



**ПРАВИЛНИК
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО -КОМУНИКАЦИОНОГ
СИСТЕМА
ЈКП „СТАНДАРД“ АДА**

Ада, децембар 2017. године

Садржај

I Уводне одредбе	4
II Коришћење ИКТ система	6
1. Управљање ИКТ системом.....	6
2. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа - Администраторски и кориснички налог...	7
3. Одговорности корисника за заштиту сопствених средстава за аутентикацију.....	7
III Предмет, мере и субјекти заштите ИКТ система.....	8
1. Предмет заштите ИКТ система	8
2. Мере и субјекти заштите ИКТ система	8
3. Обавезе корисника	8
4. Ограничење приступа подацима и средствима за обраду података	9
IV Појединачне мере заштите	10
1. Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему	10
2. Безбедност рада на даљину и употреба мобилних уређаја.....	10
3. Заштита носача података.....	11
4. Обезбеђивање исправног и безбедног функционисања средстава за обраду података.....	12
5. Заштита података и средстава за обраду података од злонамерног софтвера.....	12
6. Заштита при коришћењу интернета	12
7. Заштита од губитка података.....	13
8. Чување података о догађајима који могу бити од значаја за безбедност ИКТ система	14
9. Систем за контролу	14
10. Обезбеђивање интегритета софтвера и оперативних система	14
11. Заштита од злоупотребе безбедносних слабости ИКТ система.....	15
12. Ревизија ИКТ система.....	15
13. Заштита опреме ИКТ система	15
14. Безбедност ИКТ система у случају размене података	15
15. Заштита података који се користе за потребе тестирања ИКТ система односно делова система	16
16. Учешће трећих лица у пословима ИКТ система.....	16
17. Превентивне мере и реаговање на безбедносне инциденте	16
V Измене постојећег и успостављање новог ИКТ система.....	17
VI Мере у циљу обезбеђења континуитета обављања посла у ванредним околностима .	17
VII Провера ИКТ система	17

VIII Дисциплинска одговорност	18
IX Измена Правилника	18
X Прелазне и завршне одредбе	19

На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо - комуникационих система од посебног значаја („Службени гласник РС”, број 94/16 од 24.11.2016. године) члана 50. алинеја 1. Статута ЈКП „Стандард“ Ада, директор ЈКП „Стандард“ Ада **(у даљем тексту директор предузећа)**, дана 1. децембра 2017. године, донео је

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНОГ СИСТЕМА ЈКП „СТАНДАРД“ АДА

I Уводне 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 информационо - комуникационог система ЈКП „Стандард“ Ада (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система који користи ЈКП „Стандард“ Ада.

Члан 2.

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

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог - корисника информатичких ресурса ЈКП „Стандард“ Ада.

За праћење примене овог правилника обавезује се запослени на пословима информатичар - програмер (у даљем тексту Администратор ИКТ система).

Члан 3.

Термини употребљени у овом Правилнику имају следеће значење:

- **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 података 1. и 2. ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
 4. организациону структуру путем које се управља ИКТ системом;
- **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;

- **информациона добра** су сви ресурси ЈКП „Стандард“ Ада који садрже пословне информације, 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;
- **корисник ИКТ система** је запослени у ЈКП „Стандард“ Ада и други корисник ресурса ИКТ система;
- **Администратор ИКТ система** је запослени у ЈКП „Стандард“ Ада у чијој су надлежности послови планирања развоја, одржавања и функционисања рачунарско - комуникационе инфраструктуре и развој информационог технологија.
- **тајност** је својство које значи да податак није доступан неовлашћеним лицима;
- **интегритет** значи очуваност изворног садржаја и комплетности податка;
- **расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
- **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;
- **непорецивост** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
- **ризик** значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
- **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;
- **инцидент** је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
- **мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
- **тајни податак** је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
- **компромитујуће електромагнетно зрачење (КЕМЗ)** представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
- **криптобезбедност** је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
- **безбедносна зона** је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
- **VPN (Virtual Private Network)** је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
- **MAC адреса (Media Access Control Address)** је јединствен број, којим се врши идентификација уређаја на мрежи;
- **Backup** је резервна копија података;
- **Download** је трансфер података са централног рачунара или web презентације на локални рачунар;

- **UPS (Uninterruptible power supply)** је уређај за непрекидно напајање електричном енергијом;
- **Freeware** је бесплатан софтвер;
- **Open source** софтвер отвореног кода;
- **Firewall** је „заштитни зид“ односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
- **USB** или флеш меморија је спољшњи медијум за складиштење података;
- **CD-ROM (Compact disk - read only memory)** се користи као медијум за снимање података;
- **DVD** је оптички диск високог капацитета који се користи као медијум за складиштење података;

Члан 4.

О информационим добрима води се посебна евиденција.

Евиденцију из става 1. овог члана води администратор ИКТ система.

Члан 5.

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,
- послови предвиђени процедурама у области информационе безбедности,
- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система ЈКП „Стандард“ Ада, као и приступ, измена или коришћење средстава без овлашћења и без евиденције о томе,
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу и
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

II Коришћење ИКТ система

1. Управљање ИКТ системом

Члан 6.

ИКТ системом управља администратор ИКТ система.

Администратор ИКТ система је дужан да све кориснике ресурса ИКТ система упозна са одговорностима и правилима коришћења ресурса ИКТ система, да их обучи за коришћење ресурса ИКТ система, да по завршетку обуке од запосленог узме изјаву о обучености за коришћење ресурса ИКТ система и да о истима води евиденцију.

Члан 7.

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

Члан 8.

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

Корисник ИКТ система, коме је престало радно ангажовање по било ком основу у ЈКП „Стандард“ Ада, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

2. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа - Администраторски и кориснички налог

Члан 9.

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

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

Администраторски налог за управљање доменом може да корисити само запослени који је распоређен на послове и радне задатке администратора 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 корисника ИКТ система.

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

Администратор ИКТ система води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу потреба, у организационим јединицама ЈКП „Стандард“ Ада.

3. Одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 10.

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира по матрици **презиме.име**, латиничним писмом без употребе слова đ, ž, ć, č, dž, š. Уместо ових слова користити следеће: đ=dj, ž=z, ć=c, č=c, dž=dz, š=s.

Лозинка мора да садржи минимум шест карактера комбинованих од малих и великих слова и цифара.

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

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

Корисник ИКТ система дужан је да мења лозинку у складу са потребама.

Неовлашћено уступање корисничког налога другом лицу подлеже дисциплинској одговорности.

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

III Предмет, мере и субјекти заштите ИКТ система

1. Предмет заштите ИКТ система

Члан 11.

Предмет заштите ИКТ система су:

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

2. Мере и субјекти заштите ИКТ система

Члан 12.

Мере прописане овим Правилником се односе на све организационе јединице ЈКП „Стандард“ Ада, на све кориснике ИКТ система ЈКП „Стандард“ Ада, као и на трећа лица која користе информатичке ресурсе ЈКП „Стандард“ Ада.

Члан 13.

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

Ради заштите тајности, аутентичности и интегритета података, ЈКП „Стандард“ Ада може да размотри коришћење одговарајућих мера криптозаштите.

Члан 14.

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 „Стандард“ Ада надлежан је запослени на пословима информатичар - програмер, у складу са систематизацијом радних места у ЈКП „Стандард“ Ада бр. 266/ЈКП-1, од 08.02.2017. године.

3. Обавезе корисника

Члан 15.

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

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

1. да користи информатичке ресурсе искључиво у пословне сврхе;
2. да прихвати да су сви подаци који се складиште, преносе или обрађују у оквиру информатичких ресурса власништво ЈКП „Стандард“ Ада и да могу бити предмет надгледања и прегледања;

3. да поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. да безбедно чува своје лозинке у односу на друга лица;
5. да мења лозинке сагласно утврђеним правилима;
6. да се, пре сваког удаљавања од радне станице, одјави са система, односно закључа радну станицу;
7. да користи DVD RW, CDRW и USB екстерне меморије на радној станици само уз одобрење администратора ИКТ система;
8. да захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране надлежног руководиоца;
9. да обезбеди сигурност података у складу са важећим прописима;
10. да приступа информатичким ресурсима само на основу изричито додељених корисничких права од стране администратора ИКТ система;
11. да не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције нити да неовлашћено инсталира други антивирусни програм;
12. да не сме на радној станици да складишти садржај који не служи у пословне сврхе;
13. да израђује заштитне копије (backup) података у складу са прописаним процедурама;
14. да користи Internet, Intranet и e-mail сервис ЈКП „Стандард“ Ада 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.

4. Ограничење приступа подацима и средствима за обраду података

Члан 16.

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

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

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

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

IV Појединачне мере заштите

1. 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 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, који је обезбеђен механичком бравом. Евиденцију о уласку у ову зону води администратор ИКТ система.

Члан 18.

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

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

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

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

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

У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, администратор ИКТ система ја дужан да искључи опрему у складу са процедурама произвођача опреме.

У случају изношења опреме из просторије из става 1. овог члана ради селидбе или сервисирања, неопходно је одобрење директора предузећа 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 обавезно се дефинише обавеза заштите података који се налазе на медијима који су део ИКТ ресурса ЈКП „Стандард“ Ада.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 19.

Нерегистровани корисници путем мобилних уређаја могу приступити следећим ресурсима ИКТ система ЈКП „Стандард“ Ада: Internet-у, e-mail сервису и web site-у.

Корисници ИКТ система, могу путем мобилних уређаја или рачунара, који су у власништву ЈКП „Стандард“ Ада и који су подешени од стране администратора ИКТ система, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности као што су електронска пошта, поједине апликације везане за обављање посла и друго, а на основу писане сагласности директора предузећа.

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

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

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

Уколико се установи неовлашћен приступ, о томе се путем електронске поште одмах, а најкасније сутрадан обавештава директор предузећа.

Члан 20.

Приступ ресурсима ИКТ система са приватног уређаја није дозвољен, осим ако је уређај у власништву ЈКП „Стандард“ Ада оштећен и није обезбеђена замена.

Сагласност на коришћење приватног уређаја у случају из става 1. овог члана даје директор предузећа.

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

Члан 21.

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

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

Администратор 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 сервисирању врати податке у мобилни уређај.

3. Заштита носача података

Члан 22.

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

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

Члан 23.

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

Документи са ознаком тајности могу да сними на друге носаче (екстерни HDD, USB, CD, DVD) само директор предузећа или запослени којег директор предузећа овласти писаним путем.

Евиденцију носача на којима су снимљени подаци са ознаком тајности, води администратор 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, директор предузећа ће одредити одговорну особу и начин транспорта.

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

4. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 24.

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.

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

Члан 25.

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

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

Свакодневно се аутоматски у тачно одређено време врши допуна антивирусних дефиниција.

Сваког петка у радној недељи 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.

6. Заштита при коришћењу интернета

Члан 26.

У циљу заштите, односно упада у ИКТ систем ЈКП „Стандард“ Ада са интернета, администратор ИКТ система је дужан да одржава систем за спречавање упада.

Администратор ИКТ система у договору са руководиоцима одређује 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.

Администратор 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 корисник прикључује на интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши администратор ИКТ система.

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

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

Члан 27.

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

Члан 28.

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 ЈКП „Стандард“ Ада;
- 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.

7. Заштита од губитка података

Члан 29.

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

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

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

Члан 30.

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

Сваки примерак преносног информатичког медија са копијама - архивама, мора бити означен бројем, врстом (дневна, недељна, 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 обезбеђена физички и у складу са мерама заштите од пожара.

Члан 31.

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.

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

Члан 32.

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

Сваког последњег радног дана у недељи датотека у којој се налази дневник активности се архивира по процедури за израду копија - архива осталих података у ИКТ систему.

9. Систем за контролу

Члан 33.

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

10. Обезбеђивање интегритета софтвера и оперативних система

Члан 34.

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

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

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

Треће лице може да изврши инсталацију и подешавање софтвера када је између ЈКП „Стандард“ Ада и њега уговорено одржавање софтвера у одређеном временском периоду.

Члан 35.

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.

11. Заштита од злоупотребе безбедносних слабости ИКТ система**Члан 36.**

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

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

12. Ревизија ИКТ система**Члан 37.**

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

Администратор ИКТ система одредиће време обављања ревизије, у зависности од врсте послова и радних задатака корисника ИКТ система у ЈКП „Стандард“ Ада.

13. Заштита опреме ИКТ система**Члан 38.**

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 држати закључани.

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

Бежична мрежа коју могу да користе посетиоци објекта у надлежности ЈКП „Стандард“ Ада, мора бити одвојена од интерне мреже коју користе корисници ИКТ система и кроз коју се врши размена службених података.

Бежична мрежа из става 4. овог члана треба да буде посебно означена.

14. Безбедност ИКТ система у случају размене података**Члан 39.**

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

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

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

Члан 40.

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

16. Учешће трећих лица у пословима ИКТ система

Члан 41.

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

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

Члан 42.

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.

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

Члан 43.

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

У случају непоштовања уговорених обавеза, администратор ИКТ система је дужан да одмах обавести директора предузећа, ради предузимања мера у циљу отклањања неправилности.

17. Превентивне мере и реаговање на безбедносне инциденте

Члан 44.

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

По пријему пријаве става 1. овог члана, администратор ИКТ система је дужан да одмах обавести директора предузећа и предузме мере у циљу заштите ресурса ИКТ система.

Члан 45.

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, администратор ИКТ система је дужан да обавести директора предузећа који о инциденту обавештава надлежни орган дефинисан наведеном Уредбом.

Администратор 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.

V Измене постојећег и успостављање новог ИКТ система

Члан 46.

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

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

VI Мере у циљу обезбеђења континуитета обављања посла у ванредним околностима

Члан 47.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из просторија предузећа, администратор ИКТ система је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију.

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

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

VII Провера ИКТ система

Члан 48.

Проверу ИКТ система врши администратор ИКТ система.

Члан 49.

Провера ИКТ система се врши тако што се:

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

Члан 50.

Извештај из претходног члана овог Правилника садржи:

- назив власника ИКТ система;
- време провере;
- податке о лицима која су вршила проверу;
- извештај о спроведеним радњама провере;
- закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;
- закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
- закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система;
- оцена укупног нивоа информационе безбедности;
- предлог евентуалних корективних мера;
- потпис одговорног лица које је спровело проверу ИКТ система.

VIII Дисциплинска одговорност**Члан 51.**

Непоштовање одредби овог Правилника представља повреду радних обавеза и повлачи дисциплинку одговорност корисника информатичких ресурса ИКТ система ЈКП „Стандард“ Ада.

Члан 52.

Свако коришћење ИКТ ресурса ЈКП „Стандард“ Ада ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

Члан 53.

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

IX Измена Правилника**Члан 54.**

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, администратор ИКТ система је дужан да обавести директора предузећа, како би он могао да приступи измени овог Правилника у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивања овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Х Прелазне и завршне одредбе

Члан 55.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли ЈКП „Стандард“ Ада.

Милан Попов

директор ЈКП „Стандард“ Ада

