СЛУЖБЕНИ ЛИСТ
ГРАДА НИША

ГОДИНА XXV - БРОЈ 33	НИШ, 11. април 2017.	Цена овог броја 60 динара Годишња претплата 5000 динара

ГРАД НИШ
ГРАДСКА УПРАВА

1.

На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16), 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 24. Одлуке о Градској управи града Ниша („Сл. лист Града Ниша”, бр.143/16),

Начелник Градске управе, доноси

П Р А В И Л Н И К
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНОГ СИСТЕМА ГРАДА НИША

I ***Уводне одредбе***

Члан 1.

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

Члан 2.

Мере прописане овим правилником односе се на сва запослена, изабрана, постављена и именована лица у органима Града Ниша, Служби за послове Скупштине Града, Служби за послове Градоначелника, Служби за послове Градског већа, Канцеларији за локални економски развој и пројекте, Правобранилаштву Града Ниша, Канцеларији заштитника грађана, Буџетској инспекцији Града Ниша, Служби за интерну ревизију органа и служби Града Ниша, органе градских општина и друге институције које у раду користе ИКТ системе 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:

- електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
- 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;
- 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;
- организациону структуру путем које се управља ИКТ системом;

2) Оператор ИКТ система је свака организациона јединица која у оквиру обављања послова из своје надлежности користи ИКТ систем;

3) информациона добра су сви ресурси ИКТ система Града који садрже програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, пословне информације, 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;

4) корисник ИКТ система је свако запослено, изабрано, постављено или именовано лице у органима Града, службама и осталим организационим облицима које у свом раду користи ресурсе ИКТ система;

5) надлежни субјект ИКТ система је организациона јединица у оквиру Градске управе града Ниша у чијој су надлежности послови планирања развоја, одржавања и функционисања рачунарско-комуникационе инфраструктуре и развој информационих технологија

6) 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;

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

8) интегритет значи очуваност изворног садржаја и комплетности податка;

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

10) 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;

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

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

13) 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;

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

15) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

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

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

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

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

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

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

22) криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски

кључеви;

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

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

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

26) Backup је резервна копија података;

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

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

29) Freeware је бесплатан софтвер;

30) Opensource софтвер отвореног кода;

31) Firewall је „заштитни зид“ односносистем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

32) USB или флеш меморија је спољшњи медијум за складиштење података;

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

34) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

Члан 4.

О информационим добрима води се посебна евиденција.

Евиденцију из става 1. овог члана води надлежни субјект ИКТ система.

II *Мере заштите*

Члан 5.

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.

Члан 6.

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

За обављање послова из области безбедности целокупног ИКТ система Града Ниша, задужена је организациона јединица Градске управе града Ниша надлежана за обављање делатности из области информатичко-комуникационих технологија, односно Служба за информатичко-комуникационе технологије (у даљем тексту Служба за ИКТ).

Члан 7.

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 настанка безбедоносног инцидента шеф Службе за ИКТ обавештава начелника Градске управе, који о томе обавештава надлежне органе.

Члан 8.

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.

Корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву Града Ниша, и који су подешени од стране Службе за ИКТ, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности (електронска пошта, апликативни софтвер из делокруга обављања послова и задатака), а на основу потреба обављања послова из делокруга рада и радног места.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и листе MAC адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

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

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

Служба за ИКТ свакодневно 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 начелник Управе, 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 Града Ниша оштећен а није обезбеђена замена.

Евиденцију приватних уређаја са којих ће бити омогућен приступ, води Служба за ИКТ.

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

У случају квара, Служба за ИКТ је дужана 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.

Члан 9.

ИКТ системом управљају запослени у Служби за ИКТ, у складу са описом послова из важећег акта о систематизацији радних места.

Служба за ИКТ је дужана да сваког новог корисника упозна са одговорностима и правилима коришћења ИКТ ресурса Града Ниша и да води евиденцију о изјавама новозапослених – корисника да су упознати са правилима коришћења ИКТ ресурса.

Свако коришћење ИКТ ресурса Града Ниша од стране корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

Члан 10.

У случају промене радног места, односно надлежности корисника, Служба за ИКТ ће извршити промену права у коришћењу ИКТ система, у складу са описом радних задатака и захтева руководиоца корисника.

Члан 11.

У случају престанка радног ангажовања корисника, кориснички налог истог лица се укида.

О престанку радног односа или радног ангажовања, као и промени радног места корисника, руководилац истог је дужан да о томе обавести Службу за ИКТ, ради укидања, односно измене приступних налога тог корисника.

Корисник је, након престанка правног основа по коме је приступао ресурсима ИКТ система Града Ниша, у обавези да не открива податке који су од значаја за информациону безбедност ИКТ система.

Члан 12.

Информациона добра Града Ниша су сви ресурси који садрже пословне информације, 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 Града Ниша води Служба за ИКТ, у папирној или електронској форми.

Члан 13.

Предмет заштите, по одредбама овог правилника, јесу:

- хардверске и софтверске компоненте ИКТ система
- подаци који се обрађују или чувају на компонентама ИКТ система
- кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система
- подаци о хардверским и софтверским компонентама ИКТ система
- развојни и идејни пројекти ИКТ система
- административна зона.

Члан 14.

Подаци који се налазе у ИКТ систему представљају тајни податак који је, у складу са прописима о тајности података, одређен или означен одређеним степеном тајности.

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима.

Члан 15.

Служба за ИКТ ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са законом који регулише тајност података, тако да:

- подаци и документа (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 овлашћени корисници
- подаци и документа (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника

Документа са ознаком тајности може да сними на друге носаче (екстерни HDD, USB, CD, DVD) само начелник Градске управе или запослени којег начелник Градске управе овласти писаним путем.

Евиденцију носача на којима су снимљени подаци са ознаком тајности, води Служба за ИКТ.

Носачи на којима се налазе документи са ознаком тајности морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта носача са подацима са ознаком тајности, начелник Градске управе ће одредити одговорну особу и начин транспорта.

Приликом брисања података за ознаком тајности са носача на којима су се налазили, подаци морају бити неповратно обрисани, а ако то није могуће, такви носачи морају бити физички оштећени, односно уништени.

Члан 16.

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

Право приступа ресурсима ИКТ система имају лица која имају администраторске и/или корисничке налоге.

Руководилац Службе за ИКТ, у складу са потребама система и одредбама акта о организацији и систематизацији радних места,

доноси решења о додели администраторских налога запосленима.

Члан 17.

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

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.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог на пословима управљања људским ресурсима, односно надлежног руководиоца.

Члан 18.

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 корисника.

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

Уместо ћириличних слова, наведених у претходном ставу, користе се латиничне ознаке за иста и то: ђ – dj; ж - z ,љ - lj, њ – nj, ћ - c, ч - c , џ - dz, ш – s.

Члан 19.

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 Града Ниша се врши убацивањем медија са електронским сертификатом у читач картица.

Члан 20.

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.

Кориснички налог додељује администратор, на основу захтева запосленог задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем и то након уноса података о запосленом у софтвер за управљање људским ресурсима, а у складу са потребама обављања пословних задатака од стране корисника.

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

Члан 21.

Лозинка корисника мора да садржи минимум осам карактера 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 корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Корисник дужан је да мења лозинку најмање једном у 6 месеци.

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

Члан 22.

За послове извршене под одређеним корисничким именом и лозинком одговоран је корисник ИКТ система коме је корисничко име/налог додељен.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

Члан 23.

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;

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 у Управи 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 (анти вирус 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.

III *Криптозаштита*

Члан 24.

Приступ ресурсима ИКТ система Града Ниша не захтева посебну криптозаштиту.

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.

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

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

Члан 25.

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 компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других могућих незгода.

У простору је неопходно успоставити и одржавити одговарајућу температуру, у складу са важећим стандардима (климатизован простор).

Прозори и врата на 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.

Члан 26.

У случају изношења опреме из административне зоне, ради селидбе или сервисирања, неопходно је писано одобрење руководиоца Службе за ИКТ који ће одредити све детаље везане за изношење опреме.

Ако се опрема износи ради сервисирања, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

У случају крајње нужде, у циљу спасавања опреме, иста се може изнети без одобрења руководиоца Службе за ИКТ.

Опрема се одлаже на сигурно место и без одлагања о томе обавештава руководилац Службе.

Члан 27.

Улаз у просторију у којој се налази ИКТ опрема из члана 25. овог правилника, дозвољен је само запосленима у Служби за ИКТ.

Евиденцију о уласку у ову зону води лице запослено у Служба за ИКТ, које одређује руководилац Службе .

Члан 28.

Приступ административној зони и опреми ИКТ система Града Ниша, могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса, уз присуство надлежног лица Службе за ИКТ.

Да би трећа лица приступила административној зони и опреми ИКТ система, морају имати, у складу са законом, закључен уговор са надлежним органом Града.

Уговором из претходног става, дефинише се врста делатности по основу којих треће лице приступа опреми и ресурсима ИКТ система и прописује обавеза заштите података који се тичу опреме и осталих ИКТ ресурса.

Свако треће лице које приступа административној зони и ресурсима ИКТ система, дужно је да потпише Изјаву о тајности и поверљивости података.

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

V *Обезбеђивање исправног и безбедног функционисања средстава за обраду података*

Члан 29.

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 Службе одговарајуће мере.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију.

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

VI *Заштита података и средства за обраду података од злонамерног софтвера*

Члан 30.

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 у тачно одређено време врши допуна антивирусних дефиниција.

Сваког претпоследњег радног дана (четвртак) у недељи је потребно оставити укључене и закључане рачунаре ради скенирања на вирусе.

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

Члан 31.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса.

Ако се утврди да преносиви медиј садржи вирусе, врши се чишћење медија антивирусним софтвером - уколико је то могуће,.

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

У циљу заштите, односно упада у ИКТ систем Града Ниша са интернета, Служба за ИКТ је дужна да одржава систем за спречавање упада.

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

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему Служба за ИКТ 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 корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши Служба за ИКТ.

Приликом коришћења интернета треба избегавати сумњиве WEB странице, с обзиром да то може проузроковати проблеме - неприметно инсталирање шпијунских програма и слично.

Члан 32.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Служби за ИКТ.

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 33.

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 видеостреаминг 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.

VII *Заштита од губитка података*

Члан 34.

Базе података обавезно се архивирају на преносиве медије (CDROM, DVD, USB, „strimer" трака, екстерни хард 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 корисницима, архивирају се најмање једном месечно.

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

Недељно копирање-архивирање врши се последњег радног дана у недељи, од 20 часова, 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 часова.

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

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе.

Сваки примерак преносног информатичког медија са копијама-архивама, мора бити означен бројем, врстом (дневна, недељна, месечна, годишња), датумом израде копије-архиве, као и именом корисника који је извршио копирање-архивирање.

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 ван зграде управе.

Одлуку о посебном објекту у коме ће се чувати други примерак годишње копије – архиве доноси начелник Градске управе посебним решењем.

Члан 35.

Исправност копија-архива проверава се најмање на шест месеци и то тако што се изврши повраћај база података које се налазе на медију, при чему враћени подаци након повраћаја треба да буду исправни и спремни за употребу.

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

Члан 36.

О активностима администратора и 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 одредбама овог правилника.

IX *Систем за контролу*

Члан 37.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и др, мора бити подешен тако да одмах обавештава администратора, руководиоца организационе јединице надлежне за послове ИКТ и начелника Управе, о свим нерегуларним активностима корисника, покушајима упада и упадима у систем.

X *Обезбеђивање интегритета софтвера и оперативних система*

Члан 38.

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

Инсталацију и подешавање софтвера може да врши само Служба за ИКТ, односно корисник који има овлашћење за то.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера и правилима о тајности и поверљивости података, прописаним овим правилником.

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.

XI *Заштита од злоупотребе техничких безбедносних слабости ИКТ система*

Члан 39.

Служба за информатичко-комуникационе технологије најмање једном месечно а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.

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

Служба за информатичко-комуникационе технологије, треба да подешавањем корисничких полиса, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

XII *Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система*

Члан 40.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника.

Руководилац Службе за ИКТ одредиће време обављања ревизије, у зависности од врсте послова и радних задатака корисника ИКТ система.

Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника, чији би пословни процес био ометан.

XIII *Заштита података у комуникационим мрежама укључујући уређаје и водове*

Члан 41.

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.

Служба за ИКТ је дужана 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 Управе, мора бити одвојена од интерне мреже коју користе корисници запослени у Управи и кроз коју се врши размена службених података.

Мрежа из претходног става овог члана, треба да буде посебно означена.

XIV *Безбедност ИКТ система у случају размене података*

Члан 42.

Подаци који су означени ознаком тајности, размењују се са другим органима, организацијама или правни лицима 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.

XV *Учешће трећих лица у пословима ИКТ система*

Члан 43.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Управи, дефинише се уговором.

Трећа лица-пружаоци услуга израде и одржавања софтвера, као и других интелектуалних решења из области ИКТ система Града, 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.

Служба за ИКТ је задужена 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 Служба за ИКТ води документацију.

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

XVI *Тестирање ИКТ система односно делова система*

Члан 44.

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.

XVII *Превенција и реаговање на безбедносне инциденте*

Члан 45.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, корисник је дужан да одмах обавести Службу за ИКТ.

По пријему пријаве, Служба за ИКТ је дужана да одмах обавести начелника Управе и предузме мере у циљу заштите ресурса ИКТ система.

Члан 46.

Уколико се ради о инциденту који је дефинисан Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, Служба за ИКТ је дужна да обавести начелника Градске управе који о инциденту обавештава надлежни орган дефинисан наведеном Уредбом.

Служба за ИКТ 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.

XVII *Мере које обезбеђују континуитет обављања посла у ванредним околностима*

Члан 47.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Управе, Служба за ИКТ је дужана да у најкраћем року пренесе делове ИКТ система (или обезбеди функционисање редудантних компоненти на резервној локацији уколико постоје) 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 Служба за ИКТ, и то у три примерка, од којих се један налази код њега/е, други код запосленог надлежног за послове одбране и ванредне ситуације а трећи примерак код начелника Управе.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди начелник Управе.

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.

XIX *Провера ИКТ система*

Члан 48.

Проверу ИКТ система врши Служба за ИКТ.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на која 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 начелнику Управе.

Члан 49.

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.

XX *Дисциплинска одговрност*

Члан 50.

Непоштовање одредби овог Правилника представља повреду радних обавеза и повлачи дисциплинку одговорност корисника информатичких ресурса ИКТ система Оператора.

Члан 51.

Свако коришћење ИКТ ресурса ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

XXI *Измена Правилника*

Члан 52.

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, шеф Службе за ИКТ је дужан да обавести начелника Управе, како би он могао да приступи измени овог правилника, у циљу унапређења 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.

XXII *Прелазне и завршне одредбе*

Члан 53.

У року од 30 дана од дана ступања на снагу овог правилника, шеф Службе за ИКТ ће донети ближе упутство о коришћењу ИКТ ресурса и решења потребна за примену овог правилника.

Овај правилник ступа на снагу наредног дана од дана објављивања у „Службеном листу Града Ниша“.

Бр: 437/2017-24
У Нишу, 7. април 2017. године

ГРАДСКА УПРАВА ГРАДА НИША

НАЧЕЛНИК
Љубиша Јанић, с.р.

С А Д Р Ж А Ј

Град Ниш
Градска управа

Израда: Град Ниш – Служба за послове Скупштине Града, Улица Николе Пашића 24
Одговорни уредник Ненад Николић; технички уредник Соња Марковић
телефон 504-595 и 504-594 (Редакција и Служба претплате) E-mail msonja@gu.ni.rs
Уплатни рачун **840-742341843-24** позив на број **97 87-521**
Штампа: Служба за одржавање и информатичко- комуникационе технологије, Николе Пашића 24 Ниш , телефон 504-922