



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

Наш број: 1645/22
Датум: 29.04.2022.г.

ПРАВИЛНИК

О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

ЈКП „ГРАДСКА ТОПЛАНА“ ПИРОТ



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

На основу одредби чл.6.-8. Закона о информационој безбедности („Службени гласник РС”, број 6/16, 94/2017 и 77/2019), 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”, бр. 94/2016), Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја безбедности („Службени гласник РС”, број 94/2016) и члана 50 Статута ЈКП „Градска топлана“ Пирот (Службени лист града Ниша бр.137 од 01.12.2016 године), директор, дана 29.04.2022. године доноси:

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ЈКП „ГРАДСКА ТОПЛАНА“ ПИРОТ

I Опште одредбе

Члан 1.

Овим Правилником се у складу са Законом о информационој безбедности и Уредбом 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, утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система, (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система ЈКП „Градска топлана“ Пирот (у даљем тексту: **Оператор**).

Члан 2.

Информациона добра Оператера су сви ресурси који садрже пословне информације Оператера, односно сви ресурси 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 и сл.

О информационим добрима води се евиденција послова на посебном обрасцу.

Евиденцију из става 2. овог члана води руководиоци правног, економског и техничког сектора или запослени које они одреде (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,



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapirot.rs, e-mail: toplanapirot@gmail.com

- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Оператера, 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 управљају руководиоци правног, економског и техничког сектора или запослени које они одреде по секторима (**надлежни субјект ИКТ система**). Надлежни субјект ИКТ система је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Оператера, 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 Оператера, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

Члан 7.

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

Администраторски налог је јединствен налог којим је омогућен приступ и администрација ресурсима ИКТ система, само са једним корисничким налогом, као и отварање нових и измена постојећих налога, може да користи само запослени који за обављање радних задатака користи ресурсе ИКТ система.

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 руководилац сектора или запослени кога он одреди на основу захтева запосленог. На основу послова и радних задатака запосленог, руководилац сектора одређује права приступа у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Руководилац сектора или лице које он одреди води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге у организационим јединицама Оператера.



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

Члан 8.

Кориснички налог се састоји од корисничког имена и лозинке.

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 годишње.

III Предмет, мере и субјекти заштите ИКТ система

Члан 9.

Предмет заштите ИКТ система су:

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

Члан 10.

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

Члан 11.

Мерама заштите ИКТ система Оператера 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, Оператер може да размотри коришћење одговарајућих мера криптозаштите.

Члан 12.

Обављање послова из области безбедности ИКТ система Оператера је у надлежности запосленог по секторима кога одреди руководилац сваког сектора или фирме са којом је закључен Уговор о вршењу послова из области безбедности ИКТ система Оператера.

Члан 13.

Запослени у Оператеру су дужни да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система:

- 1) да користе информатичке ресурсе искључиво у пословне сврхе
- 2) да су упознати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Оператера и да могу бити предмет надгледања и прегледања од стране непосредних руководиоца;
- 3) да поступају са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
- 4) да безбедно чувају своје лозинке у односу на друга лица;



JKП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

- 5) да мењају лозинке сагласно утврђеним правилима;
- 6) да се, пре сваког удаљавања од радног места, одјаве са ИКТ система;
- 7) да користе DVDRW, CDRW и USB екстерне меморије само уз одобрење непосредног руководиоца у субјекту 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;
- 10) да приступа информатичким ресурсима само на основу изричито додељених корисничких права од стране надлежног субјекта;
- 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 да на радној станици складишти садржај који не служи у пословне сврхе;
- 13) да израђује заштитне копије (backup) података у складу са прописаним процедурама;
- 14) да користи Internet и Internet e-mail сервис Оператера 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.

Члан 14.

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

Запослени може да користи само свој кориснички налог који је добио и не сме да омогући другом лицу коришћење његовог корисничког налога, сем непосредном руководиоцу или трећем лицу по одобрењу Оператера, за подешавање корисничког профила и радне станице.

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

III- а Појединачне мере заштите

Члан 15.

Простор у коме се налазе рачунари за вођење база података и централни рачунар (сервер), мрежна или комуникациона опрема ИКТ система, организује се као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору и обезбеђен видео надзором.

Члан 16.

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

Приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу директора.

У просторије у којима се налази опрема из става 2. овог члана мора се налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема.



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

Прозори и врата на овим просторијама из става 1. овог члана морају увек бити затворени. Просторија мора бити континуирано климатизована током 24 сата 365 дана у години. Максимална температура просторије мора бити од 18 до 22 степена.

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, запослени који непосредно користи опрему ИКТ система је дужан да искључи опрему у складу са процедурама произвођача опреме.

У случају изношења опреме из просторија из става 2. овог члана ради селидбе, или сервисирања, неопходно је одобрење директора или непосредног руководиоца који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења директора или непосредног руководиоца, 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 обавезно се дефинише обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Оператера.

Члан 17.

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 радних задатака у оквиру њихове надлежности као што су електронска пошта, поједине апликације везане за обављање посла и друго, а на основу писане сагласности директора или непосредног руководиоца.

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 је 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 директора или непосредног руководиоца, а те 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 директор или непосредни руководиоца.

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



JKП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs, e-mail: toplanapirot@gmail.com

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 није могуће користити уређај у власништву Оператера.

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

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 и поступку означавања тајности података, односно докумената.

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 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 директора/помоћник директора/надлежни руководиоца или његовим писаним актом овлашћених запослених – корисника.

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 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.



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

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.

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 и тд.), инсталацијом нелиценцираног софтвера и сл.

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

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.

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 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 се запослени-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 да пријави надлежном субјекту ИКТ система.



ЖКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

Члан 25.

Кориснику ИКТ система коме је дозвољено коришћење интернета је забрањено гледање филмова и играње 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.

Члан 27.

Базе података обавезно се архивирају на преносиве медије (DWD, STRIMER TRAKA, EKSTERNI HDD, MREŽNI DISKOVI), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

Остали фајлови-документи се архивирају најмање једном недељно, месечно и годишње у зависности од степена важности архивираних докумената.

Подаци о запосленима-корисницима, архивирају се најмање једном месечно.

Члан 28.

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

Недељно копирање-архивирање врши се последњег радног дана у недељи, од 20 часова, у онолико недељних примерака колико има последњих радних дана у месецу.

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

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



JKП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapirot.rs , e-mail: toplanapirot@gmail.com

Члан 29.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Правилником о канцеларијском канцеларијском пословању и архивској грађи.

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 посебној просторији управне зграде.

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.

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 надлежни субјект о свим нерегуларним активностима запослених-корисника, покушајима упада и упадима у систем.

Члан 32.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Оператера, 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 може да изврши и треће лице, у случају да је софтвер набављен у поступку јавне набавке, а на начин дефинисан са Уговором о набавци.

Треће лице може да изврши Инсталацију и подешавање софтвера када је између Оператера 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.

Члан 34.

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



JKP „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

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.

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 Оператеру.

Члан 36.

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 гаск орману, закључани.

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

Члан 37.

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

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.

Члан 39.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Оператеру, 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-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.



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs , e-mail: toplanapirot@gmail.com

Члан 41.

Надлежни субјект ИКТ система је одговоран 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 надлежни субјект ИКТ система је дужан да одмах обавести директора и непосредног руководиоца ради предуземања мера у циљу отклањања неправилности.

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 става 1. овог члана надлежни субјект ИКТ система је дужан да одмах обавести директора и непоаредног руководиоца 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 директора и непосредног руководиоца обавести и надлежни орган дефинисан наведеном Уредбом.

Надлежни субјект ИКТ система води евиденцију о свим инцидентима, као и 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 измена постојећих делова ИКТ система надлежни субјект ИКТ система врши надзор над целокупним процесом.

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 управе, 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.



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs, e-mail: toplanapirot@gmail.com

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 директора и руководиоца сектора.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди директор и руководиоци сектора.

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) проверава 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 саачињава се извештај, који се доставља директору и руководиоцима свих сектора.

Члан 48.

Извештај из члана 47. Овог Правилника садржи:

- 1) назив Оператера;
- 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 словима;
- 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.



ЈКП „Градска топлана“ Пирот, ул. Нишавска бр.11, Пирот 18300;
тел: 010 321 119; тел/фах: 010324 743; инфо центар: 0800/001-004
web site: www.toplanapi.rs, e-mail: toplanapirot@gmail.com

VII Дисциплинска одговорност

Члан 49.

Непоштовање одредби овог Правилника представља повреду радних обавеза и повлачи дисциплинку 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 неовлашћено коришћење имовине.

Члан 51.

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

VIII 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 директора 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 преиспитивања овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IX Прелазне и завршне одредбе

Члан 53.

Овај Правилник на који је добијена сагласност Надзорног одбора ЈКП „Градска топлана, Пирот, ступа на снагу осмог дана од дана објављивања на огласној табли ЈКП „Градска топлана, Пирот.



Директор
Братислав Ђирић, дил.ек.