове ИКТ система.

Листу овлашћених лица за улаз у сервер салу одређује начелник Управа за послове ИКТ система. Ревизија наведене листе врши се једном годишње.

Дефинисана је листа издвојених локација у оквиру Града Ниша на којима се налазе rack ормари у којима је смештена комуникациона опрема (активна и пасивна). Сваки rack ормар је закључан и кључ се налази код овлашћеног лица.

Члан 23.

Град Ниш пројектује и примењује инструменте за обезбеђивање физичке безбедности канцеларија, просторија и средстава, тако што се онемогућава јавни приступ кључној опреми, у циљу спречавања видљивости поверљивих информација и активности споља.

Физичка заштита се мора планирати и за случајеве природних катастрофа, непријатељских напада или несрећа.

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

Члан 24.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само овлашћеним лицима на пословима ИКТ.

Осим овлашћених лица, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу руководиоца унутрашње организационе јединице надлежне за послове ИКТ система надлежне управе, уз присуство овлашћеног лица.

Приступ административној зони може имати и запослени/а на пословима одржавања хигијене уз присуство овлашћеног лица које се налази на листи овлашћених лица за улаз у сервер салу.

Просторија 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 морају увек бити затворени.

Сервери и активна мрежна опрема (switch, modem, router, firewall), 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.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења руководиоца унутрашње организационе јединице за послове информационо-комуникационе технологије.

У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење руководиоца унутрашње организационе јединице надлежне за послове ИКТ система надлежне управе, који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења руководиоца унутрашње организационе јединице надлежне за послове ИКТ система надлежне управе, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса града Ниша.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 25.

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 руководиоцу Ресорне ОЈ одговарајуће мере.

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запослених-корисника.

У случају да се на новој верзији софтвера који је уведен у оперативни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери и подаци који су намењени тестирању и развоју.

При тестирању софтвера је потребно обезбедити неометано функционисање ИКТ система. Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера, на начин који може да заустави нормално функционисање ИКТ система.

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

Члан 26.

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, имејлом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефиниција.

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.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему руководилац унутрашње организационе јединице надлежне за послове ИКТ система надлежне управе може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају 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 службеник надлежне управе.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави службенику надлежне управе на mail адресу Korisnicka.Podrska@gu.ni.rs.

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" WEB страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

Члан 27.

Недозвољена употреба интернета обухвата:

- 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 друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимање (download) података велике "тежине" које проузрокује "загушење" на мрежи;
- преузимање (download) материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и videostreaming и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже може се одузети право приступа.

16. Заштита од губитка података

Члан 28.

Израда резервних копија базе података обавезно се врши централизовано и аутоматизовано најмање једном дневно, за потребе обнове у случају губитка било ког података на дневном нивоу са дефинисаним бројем тачака опоравка од седам дневних копија.

Резервна копија бекапованих података чува се на бар две локације. На секундарној локацији чува се додатно и резервна копија за претходну седмицу. Посебно важни и осетљиви делови ИТ система чувају се додатно на трећој offsite локацији.

На одређеном месту, тј. издвојеној локацији организационе јединице града, где аутоматизован бекап није могућ због нестандардног и специфичног оперативног система, обучено и овлашћено лице врши бекап података на преносне медије по упутству руководиоца унутрашње организационе јединице надлежне за послове ИКТ система надлежне управе и стара се за чување истог.

Израда резервних копије о запосленима-корисницима, врши се након сваке промене над базом кадровске евиденције.

Конзистентност бекапованих података врши се аутоматски током процеса бекаповања.

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

Члан 29.

Систем за контролу и дојаву о грешкама обавештава овлашћена лица Управе за послове ИКТ система о инцидентима везаним за повећање температуре у сервер сали као и враћање у задате вредности, престанак напајања електричном енергијом са информацијом о преосталом капацитету система за непрекидно напајање, као и успостављања нормалног стања, неуспешног или делимичног бекапа података, пораст температуре физичких сервера. Дневници активности сервера (activitylog, history, securitylog) доступни су администраторима система.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 30.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Града Ниша односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само запослени у Управи за послове ИКТ система са администраторским овлашћењима, односно запослени који има овлашћење за то.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера.

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 техничких безбедносних слабости ИКТ система

Члан 31.

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

За решавање различитих уочених проблема користе се повремено административни алати за преглед разних системских и апликацијских логова.

Дељеним фолдерима, базама података и осталим мрежним ресурсима могу да приступе само овлашћени корисници на основу додељених права приступа.

Ажурирање и инсталирање софтвера могуће је преко налога са администраторским овлашћењима.

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 има што мањи утицај на пословне процесе корисника-запослених.

Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност начелника Управе за послове ИКТ система.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 33.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, router, firewall) се мора налазити у закључаном rack орману.

Запослени са администраторским овлашћењима у управи су дужни да стално врши контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалних неправилности.

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

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

Члан 34.

Заштита података који се преносе комуникационим средствима унутар Града Ниша, између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се потписивањем уговора и изјаве о поверљивости података.

Комуникација унутар Града Ниша одвија се путем електронске поште и интернета.

Употреба електронске поште мора бити у складу са правилима поступка, сигурна и у складу са позитивним прописима и пословном праксом.

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.

Приступ садржајима на интернету је дозвољен искључиво за пословне намене.

Безбедан пренос пословних информација између организације и трећег лица обезбеђује се поштовањем уговора о преносу информација.

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

Члан 35.

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

Управа за послове ИКТ система је задужена и 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, Управа за послове ИКТ система води документацију.

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

Члан 36.

За потребе тестирања ИКТ система односно делова система служба за ИКТ може да користи податке који нису осетљиви, које штити, чува и контролише 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.

Управа за послове ИКТ система је одговорна 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.

Управа за послове ИКТ система је одговорна 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 Управа за послове ИКТ система је, у складу са одредбама овог Правилника, дужна да предузме мере 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 начелника Управе за послове ИКТ система.

По пријему пријаве начелник Управе за послове ИКТ система је дужан да обавести Градоначелника ради евентуалног даљег поступања пред надлежним органима, као и да предузме све потребне мере у циљу заштите ресурса ИКТ система.

Управа за послове ИКТ система води евиденцију о свим инцидентима, као и пријавама инцидената, на основу којих се против одговорног лица, може водити дисциплински, прекршајни или кривични поступак.

Уколико се ради о инциденту који је дефинисан Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Службени гласник РС”, број 11/20) начелник Управе за послове ИКТ система је дужан да поред Градоначелника обавести и надлежни орган дефинисан наведеном Уредбом.

Управа за послове ИКТ система врши прикупљање, анализу као и евидентирање начина решавања инцидената који су нарушили безбедност ИКТ система, ради доказивања у случају покретања поступка против лица које је нарушило безбедност ИКТ система, као и ради идентификовања инциденти који се понављају, у циљу смањења њихове вероватноће и утицаја на систем у будућем раду.

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 40.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Града Ниша, Управа за послове ИКТ система је дужна 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.

Делови ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди Градоначелник.

Складиштење делова ИКТ система који нису неопходни се врши тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води.

II. Измена Правилника

Члан 41.

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, начелник Управе за послове ИКТ система је дужан да обавести Градоначелника града Ниша, 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 преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

III. Провера ИКТ система

Члан 42.

Проверу ИКТ система врши Управе за послове ИКТ система. О извршеној провери сачињава се извештај, који се доставља Градоначелнику.

IV. Садржај извештаја о провери ИКТ система

Члан 43.

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава;

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.

Прелазне и завршне одредбе

Члан 44.

За примену одредаба прописаних овим правилником, израду свих потребних процедура и осталих докумената који су његов саставни део, задужује се Управа за послове ИКТ система.

Члан 45.

Ступањем на снагу овог правилника, престаје да важи Правилник о безбедности информационо-комуникационог система Града Ниша бр. 316/2019-01 од 12.12.2019. године.

Овај правилник ступа на снагу осмог дана од дана објављивања у "Службеном листу Града Ниша".

Бр. 2986/2022-01

У Нишу, 31.08. 2022.

ГРАДОНАЧЕЛНИЦА

Драгана Сотировски, с.р.