На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Сл. Гласник РС", бр. 94/2016) начелник Градске управе за локални развој, привреду, урбанизам и комуналне пословеграда Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске пословеграда Ваљева, доносе:

ПРАВИЛНИК
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ГРАДСКЕ УПРАВЕ ЗА ЛОКАЛНИ РАЗВОЈ, ПРИВРЕДУ, УРБАНИЗАМ И КОМУНАЛНЕ ПОСЛОВЕ ГРАДА ВАЉЕВА И ГРАДСКЕ УПРАВЕ ЗА ДРУШТВЕНЕ ДЕЛАТНОСТИ, ФИНАНСИЈЕ, ИМОВИНСКЕ И ИНСПЕКЦИЈСКЕ ПОСЛОВЕ ГРАДА ВАЉЕВА

I Уводне одредбе

Члан 1.

Овим правилником се, у складу са законом и подзаконским актима о безбедности информационо-комуникационих система, утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева(у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Члан 2.

Мере прописане овим правилником, се односе на све организационе јединице Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и на све организационе јединице Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, на све кориснике информатичких ресурса ИКТ система, запослене као и на трећа лица која користе ресурсе ИКТ система.

Непоштовање одредби овог правилника повлачи дисциплинску одговорност корисника ИКТ система.

Праћење примене овог Правилника врши унутрашња организациона јединица Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева, надлежна за послове управљања ИКТ системом.

Члан 3.

Термини,који се користе у овом правилнику, 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 којима се 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 у сврху њихове обраде, употребе, заштите или одржавања;
(4) организациону структуру која управља ИКТ системом;

2. *оператори ИКТ система* су Градска управа за локални развој, привреду, урбанизам и комуналне послове града Ваљева и Градска управа за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, које у оквиру обављања своје делатности, односно за обављање послова из своје надлежности, користе ИКТ систем;
3. *информациона безбедност* представља скуп мера које омогућавају да подаци, којима се обрађују у ИКТ систему, 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;
4. *тајност* је својство податка које значи да тај податак није доступан неовлашћеним лицима;
5. *интегритет* податка је очуваност изворног садржаја податка и очуваност комплетности податка;
6. *расположивост* податка је својство податка које значи да је податак доступан и употребљив, на захтев овлашћених лица, онда када им је потребан;
7. *аутентичност* податкаје својство податка, које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
8. *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га није могуће накнадно порећи;
9. *ризик* је могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
10. *управљање ризиком* је систематичан скуп мера који обухвата планирање, организовање и усмеравање активности, како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
11. *инцидент* је унутрашња или спољна околност или догађај, којим се угрожава или нарушава информациона безбедност;
12. *мере заштите ИКТ система* су техничке и организационе мере управљања безбедносним ризицима ИКТ система;
13. *тајни податак* је податак који је, у складу са прописима о тајности података одређен и означен одређеним степеном тајности;
14. *ИКТ систем за рад са тајним подацима* је ИКТ систем који је, у складу са законом, одређен за рад тајним подацима;
15. *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
16. *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
17. *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
18. *криптографски производ* је софтвер или уређај којим се врши криптозаштита;
19. *криптоматеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографскикључеви;

20. *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
21. *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
22. *VPN* (Virtual Private Network)је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама, да преко јавне мреже једноставно одржавају заштићену комуникацију;
23. *„MAC адреса"* (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
24. *„Backup"* је резервна копија података;
25. *„Download"* или преузимање је трансфер података са централног рачунара, web презентације или Интернета, на локални рачунар;
26. *UPS* (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
27. *„Freeware"* је бесплатан софтвер;
28. *„Opensource"* је софтвер отвореног кода;
29. *„Firewall"* („заштитни зид") је систем,којим се врши надзор и контролише проток информација, између локалне мреже и интернета, у циљу онемогућавања злонамерних активности;
30. *USB* или *флеш меморија* је спољашњи, преносни медијум за складиштење података;
31. *CD-ROM* (Compact disk-read only memory) се користи као спољашњи, преносни медијум за снимање података;
32. *DVD* је оптички диск високог капацитета који се користи као спољашњи, преносни медијум за складиштење података;
33. *кориснички налог* је скуп података у електронском облику о кориснику ИКТ система, којим се омогућава приступ ИКТ систему и који садржи, између осталих података, корисничко име и лозинку који се могу уносити 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 корисника ИКТ система;
34. *корисник* је запослени код Оператора ИКТ система или треће лице које је овлашћено за приступ ИКТ систему;
35. *домен* је врста рачунарске мреже у којој су подаци о свим ресурсима уписани у централним базама података, које се налазе на рачунарима (серверима), контролерима домена који управљају том рачунарском мрежом;
36. *администраторски налог* је кориснички налог ИКТ система, којим је омогућен приступ ИКТ систему, којем су додељена сва права у ИКТ систему и којим је омогућена управљање свим ресурсима ИКТ система, као и којим је омогућено отварање нових и измена постојећих корисничких налога у ИКТ систему; администраторски налог може бити локални и доменски;
37. *администратор ИКТ система* је лице коме је додељен администраторски налог и који је овлашћен за управљање свим ресурсима ИКТ система;
38. *редундантне компоненте ИКТ система* („дупле" компоненте, критичне компоненте за доступност ИКТ система) су компоненте ИКТ система, које су исте или сличне компонентама ИКТ система које се користе, а намењене су коришћењу када се доступност ИКТ система не може гарантовати коришћењем компоненти ИКТ система које су у раду.

II Мере заштите

Члан 4.

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

Мере прописане овим Правилником се односе на све организационе јединице Оператора ИКТ система и на све кориснике ИКТ система, као и на трећа лица,која су овлашћена да користе ресурсе ИКТ система.

Ради заштите тајности, аутентичности и интегритета података, Оператор ИКТ система може да уведе одговарајуће мере криптозаштите.

Мере заштите ИКТ система спроводи надлежна организациона јединица Оператора ИКТ система.

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

Члан 5.

Сваки запослени, корисник ресурса ИКТ система или треће лице, које је овлашћено за коришћење ресурса ИКТ система, је одговорно за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности.

Контролу и надзор над обављањем послова запослених, корисника и трећих лице која су овлашћена за коришћење ресурса ИКТ система, у циљу заштите и безбедности ИКТ система, као и за обављање послова у области безбедности целокупног ИКТ система, обавља надлежна организациона јединица Оператора ИКТ система, у складу са правилником о унутрашљем уређењу и систематизацији радних места у градској управи града Ваљева у чијој надлежности су послови управљања ИКТ системом.

Члан 6.

Послови у области информационе безбедности су:

1. послови заштите информационих добара, односно средстава иимовине за надзор над пословним процесима од значаја за информациону безбедност;
2. послови управљање ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности;
3. послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система, као и послови онемогућавања приступа, онемогућавања измене или онемогућавања коришћења средстава без овлашћења и без евиденције о томе
4. праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу;
5. обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента у ИКТ систему, корисник ИКТ система је дужан да, одмах, обавестируководиоца свог одељења. Руководилац одељења, одмах о томе, обавештава руководиоца Оператора ИКТ система.Уколико руководилац одељења није доступан, корисник ИКТ системаје дужан да, одмах, обавести руководиоца Оператора ИКТ система.

По пријему пријаве изпретходног става, руководилац Оператора ИКТ система је дужан да, одмах предузме мере, у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту у ИКТ систему, 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,руководилац Оператора ИКТ система, о том инциденту обавештава надлежни орган,одређен наведеном Уредбом.

Организациона јединицаОператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система води евиденцију о свим инцидентима, као и свим пријавама инцидената, у складу са Уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

2.Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Нерегистровани корисници, коришћењем мобилних уређаја, могу да приступе само оним деловима ИКТ система, који су конфигурисани тако, да свима омогућавају јаван и отворен приступ Интернету и веб сајту, али не и деловима ИКТ системакроз коју се обавља службена комуникација.

Запослени и корисници ИКТ система, коришћењем мобилних уређаја, који су у власништву града Ваљева, и које су подесилизапослени у организационој јединициОператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, могу да приступају само оним деловима ИКТ система, који им омогућавају обављање радних задатака, у оквиру њихове надлежности (електронска пошта), а на основу писане сагласности начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева илиначелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

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

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

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

Надлежни запослени, у организационој јединициОператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, свакодневно контролишу приступ ресурсима ИКТ система и проверавају да ли има приступа са непознатих уређаја (са непознатих MAC адреса). Уколико се установи неовлашћен приступ ИКТ систему, о томе се, електронском поштом одмах, а најкасније сутрадан обавештавају начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске

управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, а тојMAC адреси се онемогућава приступ ИКТ систему, уносом те MAC адресе у листу блокиранихMAC адреса („block“ листу),у софтвера који се користи за контролу приступа ИКТ систему.

Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен, осим ако је уређај, који је у власништву града Ваљева оштећен и није обезбеђена замена том, оштећеном, уређају.

Сагласност за коришћење приватног уређаја, у ИКТ систему, даје начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева

Приступ ресурсима ИКТ система са приватног уређаја није дозвољен без сагласности начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Евиденцију приватних уређаја, са којих ће бити омогућен приступ, води организациона јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система а по одобрењу начелника Градске управе.

Приватни уређаји, са којих ће се приступати ресурсима ИКТ система,могу се користити само за обављање послова у надлежности корисника-запосленог и то само у периоду када није могуће користити уређај, који је у власништву града Ваљева. Те уређаје морају подесити запослени у организационој јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система.

У случају да се приватни уређај, за који је дата сагласност начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева за приступ ресурсима ИКТ система, предаје овлашћеном сервису, корисник тог уређаја је дужан да о томе писмено обавести начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Запослени у организационој јединициОператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ системаје дужан је да, пре предаје приватног уређаја, који се предаје овлашћеном сервису, уколико квар није такве врсте да то онемогућава,уради *backup*службених података који се налазе у мобилном уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати те податке у мобилни уређај.

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

Члан 8.

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

Запослени који управљају ИКТ системом, у складу са важећом систематизацијом радних места, обавезно ће се оспособљавати и усавршавати, између осталог и упућивањем на обуке из области безбедности ИКТ система, управљања ИКТ системима и других ИКТ области, најмање једном на сваких шест месеци.

Евиденцију о обукама запослених који управљају ИКТ системом води организациона јединици Оператора ИКТ система, која је надлежна за управљање људским ресурсима.

Руководилац или надлежни запослени у организационој јединици Оператора ИКТ система, која је надлежна за управљање људским ресурсима, је дужан да, сваког запосленог или корисника ИКТ ресурса, упозна са одговорностима и правилима коришћења ИКТ система, као и да води евиденцију о изјавама запослених и корисника ИКТ система, о томе да су упознати са правилима коришћења ИКТ система.

Руководилац или надлежни запослени у организационој јединици Оператора ИКТ система, која је надлежна за управљање људским ресурсима, је дужан да, сваког новог запосленог или новог корисника ИКТ система, упозна са одговорностима и правилима коришћења ИКТ система, као и да води евиденцију о изјавама нових запослених и нових корисника ИКТ система, о томе да су упознати са правилима коришћења ИКТ система.

Свако коришћење ИКТ ресурса града Ваљева,запосленог или корисника ИКТ система, ван додељених овлашћење, подлеже дисциплинској одговорности запосленог или корисника ИКТ система, 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 9.

Актом о попуњавању радних места који доноси начелник градске управе, обавезује се службеник да чува поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система које сазна у обављању својих дужности, као и да примењује мере њихове заштите прописане овим Правилником и другим прописима којима се уређује тајност података.

Истим актом утврђује се и обавеза запосленог из става 1. овог члана и по престанку радног односа.

О престанку радног односа или радног ангажовањазапосленог или корисника ИКТ система, као и промени радног места запосленог или корисника ИКТ система, руководилац организационе јединице Оператора ИКТ система, надлежне за управљање људским ресурсимаје дужан даписмено обавести руководиоца организационе јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, ради укидања, или измене приступних привилегија тог запосленог или корисника ИКТ система.

У случају промене послова, односно промене надлежности запосленог или корисника ИКТ система, руководилац организационе јединице Оператора ИКТ система надлежне за управљање људским ресурсима, даје писмени налог руководиоцу организационе јединице Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, за промену привилегија које је запослени или корисник ИКТ система има.

Надлежни запослени у организационој јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, на основу писменог налога руководиоца организационе јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, врши промену административних овлашћења које је запослени или корисник ИКТ система има.

У случају престанка радног ангажовања запосленог или корисника ИКТ система, руководилац организационе јединице Оператора ИКТ система надлежне за управљање људским ресурсима, даје писмени налог за укидање корисничког налога руководиоцу организационе јединице Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система.

Надлежни запослени у организационој јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система,укида и онемогућава тај кориснички налог, на основу писменог налога руководиоца организационе јединице Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система.

Корисник ИКТ ресурса (и запослени и трећа лица која су овлашћена за коришћење ИКТ система), за време свог радног ангажовања и након престанка свог радног ангажовања, не сме да открива податке који су значајни за информациону безбедност ИКТ система.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра су сви ресурси који садрже пословне информације, којима 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.

О информационим добрима води се посебна евиденција и посебна класификација.

Попис информационих добара, односно средстава и имовине спроводи, организациона јединица Оператора ИКТ система, која је надлежна за заједничке послове.

Организациона јединица Оператора ИКТ система, која је надлежна за заједничке послове, успоставља, води,одржава и редовно ажурира евиденцију и класификацију информационих добара.

Оператор ИКТ система је дужан да класификацију из става 2. овог члана врши према степену осетљивости и критичности, узимајући у обзир могуће последице нарушавања поверљивости, интегритета и расположивости информационих добара, да доследно примењује ту класификацију, као и да у складу с тим, обезбеди адекватан ниво заштите информационих добара.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева дају сагласност на класификацију информационих добара.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљеваодређујулице, које је задужено за заштитусваког информационог добра, односно средства и имовине.

Организациона јединица Оператора ИКТ система, која је надлежна за заједничке послове, успоставља, води,одржава и редовно ажурира евиденцију о гаранцијама, гарантним роковима, уговорним обавезама испоручиоца опреме у гарантном року и ван гарантног рока, сервисирању у гарантном року и ван гарантног рока, и одржавању информационих добара, односно средстава и имовине која се користи у ИКТ систему, укључујући и опрему за климатизацију, заштиту и обезбеђењеинформационих добара, односно средстава и имовине која се користи у ИКТ систему.

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

Члан 11.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева одређују шему класификације података, према којој се подаци класификују узимајући у обзир осетљивост, важност података, штету која може да настане услед неовлашћеног откривања, измене или брисање података и прописе који уређују заштиту података (о тајним подацима, пословној тајни, подацима о личности и сл.).

Ради ордеђивања групних и појединачних права приступа ИКТ систему, класификациојом података се одређује, између осталог, и којим подацима могу приступати сви запослени и сви корисници ИКТ система, којим подацима којима можеприступати више запослених или више корисника ИКТ система који су овлашћени за то (група корисника) и којим подацима могу приступати само поједини запослени или поједини корисници ИКТ система, који су овлашћени за то.

Подаци који се налазе у ИКТ систему представљају тајну ако су као такви дефинисани посебним прописима.

Подаци који се налазе у ИКТ систему, који су у складу са прописима о тајности података, одређени или означени одређеним степеном тајности, представљају тајне податке.

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).

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева,ће усвојити акт о успостављању организацијеприступа подацима, посебно оним подацима који буду означени тајним, у складу са Законом о тајности података.

Документи, са ознаком тајности, могу да се сниме, односно архивирају или запишу на фајл серверу, у фолдеру коме право приступа имају само корисници ИКТ система, који су за то овлашћени и који су добили право приступа том фолдеру.

Организациона јединица Оператора ИКТ система, која је надлежна за управљање ИКТ системом, врши процену ризика угрожавања заштите података, врши процену потреба за превенцијом ризика угрожавања заштите података и предлаже мере отклањања последица ризика који се остварио, укључујући све врсте ванредних околности.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева доносе акт о процени ризика,потреби за превенцијом ризика и отклањању последица ризика који се остварио, укључујући све врсте ванредних околности, на предлог организационе јединице Оператора ИКТ система, која је надлежна за управљање ИКТ системом. Избор и ниво примене мера заштите података се заснива на овом акту.

7. Заштита носача података

Члан 12.

Надлежнаорганизациона јединица Оператора ИКТ система, ће успоставити организацију приступа и рада са подацима, посебно оним подацима који буду означени степеном службености или тајности, у складу са Законом о тајности података, тако да:

1. подаци и документи, а посебно подаци 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 или корисници ИКТ система, којима је то право дато одлуком начелникаГрадске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелникаГрадске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева;
2. подаци и документи, а посебно подаци са ознаком тајности,могу да сниме на друге носаче података (екстерни хард диск, USB, CD, DVD и сл.) само овлашћени запослени или овлашћени корисници ИКТ система, које је овластио начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева одређују, својим актом, податке, у складу са шемом класификације података, за које треба водити евиденцију о коришћењу носача података и предузетим поступцима заштите података и носача података.

Евиденцију о коришћењу носача података и предузетим поступцима заштите података и носача података успоставља, води и редовно ажурира организациона јединица Оператора ИКТ система која је надлежна за заједничке послове.

Руководилац свакогодељења Оператора ИКТ система води евиденцију носача података, у складу са атком из става 2. овог члана, за које је надлежан и који су направљени у обављању послова из своје надлежности. Евиденција носача података садржи, осим осталих података и рокове чувања података, у складу са прописима.

Када истекну рокови за чување података уписаних на носаче података, или када подаци уписани на носаче података нису више потребни,подаци са тих носача података се неповратно бришу. Уколико се подаци не могу неповратно обрисати са носача података, ти носачи података се предају организационој јединици Оператора ИКТ система која је надлежна за заједничке послове, ради уништавања. О овој предаји носача података сачињава се записник.

Носачи података који су покварени или који се више не употребљавају, предају се организационој јединици Оператора ИКТ система која је надлежна за заједничке послове, ради уништавања.О овој предаји носача података сачињава се записник.

Приликом расходовања информационог добра, опреме, средстава или имовине, која у свом склопу садржи носач података (рачунар, преносни рачунар, мобилни уређај, мобилни телефон и сл.), подаци на тим носачима података се неповратно бришу, а ако се подаци на тим носачима података не могу обрисати, тај носач података се неповратно уништава.

Документ, са ознаком тајности, може да сними, на друге носаче података (екстерни HDD, USB, CD, DVD и сл.), само начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, или запослени когаписмено овласти начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Евиденцију носача података, на којима су снимљени подаци са ознаком тајности, води организациона јединица Оператора ИКТ система која је надлежна за заједничке послове.

Носачи података, 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 података са подацима са ознаком тајности, начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, ће одредити одговорну особу за транспорт носача података са подацима са ознаком тајностии начин транспортаносача податакаса подацима са ознаком тајности.

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

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

Приступ ресурсима ИКТ система одређен је корисничким налогом који запослени или корисник ИКТ система има у ИКТ систему, у складу са класификациојом података.

Писмени налог за отварање корисничког налога издаје руководилац организационе јединице Оператора ИКТ система, која је надлежна за управљање људским ресурсима.
Налог за отварање корисничког налога, руководилац организационе јединице Оператора ИКТ система, која је надлежна за управљање људским ресурсима доставља руководиоцу

организационе јединице Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система.

Налог за отварање корисничког налога, поред осталих података, садржи и опис права приступа, у складу са класификациојом података и на основу послова и радних задатака запосленог или корисника ИКТ система.

На образац налога за отварање корисничког налога, сагласност дају начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Надлежни запослени у организационој јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, на основу писменог налога руководиоца организационе јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, отвара кориснички налог у ИКТ систему.

Руководилац организационе јединици Оператора ИКТ система, која је надлежна да спроводи мере заштите ИКТ система, на основу налога за отварање корисничког налога, доставља податке о корисничком налогу организационој јединици Оператора ИКТ система, која је надлежна за управљање људским ресурсима.

Надлежни запослени у организационој јединици Оператора ИКТ система, која је надлежна за управљање људским ресурсима, саопштава лицу податке о његовом корисничком налогу и поступа у складу са чланом 8. овог Правилника.

О налозима за отварање корисничких налога се води евиденција.

О налозима за укидање корисничких налога се води евиденција.

Евиденцију налога за отварање корисничких налога у ИКТ систему и евиденцију о налозима за укидање корисничких налога води организациона јединица Оператора ИКТ система надлежна за управљање људским ресурсима. Један примерак налога за отварање корисничког налога у ИКТ систему се чува у персоналном досијеу лица. За лица, за која се не води персонални досије, један примерак налога за отварање корисничког налога у ИКТ систему се чува на примерен начин.

Кориснички налози се могу организовати у групе корисника, у складу са класификацијом података. Права приступа ресурсима ИКТ система могу бити организована на права која се дају свим запосленима и свим корисницима ИКТ система, посебна права која се дају члановима једне групе запослених или групе корисника ИКТ система и посебна права која се дају појединачном запосленом или појединачном кориснику ИКТ система.

Запослени који има администраторски налогза приступ ИКТ систему (администратор ИКТ система), има права приступа свим ресурсима ИКТ система (подацима, софтверским, хардверским, мрежним ресурсима и осталим ресурсима ИКТ система) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Запослени или корисник ИКТ система може да користи само свој кориснички налог, који је добио и не сме да омогући другом лицу коришћење свог корисничког налога, сем администратору ИКТ система, ради подешавање корисничког профила и радне станице.

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

Сваки корисник ИКТ система (и запослени и трећа лица која су овлашћена за коришћење ИКТ система) је дужан да поштује и следећа правила безбедног и примереног коришћења ИКТ система:

1. да користи ресурсе ИКТ система искључиво у пословне сврхе;
2. да прихвати да су сви подаци који се складиште, преносе или обрађују у оквиру ИКТ система власништво Оператора ИКТ система и да могу бити предмет надгледања и прегледања;
3. да поступа поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. да безбедно чува своје лозинке, своје електронске сертификате и PIN податке;
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 користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење руководиоца Оператора ИКТ система;
8. да захтев за инсталацију софтвера или хардвера подноси у писаној форми, који одобрава надлежни руководилац;
9. да обезбеди сигурност података у складу са важећим прописима;
10. да приступа ресурсима ИКТ система само на основу изричито, додељених својих корисничких права;
11. да не сме да зауставља рад или брише антивирусни програм, мења подешене опције антивирусног програма нити да неовлашћено инсталира други антивирусни програм;
12. да не сме на радној станици да складишти садржај који не служи у пословне сврхе;
13. да израђује заштитне копије (backup) својих података у складу са прописаним процедурама;
14. да користи Internet, Intranet и e-mail сервис Оператора ИКТ система, у складу са прописаним процедурама;
15. да прихвати да се одређене врсте информатичких интервенција обављају у утврђено време;
16. да прихвати да сви приступи ресурсима ИКТ система и информацијама треба да буду засновани на принципу минималне неопходности;
17. да прихвати инсталацију програма у циљу сигурности ИКТ система;
18. да не сме самостално да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер или било који други софтвер.

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

Члан 14.

Право приступа ИКТ системуимају само запослени, корисници или трећа лица која су овлашћена да приступе ИКТ систему и која су овлашћена да користе ИКТ систем и којимаје додељенкорисничкиили администраторски налог у ИКТ систему.

Администраторски налог може да користи само запослени у надлежној организационој јединици Оператора ИКТ система или лице које, на основу закона, писмено овласти

начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Администраторски налог за управљање базом података може да користисамо запослени на пословима који су за то одређени у надлежној организационој јединици Оператора ИКТ система.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати тастатуром или података који се могу читати са медија на коме постоји електронски сертификат, којима се врши аутентификација (провера идентитета) и ауторизација (провера права приступа), и којима се вршипровера права коришћења ресурса ИКТ система корисника ИКТ система.

Кориснички налог отвара администратор ИКТ система, на основу писменог налога за отварање корисничког налога руководиоца организационе јединице Оператора ИКТ система, надлежне за управљање људским ресурсима и писменог налога руководиоца организационе јединице Оператора ИКТ система, надлежне за управљање ИКТ системом.

Кориснички налог мења администратор ИКТ система, на основу писменог налога за промену корисничког налога руководиоца организационе јединице Оператора ИКТ система, надлежне за управљање људским ресурсима и писменог налога руководиоца организационе јединице Оператора ИКТ система, надлежне за управљање ИКТ системом.

Кориснички налог укида администратор ИКТ система, на основу писменог налога за укидање корисничког налога руководиоца организационе јединице Оператора ИКТ система, надлежне за управљање људским ресурсима и писменог налога руководиоца организационе јединице Оператора ИКТ система, надлежне за управљање ИКТ системом.

Администратор ИКТ система води евиденцију о корисничким налозима у електронском облику, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу писменог налога руководиоца организационе јединице Оператора ИКТ система, надлежне за управљање људским ресурсима и писменог налога руководиоца организационе јединице Оператора ИКТ система, надлежне за управљање ИКТ системом, у складу са овим Правилником.

Руководиоци организационе јединице Оператора ИКТ система, надлежне за управљање људским ресурсима и организационе јединице Оператора ИКТ система, надлежне за управљање ИКТ системом, најмање једном годишње, врше проверу и усклађивање евиденција корисничких налога, које су надлежни да воде. Посебно се пажљиво проверавају администраторски налози у ИКТ систему.

О провери и усклађености евиденција корисничких налога, које воде.организационе јединице Оператора ИКТ система, надлежне за управљање људским ресурсима и организационе јединице Оператора ИКТ система, надлежне за управљање ИКТ системом саставља се записник. По једна копија, овог записника, се доставља начелнику Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева иначелнику Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева. У случају неусклађености ове две евиденције начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове

града Ваљева иначелнику Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева налажу мере за усклађивање ових евиденција.

Кориснички налог се може закључати ако се унесе погрешна лозинка узастопно пет пута.

У случајевима промене радног места, престанка радног односа и, по потреби, у другим случајевима, укидање права приступа ИКТ систему се спроводи у складу са чланом 9. и чланом 13. овог Правилника.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Корисничко име се прави по моделу **име.презиме**, латиничним словима енглеске абецеде, без употребе великих или малих слова ђ,ж,љ, њ, ћ, ч, џ, ш.

Уместо слова, из става 1. овог члана,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 најмање осам знакова, комбинованих од малих и великих слова, цифара и специјалних знакова.

Лозинка по правилу не садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке запосленог односно корисника ИКТ система.

Ако запослени или корисник ИКТ система посумња да је друго лице открило његову лозинку, дужан је да своју лозинку одмах промени.

Запослени или корисник ИКТ система по правилу мења лозинку, најмање једном у шест месеци.

Иста лозинка се не сме понављати у временском 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 квалификованим електронским сертификатом).

Пријављивање у ИКТ систем се врши уписивање корисничког имена и лозинке или убацивањем медија са електронским сертификатом у читач картица.

Неовлашћено уступање корисничког налога или медија са електронским сертификатом другом лицу, подлеже дисциплинској одговорности.

За послове извршене под одређеним корисничким именом или под одређеним електронским сертификатом, одговоран је корисник ИКТ система коме је додељено то корисничко име или коме је додељен тај електронски сертификат.

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

Члан 16.

Приступ ресурсима ИКТ система,не захтева посебну криптозаштиту.

За приступ ресурсима ИКТ система који се односе на послове одбране, односно, за које је надлежно министарство прописало коришћење криптозаштите, посебним правилником ће бити дефинисана употреба одговарајућих мера криптозаштите, узимајући у обзир осетљивост информација које треба да се штите, пословне процесе који се спроводе, ниво захтеване заштите, имплементацију примењених криптографских техника и управљање криптографским кључевима.

Запослени или корисници ИКТ система могу да користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама.

Запослени у организационој јединици Оператора ИКТ система надлежној за управљање ИКТ системом, су задужени за инсталацију потребног софтвера и хардвера за коришћење квалификованих електронских сертификата.

Запослени или корисници ИКТ система су дужни да чувају своје носаче квалификованихелектронских сертификата, 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 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.

Административна зона мора да буде обезбеђена од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њој треба да буде одговарајућа температура (климатизован простор).

Улазак у едминистративну зону се контролише.

Евиденцију лица којима је дозвољен улазак у административну зону и евиденцију овлашћења за улазак у административну зону, водиорганизациона јединица Оператора ИКТ система која је надлежна за управљање људским ресурсима.

Евиденцију улазака у административну зона води организациона јединица Оператора ИКТ система која је надлежна за управљање ИКТ системом.

У случају елементарних непогода, злонамерних напада, несрећа или намерног уништавања објеката, просторија, средстава и докумената ИКТ система, у периоду трајања тих околности, организује се посебно, целодневно (24 сата), физичко обезбеђење административне зоне, тако што један запослени организационе јединице Оператора ИКТ система, који обавља послове обезбеђења, врши стално и непосредно физичко обезбеђење административне зоне.

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

Члан 18.

Улаз у административну зону, дозвољен је само:

1. начелнику Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и његовом заменику;
2. начелнику Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева и његовом заменику;
3. руководиоцу организационе јединице Оператора ИКТ система која је надлежна за управљање ИКТ системом и његовом заменику;
4. администраторима ИКТ система и лицима запосленим у организационој јединици Оператора ИКТ система која је надлежна за управљање ИКТ системом;
5. лицима која, за то, писмено овласти начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева;
6. лицима која обављају послове одржавања хигијене, под условима оређеним овим Правилником;
7. лицима која обављају послове обезбеђења, под условима оређеним овим Правилником.

Приступ административној зони могу имати и трећа лица,ради инсталације и сервисирања одређених ресурса ИКТ система, а по претходном писменом одобрењу начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, и уз присуство надлежног лица,запосленог у организационој јединица Оператора ИКТ система надлежној за управљање ИКТ системом.

Приступ административној зони може имати и запослени на пословима одржавања хигијене уз присуство надлежног лица, запосленог у организационој јединица Оператора ИКТ система надлежној за управљање ИКТ системом.

Приступ административној зони може имати и запослени на пословима обезбеђења, у хитним и ванредним ситуацијама.

Административна зона мора бити видљиво обележена и у њој се мора налазити одговарајућа 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.

Није дозвољен рад сервера уколико уређаји за климатизацију сервер сале не раде исправно.

У сервер сали обавезно се постављају два уређаја за климатизацију, истог капацитета. Уколико је то могуће постићи, други уређај за климатизацију сервер сале треба аутоматски да се укључи, уколико први уређај престане да ради.

Уређаји за климатизацију сервер сале се морају одржавати и чистити редовно и у складу са прописаним процедурама произвођача те опреме.

Противпожарна опрема у административној зони се мора одржавати и у складу са прописаним процедурама произвођача те опреме.

Температура у сервер сали се одржава у складу са прописаном температуром произвођача сервера.

У сервер сали се може користити опрема за аквизицију података о температури и слање обавештења,овлашћеним лицима, о прекорачењима прописане температуре у сервер сали.

Прекид напајања електричном енергијом из јавне електричне мреже се сматра инцидентом и о томе се води евиденција као о инциденту.

Прекид рада уређаја за климатизацију сервер сале се сматра инцидентом и о томе се води евиденција као о инциденту.

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

У случају прекида напајања електричном енергијом из јавне електричне мреже, уређаји за непрекидно напајање (UPS)сервера и сервери морају бити тако подешени да се сервери аутоматски искључују, пре него што уређај за непрекидно напајање (UPS) потроши енергију за напајање сервера, у складу са процедурама произвођача опреме.

У случају прекида напајања електричном енергијом из јавне електричне мреже, у периоду дужем од периода за који је капацитетуређаја за непрекидно напајање (UPS) довољан за напајање сервера, овлашћено лице је дужно да провери да ли су сервери искључени и ако сервери нису искључени да искључи сервере, у складу са процедурама произвођача опреме.

У случају прекида напајања електричном енергијом из јавне електричне мреже, овлашћено лице је дужно да провери исправност рада уређаја за климатизацију сервер сале.

У случају непосредне опасности (пожар, временске непогоде и сл.) ИКТ опрема семоже изнети из просторије без одобрења начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

У случају изношења ИКТ опреме из пословне просторије или административне зоне, ради селидбе или сервисирања, неопходно је претходно одобрење начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелника

Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, који ће одредити услове, начин и место изношења ИКТ опреме.

Ако се ИКТ опрема износи ради сервисирања, поред одобрења начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, потребно је сачинити записник у коме се наводи и назив и тип опреме, инвентарни број, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Уговором са сервисером, обавезно, се дефинише обавеза заштите података који се налазе на ИКТ опреми или медијима који су део ИКТ система Оператера.

У случају престанка напајања електричном енергијом, у дужем трајању од 15 минута, у периоду ван редовног радног времена, запослено лице на пословима обезбеђења је дужан да, о томе одмах обавести руководиоца организационе јединице Оператора ИКТ система која је надлежна за управљање ИКТ системом, администратора ИКТ система или неког од запослених лица у организационој јединици Оператора ИКТ система надлежној за управљање ИКТ системом. Уколико нико од наведених лица није доступан, запослени на пословима обезбеђења је дужан да, о томе одмах обавести начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелнику Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Сви ресурси ИКТ система распоређују се, организационим јединицама Оператора ИКТ система, одлуком начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева илиодлуком начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Сви ресурси ИКТ система премештају се из једне организационе јединице Оператора ИКТ система у другу организациону јединицу Оператора ИКТ система одлуком начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева илиодлуком начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева

На основу одлуке из става 1. овог члана, приликом увођења у рад новог рачунара у ИКТ систем, надлежни запослени проверава исправност рачунара и остале рачунарске опреме (кућиште, монитор, тастатура, миш, штампач, скенер и сл.). Уколико су рачунар и рачунарска опрема исправни, надлежни запослени инсталира и лиценцира оперативни систем и остале.

Сваком рачунару, који се пријављује у домен, додељује се једнозначан назив рачунара. Тај назив рачунара се састоји од слова и четири цифре.Слова у називу рачунара се додељују према називу организационе јединице Оператора ИКТ система, у коју је распоређен тај рачунар.Назив се може допунити и додатним словима, уколико се за то укаже потреба. Прве две цифре, у називу рачунара, се додељују као последње две цифре године у којој је набављен тај рачунар. Последње две цифре, у називу рачунара, се додељују као редни

број рачунара који је, те године, уведен у ИКТ систем. Након додељивања назива рачунару, уписује се инвентарни број уређаја и остали,познати, описни подаци о том рачунару.

Назив рачунара се не мења приликом премештања рачунара, на основу одлуке из става 2. овог члана, из једне организационе јединице Оператора ИКТ система у другу организациону јединицу Оператора ИКТ система. Сви остали описни подаци, о том рачунару, обавезно се мењају, у складу са одлуком из става 2. овог члана.

Назив рачунара се не мења приликом промене назива организационе јединице Оператора ИКТ система.

Приликом премештања ресурси ИКТ система, на основу одлуке из става 1. овог члана, назив рачунара се не мења

Сваком уређају, који се користи у ИКТ систему (штампачи, скенери и сл.) уколико је то могуће, уписује се у описно поље, најмање инвентарни број, текст који садржи месец и годину набавке опреме и назив испоручиоца опреме.

Организациона јединица Оператора ИКТ система која је надлежна за управљање ИКТ системом, чува по бар једну копију носача података који садржи драјвере за тај уређај.

Сваки запослени и сваки корисник ИКТ система, на почетку радног времена, укључује опрему ИКТ система, и пријављује се у ИКТ систем својим корисничким налогом.

Сваки запослени и сваки корисник ИКТ система који се удаљава од своје радне станице, је дужан да се одјави из свих програма којејје користио и да се одјави из ИКТ система.

Сваки запослени и сваки корисник ИКТ система крају радног времена, је дужан да се одјави из ИКТ система и да на исправан начин искључи опрему ИКТ система коју користи (рачунар, лаптоп, мобилни уређај и сл.).

Запослени или корисник пријављује отказ или квар опреме која се користи у ИКТ систему, у складу са овим Правилником и Правилником за пријаву квара рачунара или рачунарске опреме. Пре сервисирања уређаја, чији је квар или отказ пријављен, обавезно се проверава да ли је у уређај у уговорном гарантном року испоручиоца опреме.

Руководилац и запослени у организациној јединици Оператора ИКТ система, која је надлежна за управљање ИКТ системом, континуирано надзиру и проверавају функционисање средстава за обраду података, управљају ризицима који могу утицати на безбедност ИКТ система и у складу са тим планирају и предлажу начелнику Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелнику Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, предузимање одговарајућих мера.

При тестирању софтвера потребно је обезбедити неометано функционисање ИКТ система.

За развој и за тестирање софтвера, пре увођења у рад у ИКТ систему, морају се користити сервери, ИКТ опрема и подаци, који су искључиво намењени тестирању и развоју.

Забрањено је коришћење сервера, ИКТ опреме и података,који се користе у редовном раду, за тестирање софтвера.

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

Инсталирање новог софтвера као и ажурирање постојећегсофтвера, односно инсталација нове верзијесофтвера, може се вршити на начин који не омета редован рад запослених или корисника ИКТ система.

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.

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

Члан 20.

Заштита ИКТ система од злонамерног софтвера спроводи се у циљу заштите ИКТ система од рачунарских вируса и других врста злонамерног рачунарског кода, који у ИКТ систем могу доспети интернет конекцијом, мејлом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од злонамерног софтвера,на сваком рачунару, на сваком преносном уређају и на сваком уређају који се користи у ИКТ систему, на коме се може инсталирати софтвер за заштиту од злонамерног софтвера, инсталира селиценциран софтвер за заштиту од злонамерног софтвера.

Софтвер за заштиту од злонамерног софтверасе подешава тако, да се може свакодневно, аутоматски,вршити допуна антивирусних дефиницијана сваких 10минута.

Једном недељно се, аутоматски, укључује проверасвих уређаја програмом за заштиту од злонамерног софтвера.

Забрањено је заустављање и искључивање програма за заштиту од злонамерног софтвератоком провере преносних медија.

Забрањено је коришћење приватних преносних меморијских медијума (спољни дискови, USB флеш и сл.).

Преноснимемморисјки медијуми, пре коришћења, морају бити проверени програмом за заштиту од злонамерног софтвера. Ако се посумња или ако се утврди да преносни медиј садржи злонамерни софтвер, уколико је то могуће, врши се чишћење преносногмедија програмом за заштиту од злонамерног софтвера. Уколико није могуће очистити преносни меморијски медијум од злонамерног софтвера, тај преносиви меморијски медијум се уништава.

Ризик од евентуалног губитка података приликом чишћења медија од злонамерног софтверасноси корисник тог меморијског медијума.

У циљу заштите од упада у ИКТ систем,надлежни запослени у организационој јединици Оператора ИКТ система, која је надлежна за управљање ИКТ системом,су дужни да одржавају систем за спречавање упадау ИКТ систем.

На свим ресурсима ИКТсистема, на којима је то могуће (сервери, рачунари, лаптопови, мобилни телефони, таблети и сл.), морају бити инсталиране најновије допуне и изменесвих програма, које произвођач,тог програма,означи као критичне, важне или препоручене (тзв „закрпе“). Проверу инсталације најновијих безбедносних или других допуна или измена врше надлежни запослени у организационој јединици Оператора ИКТ система која је надлежна за управљање ИКТ системом.

Запослени и корисници ИКТ система,који користе службени или приватни преносни рачунар за службене потребе (лаптоп, нотбук и сл.), су дужни су да омогуће, надлежном запосленом, проверу инсталације најновијих сервисних и безбедносих допуна или измена софтвера најмање једном месечно.

Запослени и корисници ИКТ система, који користе службени преносни мобилни телефон или приватни мобилни телефон за службене потребе, су дужни су да омогуће надлежном запосленом проверу инсталације најновијих сервисних и безбедносих допуна или измена софтвера најмање једном у три месеца.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, одређују који запослени или корисници ИКТ система имају право приступа Интернету, ради прикупљања података и осталих информација потребних за обављање послова у њиховој надлежности.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на Интернет,преко сопственог уређаја.

Функционери, запослени и корисници ИКТ система, којима је одобрено коришћење Интернета и електронске поште, дужни су да приликом коришћења Интернета и електронске поште, поступају по међународним конвенцијама и правилима понашања на Интернету.

Корисницима ИКТ система,који неоговарајућим коришћењем Интернета, узрокују загушење ИКТ система, прекид у раду ИКТ система или нарушавају безбедност ИКТ система, може се одузети право приступа Интернету и електронској пошти.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, може кориснику укинути приступ Интернету и електронској пошти, у случају доказане злоупотребе Интернета и електронске поште.

Корисници ИКТ система, којима је одобрено коришћење Интернета и електронске поште, дужни су да се придржавају мера заштите од злонамерног софтвераи мера заштите од неовлашћеног упада у ИКТ системса Интернета.

Сваки рачунар, чији се корисник прикључује на Интернет, мора бити одговарајуће подешен за коришћење Интернета и заштићен од злонамерног софтвера и неовлашћеног упада у ИКТ систем са Интернета.Подешавање рачунара за коришћење Интернета врши надлежни запослени у организациној јединици Оператора ИКТ система, која је надлежна за управљање ИКТ системом.

Приликом коришћења Интернета, корисник ИКТ система коме је одобрено коришћење Интернета, дужан је да избегава 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, пријави свом руководиоцу и надлежном запосленом у организационој јединици ператора ИКТ система, која је надлежна за управљање ИКТ системом.

Строго је забрањено гледање филмова, слушање музике преко Интернета, отварање ТВ станицапреко Интернета, отварање радио станица преко Интернета, инсталирање и играње игрица на рачунарима.

Строго је забрањено коришћење портабилних програма или програма који се користе без инсталације. Уколико је кориснику потребан такав програм, корисник о томе саставља писани захтев свом руководиоцу. Руководилац тог корисника доставља писмени захтев за коришћење портабилних програма или програма који се користе без инсталације, начелнику Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелнику Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева одлучују о том захтеву.

Уколико Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, изда писмену сагласност кориснику за коришћење захтеваног, бесплатног,портабилног програма или захтеваногбесплатног програм који се користи без инсталације, корисник може користити захтевани бесплатни програм, у складу са датом сагласношћу.

Начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева обавештава руководиоца организационе јединице, која је надлежна за вођење евиденције о информационим добрима, о издатој сагласности кориснику за коришћење захтеваног,бесплатног,портабилног програма или захтеваног програм који се користи без инсталације.

Строго је забрањено отварање WEB страница које садрже недоличан садржај, као и самовољно преузимање недоличног садржај са Интернета.

Коришћење друштвених мрежа и коришћење других Интернет садржаја уређују, својом одлуком,начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Недозвољена употреба Интернета обухвата следеће:

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

2. нарушавање сигурности ИКТ система или онемогућавање пословне интернет комуникације на други начин;
3. намерно ширење деструктивних и опструктивних програма на Интернету (Интернет вируси, Интернет тројански коњи, Интернет црви и друге врсте злонамерног софтвера);
4. недозвољено коришћење друштвених мрежа и других интернет садржаја, које је ограниченоодлуком начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева;
5. преузимање („download“) података велике “тежине” које проузрокује “загушење” на рачунарској мрежи;
6. преузимање („download“) материјала заштићених ауторским правима;
7. коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
8. недозвољени приступ садржају, недозвољенапромена садржаја, недозвољено брисање или недозвољена прерада садржаја преко интернета.

16. Заштита од губитка података

Члан 21.

Оператор ИКТ система врши израду резервних копија, које треба да обухвате све системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

Базе података се обавезно архивирају на уређаје за снимање резервних копија података и на преносиве медије (CDROM, DVD, USB, „strimer“ трака, екстерни хард диск), за потребе обнове базе података,једном дневно, једном недељно, једном месечно и једном годишње.

Остали фајлови (документи) се архивирају једном недељно, једном месечно и једном годишње.

Подаци о запосленима и корисницима ИКТ системасе архивирају најмање једном месечно.

Дневно копирање (архивирање)података врши се сваки радни дан у седмици, од 20 часова, сваког радног дана.

Недељно копирање (архивирање)података врши се последњег радног дана у недељи, од 20 часова, у онолико недељних примерака колико има недеља у том месецу.

Месечно копирање (архивирање)података врши се последњег радног дана у месецу, за сваки месец посебно, од 20 часова.

Годишње копирање (архивирање)података врши се последњег радног дана у години.

Сваки примерак годишње копије (архиве)података се чува у року, који је дефинисан Упутством о канцеларијском пословању органа државне управе („Сл. Гласник РС“, бр 10/93, 14/93-испр. и 67/2016).

Сваки примерак преносног меморијског медијума, који садржикопије (архиву) података, мора бити означен бројем, врстом (дневна, недељна, месечна, годишња), датумом израде

копије (архиву) података, као и именом запосленог или корисника ИКТ система, који је извршио копирање (архивирање) података.

Дневне, недељне и месечне копије (архиве) податакасе чувају у просторији која је физички обезбеђенаи која је обезбеђена у складу са мерама заштите од пожара.

Годишње копије (архиве) податакасе израђују у два примерка.Један примерак годишње копије (архиве) податакасечува у просторији, у којој се чувају дневне, недељне и месечне копије (архиве) података, а други примерак годишње копије (архиве) податакау у посебном објекту, ван зграде Градских управа града Ваљева.

Одлуку о посебном објекту, у коме ће се чувати други примерак годишње копије (архиве) података, доносе начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, посебним актом.

Исправност копије (архиве) податакапроверава се најмање једном на шест месеци и то тако што се врши враћање база података изкопија (архива) података, које се налазе на медију за чување копије (архиве) података, при чему враћени подацитреба да буду исправни и спремни за употребу, након враћања.

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

Члан 22.

У циљу обезбеђивања поузданости записа времена, у свим подсистемима ИКТ система морају бити синхронизована међусобно, као и са референтним тачним временом.

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

Сваког последњег радног дана у недељи, датотеке у којима се налази дневник активности, се копирају (архивирају), по процедури за израду копија (архива) осталих података у ИКТ систему, у складу са чл. 21 овог правилника.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца, у власништву града Ваљева, односно потпуно бесплатна Freewareверзија софтвераилипотпуно бесплатна Opensource верзија софтера.

Инсталацију и подешавање софтвера може да врши само администраторИКТ система, односно запослени или корисник, који има овлашћење за то.

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

Пре сваке инсталације нове верзије софтвера, односно промене подешавањасофтвера, неопходно је направити копију постојећегсофтвера, уколико је то могуће, како би се

обезбедила могућност повратка стања софтвера на претходно стање софтвера, у случају неочекиваних ситуација током инсталације нове верзије софтвера илипромене подешавањасофтвера.

Уколико није могуће направити копију постојећегсофтвера, пре инсталације нове верзије софтвера, односно пре промене подешавањасофтвера, неопходно је направити копију постојећегстања подешавањасофтвера, уколико је то могуће, како би се обезбедила могућност повратка стања софтвера на претходно стање софтвера, у случају неочекиваних ситуација током инсталације нове верзије софтвера илипромене подешавањасофтвера.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

Надлежна организациона јединица Оператора ИКТ система,врши анализу дневника активности,најмање једном месечно, а по потреби и чешће (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се анализом дневника активности идентификују слабости ИКТ система, које могу да угрозе безбедност ИКТ система, руководилац надлежне организационе јединица Оператора ИКТ системаје дужан да одмах о томе обавести начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Након пријема обавештења о идентификованим слабостима ИКТ система, начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева или начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева налаже спровођење мера, кој ће отклонити уочене слабости, у складу са овим Правилником.

Надлежна организациона јединица Оператора ИКТ система треба да онемогући неовлашћено инсталирање софтвера, који може довести до угрожавања безбедности ИКТ система,одговарајућим подешавањем корисничких полиса у домену.

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

Члан 25.

Ревизија ИКТ система се мора вршити тако, да има што мањи утицај на пословне процесе запослених и корисника ИКТ система. Уколико ревизију ИКТ система није могуће урадити у радно време, онда се ревизија ИКТ системаврши након завршетка радног времена запослених и корисника ИКТ система, чији би пословни процес био ометан, уз претходну сагласност начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 26.

Комуникациони каблови и каблови за напајање у ИКТ систему, морају бити постављени у зиду или каналицама, где год је то могуће,тако да се тиме онемогући неовлашћен приступ тим кабловима, односно да се изврши изолација тих каблова од могућег оштећења.

Мрежна опрема (switch, router, firewall) се мора налазити у закључаном „rack" орману. Запослени у надлежној организационој јединици Оператора ИКТ система су дужни, да стално врше контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности у раду мрежне опреме.

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

Та мрежа,коју могу да користе посетиоци објеката који су у надлежности града Ваљева,треба да буде означена идентификатором („SSID") по моделу „ВаљевоПровајдер".

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

Члан 27.

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

- Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са правилима поступка у оквиру ког се користи електронска пошта. Употреба електронске поште мора бити 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 и прописима о заштити података о личности.

- Правила коришћења Интернета

Приступ садржајима на Интернету је дозвољен искључиво за пословне намене. Интернет саобраћај се надзире и контролише. Начин надзора и контроле саобраћаја уређује начелник Градске управе која је надлежна за управљање ИКТ системом.

- Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Коришћење информационих ресурсаза друге намене одобрава начелник Градске управе, на образложени писани захтев корисника.

-Споразуми о преносу информација

Безбедан пренос информација између организације и трећег лица обезбеђује се споразумом о преносу информација.

Споразуми о преносу информација треба да укључе следеће:

1) одговорности руководства за контролу и извештавање о преносу, отпреми и пријемуинформација;
2) процедуре за обезбеђење следљивости и непорецивости процеса преноса информација;
3) минималне техничке стандарде за паковање и преносинформација;
4) стандарде за идентификовање лица које преноси информације или лица које преноси носаче података;
5) обавезе и одговорности службених лица, у случају инцидената нарушавања безбедности информација, као што је губитак података;
6) коришћење прописаног система означавања осетљивих, критичних или ин информација у документима који су означени ознаком тајности, уз осигуравање да је значење ознака одма разумљиво и да су те информације одговарајуће заштићене;
7) посебне контроле које су потребне да би се заштитили осетљиви подаци, попут криптографије;
8) одржавање ланца надзора над процесом преношења информација;
9) разумно уверавање да сви субјекти који размењују податке или информације користе поуздане систем за заштиту од злонамерног софтвера, да се не би злонамерни програми пренели из једног у други у ИКТ систем.

Уколико постоји сумња, да је ИКТ систем у који се преносе информације или постоји сумњада је ИКТ систем из којег се преносе информације или подаци, угрожен злонамерним софтвером, не сме се вршити пренос података или пренос информацијаса ИКТ системом за који се сумња да је угрожен злонамерним софтвером.

Информације и подаци се размењују у складу са прописаном процедуром о безбедности у поступку електронске размене информација или података.

Начелник Градске управе прописује процедуру размене информација.

-Процедура о безбедности у поступку електронске размене информација или податакатреба обухвата:
- заштиту информација или података од неовлашћеног приступа;
- заштиту информација или података од неовлашћеног модификовања;
- осигурање исправног адресирања и осигурање исправног транспорта информација или података;
- осигурање поштовањс законских одредби, на пример одредби о електронском потпису;
- давање одобрења за коришћења јавних услуга, као што су размена хитних порука, приступ и коришћење друштвених мрежа или заједничко коришћење датотека;
- нивое утврђивања веродостојности, контролисањем приступа из мрежа са јавним приступом.

Опретор ИКТ система склапа Споразумом о поверљивости или неоткривању информација и података, у поступку размене података или информација, којим се обавезују потписници да штите информације и податке који се размењују, у складу са законом,те да користе и објављују податке и информације које размењују на одговоран и законит начин.

Споразум о поверљивости или неоткривању информација и података, треба да садржи, између осталог:
1) дефиницију информација и података које треба заштитити;

2) очекивано трајање споразума, укључујући случајеве у којима је потребно да се поверљивост одржи неограничено;
3) поступања са информацијама или подацима по истеку споразума, попут повраћаја или уништавања информација и података;
4) дефиницију дозвољеног коришћењаинформација или података означених ознаком тајности;
5) право провере и праћење послова за које је склопљен тај споразум;
6) процес за обавештавање и извештавање о неовлашћеном откривању или приступу поверљивим информацијама;
7) радње које треба предузети у случају кршења тог споразума.

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

Члан 28.

Начин инсталирања новихресурса ИКТ система, замена и одржавање постојећих ресурса ИКТ система, које врше трећа лица, која нису запослена у Градским управама града Ваљева, или које врше друга правна лица, се уређује уговором, који се склапа са тим лицимаса тим правним лицима.

Надлежна организациона јединица Оператора ИКТ системаје задужена за технички надзор, над реализацијом уговорених обавеза трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова ИКТ система и изменама постојећих делова ИКТ система,надлежна организациона јединица Оператора ИКТ системаводи документацију.

Документација из претходног става, мора да садржи описе свих процедураза успостављању новог ИКТ система, односно увођења нових делова ИКТ система и изменама постојећих делова ИКТ система, 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 29.

За потребе тестирања ИКТ система односно делова ИКТ система,надлежна организациона јединица Оператора ИКТсистема, може да користи само оне податке који нису осетљиви, али које штити, чува и контролише на одговарајући начин.

Приликом тестирања система, подацима који су означени ознакомтајности, службеностикао поверљиви подаци, или подацимао личности, поступасе у складу са прописима, којима је дефинисана употреба и заштита такве врсте података.

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

Члан 30.

Трећа лица или 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 приступуређен уговором.

Надлежна организациона јединица Оператора ИКТ система врши контролу приступа и врши надзор над извршењем уговорених обавеза.

Надлежна организациона јединица Оператора ИКТ система вршипроверу поштовање одредби овог Правилника, током спровођења активности дефинисаних уговореним обавезама.

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

Члан 31.

Град Ваљево или Градске управе града Ваљева, могусклопити уговор са трећим лицима за пружање услуга информационе безбедности.

Надлежна организациона јединица Оператора ИКТ система врши надзор над поштовањем уговорених обавеза трећих лица или пружалаца услуга, посебно у области поштовања одредби којима је уређена информациона безбедност ресурса ИКТ система. У случају непоштовања уговорених обавеза,руководилац надлежне организациона јединица Оператора ИКТ система,је дужан да одмах обавести начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, како би они могли да предузму 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 32.

У случају било каквог инцидента, који може да угрози безбедност ресурса ИКТ система, запослени или корисник ИКТ система, је дужан да одмах обавести свог руководиоца и руководиоца организационе јединице Оператора ИКТ системанадлежне за управљањем ИКТ системом.

По пријему пријаве из претходног става,руководилац организационе јединице Оператора ИКТ система надлежне за управљањем ИКТ системом, је дужан да одмах обавести начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљеваи предузме мере, у циљу заштите ресурса ИКТ система.

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 („Сл. Гласник РС“, бр, 94/2016), начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљевасу дужни да обавесте надлежни орган, дефинисан поменутом Уредбом.

Организациона јединице Оператора ИКТ система која је надлежна за управљањем ИКТ системом,води евиденцију о свим инцидентима, као и евиденцију о пријавама инцидената, у складу са 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), на основу којемогу да се воде дисциплински, прекршајни или кривични поступци против одговорног лица.

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

У ванредних ситуацијама, које могу да узрокујуизмештање ИКТ система из зграде Градских управа града Ваљева, организациона јединица Оператора ИКТ система која је надлежна за управљањем ИКТ системом, је дужнада 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 ситуацијамаили обезбеди функционисање редудантних компоненти ИКТ система,на резервној локацији, уколико постоје редудантне компоненти ИКТ системана резервној локацији.

Спецификацију делова ИКТ система, који су неопходни за функционисање у ванредним ситуацијама израђује организациона јединица Оператора ИКТ системакоја је надлежна за управљањем ИКТ системом,у четири примерака, од којих се један налази код руководиоца организационе јединици Оператора ИКТ система која је надлежна за управљањем ИКТ системом, други примерак код запосленог надлежног за послове одбране и ванредне ситуације и по један примерак код начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

На спецификацију делова ИКТ система, који су неопходни за функционисање у ванредним ситуацијама дају сагласност начелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева

Делови ИКТ система, који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одређеначелник Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелник Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

Складиштење делова ИКТ система који нису неопходниза функционисање у ванредним ситуацијама, се врши тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о тој опреми води.

III Измена Правилника о безбедности

Члан 34.

У случају настанка промена, које могу наступити услед техничко-технолошких, кадровских, организационих или других промена у ИКТ систему и догађаја на глобалном и националном нивоу, који могу нарушити информациону безбедност, надлежна организациона јединица Оператора ИКТ система дужна једа благовремено обавести начелника Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелника Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева, како би они могли да приступе 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.

IV Провера ИКТ система

Члан 35.

Проверу ИКТ система врши организациона јединица Оператора ИКТ система која је надлежна за управљањем ИКТ системом.

Проверу ИКТ система може вршити и треће лице, које буде изабрано у складу са одредбама Закона о јавним набавкама. Провера ИКТ система ће се вршити последњег месеца у години.

Провера ИКТ система се врши тако што се:

1. проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилникена 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, користећи методе 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, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

О извршеној провери ИКТ система сачињава се извештај, који се доставља начелнику Градске управе за локални развој, привреду, урбанизам и комуналне послове града Ваљева и начелнику Градске управе за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева.

V Садржај извештаја о провери ИКТ система

Члан 36.

Извештај о провери ИКТ система садржи:

1. назив Оператора ИКТ система који се проверава;
2. време и датуме провереИКТ система;
3. податке о лицима која су вршила проверуИКТ система;
4. извештај о спроведеним радњама провереИКТ система;
5. закључке о усклађености Правилника о безбедности ИКТ система са прописаним условима;
6. закључке о адекватним применама предвиђених мера заштите у оперативном радуИКТ система;
7. закључке о евентуалним безбедносним слабостима, на нивоу техничких карактеристика компоненти ИКТ система;

8. оцену укупног нивоа информационе безбедностиИКТ система;
9. предлог евентуалних корективних мера;
10. потпис одговорног лица које је спровело проверу ИКТ система.

VI Прелазне и завршне одредбе

Члан 37.

Овај Правилник ступа на снагу осмог дана, од дана објављивања у „Службеном гласнику града Ваљева".

Број: 091-3/2017-02
Датум: 14.09.2017.

Градска управа за локални развој, привреду, урбанизам и комуналне послове града Ваљева
в.д. начелника
Владан Јеринић

Градска управа за друштвене делатности, финансије, имовинске и инспекцијске послове града Ваљева
начелник
Александар Пурић