На основу Закона о информационој безбедности („Службени гласник РС“, бр. 6/2016, 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), Закона о јавним предузећима („Службени гласник Републике Србије", број 15/2016 и 88/2019), Надзорни одбор ЈКП „Обједињена наплата“, дана_____ године, на својој_____седници, донео је

ПРАВИЛНИК
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА
У ЈКП „ОБЈЕДИЊЕНА НАПЛАТА“

Тако да исти гласи:

I. УВОДНЕ ОДРЕДБЕ

Члан 1.

Овим правилником одређују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система од посебног значаја (у даљем тексту: ИКТ систем) у организационим оквирима ЈКП „Обједињена наплата“ Ниш (у даљем тексту: Предузеће).

Члан 2.

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

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса.

За праћење примене овог правилника обавезује се Помоћник директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова.

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

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

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

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

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

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

2) *информациона безбедност* представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;
3) *тајност* је својство које значи да податак није доступан неовлашћеним лицима;
4) *интегритет* значи очуваност изворног садржаја и комплетности податка;
5) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
6) *аутентичност* је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
7) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
8) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
9) *управљање ризиком* је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
10) *инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
11) *мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
12) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
13) *ИКТ систем за рад са тајним подацима* је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
14) *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
15) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
16) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
17) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;
18) *криптоматеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
19) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
20) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
21) VPN (Virtual Private Network)-је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
22) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
23) Backup је резервна копија података;
24) Download је трансфер података са централног рачунара или web презентације на локални рачунар;
25) UPS (Uninterruptible power supply*)* је уређај за непрекидно напајање електричном енергијом;
26) Freeware је бесплатан софтвер;

27) Opensource софтвер отвореног кода;
28) Firewall је „заштитни зид“ односносистем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
29) USB или флеш меморија је спољшњи медијум за складиштење података;
30) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;
31) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

II. МЕРЕ ЗАШТИТЕ

Члан 4.

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

Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу утврђује се Правилником о организацији и систематизацији послова.

Члан 5.

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

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Предузећа надлежан је Помоћник директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова .

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава 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 Предузећа, као и приступ, измене 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.

У случају инцидента Помоћник директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова, обавештава Директора Предузећа, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2.Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Рад на даљину и употреба мобилних уређаја у ИКТ систему није омогућен.

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

Помоћник директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава Директор Предузећа, а та MAC адреса се уноси у «block“ листу софтвера који се користи за контролу приступа.

Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води Помоћник директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова, а по одобрењу Директора Предузећа.

Помоћник директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова је дужан да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради *backup* података који се налазе у мобилном уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати податке у мобилни уређај.

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

Члан 8.

ИКТ системом управљају запослени у складу са важећим Правилником о организацији и систематизацији послова.

Помоћник директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова је дужан/на да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Предузећа, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденцију о изјавама новозапослених – корисника да су упознати са правилима коришћења ИКТ ресурса.

Свако коришћење ИКТ ресурса Предузећа од стране запосленог-корисника, ван додељених овлашћење, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

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

Члан 9.

У случају промене послова, односно надлежности корисника-запосленог, Помоћник Директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова ће извршити промену

привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

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

О престанку радног односа или радног ангажовања, као и промени радног места, лице одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова (послови евиденције запослених – кадровски послови) ће обавестити Помоћника Директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова, ради укидања, односно измену приступних привилегија тог запосленог-корисника.

Корисник ИКТ ресурса, након престанка радног ангажовања у Предузећу, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона база Предузећа представља све ресурсе који садрже пословне информације Предузећа, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем и сл.)

Евиденцију о информационим добрима води Помоћник Директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова, у папирној или електронској форми.

Предмет заштите су:

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

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

Члан 11.

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

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Службени гласник РС“, бр. 53/2011).

7. Заштита носача података

Члан 12.

Помоћник Директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова, ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да:

1) подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено одлуком директора;
2) подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених.

Евиденцију носача на којима су снимљени подаци, води Помоћник Директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, Директор Предузећа ће одредити одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на медијима, подаци морају бити неповратно обрисани, а ако то није могуће, такви медији морају бити физички оштећени, односно уништени.

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

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

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

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

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

Запослени-корисник дужан је да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система, и то да:

1) користи информатичке ресурсе искључиво у пословне сврхе;
2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Предузећа и да могу бити предмет надгледања и прегледања;
3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4) безбедно чува своје лозинке, односно да их не одаје другим лицима;
5) мења лозинке сагласно утврђеним правилима;
6) пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу;
7) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8) обезбеди сигурност података у складу са важећим прописима;
19) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) на радној станици не сме да складишти садржај који не служи у пословне сврхе, уколико наведено буде експлицитно забрањено;
12) израђује заштитне копије (backup) података у складу са прописаним процедурама;
13) користи интернет и електронску пошту у Предузећу у складу са прописаним процедурама;

14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
15) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
16) прихвати да технике сигурности (анти вирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;
17) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 14.

Право приступа имају само запослени/корисници који имају администраторске или корисничке налоге.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Администраторски налог може да користи само запослени у Служби која је Правилником о организацији и систематизацији послова овлашћена за управљање информационом базом Предузећа.

Администраторски налог за управљање доменом може да користи само запослени у Служби која је Правилником о организацији и систематизацији послова овлашћена за управљање информационом базом Предузећа.

Адинистраторски налог за управљање базом података могу да користе само запослени у Служби која је Правилником о организацији и систематизацији послова овлашћена за управљање информационом базом Предузећа

Кориснички налог се састоји од корисничког имена и лозинке.

Кориснички налог запосленом додељује администратор, на основу захтева Шефа службе и његовог непосредног руководиоца.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог на пословима управљања људским ресурсима, односно надлежног руководиоца.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

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

Запослени-корисник дужан је да мења лозинку најмање једном у 6 месеци, уколико другом Одлуком није другачије уређено.

Иста лозинка, уколико је предмет промена, не сме се понављати у временском периоду од годину дана.

Кориснички налог може да се се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр. лична карта са чипом и уписаним сертификатом).

Пријављивање у ИКТ систем Предузећа се врши уписивањем корисничког имена и лозинке.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 16.

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

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

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

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

Члан 16.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује са као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом.

Простор мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор).

Евиденцију о уласку у ову зону води Шеф надлежне Службе на основу Правилника о организацији и систематизацији послова.

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

Члан 17.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система/запосленима на пословима ИКТ и другим запосленима у Служби која у предметним просторијама обавља своје пословне активности на основу Правилника о организацији и систематизацији послова.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу Директора Предузећа, и уз присуство Шефа надлежне Службе на основу Правилника о организацији и систематизацији послова.

Приступ административној зони може имати и запослени/а на пословима одржавања хигијене уз присуство Шефа надлежне Службе на основу Правилника о организацији и систематизацији послова

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

Прозори и врата на овој просторији морају увек бити затворени.

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

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

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

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

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

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

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 18.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим, планирају, односно предлажу Директору Предузећа одговарајуће мере.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију.

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запослених-корисника.

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

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

Члан 19.

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

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски у 10 сати врши допуна антивирусних дефиниција.

Сваког петка у седмици је потребно оставити укључене и закључане рачунаре ради скенирања на вирусе.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

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

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

У циљу заштите, односно упада у ИКТ систем Предузећа са интернета, систем инжењер информационих технологија је дужан да одржава систем за спречавање упада.

Надлежни помоћници директора или друга овлашћена лица на основу важећег Правилника о организацији и систематизацији послова одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове могу укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени-корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врше лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове.

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

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави лицима која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове.

Недозвољена употреба интернета обухвата:

1) инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
2) нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
3) намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
4) недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
5) преузимање (download) података велике “тежине” које проузрокује “загушење” на мрежи;
6) преузимање (download) материјала заштићених ауторским правима;
7) коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
8) недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

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

16. Заштита од губитка података

Члан 20.

Базе података обавезно се архивирају на преносиве медије (CDROM, DVD, USB, „strimer“ трака, екстерни хард диск), најмање једном недељно, за потребе обнове базе података.

Остали фајлови-документи се архивирају најмање једном недељно.

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

Недељно копирање-архивирање врши се последњег радног дана у недељи.

Сваки примерак копије-архиве чува се у року који је дефинисан позитивним прописима.

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

Недељне копије се чувају у просторији која је физички и у складу са мерама заштите од пожара обезбеђена или у сефу Банке који је у власништву ЈКП „Обједињена наплата“.

Исправност копија-архива проверава се најмање на шест месеци и то тако што се изврши повраћај база података које се налазе на медију, при чему враћени подаци након повраћаја треба да буду исправни и спремни за употребу.

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

Члан 21.

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

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

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 22.

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

Инсталацију и подешавање софтвера могу да врше само лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове.

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

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

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 23.

Лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове најмање једном месечно а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове су дужна да одмах изврши подешавања, односно инсталирају софтвер који ће отклонити уочене слабости.

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

Члан 24.

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

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 25.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, router, firewall) се мора налазити у закључаном rack орману.

Лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове су дужна да стално врше контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалних неправилности.

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

Члан 26.

Размена података са другим правним лицем који су означени неком од ознака тајности се врши у складу са Уговором (протоколом о сарадњи).

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

Члан 27.

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

Лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове су задужена за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове води документацију.

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

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

Члан 28.

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.

Лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове су одговорна за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

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

Члан 29.

Лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове су одговорна 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 иста лица су дужна да одмах обавесте Директора Предузећа, како би он могао да предузме мере у циљу отклањања неправилности.

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

Члан 30.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести систем инжењера информационих технологија.

По пријему пријаве Лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове су дужна да одмах обавесте Директора Предузећа и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Службени гласник РС“, бр, 94/2016), лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове, су дужна да поред Директора Предузећа обавесте и надлежни орган.

Лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове воде евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 31.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из пословне зграде Предузећа лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове, су дужна да у најкраћем року пренесу 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 лице које одреди Директор Предузећа, и то у три примерка, од којих се један налази код њега/е, други код запосленог надлежног за послове одбране и ванредне ситуације а трећи примерак код Директора Предузећа.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди Директор Предузећа. Складиштење делова ИКТ система који нису неопходни, се врши тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води.

III. ИЗМЕНА ПРАВИЛНИКА О БЕЗБЕДНОСТИ

Члан 32.

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, лица која су на основу важећег Правилника о организацији и систематизацији послова одговорна за ИКТ послове су дужна да обавесте Директора Предузећа и Надзорни одбор, како би се приступило измени овог правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IV. ПРОВЕРА ИКТ СИСТЕМА

Члан 33.

Проверу ИКТ система врши треће лице- давалац услуга или се Помоћник директора за информационо-телекомуникационе и послове системске подршке или друго лице посебном Одлуком овлашћено од стране Директора или одређено описом послова у складу са важећим Правилником о организацији и систематизацији послова.

Провера ће се вршити последњег месеца у години.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на која се врши упућивање, са прописаним условима, односно проверава да ли су правилником адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;
2) проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама интервјуа, симулације, посматрања, увида у предвиђене евиденције и другу документацију;
3) врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

О извршеној провери сачињава се извештај, који се доставља Директору Предузећа.

I. Садржај извештаја о провери ИКТ система

Члан 34.

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава;
2) време провере;
3) подаци о лицима која су вршила проверу;
4) извештај о спроведеним радњама провере;
5) закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;
6) закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
7) закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система;
8) оцена укупног нивоа информационе безбедности;
9) предлог евентуалних корективних мера;
10) потпис одговорног лица које је спровело проверу ИКТ система.

V. ЗАВРШНЕ ОДРЕДБЕ

Члан 35.

Овај правилник ступа на снагу даном доношења.

Председник Надзорног одбора

Данијела Милићевић,*дипл.прав.*