

БРОЈ:2/162/1

ДАТУМ:25.02.2019.године

ГОРЊИ МИЛАНОВАЦ

На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја и садржају извештаја о значаја, начину провере информационо-комуникационих система од посебног значаја („Сл. Гласник РС”, бр. 94/2016) и члана 25. и 26. Статута Дома здравља Горњи Милановац, Управни одбор Дома здравља Горњи Милановац, на седници одржаној 25.02.2019.године, донео је

ПРАВИЛНИК о безбедности информационо - комуникационог система Дом Здравља Горњи Милановац

I Опште одредбе

Члан 1.

Овим правилником се, 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 („Сл. Гласник РС”, бр. 94/2016), утврђују мере заштите, принципи, начин и процедуре и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС”, бр. 94/2016), утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационих система (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система Дома здравља Горњи Милановац (у даљем тексту: Оператор).

Члан 2.

Информациона добра Оператора су сви ресурси који садрже пословне информације Оператора, односно сви ресурси путем којих се врши обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и сл. О информационим добрима води се евиденција на посебном обрасцу. Евиденцију из става 2. овог члана води запослени у складу са важећом систематизацијом радних места (у даљем тексту: надлежни субјект ИКТ система).

Члан 3.

Под пословима из области безбедности ИКТ система, сматрају 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 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;

обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

II Коришћење ИКТ система

Члан 4.

Икт системом управља надлежни субјект ИКТ система. Надлежни субјект ИКТ система је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Оператора, да га обучи за коришћење ресурса ИКТ система, да по завршетку обуке од запосленог узме изјаву о обучености за коришћење ИКТ ресурса и да о истима води евиденцију.

Члан 5.

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

Члан 6.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида. Корисник ИКТ ресурса, 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.

Администраторски и кориснички налог

Члан 7.

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

Администраторски налог је јединствен налог којим је омогућен приступ и администрација свих ресурса ИКТ система, само са једним корисничким налогом, као и отварање нових и измена постојећих налога.

Администраторски налог може да користи само запослени које је распоређен на пословима и радним задацима администратора.

Кориснички налог је налог који садржи корисничко име и лозинку, који се могу 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 запосленог-корисника.

Кориснички налог додељује администратор, на основу захтева запосленог и то тек након уноса података о запосленом у софтвер. На основу послова и радних задатака запосленог, администратор одређује права приступа у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог, односно надлежног руководиоца у организационим јединицама Оператора.

Одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 8.

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:

Ђирилична 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 латиничног писма комбинованих од малих и великих слова, цифара и специјалних знакова.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона, 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 периоду од годину дана.

III Предмет, мере и субјекти заштите ИКТ система

Члан

9.

Предмет заштите ИКТ система 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

Члан 10.

Мере прописане овим актом се односе на све организационе јединице ИКТ система Оператора, на све запослене-кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Оператора.

Члан 11.

Мерама заштите ИКТ система Оператора обезбеђује се превенција од настанка инцидента, односно превенција и минимизација штете од инцидента 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 12.

За обављање послова из области безбедности ИКТ система Оператора надлежно је

Обавезе запослених

Члан 13.

Запослени у Оператору 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 и процесирају 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 или кориснички налог.
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 непосредног руководиоца;
9. да обезбеди сигурност података у складу са важећим прописима;

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

Безбедност рада на даљину и употреба мобилних уређаја

Члан 17.

Приступ ресурсима ИКТ система Оператора нерегистрованим корисницима, путем мобилних уређаја, омогућен је само преко врп конекције.

Запослени корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву Оператера и који су подешени од стране надлежног субјекта у ИКТ систему, да приступају само оним деловима ИКТ система који им омогућавају обављање разних задатака у оквиру њихове надлежности као што су поједине апликације везане за обављање посла и друго, а на основу сагласности начелника управе или директора.

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

Запосленом је забрањена самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја неовлашћеним лицима.

Надлежни субјект у ИКТ систему свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја, односно непознатих MAC адреса.

Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава начелник управе или директор установе, а та MAC адреса се уноси у блок листу софтвера који се користи за контролу приступа.

Члан 18.

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

Сагласност на коришћење приватног уређаја у случају из става 1. овог члана даје начелник управе или директор установе.

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

Члан 19.

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-запосленог и то само у периоду када нијемогуће користити уређај у власништву Оператера.

Надлежни субјект ИКТ система је дужан да пре предаје уређаја овлашћеном сервису, уради back up података који се налазе у мобилном уређају, а потом их избрише из уређаја, а да по извршеном сервисирању врати податке у мобилни уређај.

Заштита носача података

Члан 20.

Подаци који се налазе у ИКТ систему представљају тајну у складу са одредбама Закона о слободном приступу информацијама од јавног значаја, Закона о заштити података о личности, Закона о тајности података, као и Уредбе о начину поступку означавања тајности податка, односно документа.

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

Члан 21.

Надлежни субјект у ИКТ систему 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 запослени-корисници који на то буду имали право.

Документи са ознаком тајности могу да се сниме на друге носаче (екстерни HDD, USB, CD, DVD) само од стране надлежног ИКТ субјекта.

Евиденцију носача на којима су снимељени 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 управе ће одредити одговорну особу и начин транспорта.

Приликом брисања података са 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.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 22.

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.

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије врши се по завршетку радног времена, како не би био заустављен оперативни рад запослених-корисника.

Заштита података и средства за обраду података од злонамерног софтвера

Члан 23.

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, е-маил-ом, зараженим преносним медијима (УСБ меморија, ЦД, итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару се инсталира антивирусни програм. Свакодневно се аутоматски у тачно одређено време врши допуна антивирусних дефиниција, ради скенирања на вирусе.

Заштита при коришћењу интернета

Члан 24.

У циљу заштите, односно упада у ИКТ систем Оператора 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 забрањено је самостално прикључење на интернет, односно прикључење преко сопственог модема.

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

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 сезапослени-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 25.

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

Члан 26.

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.

Заштита од губитака података

Члан 27.

Базе података обавезно се архивирају на back-up сервер сваког дана. Остали фајлови-документи се архивирају месечно и на крају године. Подаци о запосленима-корисницима, архивирају се једном месечно.

Члан 28.

Дневно копирање-архивирање врши се за сваки радни дан у седмици. Недељно копирање-архивирање врши се последњег радног дана у недељи.

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

Члан 29.

Сваки примерак годишње копије-архиве чува се у року од годину дана.
Дневне, недељне и месечне копије-архиве се чувају у просторији која је физички и у складу са мерама заштите од пожара обезбеђена.
Годишње копије-архиве се израђују у два примерка, од којих се један чува у просторији у којој се чувају дневне, недељне и месечне копије-архиве, а други примерак у посебном објекту који је најмање 1 км удаљен од зграде управе.
Одлуку о посебном објекту у коме ће се чувати други примерак годишње копије-архиве доноси ----- посебним решењем.

Члан 30.

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

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

Систем за контролу

Члан 31.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и другим могућим проблемима у ИКТ систему, мора бити подешен тако да одмах обавештава администратора о свим нерегуларним активностима запослених-корисника, покушајима упада у систем.

Обезбеђивање интегритета софтвера и оперативних система

Члан 32.

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 субјект ИКТ система, односно запослени-корисник који има овлашћење за то.
Инсталацију и подешавање софтвера можда да изврши и треће лице, у случају да је софтвер набављен у поступку јавне набавке, а на начин дефинисан 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 33.

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.

Заштита од злоупотребе безбедносних слабости ИКТ система

Члан 34.

Надлежни субјект ИКТ система најмање једном месечно, а по потреби и чешће врши анализу активности 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.

Надлежни субјект ИКТ система, дужан је да подешавањем корисничких полиса, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

Ревизија ИКТ система

Члан 35.

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

Надлежни субјект ИКТ система одредиће време обављања ревизије, у зависности од врсте послова и радних задатака запослених-корисника у Оператору.

Заштита опреме ИКТ система

Члан 36.

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

Мрежна опрема (switch, router, firewall) мора се налазити у гаск орману, закључана.

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

Безбедност ИКТ система у случају размене података

Члан 37.

Размена података који су означени ознаком тајности са другим органима, организацијама или правним лицима, врши се 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.

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

Члан 38.

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

Учешће трећих лица у пословима ИКТ система

Члан 39.

Начин инсталирања нових, замена и одржавања 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 40.

Трећа лица-пужаоци 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 41.

Надлежни субјект ИКТ система је одговоран за надзор над поштовањем уговорених обавеза од стране трећих лица-пужаоца услуга, посебно 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 управе или директора ради предузимања мера у циљу отклањања неправилности.

Превентивне мере и реаговање на безбедносне инциденте

Члан 42.

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

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

Члан 43.

Уколико се ради о инциденту који је дефинисан Уредбом о поступку достављања података, листи, врстама и значају инцидента и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, надлежни субјект ИКТ је дужан да поред начелника обавести и надлежни орган дефинисан наведеном Уредбом.

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

IV Измене постојећег и успостављање новог ИКТ система

Члан 44.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система надлежни субјект ИКТ система врши надзор целокупног процеса.

V Мере у циљу обезбеђења континуитета обављања посла у ванредним околностима

Члан 45.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде, надлежни субјект ИКТ система је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује надлежни субјект ИКТ система, у три примерка, од којих се један налази код њега, други код запосленог надлежног за послове одбране и ванредне ситуације, а трећи примерак
код
начелника.

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

Складиштење делова ИКТ система који нису неопходни врши се на начин да опрема буде безбедна и обележена.

VI Провера ИКТ система

Члан 46.

Проверу ИКТ система врши надлежни субјект ИКТ система.

Члан 47.

Провера ИКТ система се врши тако што се:

1. провера усклађеност Правилника о безбедности ИКТ система, 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 управе.

Члан 48.

Извештај из члана 45. овог Правилника садржи:

1. назив Оператора;
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.

VII Дисциплинска одговорност

Члан 49.

Непоштовање одредби овог Правилника представља повреду радних обавеза и повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса Оператера.

Члан 50.

Свако коришћење ИКТ ресурса Оператера од стране запосленог-корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за коришћење

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

VII Измена Правилника

Члан 52.

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

VIII Прелазне и завршне одредбе

Члан 53.

Овај правилник ступа на снагу даном објављивања

Председник Управног одбора
др Невена Тешић

