СЛУЖБЕНИ ЛИСТ ГРАДА УЖИЦА

XLXX 18. фебруар 2019. године Број 5/19

23. На основу члана 61. Статута Градске општине Севојно („Службени лист града Ужица“, број 20/14), Скупштина Градске општине Севојно, на седници одржаној 18.02.2019. године, донела је

ОДЛУКУ
О ПРИСТУПАЊУ ИЗМЕНАМА И ДОПУНАМА СТАТУТА ГРАДСКЕ ОПШТИНЕ СЕВОЈНО

I Приступа се изменама и допунама Статута Градске општине Севојно.

II Именује се Комисија за израду Нацрта акта о измени Сатута Градске општине Севојно у саставу:

За председника:
1. Бојана Оташевић

За чланове:
1. Славица Виторовић
2. Данијела Плакаловић
3. Александар Ћалдовић
4. Жарко Вукотић

III Комисија из тачке 2. ове одлуке ће израдити Нацрт акта о изменама и допунама Статута Градске општине Севојно, ради усклађивања са изменама и допунама Статута града Ужица које су усвојене на седници Скупштине града 07.02.2019. године и Нацрт доставити Општинском већу ради утврђивања предлога за Скупштину.

IV Одлука ступа на снагу даном објављивања у „Службеном листу града Ужица“.

РЕПУБЛИКА СРБИЈА
ГРАД УЖИЦЕ
СКУПШТИНА ГРАДСКЕ ОПШТИНЕ СЕВОЈНО
I Број: 06-93/19, 18.02.2019.године

ПРЕДСЕДНИК СКУПШТИНЕ
ГРАДСКЕ ОПШТИНЕ СЕВОЈНО
Никола Гогић, с.р.

24. На основу члана 10. Статута Градске општине Севојно ("Службени лист града Ужица" број 20/14), Скупштина Градске општине Севојно, на седници одржаној 18.02.2019. године, доноси

ОДЛУКУ

1. Усваја се Локални акциони план запошљавања Градске општине Севојно за 2019. годину.
2. Одлука ступа на снагу даном доношења и објавиће се у „Службеном листу града Ужица“.

РЕПУБЛИКА СРБИЈА
ГРАД УЖИЦЕ
ГРАДСКА ОПШТИНА СЕВОЈНО
СКУПШТИНА
I број 06 - 94/19, 18.02.2019. године

ПРЕДСЕДНИК СКУПШТИНЕ
ГРАДСКЕ ОПШТИНЕ СЕВОЈНО
Никола Гогић, с.р.

25. На основу члана 30. Став 17. Статута Градске општине Севојно ("Службени лист града Ужица" бр.20/14), Скупштина градске општине Севојно на седници одржаној 18.02.2019. године донела је

ОДЛУКУ
О ПРИСТУПАЊУ ГРАДСКЕ ОПШТИНЕ СЕВОЈНО ТРАДИЦИОНАЛНОЈ СМОТРИ И МАНИФЕСТАЦИЈИ СПОРТА И ФИЗИЧКЕ КУЛТУРЕ МОСИ

I У циљу успостављања и јачања веза између градова и општина у области спорта, физичке културе, размене искустава и заједничког деловања, Градска општина Севојно приступа традиционалној смотри и манифестацији спорта и физичке културе МОСИ – Међуопштинске омладинске спортске игре.

II Одлука ступа на снагу даном објављивања у „Службеном листу града Ужица".

РЕПУБЛИКА СРБИЈА
ГРАД УЖИЦЕ
СКУПШТИНА ГРАДСКЕ ОПШТИНЕ СЕВОЈНО
I Број: 06-95/19, 18.02.2019.године

ПРЕДСЕДНИК СКУПШТИНЕ
ГРАДСКЕ ОПШТИНЕ СЕВОЈНО
Никола Гогић, с.р

26. На основу члана 12. Закона о информационом систему Републике Србије ("Сл. гласник РС" бр. 12/96), члана 51. Одлуке о градским управама ("Службени лист града Ужица" бр.14/08), начелник Градске управе за послове органа града, општу управу и друштвене делатности дана 09.07.2015. године доноси

ПРАВИЛНИК О ИНФОРМАЦИОНОМ СИСТЕМУ ГРАДСКИХ УПРАВА ГРАДА УЖИЦА

1. ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим правилником уређују се функционисање, развој и начин коришћења ресурса Информационог система Градских управа града Ужица (у даљем тексту: Информациони систем) као и мере његовог обезбеђивања и заштите. Правилник се примењује на све запослене у Градским управама као и на све привремене или сталне кориснике Информационог система.

Члан 2.

Поједини изрази употребљени у овом Правилнику имају следеће значење:

- *Информациони систем чине*: рачунарска и комуникациона опрема (рачунари, штампачи, мрежни уређаји, уређаји за непрекидно напајање електричном енергијом, каблови...), рачунарски програми и подаци неопходни за исправан рад Информационог система;
- *Системска администрација* је скуп послова којима се одржава функционалност Информационог система;
- *Администратори информационог система* (Инжењр система и БП. Администратор мреже и комуникација и Пројектант - аналитичар) су запослени у Одељењу за информационе технологије и комуникације (у даљем тексту: ИТ одељење), који обављају послове системске администрације Информационог система;
- *Корисници Информационог система* су сви запослени у Градским управама или друга лица, којима су дата стална или привремена права за коришћење Информационог система од стране овлашћене особе (начелника Градске управе), при чему је у том случају обавезно пријављивање корисничким именом задатим од стране ИТ одељења;
- *Корисничко име и лозинка* су подаци који служе за приступ Информационим систему. Сваки корисник се идентификује својим корисничким именом и својом лозинком. Корисничко име је јавни, а лозинка тајни податак;
- *Системски програми* су скуп програма који управљају радом рачунара (оперативни систем, базе података, антивирусни програм и сл.)
- *Апликативни програми* су програми које корисници извршавају на рачунару (програми за куцање текста, израду табела, рад са базама података, обраду слика, цртање и слично)
- *IP адреса* представља привремени идентификациони број сервера и/или радне станице у оквиру рачунарске мреже;
- *Домен* је назив који идентификује јединствену радну групу коју чине сви рачунари, штампачи, радне јединице и корисници у оквиру мреже;
- *Доменска полиса* је назив за правило којим се директно одређују права и наследна својства свих чиниоца домена;

- *Сервер ј*е централни рачунар у мрежи који контролише домен, на којем су одређене доменске полисе, на којем се врши централно складиштење података, који садржи целокупну базу свих корисника и програма који су њима придружени; Уколико постоји више сервера у систему, они врше следеће послове: DC (domain controler, контролише рад рачунара и корисника), WEB сервер (контролише везу са Интернетом), MAIL сервер (размена електронских порука), APLICATION сервер (на њему се налазе инсталирани програми - апликације), DATABASE сервер (на њему су базе података), итд;

- *Радна станица* је рачунар на коме запослени обављају своје послове.

- *Потрошни материјал* обухвата магнетне и оптичке медијуме за складиштење података (CD, DVD, USB ...) тонере за штампаче и други материјал.

2. РАЧУНАРСКА И КОМУНИКАЦИОНА ОПРЕМА

Члан 3.

Рачунарска и комуникациона опрема се налази у својини Градских управа и о њеном функционисању и коришћењу стара се ИТ одељење, а о детаљној евиденцији са одговарајућом службом књиговодства.

Члан 4.

Набавка рачунарске и комуникационе опреме врши се у складу са законом и усвојеним планом за јавне набавке. План набавке опреме предлаже ИТ одељење, у складу са развојем информационог система и појединачним захтевима за набавком рачунарске и комуникационе опреме добијеним од стране Градских управа.

Појединачне захтеве за набавку рачунарске и комуникационе опреме потребно је доставити ИТ одељењу најкасније до краја текуће календарске године, односно до израде одговарајућих финансијских планова, како би трошкови набавке били укључени у план буџета за наредну годину.

Појединачни захтев за набавку рачунарске опреме треба да садржи: назив организационе јединице и радног места за које се подноси захтев, хитност набавке, захтевану количину рачунарске опреме, опис и обим послова који ће се обављати на траженој рачунарској опреми, образложење о могућим уштедама које би се добиле набавком опреме и какав би то ефекат имало на пословање Градске управе;

На основу појединачног захтева за набавку рачунарске и комуникационе опреме, ИТ одељење одређује неопходне техничке особине опреме које задовољавају исказане потребе у захтеву за набавку опреме и њемо умрежавање.

Након завршеног поступка јавне набавке, ИТ одељење врши распоређивање и инсталацију набављене опреме, а увођење у евиденцију заједно са надлежним службама рачуноводства за вођење основних средстава.

Члан 5.

Потрошни рачунарски материјал (тонери за штампаче, CD и DVD медијуме и др.) набавља организациона јединица за опште послове са службом за јавне набавке, према техничким карактеристикама које дефинишу са ИТ одељењем.

Члан 6.

Просторије у којима ради рачунарска и комуникациона опрема морају задовољити услове који су прописани законом, техничким стандардима и техничким одредницама произвођача опреме.

Рачунарска и комуникациона опрема мора испуњавати законске прописе и техничке стандарде у области заштите на раду, телекомуникација и остале прописе који уређују ову област.

Члан 7.

Кућиште рачунара треба да стоји тако да буде омогућено слободно струјање ваздуха, не сме се држати никакав материјал на кућишту или непосредно наслоњен на кућиште. Забрањено је премештање кућишта без предходне консултације са ИТ одељењем.

Рачунар се напаја електричном енергијом преко уређаја за непрекидно напајање. Забрањено је прикључивање великог корисника електричне енергије (решо, грејалица, ...) на место где је прикључен рачунар као и прикључивање штампача или било ког другог потрошача електричне енергије на уређај за непрекидно напајање електричном енергијом.

У непосредној близини рачунара забрањено је конзумирање хране, кафе и пића.

3. ИДЕНТИФИКАЦИЈА И КОРИШЋЕЊЕ РАЧУНАРСКЕ ОПРЕМЕ

Члан 8.

Прикључење рачунарске опреме на Информациони систем или њено искључење из Информационог система обавља ИТ одељење.

Пре самог прикључења рачунар мора бити правилно конфигурисан, са инсталисаним потребним програмима, који су дефинисани доменском полисом, заштићен од неовлаштеног приступа и означен идентификационом маркицом.

Сваки рачунар конфигурисан је са становишта хардвера и софтвера да максимално подржава обављање послова у Градској управи као и да омогући стабилан и непрекидан рад.

Члан 9.

Сваки рачунар и штампач прикључени на Информациони систем имају свој назив.

Називи рачунара (осим серверских система) и штампача састоје се од седам знакова (комбинација слова и бројева) који администратору система указују на место и доба инсталирања, односно, активирања опреме.

Давање имена, IP адреса и других идентификационих података о рачунарској опреми обављају администратори информационог система.

Члан 10.

Рад свих сервера је непрекидан - 24 часа, сем у случају нестанка електричне енергије.

Управљање радом сервера, опреме прикључене непосредно на сервер, активном мрежном опремом и системским штампачима врше администратори информационог система.

Радне станице и периферна рачунарска опрема, осим уређаја за непрекидно напајање, се искључују након завршетка радног времена. Искључивање и укључивање опреме коју користе корисници Информационог система врше сами корисници Информационог система.

На уређај за непрекидно напајање електричном енергијом могу се прикључити рачунар (кућиште), монитор и уређај за повезивање рачунара на рачунарску мрежу.

Пре сваког напуштања радног места (и у току радног времена) обавезно је одјавити се из радног окружења на рачунару да би се онемогућио приступ Информационом систему неовлашћеним лицима или приступ Информационом систему од стране другог корисника.

Приликом сваког квара или неуобичајеног рада рачунарске и комуникационе опреме, потребно је одмах обавестити ИТ одељење.

4. ИДЕНТИФИКАЦИЈА КОРИСНИКА ИНФОРМАЦИОНОГ СИСТЕМА

Члан 11.

Информациони систем се може користити само за обављање послова из надлежности Градских управа.

Само администратори информационог система могу имати администраторске привилегије у Информационом систему.

Члан 12.

Сваки корисник се идентификује својим корисничким именом и својом лозинком .

Корисничко име одређује администратор информационог система и састоји се од имена, тачке (.) и презимена корисника. Уколико постоји више корисника који би имали исто корисничко име, разлику одређује администратор система у договору са корисником коме отвара корисничко име.

Почетну корисничку лозинку одређује администратор информационог система самостално или у договору са корисником . Сваки корисник је обавезан да памти своју лозинку и да је мења у складу са потребама, а најмање једанпут месечно, на шта га систем упозорава.

За послове извршене под одређеним корисничким именом и лозинком, одговоран је корисник чије су они власништво.

Члан 13.

Администратор информационог система може опоменути корисника Информационог система који се не придржава овог Правилника и тиме угрожава безбедност Информационог система.

Администратор информационог система може привремено ускратити приступ кориснику који угрожава безбедност Информационог система. Уколико корисник након опомене и привременог ускраћивања приступа Информационом систему понови радње којима угрожава безбедност Информационог система, администратор информационог система може, уз сагласност руководиоца ИТ одељења и начелника Градске управе, трајно ускратити приступ том кориснику.

5. РАЧУНАРСКИ ПРОГРАМИ

Члан 14.

На основу захтева за набавку рачунарске опреме и развоја информационог система, администратори информационог система дужни су да одреде и инсталирају системске и апликативне програме, који ће се користити на појединим рачунарима, о чему се води евиденција.

За сваки рачунар ИТ одељење прави листу лиценцираних системских и апликативних програма који су инсталирани у моменту предаје рачунара на коришћење. Сваку промену (инсталација/деинсталација) администратор информационог система је дужан да евидентира.. Корисник одговара за свако одступање од наведене листе.

Члан 15.

Уколико постоји потреба за инсталацијом додатних апликативних програма у оквиру Градских управа, или других лица ван Градских управа, захтев се упућује руководиоцу ИТ у писаној форми, који уз сагласност начелника Градске управе доноси одлуку о њиховој оправданости..

Строго је забрањена свака самоиницијативна набавка и инсталација системских и апликативних програма без консултација са руководиоцем ИТ одељења.

6. РАЗМЕНА ПОДАТАКА, ИНТЕРНЕТ И ЕЛЕКТРОНСКА ПОШТА

Члан 16.

У циљу лакше комуникације и једнообразности за креирање докумената користити фонт «Times New Roman» или «Arial», величине 12.

Сваки документ који је од значаја треба чувати на мрежном серверу, на једној од предвиђених локација, у договору са администратором информационог система. На овај начин архивирања подаци су безбедни од неовлашћеног коришћења и случајног брисања.

За податке архиване у локалу, на радној станици, одговоран је сам корисник.

Члан 17.

Приступ интернету обезбеђен је запосленим у Градским управама у мери која им је неопходна за обављање свакодневних послова, дефинисаних описом радног места, а обезбеђује га администратор информационог система у складу са овим Правилником.

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

Приступ интернету, коришћењем рачунарских ресурса Градских управа, омогућиће се и трећим лицима, под одређеним условима дефинисаним овим Правилником.

Приступ интернету лицима који су гости Градске куће и не обављају никакве пословне процесе за потребе градских управа се обезбеђује кроз изолован мрежни сегмент под надзором администратора информационог система (Велика сала, Мала сала, Кабинет, ...).

Члан 18.

Свако ко користи интернет и електронску пошту треба да поступа по међународним конвенцијама и правилима понашања.

Корисницима који су прикључени на Информациони систем је забрањено самостално прикључење на интернет (прикључење преко сопственог модема), при чему администратор информационог система може укинути приступ интернету у случају доказане злоупотребе.

Корисници Информационог система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у Информациони систем.

Сваки умрежен рачунар мора бити одговарајуће подешен и заштићен, при конфигурисању и инсталацији код корисника, од стране администратора информационог система.

Приликом коришћења интернета избегавати сумњиве WEB странице. У случају да корисник примети необично понашање рачунара, запажање треба, без одлагања, да пријави ИТ одељењу.

Строго је забрањено приступање аудио и видео садржајима у било ком облику и "крстарење" WEB страницама које садрже порнографски и остали недоличан садржај, као и самовољно преузимање истих са интернета.

На серверима и радним станицама смеју се чувати само подаци стриктно неопходни за послове Градских управа и не смеју се снимати слике, музика, филмови, игрице и сл. који ће, у том случају, бити обрисани са сервера.

Уколико постоји потреба за преузимањем одређених недоступних садржаја са интернета захтев треба упутити ИТ одељењу у писаној форми, које је дужно да процени оправданост захтева у року од 24 часа.

7. ЗАШТИТА ИНФОРМАЦИОНОГ СИСТЕМА

Члан 19.

Заштита Информационог система подразумева безбедност података од брисања, неовлашћеног приступа, заштиту од неовлашћене измене, заштиту од вируса и свих других видова угрожавања података.

Правилним коришћењем Информационог система од стране корисника, односно коришћењем у складу са одредбама овог Правилника, стварају се услови за безбедно функционисање Информационог система. У том случају, сваки податак, односно документ, ће бити правилно сачуван на серверу.

Члан 20.

Креирање дневних копија база података са сервера (на неком од медија) се извршава сваког радног дана после 22 часа, од стране ИТ одељења, што значи да већ наредног дана подаци потребни за враћање на претходно стање могу бити рестаурирани. На овај начин сачувани подаци ће бити доступни за више радних дана, након чега се исти преписују новим садржајем.

Петнаестодневне резервне копије се праве последњег радног дана у недељи, по истеку сваке друге седмице и чувају као резерва копија из става 1. овог члана..

За трајно чување свих других докумената (дељени-заједнички на серверима и са појединачних радних станица) треба користити CD, DVD и USB медијуме. За сву осталу помоћ око чувања и архивирања података треба се обратити ИТ одељењу.

Члан 21.

Дневне копије се чувају у сервер сали, а петнестодневне у просторији изван сервер сале.

Дневне и петнаестодневне резервне копије су предвиђене се опоравак система у следећим случајевима: квар на серверу, нестанак струје, губитак опреме, напад вирусом, крађа и пожар.

Члан 22.

У циљу бољег функционисања опреме Информационог система превентивним одржавањем, у препорученим временским размацима, врши се замена делова рачунарске и комуникационе опреме.

Послове из става 1. овог члана обављају запослени ИТ одељења.

Члан 23.

За успешну заштиту рачунарске опреме од злонамерног софтвера, администратор информационог система, на сваком рачунару инсталира антивирусни програм и редовно прати ажурност антивирусних дефиниција. Забрањен је сваки покушај корисника да ову заштиту неутралише.

8. КАЗНЕНЕ ОДРЕДБЕ

Члан 24.

Запослени чини лакшу повреду радне обавезе уколико:

- уступа корисничко име и лозинку другој особи,
- у непосредној близини рачунара: конзумира храну, кафу и пиће,
- на кућишту рачунара или са стране одлаже други материјал, који онемогућева циркулацију ваздуха и потребно хлађење.

Члан 25.

Запослени чини тежу повреду радне обавезе уколико:

- прикључи великог потрошача енергије (на пример: решо, грејалица, ...) на место где је прикључена радна станица,
- прикључи на уређај за непрекидно напајање електричном енергијом штампач или други потрошача електричне енергије,
- покуша да изврши самоиницијативну инсталацију било ког рачунарског програма или копира инсталиране програме без сагласности ИТ одељења,
- на било који начин уноси или износи податке (путем e-maila, помоћу преносивих медијума) без сагласности и провере од стране свог непосредног руководиоца што се тиче садржине и без консултација са запосленима ИТ одељења, са аспекта заштите од вируса уколико постоји сумња да је медијум заражен,
- корисник након опомене и привременог ускраћивања приступа Информационом систему понови радње којима угрожава безбедност Информационог система,
- користи потрошни материјал за који ИТ одељење није дало одобрење за коришћење,
- "крстари" WEB страницама које садрже порнографски и остали недоличан садржај, као и њихово самовољно преузимање са интернета.

9. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 26.

Овај Правилник ступа на снагу осмог дана од дана објављивања у ”Службеном листу града Ужица".

РЕПУБЛИКА СРБИЈА
ГРАД УЖИЦЕ
ГРАДСКА УПРАВА ЗА ПОСЛОВЕ ОРГАНА ГРАДА,
ОПШТУ УПРАВУ И ДРУШТВЕНЕ ДЕЛАТНОСТИ
IV Број: 039-1-1 /15, 09.07. 2015. године

НАЧЕЛНИК
Петар Вујадиновић, с.р.

27. На основу члана 8. став 1. 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 („Службени гласник РС“, број 94/16) и члана 100. Статута града Ужица („Службени лист града Ужица“, број 25/17 – пречишћен текст) градоначелник града Ужица, дана 12.02. 2018. године, донео је

ПРАВИЛНИК
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ГРАДСКЕИХ УПРАВА ГРАДА УЖИЦА

1. Опште одредбе

Члан 1.

Овим Правилником се утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система Градских управа града Ужица (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система који користе Градске управе града Ужица.

Члан 2.

Поједини термини употребљени у овом Правилнику имају следеће значење:

1) *Оператор* су Градске управе града Ужица које, у оквиру обављања своје делатности, односно за обављање послова из своје надлежности, користи ИКТ систем;

2) *информациона добра* су сви ресурси Градских управа града Ужица који садрже пословне информације, односно сви ресурси путем којих се врши израда, обрада, чување, пренос, брисање и уништвање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и сл;
3) *корисник ИКТ система* је запослени у Градским управама града Ужица и други корисник ресурса ИКТ система;
4) *надлежни субјект ИКТ система* је организациона јединица Градске управе за послове органа града, општу управу и друштвене делатности – Одељење за информационе технологије и комуникације, у чијој су надлежности послови планирања развоја, одржавања и функционисања рачунарско-комуникационе инфраструктуре и развој информационих технологија.

Члан 3.

О информационим добрима води се посебна евиденција.

Евиденцију из става 1. овог члана, у делу праћења основних средстава, води организациона јединица Оператора надлежна за послове финансија, а у делу инсталације и одржавања надлежни субјект ИКТ система.

Члан 4.

Под пословима из области безбедности ИКТ система утврђују се:

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

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

2. Коришћење ИКТ система

2.1. Управљање ИКТ системом

Члан 5.

ИКТ системом управља надлежни субјект ИКТ система.

Надлежни субјект ИКТ система, по завршеној инсталацији опреме, дужан је да све кориснике ресурса ИКТ система обучи за њихово коришћење и упозна са одговорностима и правилима коришћења ресурса ИКТ система.

Члан 6.

У случају промене радног места, односно надлежности корисника ИКТ система, надлежни субјект ИКТ система ће извршити промену права у коришћењу ИКТ система које је корисник ИКТ система имао у складу са описом радних задатака.

Члан 7.

У случају престанка радног ангажовања корисника ИКТ система, кориснички налог се укида.

О престанку радног односа или радног ангажовања, као и промени радног места, организациона јединица Оператора надлежна за послове управљања људским ресурсима, у сарадњи са непосредним руководиоцем, је дужана да обавести надлежни субјект ИКТ система ради укидања, односно измену приступних привилегија тог запосленог-корисника.

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

2.2. Администраторски и кориснички налог

Члан 8.

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

Администраторски налог је јединствен налог којим је омогућен приступ и администрација свих ресурса ИКТ система. Администраторски налог може да користи само запослени надлежног субјекта ИКТ система, који је распоређен на послове и радне задатке администратора ИКТ система.

Кориснички налог се може укуцавати или читати са медија на коме постоји електронски сертификат, на основу којих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране корисника ИКТ система.

Кориснички налог додељује администратор ИКТ система, на основу захтева руководиоца у организационим јединицима Оператора. На основу послова и радних задатака, администратор ИКТ система одређује права приступа у складу са потребама обављања пословних задатака од стране корисника ИКТ система.

Администратор ИКТ система води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева организационе јединице Оператора надлежне за управљање људским ресурсима, односно руководиоца у организационим јединицима Оператора.

2.3. Одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 9.

Кориснички налог се састоји од корисничког имена и лозинке.

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

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

Лозинка мора да садржи минимум четири карактера комбинована од малих и великих слова и цифара.

Лозинка не сме да садржи препознатљиве податке корисника ИКТ система.

Ако корисник ИКТ система посумња да је друго лице открило његову лозинку дужан је да о томе одмах обавести администратора ИКТ система.

Корисник ИКТ система дужан је да мења лозинку у складу са потребама и када га систем на то упозорава.

Неовлашћено уступање корисничког налога другом лицу подлеже дисциплинској одговорности.

За послове извршене под одређеним корисничким именом и лозинком одговоран је корисник ИКТ система којем су додељени.

3. Предмет, мере и субјекти заштите ИКТ система

3.1. Предмет заштите ИКТ система

Члан 10.

Предмет заштите ИКТ система су:

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

3.2. Мере и субјекти заштите ИКТ система

Члан 11.

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

Члан 12.

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

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

Члан 13.

Послове из области безбедности ИКТ система Оператора обавља надлежани субјект ИКТ система.

3.3. Обавезе корисника

Члан 14.

Корисник ИКТ система је дужан да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система:

1) да користи информатичке ресурсе искључиво у пословне сврхе;

2) да прихвати да су сви подаци који се складиште, преносе или обрађују у оквиру информатичких ресурса власништво

Оператора и да могу бити предмет надгледања и прегледања;

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

4) да безбедно чува своје лозинке у односу на друга лица;

5) да мења лозинке сагласно утврђеним правилима;

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

7) да користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење надлежног субјекта ИКТ система;

8) да захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране надлежног руководиоца;

9) да обезбеди сигурност података у складу са важећим прописима;

10) да приступа информатичким ресурсима само на основу изричито додељених корисничких права од стране надлежног субјекта ИКТ система;

11) да не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције 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) података у складу са прописаним процедурама;

14) да користи Internet, Intranet и e-mail сервис Оператора у складу са прописаним процедурама;

15) да прихвати да се одређене врсте информатичких интервенција обављају у утврђено време;

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

17) да прихвати инсталацију техника и програма у циљу сигурности ИКТ система;

18) да не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

3.4. Ограничење приступа подацима и средствима за обраду података

Члан 15.

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

Корисник ИКТ система 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.

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

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

4. Појединачне мере заштите

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

Члан 16.

Простор у коме се налазе рачунари за вођење база података и централни рачунар (сервер), 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.

Члан 17.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само запосленима у надлежном субјекту ИКТ система.

Осим лица из става 1. овог члана, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу надлежног субјекта ИКТ система.

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

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

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

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

У случају изношења опреме из просторије из става 1. овог члана ради селидбе или сервисирања, неопходно је одобрење надлежног субјекта ИКТ система, који ће одредити услове, начин и место изношења опреме.

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

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

4.2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 18.

Нерегистровани корисници путем мобилних уређаја могу приступити следећим ресурсима ИКТ система Оператора: Internet-у, e-mail сервису и web site-у.

Корисници ИКТ система, могу путем мобилних уређаја или рачунара, који су у власништву Оператора и који су подешени од стране надлежног субјекта ИКТ система, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности као што су електронска пошта, поједине апликације везане за обављање посла и друго, а на основу писане сагласности начелника Градске управе.

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

Кориснику ИКТ система је забрањена самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја неовлашћеним лицима.

Надлежни субјект ИКТ система свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја.

Уколико се установи неовлашћен приступ, о томе се путем електронске поште одмах, а најкасније сутрадан обавештава начелника Градске управе.

Члан 19.

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

Сагласност на коришћење приватног уређаја у случају из става 1. овог члана даје начелник Градске управе, на захтев надлежног субјекта ИКТ система.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води надлежни субјект ИКТ система.

Члан 20.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране надлежног субјекта ИКТ система.

Приватни уређаји са којих се може приступати ресурсима ИКТ система могу се користити само за обављање послова у надлежности корисника ИКТ система и то само у периоду када није могуће користити уређај у власништву Оператора.

4.3. Заштита носача података

Члан 21.

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

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

Члан 22.

Надлежни субјект ИКТ система ће успоставити организацију приступа подацима, посебно онима који буду означени тајним у складу са Законом о тајности података, тако да документи са ознаком тајности могу да се сниме, односно архивирају или запишу на фајл серверу у фолдеру над којим ће право приступа имати само корисници ИКТ сервиса који на то буду имали право.

Документа са ознаком тајности могу се сними на друге носаче (екстерни HDD, USB, CD, DVD) по одобрењу начелника Градске управе.

Евиденцију носача на којима су снимљени подаци са ознаком тајности, води надлежни субјект ИКТ система.

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

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

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

4.4. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 23.

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

Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера.

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

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

Члан 24.

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

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

Свакодневно се аутоматски у одређено време врши допуна антивирусних дефиниција.

4.6. Заштита при коришћењу интернета

Члан 25.

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

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

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

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

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

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

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

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

Члан 26.

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

Члан 27.

Недозвољена употреба интернета обухвата и:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друга врста недозвољених софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено одлуком надлежног органа Оператора;
- преузимање података у количини која проузрокује велико оптерећење на мрежи;
- преузимање материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом;
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

4.7. Заштита од губитка података

Члан 28.

За потребе обнове, базе података обавезно се архивирају на преносиве медије (CD, DWD, STRIMER TRAKA, EKSTERNI HDD), најмање једном дневно, петнастдневно и годишње, након радног времена.

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

Подаци о корисницима ИКТ система, архивирају се најмање једном месечно.

Члан 29.

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

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

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

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

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

Члан 30.

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

4.8. Чување података о догађајима који могу бити од значајаза безбедност ИКТ система

Члан 31.

О активностима администратора ИКТ система и корисника ИКТ система води се дневник активности.

Сваког последњег радног дана у недељи датотека у којој се налази дневник активности се архивира по процедури за израду копија-архива осталих података у ИКТ систему, у складу са чланом 28. овог Правилника.

4.9. Систем за контролу

Члан 32.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и другим могућим проблемима у ИКТ систему, мора бити подешен тако да одмах обавештава администратора ИКТ система, руководиоца организационе јединице у чијој су надлежности послови информационих технологија и начелника Градске управе о свим нерегуларним активностима корисника ИКТ система, покушајима упада и упадима у систем.

4.10. Обезбеђивање интегритета софтвера и оперативних система

Члан 33.

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

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

Инсталацију и подешавање софтвера може да изврши и треће лице, у случају да је софтвер набављен у поступку јавне набавке, а на начин који се дефинише уговором о набавци.

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

Члан 34.

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.

4.11. Заштита од злоупотребе безбедносних слабости ИКТ система

Члан 35.

Надлежни субјект ИКТ система најмање једном месечно, а по потреби и чешће врши анализу дневника активности у циљу идентификације потенцијалних слабости ИКТ система.

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

4.12. Ревизија ИКТ система

Члан 36.

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

Надлежни субјект ИКТ система одредиће време обављања ревизије, у зависности од врсте послова и радних задатака корисника ИКТ система код Оператора.

4.13. Заштита опреме ИКТ система

Члан 37.

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

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

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

Бежична мрежа, коју могу да користе посетиоци објеката у надлежности Градске управе, мора бити одвојена од интерне мреже коју користе корисници ИКТ система и кроз коју се врши размена службених података.

4.14. Безбедност ИКТ система у случају размене података

Члан 38.

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

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

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

Члан 39.

За потребе тестирања ИКТ система, односно делова система надлежни субјект ИКТ система може да користи податке који нису означени ознаком тајности, односно службености.

4.16. Учешће трећих лица у пословима ИКТ система

Члан 40.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Оператору, регулише се међусобно закљученим уговором.

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

Члан 41.

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

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

Члан 42.

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

У случају непоштовања уговорених обавеза, надлежни субјект ИКТ система је дужан да одмах обавести начелника Градске управе, ради предузмања мера у циљу отклањања неправилности.

4.17. Превентивне мере и реаговање на безбедносне инциденте

Члан 43.

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

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

Члан 44.

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, надлежни субјект ИКТ система је дужан да обавести начелника Градске управе који о инциденту обавештава надлежни орган дефинисан наведеном Уредбом.

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

5. Измене постојећег и успостављање новог ИКТ система

Члан 45.

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

Документација из става 1. овог члана мора да садржи описе свих процедура, а посебно процедура које се односе на безбедност ИКТ система.

6. Мере у циљу обезбеђења континуитета обављања посла у ванредним околностима

Члан 46.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Градске управе, надлежни субјект ИКТ система је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију.

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

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

7. Провера ИКТ система

Члан 47.

Проверу ИКТ система врши надлежни субјект ИКТ система.

Члан 48.

Провера ИКТ система се врши тако што се:

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

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

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

О извршеној провери сачињава се извештај, који се доставља начелнику Градске управе.

Члан 49.

Извештај из члана 48. овог Правилника садржи:

1) назив Оператора;
2) време провере;
3) податке 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.

8. Дисциплинска одговрност

Члан 50.

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

Члан 51.

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

Члан 52.

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

9. Измена Правилника

Члан 53.

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

10. Прелазне и завршне одредбе

Члан 54.

Овај Правилник ступа на снагу осмог дана од дана објављивања у „Службеном листу града Ужица“.

РЕПУБЛИКА СРБИЈА
ГРАД УЖИЦЕ
ГРАДОНАЧЕЛНИК
II Број: 039-1/18, 12.02.2018. године

ГРАДОНАЧЕЛНИК
Тихомир Петковић, с.р.

САДРЖАЈ БРОЈ 5/19

Издаје и штампа: Скупштина града Ужица - Одговорни уредник: Петар Вујадиновић, секретар Скупштине града - Технички уредник: Срђан Петровић - Редакција и администрација: Градска управа за послове органа града, општу управу и друштвене делатности - Телефон: 031/590-151