На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16, 94/17 и 77/19), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. гласник РС", бр. 94/2016) и члана 85. Статута Општине Крупањ („Сл. лист општине Крупањ", бр.4/2019) и члана 34. Одлуке о организацији општинске управе општине Крупањ Начелник општинске управе дана начелник Управе дана 20.11.2020. године донео је

ПРАВИЛНИК
о безбедности информационо - комуникационог система општине Крупањ

I. Уводне одредбе

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности и Уредбом 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,Правилника о заштити података о личности у општинској управи општине Крупањ, утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационих система (у даљем тексту: информациона безбедност), као и овлашћења и одговорности у вези са информационом безбедношћу и ресурсима ИКТ система Општине Крупањ (у даљем тексту: ИКТ систем).

Под информационо-комуникационим системом који је предмет заштите од безбедносних ризика подразумевају се електронске комуникационе мреже, електронски уређаји на којима се чува и врши обрада података коришћењем рачунарског програма, оперативни и апликативни рачунарски програми, програмски кôд, подаци који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациона структура путем које се управља ИКТ системом, кориснички налози, тајне информације за проверу веродостојности као и техничка и корисничка документација.

Члан 2.

Циљеви доношења Правилника су:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа информационе безбедности Општине;
2. спречавање и ублажавање последица инцидената, којима се угрожава или нарушава информациона безбедност;
3. подизање свести код доносилаца одлука, посебно руководилаца органа Општине и запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;

4. прописивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система;
5. свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите у Општини.

Члан 3.

Мере прописане овим правилником служе превенцији од настанка инцидената и минимизацији штете од инцидената и примењују се у свим организационим јединицама Управе општине Крупањ, у свим службама и организацијама, које оснива надлежни орган Општине Крупањ, према посебном закону, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Општине Крупањ.

Запослени у Општинској управи односно у свим службама и организацијама, које оснива надлежни орган Општине Крупањ, потписују изјаву да су упознати са одредбама овог Правилника. Један примерак ове изјаве се чува у персоналном досијеу запосленог, са јасно видљивим датумом потписивања.

За праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама одговорни су начелник Општинске и техничар система и мреже.

Поједини термини у смислу овог правилника имају следеће значење:

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

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

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

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

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

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

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

4) *интегритетзначм* очуваност изворног садржаја и комплетности податка;

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

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

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

података;

II. Мере заштите

Члан 4.

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

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

Члан 5.

Општина Крупањ у оквиру организационе структуре утврђује послове и одговорности руководилаца и запослених у циљу управљања информационом безбедношћу.

Правилником о унутрашњој организацији и систематизацији радних места утврђују се радна места на којима се обављају послови од значаја за обезбеђивање и праћење безбедности информационог система у сваком од органа Општине, степен обуке и квалификација запослених и нивои приступа информационим ресурсима.

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

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Општине Крупањ надлежан/на је начелник Општинске управе и руководилац основне организационе јединице у чијем су делокругу ИКТ послови-Одељење за општу управу друштвене делатности, послове органа општине и заједничке послове, односно руководилац службе и организације, које оснива надлежни орган Општине Крупањ, према посебном закону.

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава иимовине 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 Општине, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе;

8) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
9) *управљање ризиком* је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
10) *инцидент]е* сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система;
11) *мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
12) *тајни податак]е.* податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
13) ***ИКТ** систем за рад са тајним подацима* је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
14) *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
15) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
16) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
17) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;
18) *криптоматеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
19) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
20) *информациона добра* обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично;
21) *VPN (Virtual Private Netvvork)* - је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
22) *MAC адреса* (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
23) *Backupje* резервна копија података;
24) *Dovvnioad* је трансфер података са централног рачунара или web презентације на локални рачунар;
25) *UPS* (Uninterruptible power supply^ је уређај за непрекидно напајање електричном енергијом;
26) *Freeware]e* бесплатан софтвер;
27) *Opensource*софтвер отвореног кода;
28) *Firewaii* је „заштитни зид" односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
29) *USB*или флеш меморија је спољшњи медијум за складиштење података;
30) *CD-ROM* (Compact disk - read only тетогу) се користи као медијум за снимање података;
31) *DVD* је оптички диск високог капацитета који се користи као медијум за складиштење

- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу;
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента Техничар система и мреже, обавештава начелника ОУ, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедносног инцидента.

2.Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву Општине, и који су подешени од стране техничара система и мреже, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности (електронска пошта, навести апликације којима је дозвољен приступ), а на основу писане сагласности начелника Управе.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и листе MAC[1] адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

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

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

Техничар система и мреже, 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 Општине, оштећен и није обезбеђена замена.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води Техничар система и мреже, а по одобрењу начелника Управе.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране Техничар система и мреже, могу се користити само за обављање послова у

---

[1]Media Access Control (MAC address)

надлежности корисника-запосленог и то само у периоду када није могуће користити уређај у власништву Општине Крупањ. Техничар система и мреже, је дужан/на да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради *backup* података који се налазе у мобилном уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати податке у мобилни уређај.

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

Члан 8.

Начелник општинске управе општине Крупањ се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају. Њихове одговорности се утврђују процедуром о правима приступа информационом систему, решењем о распоређивању на одређено радно место (за службенике), уговором о раду (за намештенике), посебним уговорима (о привременим и повременим пословима и сл.) за радно ангажована лица по другом основу и споразумом о поверљивости.

Руководилац организационе јединице надлежне за ИКТ и службеници који управљају ИКТ системом се процедуром о правима приступа информационом систему и/или решењем о распоређивању овлашћују за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

У поступку заснивања радног односа за запослене који управљају ИКТ системом односно запослене који користе ИКТ систем у општинској управи се проводе радње у циљу провере испуњености услова сразмерно пословним захтевима, класификацији информација којима се на радном месту које се попуњава одобрава приступ и сагледаним ризицима.

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

Програмима стручног усавршавања у општинској управи се обезбеђује да се запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура у области информационе безбедности континуирано обучавају у циљу унапређења техничког и технолошког знања. Сви службеници општинске управе су у обавези да заврше одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и у

примени у Општини. Дисциплински поступак се покреће по предлогу начелника општинске управе односно руководиоца служби и организацијама, које оснива надлежни орган Општине Крупањ, према посебном закону.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања. Дужности и обавезе које остају важеће и после престанка ангажовања су садржане у тексту решења о распоређивању, уговора о раду, односно уговора о ангажовању лица ван радног односа.

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

Члан 9.

За поступања приликом престанка запослења или ангажовања задужен/а је службеник (организациона јединица) за људске ресурсе у сарадњи са службеницима који управљају ИКТ системом који предузимају следеће активности:

1) проверавају испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату;
2) прегледају све налоге и приступе систему који су били доступни службенику односно намештенику, преузимају од њега електронске и друге мобилне уређаје;
3) проверавају враћене мобилне уређаје и уређаје за преношење података;
4) дају налог за укидање налога електронске поште и свих других права приступа систему на дан престанка радног односа или другог основа ангажовања;
5) прегледају све налоге за приступ и прикупљају приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
6) преузимају картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

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

Евиденцију о информационим добрима води Одељење за општу управу друштвене делатности, послове органа општине и заједничке послове, у папирној или електронској форми.
У складу са Законом о буџетском рачуноводству, Уредбом о буџтском рачуноводству и Правилником о систематизацији и организацији радних места општинске управе општине Крупањ надлежна организациона јединица за буџет и финансије у сарадњи са службеницима који управљају ИКТ системом врши идентификацију имовине која је предмет заштите и документује њен животни циклус.

Предмет заштите су:
- 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

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

Члан 11.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем. Класификациона шема поверљивости информација је заснована на четири нивоа:

1) откривање не изазива никакву штету;
2) откривање изазива мању непријатност или мању штету;
3) откривање има значајан краткорочни утицај на обављање послова из делокруга Општине;
4) откривање има озбиљан утицај на дугорочне стратешке циљеве или обављање послова из делокруга Општине.

Град/општина/градска општина врши класификацију ради:

1) јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење;
2) подизања свести о вредности информације или документа;
3) заштите података у покрету ради боље и интелигентније интеграције са DLP, WEB gateway и осталим производима за заштиту параметара и крајњих уређаја.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебним прописима [2].

---

[2]Закон о слободном приступу информацијама од јавног значаја („Сл. гласник РС", бр.120/04, 54/07, 104/09 I 36/10), Закон о заштити података о личности („Сл. гласник РС", бр.87/18), Закон о 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 („Сл. гласник РС", бр. 53/2011 55/05, 71/05 – исправка, 101/07, 65/08 и 16/11).

Детаљан опис информација, носачима информација и доступности података налази се у Информатору о раду општине Крупањ

7. Заштита носача података

Члан 12.

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

- подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено одлуком начелника.
- подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника (назив радног места на коме се обављају послови безбедности и др. начелник, администратор, руководилац организационе јединице)

Евиденцију носача на којима су снимљени подаци, води Техничар система и мреже и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.
У случају транспорта медија са подацима, начелник Управе ће одредити одговорну особу и начин транспорта.
У случају истека рокова чувања података који се налазе на медијима, подаци морају бити неповратно обрисани, а ако то није могуће, такви медији морају бити физички оштећени, односно уништени.

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

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

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

података („Сл. гласник РС", 104/2009), као и Уредба о начину и поступку означавања тајности података, односно докумената („Сл. гласник РС", бр. 8/2011)

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

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

Запослени-корисник дужан је да поштује и следећа правила *(у складу са архитектуром ИКТ система (домен-без домена), прилагодити правила систему)* 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 Општине Крупањ 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;
19) 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 општине Крупањ
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, осим ако то није склопу одржавања система или отклањања проблема, уз сагласност надређеног.

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

Члан 14.

Право приступа имају само запослени/корисници који имају администраторске или корисничке налоге.
Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Администраторски налог за управљање доменом у ЛПА може/могу да користе само запослени на пословима техничар система и мреже, Шеф Одсека локалне пореске администрације и послови утврђивања локалних јавних прихода
Администраторски налог за управљање базама података може/могу да користе само запослени на пословима техничар система и мреже.
Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу кога/јих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налози су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности. Кориснички налог додељује администратор, на основу захтева запосленог задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима, а у складу са потребама обављања пословних задатака од стране запосленог-корисника. Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

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.

Коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење. Корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички налози. Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима. Администратор ИКТ система сваких 12 месеци врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај запослења).

Редовне пословне активности се не врше из привилегованих корисничких налога. Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

(Пример:Корисничко име се креира по матрици име.презиме, латиничним писмом без употребе слова ђ,ж,љ, њ, ћ, ч, џ, ш.
(Препорука: Уместо ових слова користити слова из табеле.)

Ћирилична слова	Латинична слова
Ђ	dj
Ж	z
Љ	lj
Њ	nj
Ћ, Ч	c
Ш	s
Џ	dz

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

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

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

Запослени-корисник дужан је да мења лозинку најмање једном у 6 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 сертификатом).

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

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 16.

Приступ ресурсима ИКТ система Општине Крупањ не захтева посебну крипто заштиту.

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

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

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

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

Члан 17.

У општинској управи општине Крупањ простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система се налазе у посебној просторији која је обезбеђена механичком бравом, прозори су обезбеђени решеткама и просторија је климатизована.

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

Члан 18.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система/запосленима на пословима ИКТ.
Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу начелника Управе, и уз присуство надлежног лица -Техничар система и мреже.
Приступ административној зони може имати и запослени/а на пословима одржавања хигијене уз присуство надлежног лица -Техничар система и мреже.

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

Прозори и врата на овој просторији морају увек бити затворени, и по потреби обезбеђени решетком.

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

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

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења начелника.

У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење начелника који ће одредити услове, начин и место изношења опреме.

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

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

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим, планирају, односно предлажу начелнику Управе 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 запослених-корисника.

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

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

Члан 20.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

- 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.

Члан 21.

Листа провера које се спроводе у циљу заштите од злонамерног софтвера обухвата али се не ограничава на:

а) проверу, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер;

б) проверу, пре коришћења, садржаја прилога електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер; ова провера се спроводи на разним местима, нпр. на серверима за електронску пошту, на стоним рачунарима или приликом уласка у мрежу оператора ИКТ система;

в) проверу постојања злонамерних софтвера на веб-страницама;

г) обука за извештавање и опоравак од напада злонамерним софтвером;

д) припрему одговарајућих планова за континуитет пословања приликом опоравка од напада злонамерним софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак;

ђ) имплементацију процедура за редовно прикупљање информација, као што је претплата на адресне спискове за доставу или провера веб-страница на којима се дају информације о новим злонамерним софтверима;

е) имплементацију процедура за верификовање информација о злонамерним софтверима и обезбеђење да су упозоравајући извештаји тачни и информативни; за разликовање лажних од стварних злонамерних софтвера користе се квалификовани извори, нпр. проверени часописи, поуздане странице на Интернет мрежи или испоручиоци програма против злонамерних софтвера.

16. Заштита од губитка података

Члан 22.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују. Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски у 9.00 сати врши допуна антивирусних дефиниција.
Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

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

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

У циљу заштите, односно упада у ИКТ систем Општине Крупањ са интернета, Техничар система и мреже је дужан 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 Техничар система и мреже може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени-корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши Техничар система и мреже.

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

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Техничар система и мреже.
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.

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);

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

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система. За чување заштитних копија користе се магнетне траке, екстерни хард дискови и CD/DVD медији.
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 21 час.

Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно, од 22 часа.

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 („Сл. гласник РС", бр 10/93, 14/93-испр, 67/2016 и 3/2017).

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

Дневне, недељне и месечне копије-архиве се чувају у безбедносној зони.

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

Члан 23.

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

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

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

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

Инсталацију и подешавање софтвера може да врши само Техничар система и мреже, односно запослени-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.

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

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

Техничар система и мреже 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, Техничар система и мреже је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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

Члан 26.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност начелника Управе.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 27.

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.

Техничар система и мреже је дужан/а 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.

Та мрежа треба да буде означена (ССИД) по моделу opstina krupanj guest

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

Члан 28.

Локална самоуправа не врши размену података који су означени неком од ознака тајности са другим органима и организацијама.

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

Члан 29.

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

Техничар система и мреже је задужен и за технички надзор над реализацијом уговорених обавеза од стране трећих лица.
О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система Техничар система и мреже води документацију.

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

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

Члан 30.

Приликом тестирања система, подаци који су означени ознаком тајности, односно службености као поверљиви подаци, или су лични подаци одговара за податке 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 31.

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

Техничар система и мреже је одговоран/на за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

Пре отпочињања преговора, потенцијални пружалац услуга у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, која садржи обавезу за пружаоца услуга да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране Општине Крупањ као уговорне стране, а за потребе извршења предмета преговора.

Изјава о поверљивости, односно уговор о пружању услуга, садржи одредбу о поверљивости са јасно утврђеном обавезом и одговорношћу пружаоца услуге уз претњу раскида уговора и накнаде штете у корист Општине Крупањ у случају повреде ове одредбе.

Изјава о поверљивости обавезно гласи:

"Сви подаци и информације садржани у овом Уговору о пружању услуга се сматрају поверљивим пословним подацима и не смеју бити саопштени или на други начин учињени доступним трећим лицима. Нарочито се сматрају поверљивим сви пословни подаци и информације које једна страна учини доступним другој уговорној страни ради извршења обавеза из овог уговора, уколико ти подаци нису јавно доступни нити су били претходно познати другој страни.

Свака уговорна страна се обавезује да податке и информације које јој буду учињене доступним у складу са овим уговором и обавезом извршења уговорених послова и обавеза, буду стављене на располагање и увид запосленима, уколико је то неопходно ради извршења обавеза из овог уговора.

Уговорне стране се нарочито обавезују да поступају обазриво са подацима о личности до којих могу доћи у поступку извршења услуга за оператора ИКТ система, као и да те податке чувају и поступају у свему у складу са прописима који уређују заштиту података о личности.

У случају повреде ове обавезе уговорна страна чији су подаци коришћени има право раскида уговора и право да захтева накнаду штете услед неовлашћеног коришћења података и информација друге стране."

Пружаоци услуга дужни су да захтеве Општине Крупањ у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе.

Руководилац одељења за општу управу друштвене делатности, послове органа општине и заједничке послове је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби правилника којима су такве активности дефинисане.

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

Члан 32.

Општина тренутно нема склопљен уговор са трећим лицима за пружање услуга информационе безбедности.

У случају да општина у неком наредном периоду склопи уговор за услуге информационе безбедности, руководилац одељења за општу управу друштвене делатности, послове органа општине и заједничке послове је одговоран/а за надзор над поштовањем уговорених обавеза од стране трећих лица-пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система. У случају непоштовања уговорених обавеза руководилац одељења за општу управу друштвене делатности, послове органа општине и заједничке послове је дужан/а да одмах обавести начелника, како би он могао да предузме мере у циљу отклањања неправилности.

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

Члан 33.

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

По пријему пријаве Техничар система и мреже је дужан/а да одмах обавести начелника Управе и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан 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), Техничар система и мреже, је дужан/а да поред начелника обавести и надлежни орган дефинисан овом уредбом.

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

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 34.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Управе, Техничар система и мреже, је дужан/а 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 Техничар система и мреже , 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.

III. Измена Правилника о безбедности

Члан 35.

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, Техничар система и мреже је дужан/а да обавести начелника Управе, како би он могао да приступи измени овог правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IV. Провера ИКТ система

Члан 36.

Проверу ИКТ система ће вршити лице које буде изабрано у складу са одредбама Закона о јавним набавкама, односно Техничар мреже у случају када не буде закључен уговор у складу одредбама Закона о јавним набавкама. Провера ће се вршити последњег месеца у години.

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.

V. Садржај извештаја о провери ИКТ система

Члан 37.

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.

VI. Прелазне и завршне одредбе

Члан 38.

Овај правилник ступа на снагу даном објављивања у „Службеном листу Општине Крупањ".

Република Србија
Општина Крупањ
Општинска управа
Начелник Управе

III Број:110-12/2020
У Крупању, дана 20.11.2020.

Република Србија • Општина Крупањ • Општинска управа •

Начелник
Општинске управе општине Крупањ