На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС”, број 94/16), и члана 48. Статута јавног комуналног предузећа Водовод Лесковац, Надзорни одбор предузећа дана _____ године доноси:

П Р А В И Л Н И К
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНОГ СИСТЕМА ЈАВНО КОМУНАЛНОГ ПРЕДУЗЕЋА ВОДОВОД ЛЕСКОВАЦ

ЈАВНО КОМУНАЛНО ПРЕДУЗЕЋЕ "ВОДОВОД" БР. 64/18-1 ДАТУМ: 02.11.2018 ГОД ЛЕСКОВАЦ

I ОПШТЕ ОДРЕДБЕ

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности и Уредбом о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начин провере информационо-комуникационих система од посебног значаја и садржај извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС“, бр. 94/2016), утврђују 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 ИКТ система Јавно комуналног предузећа Водовод Лесковац (у даљем тексту: ИКТ систем).

Члан 2.

Запослени у ЈКП Водовод Лесковац су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

Непоштовање одредби Правилника о безбедности информационо - комуникационог система Јавно комуналног предузећа Водовод Лесковац, као и свако угрожавање или нарушавање информационе безбедности, повлачи повреду радне обавезе и радне дисциплине запослених.

Члан 3.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

II МЕРЕ ЗАШТИТЕ

Члан 4.

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

1 Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру ЈКП Водовод Лесковац

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 ЈКП Водовод Лесковац надлежан је самостални инжењер информационих технологија у складу са систематизацијом радних места у ЈКП Водовод Лесковац бр. 3762/1, од 07.05.2018. године.

Члан 6.

Под пословима из области безбедности подразумевају се:

- послови заштите информационих добара, односно средстава и имовине од значаја за информациону безбедност
- послови управљање ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности
- послови онемогућавања и спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система ЈКП Водовод лесковац
- послови онемогућавања и спречавања приступа, измене или коришћење средстава без овлашћења и без евиденције о томе
- праћење активности и надзора у оквиру управљања информационом безбедношћу
- обавештавање надлежних о инцидентима у ИКТ систему.

У случају инцидента самостални инжењер информационих технологија, обавештава директора предузећа у циљу решавања насталог безбедоносног инцидента.

2 Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

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

Самостални инжењер информационих технологија контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја. Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава руководилац/директор.

Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен, осим ако је по одобрењу руководилац/директор.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране самосталног инжењера информационих технологија, могу се користити само за обављање послова у надлежности корисника-запосленог и то само у одређеном периоду.

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 важећом систематизацијом радних места.

Самостални инжењер информационих технологија је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса ЈКП Водовод Лесковац, као и да га упозна са правилима коришћења ресурса ИКТ система.

Свако коришћење ИКТ ресурса ЈКП Водовод Лесковац 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.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања. Дужности и обавезе које остају важеће и после престанка запослења треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа.

У случају промене послова, односно надлежности корисника-запосленог, самостални инжењер информационих технологија 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 онемогућава за коришћење.

О престанку радног односа или радног ангажовања, као и промени радног места корисника-запосленог, први предпостављени у сарадњи са непосредним руководиоцем, је дужан/а да обавести самосталног инжењера информационих технологија, ради укидања, односно измену приступних привилегија тог запосленог-корисника.

5 Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Евиденцију о информационим добрима води самостални инжењер информационих технологија, 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

Запослени и екстерни корисници су обавезни да врате сву имовину ЈКП Водоводу Лесковац коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

6 Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности

Члан 11.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем за ЈКП Водовод Лесковац.

ЈКП Водовод Лесковац означава типове података као поверљиве, интерне или јавне.

ЈКП Водовод Лесковац класификациону шему поверљивости података базира на три нивоа:

- откривање не изазива никакву штету;
- откривање изазива мању непријатност или мању штету;
- откривање има значајан утицај на пословање или тактичке циљеве;

Класификација података мора да буде усклађена са правилима контроле приступа.

7 Заштита носача података

Члан 12.

ЈКП Водовод Лесковац обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, води самостални инжењер

информационих технологија и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

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 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 ЈКП Водовод Лесковац 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;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (backup) података у складу са прописаним процедурама;
13) користи интернет и електронску пошту у ЈКП Водовод Лесковац 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.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Додељивање привилегованих (администраторских) права на приступ врши се на основу самосталног инжењера информационих технологија.

Привилегована права на приступ која треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности. Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора. Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

Шифре за приступ општим корисничким идентификаторима администратора мењају се променом корисника.

Запосленима лицима и екстерним корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.

10 Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

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

(Препорука: Уместо ових слова користити слова из табеле.)

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

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

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

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

Запослени-корисник дужан је да мења лозинку најмање једном у три месеца.

Иста лозинка се не сме понављати у временском периоду од годину дана.

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

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 16.

Приступ ресурсима ИКТ система ЈКП Водовод Лесковац не захтева посебну криптозаштиту.

Запослени-корисници користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим порталима у надлежности Владе републике Србије.

Запослени на пословима самостални инжењер информационих технологија су задужени за инсталацију потребног софтвера и хардвера за коришћење сертификата.

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

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

Члан 17.

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.

Ова области мора бити заштићена одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ.

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).

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

Члан 18.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је самосталном инжењеру информационих технологија, руководиоцу електро одржавања и система надзора, техничару информационих технологија и процесном инжењеру електро одржавања.

Пприступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, и уз присуство самосталног инжењера информационих технологија.

Приступ административној зони може имати и запослени/а на пословима одржавања хигијене уз присуство самосталног инжењера информационих технологија, техничара за информационе технологије или процесног инжењера електро одржавања.

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.

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.

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

14 Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ

система и, у складу са тим, планирају, односно предлажу руководиоцу 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.

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

При тестирању софтвера је потребно обезбедити неометано функционисање ИКТ система. Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера, на начин који може да заустави нормално функционисање ИКТ система.

15 Заштита података и средства за обраду података од злонамерног софтвера

Члан 20.

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

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм.

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.

Извршни директори сектора 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.

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

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 самосталном инжењеру информационих технологија.

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" WEB страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

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 21.

Базе података обавезно се архивирају на преносиве медије (хард диск, CDROM, DVD, USB, екстерни хард диск), најмање једном дневно.

Остали фајлови-документи, софтвер, сервиси, лог фајлови се архивирају најмање једном недељно, месечно или годишње.

Дневно копирање-архивирање врши се за сваки радни дан у седмици, од 8 часова за претходни дан.

Недељно копирање-архивирање врши се првог радног дана у недељи, од 8 часова за претходну недељу.

Месечно копирање-архивирање врши се првог радног дана у месецу за претходни месец од 8 часова.

Годишње копирање-архивирање врши се првог радног дана у години за претходну годину од 8 часова.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе („Сл. Гласник РС“, бр 10/93, 14/93-испр. и 67/2016).

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

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

Исправност копија-архива проверава се најмање на шест месеци.

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

Члан 22.

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

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и др, мора бити подешен тако да одмах обавештава администратора, руководиоца организационе јединице надлежне за послове ИКТ и начелника Управе, о свим нерегуларним активностима запослених-корисника, покушајима упада и упадима у систем.

18 Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

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

Инсталацију и подешавање софтвера може да врши само самостални инжењер информационих технологија или техничар информационих технологија, односно запослени-корисник који има овлашћење за то.

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

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

19 Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, самостални инжењер информационих технологија је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене рањивости. Прво се узимају у разматрање системи са високим ризиком.

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедносним слабостима.

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

Члан 25.

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 руководиоца/директора.

21 Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 26.

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.

Самостални инжењер информационих технологија је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коју могу да користе посетиоци објеката у надлежности Управе, мора бити одвојена од интерне мреже коју користе корисници запослени у Управи и кроз коју се врши размена службених података.

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

Члан 27.

Заштита података који се преносе комуникационим средствима унутар ЈКП Водовод Лесковац, између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са правилима поступка, сигурна и у складу са позитивним прописима и пословном праксом. Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

Правила коришћења интернета

Приступ садржајима на интернету је дозвољен искључиво за пословне намене. Мрежа користи поступак ревизије логовања, како на пријему тако и на слању, и периодично се надзире и контролише.

Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намена коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

Одговорност запослених

Непоштовање правила заштите података, коришћења електронске поште, интернета и информационих ресурса, из члана 27 овог Правилника, представљају повреду радне обавезе и дисциплине запосленог, као и одредаба Правилника о раду ЈКП Водовод.

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

Члан 28.

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

Самостални инжењер информационих технологија је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

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

Члан 29.

За потребе тестирања ИКТ система односно делова система самостални инжењер информационих технологија може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

25 Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 30.

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.

Самостални инжењер информационих технологија је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

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

Члан 31.

Самостални инжењер информационих технологија 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 самостални инжењер информационих технологија је дужан да одмах обавести директора предузећа како би он могао да предузме мере у циљу отклањања неправилности.

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

Члан 32.

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

информационих технологија.

По пријему пријаве самостални инжењер информационих технологија је дужан/а да одмах обавести директора предузећа и предузме мере у циљу заштите ресурса ИКТ система.

Самостални инжењер информационих технологија води евиденцију о свим инцидентима, као и пријавама инцидената.

28 Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Управе, самостални инжењер информационих технологија, је дужан/а да у најкраћем року организује пренос 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 самостални инжењер информационих технологија, 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 34.

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, самостални инжењер информационих технологија је дужан/а да обавести директора предузећа, како би он могао да приступи измени овог правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IV ПРОВЕРА ИКТ СИСТЕМА

Члан 35.

Проверу ИКТ система врши самостални инжењер информационих технологија једном годишње.

Члан 36.

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 непосредном руководиоцу.

Члан 37.

Садржај извештаја о провери ИКТ система из члана 38. овог Правилника 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 ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 38.

Овај Правилник ступа на снагу у року од 8 дана од дана објављивања на огласној табли.

Председник Надзорног одбора

Славиша Здравковић, дипл.екон.