



201802603

**ЈАВНО ПРЕДУЗЕЋЕ ЗА СКЛОНИШТА, БЕОГРАД-НОВИ БЕОГРАД  
БУЛЕВАР МИХАИЛА ПУПИНА БР. 117А**

ЈАСНО ПРЕДУЗЕЋЕ ЗА СКЛОНИШТА  
Бр. 3-4/2018-1  
15.03.2018.  
односно Радијо Авионика Београд

**ПРАВИЛНИК  
о безбедности информационо - комуникационих система  
Јавног предузећа за склоништа Београд – Нови Београд**

**Београд, март 2018. године**

На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/2016 и 94/2017), 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 („Сл. гласник РС“, бр. 94/2016) и члана 27. Статута Јавног предузећа за склоништа, а у складу са Законом о ванредним ситуацијама („Службени гласник РС“ бр. 111/2009, 92/2011 и 93/2012), Надзорни одбор Јавног предузећа за склоништа, доноси

**ПРАВИЛНИК  
о безбедности информационо - комуникационих система  
Јавног предузећа за склоништа Београд – Нови Београд**

**УВОДНЕ ОДРЕДБЕ**

**Предмет**

Члан 1.

Овим правилником ближе се дефинишу и утврђују мере заштите информационо-комуникационих система, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења, дужности и одговорности корисника информатичких ресурса у Јавном предузећу за склоништа Београд – Нови Београд (у даљем тексту: ЈП за склоништа).

**Циљеви**

Члан 2.

Циљеви доношења правила су:

- 1) Одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
- 2) Спречавање и ублажавање последица инцидента, којим се угрожава или нарушава информациона безбедност;
- 3) Подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
- 4) Прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
- 5) Свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Члан 3.

Мере прописане овим правилником су обавезујуће за све организационе јединице ЈП за склоништа и за све запослене - кориснике информатичких ресурса.

Непоштовање одредби овог правилника представља повреду радне дисциплине запосленог-корисника информатичких ресурса ЈП за склоништа.

За праћење примене овог правилника одговоран је помоћник директора за техничке послове (у даљем тексту: помоћник директора надлежног сектора), шеф Службе за техничку припрему одржавања (у даљем тексту: шеф надлежне службе) и запослени у Сектору за техничке послове на радним местима Координатор ИТ послова и ИТ подршка и развој (у даљем тексту: надлежни запослени).

#### Члан 4.

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 података (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 извornog 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 криптоштиту, управљање криптоматеријалима и развој метода криптоштите;
- 16) *криптоштита* 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 криптоштита;
- 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 код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правила, процедуре и слично;
- 21) VPN (Virtual Private Network)-је „приватна“ комуникациони мрежа која омогућава корисницима на развојеним 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) Open source софтвер отвореног кода;
- 28) Firewall је „заштитни зид“ односно систем прекокога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
- 29) USB или флеш меморија је спољашњи 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;

## **МЕРЕ ЗАШТИТЕ**

### **Члан 5.**

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности ЈП за склоништа, односно од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

*Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру ЈП за склоништа*

### **Члан 6.**

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 ЈП за склоништа, надлежни супомоћник директора надлежног сектора, шеф надлежне службе и надлежни запослени.

### **Члан 7.**

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 управљање 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 Јавног предузећа за склоништа, као и приступ, измене или коришћење средстава без овлашћења и без евидентије 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, корисник информатичких ресурса дужан је да, у циљу решавања насталог безбедносног инцидента, без одлагања, пријави инцидент непосредном руководиоцу, који ову информацију прослеђује електронским путем шефу надлежне службе и надлежном запосленом, који у складу са прописима обавештавају надлежне органе у циљу решавања насталог безбедносног инцидента.

## ***Безбедност рада на даљину и употреба мобилних уређаја***

### **Члан 8.**

Нерегистровани корисници, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ Интернету али не и деловима мреже кроз коју се обавља службена комуникација.

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву ЈП за склоништа, и који су подешени од стране надлежних запослених, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности (електронска пошта, Информациони систем), а на основу писане сагласности помоћника директора надлежног сектора.

Приступ ресурсима ИКТ система ЈП за склоништа са удаљених локација, од стране запослених-корисника, у циљу обављања радних задатака, омогућен је путем заштићене VPN/интернет конекције.

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

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

Надлежни запослени редовно контролишу приступ ресурсима ИКТ система и проверавају 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 ујутру обавештава помоћник директора надлежног сектора, а та MAC адреса се уноси у «block» листу софтвера који се користи за контролу приступа.

Приступ ресурсима ИКТ система са приватног уређаја запосленог није дозвољен, осим у случају ако је уређај у власништву ЈП за склоништа оштећен, није обезбеђена замена, а неопходно је због несметаног функционисања пословних процеса, уз одобрење помоћника директора надлежног сектора.

Трећем лицу могу се одобрити права приступа ИКТ систему уз претходно закључен одговарајући уговор, којимсе прецизно дефинишу услови и обим права приступа, укључујући све релевантне безбедносне захтеве.

Евиденцију приватних уређаја са којих ће бити омогућен приступ воде надлежни запослени.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране надлежног запосленог, који обавља послове ИТ подршка и развој. Уређаји се могу користити само за обављање послова у надлежности корисника-запосленог и то само у периоду када није могуће користити уређај у власништву ЈП за склоништа.

У случају квара мобилног уређаја, надлежни запослени из претходног става је дужан да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, урадиваскир података који се налазе у мобилном уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати податке у мобилни уређај.

У случају губитка или крађе мобилног уређаја, корисник мобилног уређаја у обавези је да крађу или губитак мобилног уређаја пријави шефу надлежне службе без одлагања, а у року од 24 сата да достави писану изјаву о околностима губитка или крађе мобилног уређаја. Надлежни запослени је у обавези да, по пријави крађе или губитка мобилног уређаја, неодложно блокира несталом мобилном уређају приступ информационом систему и кориснику промени креденцијале за приступ.

У случају да се пронађе мобилни уређај чији нестанак је пријављен, надлежни запослени ће извршити преглед уређаја и утврдити да ли он може бити поново коришћен за рад на даљину или не.

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

Члан 9.

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

Сви запослени и радно ангажовани појединци по другом основу којима је додељен приступ поверљивим информацијама, морају потписати изјаву о пословној тајни и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Надлежни запослени, који обавља послове ИТ координатора је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса ЈП за склоништа, 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.

Сви запослени - корисници ИКТ ресурса су обавезни да прођу одговарајућу обуку, као и да редовно стичу нова и обнављају постојећа знања о процедурима које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Надлежни запослени су дужни да се континуирано обучавају у циљу унапређења техничког и технолошког знања у овој области. Они су ауторизовани за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Свако коришћење ИКТ ресурса ЈП за склоништа од стране запосленог-корисника, ван додељених овлашћења, којим се нарушава безбедност информација или на други начин врши повреда правила и политика које су у примени у ЈП за склоништа, представља повреду радне дисциплине која се санкционише у складу са прописима о раду.

О елементима повреде радне дисциплине, надлежни запослени обавештава непосредног руководиоца запосленог, који је дужан да о наведеном обавести директора, у циљу спровођења прописаних мера у случају повреде радне дисциплине.

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

##### Члан 10.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система и након престанка или промене радног ангажовања.

У случају промене послова, односно надлежности корисника-запосленог, надлежни запослени ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева непосредног руководиоца.

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

О престанку радног односа или радног ангажовања, као и промени радног места, служба за правне и кадровске послове је дужна да након пријема потписаног акта о престанку радног односа, радног ангажовања или промени радног места, електронским путем обавести помоћника директора надлежног сектора и надлежне запослене, ради укидања, односно измене приступних привилегија запосленог-корисника.

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

## ***Идентификовање информационих добара и одређивање одговорности за њихову заштиту***

### **Члан 11.**

Информациона добра ЈП за склоништа су сви ресурси који садрже пословне информације предузећа, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записи, 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 шеф надлежне службеу папирној или електронској форми.

Предметзаштите су:

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

Запослени и екстерни корисници су обавезни да врате сву имовину ЈП за склоништа коју поседују након престанка радног односа, уговора или споразума о ангажовању на одређеним пословима и задацима.

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

### **Члан 12.**

Подаци који се налазе у ИКТ систему представљају пословну тајну.

Подаци који су означени као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телеkomуникационим системима („Сл. Гласник РС“, бр. 53/2011).

Детаљан опис информација, подаци о носачима информација и доступности података који су одређени степеном тајности, одређени су Правилником о пословној тајни и Одлуком о одређивању тајних података у ЈП за склоништа.

## *Заштита носача података*

### Члан 12.

Шеф надлежне службе и надлежни запослени ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података и интерним актима, тако да подаци и документа могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) запослених – корисника, искључиво по писаном одобрењу непосредног руководиоца.

Евиденцију носача на којима су снимљени подаци, води надлежни запослени, у сарадњи са одговорним лицем за вођење евиденције о документима и подацима означеним као пословна тајна.

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

У случају транспорта медија са подацима, директор ће одредити одговорно лице 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 комисијски уништени.

## *Ограниччење 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 надлежног запосленог - администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, осим надлежном запосленом у циљу подешавања корисничког профила и радне станице.

Запослени-корисник који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној одговорности и одговорности због повреде радне дисциплине.

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 ЈП за склоништа 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 складиши 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 ЈП за склоништа 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.

***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 за управљање доменом и базом података, могу да користе само надлежни запосленина пословима ИТ координатор и ИТ подршка и развој.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу кога/јих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налог додељује администратор, на основу захтева службе за правне и кадровске послове, у сарадњи са непосредним руководиоцем и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евидентију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева службе за правне и кадровске послове, односно надлежног руководиоца.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.  
ЈП за склоништа једном годишње врши преиспитивање права корисника на приступ, као и након сваке промене (промена радног места и описа послова, престанак радног односа).

### ***Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију***

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира по матрици: име, презиме, латиничним писмом без употребе слова Ђ, Ж, Ј, Њ, Ћ, Ч, Џ, Ш. Уместо ових слова користити слова из табеле.

Ћирилична слова	Латинична слова
Ђ	Dj
Ж	Z
Ј	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. Специјални знакови се могу комбиновати у зависности од врсте и поставке тастатуре („US“ тастатура, „Lat“ тастатура, „Cyr“ тастатура).

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 6 месеци.

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

Неовлашћено уступање корисничког налога другом лицу, представља повреду радне дисциплине.

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

**Члан 16.**

Приступ ресурсима ИКТ система Јавног предузећа за склониште не захтева посебну криптозаштиту.

За приступ ресурсима ИКТ система који се односе на послове одбране, односно, 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 квалифициране електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама.

Надлежни запослени су задужени за инсталацију потребног софтвера и хардвера за коришћење сертификата.

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

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

Члан 17.

ЈП за склоништаје дужано да предузме мере ради спречавања неовлашћеног физичког приступа просторијама, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација ЈП за склоништа и опреме за обраду информација.

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 и видео надзором.

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 надлежни запослени.

***Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средства која чине ИКТ систем***

Члан 18.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само надлежним запосленим на пословима одржавања ИКТ система.

Осим наведених, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу шефа надлежне службе, и уз присуство надлежног запосленог.

Приступ административној зони може имати и запослени на пословима одржавања хигијене уз присуство надлежног запосленог.

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, надлежни запослени је дужан да искључи опрему у складу са процедурима произвођача опреме.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења директора или помоћника директора надлежног сектора.

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

Ако се опрема износи ради сервисирања, поред одобрења помоћника директора надлежног сектора, 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 ЈП за склоништа.

Сви делови опреме који садрже медијуме за чување података треба да се верификују да би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњени.

Корисници треба да осигурају да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

### *Обезбеђивање исправног и безбедног функционисања средстава за обраду података*

#### **Члан 19.**

Шеф надлежне службе и надлежни запослени 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 одговарајуће мере помоћнику надлежног сектора.

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 тестирање софтвера пре увођења у рад у ИКТ систем морају се користити тестне платформе и подаци који су намењени тестирању.

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.

### *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. Свакодневно се аутоматски у 8 сати врши допуна антивирусних дефиниција.

Сваког четвртка у току радног времена потребно је оставити укључене 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 софтером.

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

У циљу заштите, односно упада у ИКТ систем ЈП за склоништа са интернета, надлежни запослени на пословима ИТ подршка и развој је дужан да одржава систем за спречавање упада.

Руководиоци организационих јединица одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Корисницима који су приклучени на ИКТ систем је забрањено самостално приклучивање на интернет (приклучивање преко сопственог модема), при чему надлежни запослени може 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 приклучује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши надлежни запослени.

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 надлежном запосленом.

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.

Недозвољена употреба интернета обухвата:

- 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 друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимање (download) података велике “тежине” које проузрокује “загушење” на мрежи;
- преузимање (download) материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

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

### *Заштита од губитка података*

#### Члан 21.

ЈП за склоништа врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих и log фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

За чување заштитних копија користе се магнетне траке, екстерни хард дискови и CD/DVD медији.

Шеф надлежне службе и надлежни запослени, редовно врше следеће задатке:

- процену осетљивих и критичних података за које је потребно правити резервне копије;
- креирање плана прављења резервних копија;
- израду заштитне копије серверског оперативног система и података, комуникационог оперативног система и конфигурационих фајлова, апликација, сервиса и база података;
- верификацију успешно прављених резервних копија;
- вођење евиденције урађених резервних копија;
- одлагање копија на безбедно место;
- тестирање исправности резервних копија и процедуре за прављење заштитних копија;
- рестаурирање података са резервних копија.

За заштиту од губитка података одговоран је шеф надлежне службе.

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

Члан 22.

У ИКТ систему ЈП за склоништа формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

ЈП за склоништа прави записи о догађајима и бележи активности корисника, грешке и догађаје у вези са безбедношћу информација, који се морају чувати и редовно преиспитивати.

Надлежни запослени -администратори система немају дозволу да бришу или деактивирају дневнике о сопственим активностима.

Записи о догађајима садрже:

- идентификаторе корисника;
- активности система;
- датуме, време и детаље кључних догађаја, нпр. пријављивања и одјављивања;
- идентитет или локацију уређаја, ако је могуће, и идентификатор система;
- записи о успешним и одбијеним покушајима приступа систему;
- записи о успешним и одбијеним покушајима приступа подацима и другим ресурсима;
- промене у конфигурацији система;
- коришћење привилегија;
- коришћење системских помоћних функција и апликација;
- датотеке којима се приступало и врсте приступа;
- мрежне адресе и протоколе;
- аларме које је побудио систем за контролу приступа;
- активирање и деактивирање система заштите, као што су антивирусни системи и системи за откривање упада.

Средства за записивање и записане информације су заштићени од неовлашћеног мењања и приступа.

Забрањено је неовлашћено уношење следећих измена:

- мењање типова порука које се записују;
- уношење измена у датотеке са записима или њихово брисање;
- препуњавање медијума за записи, што доводи до отказа записивања догађаја или уписивања преко већ раније записаног.

Активности надлежних запослених се записују, а записи штите и редовно преиспитују. Власници привилегованих корисничких налога могу бити у стању да управљају записима на опреми за обраду информација која је под њиховом директном контролом, на који начин се штите и прегледају записи да би се одржала одговорност за привилеговане кориснике.

Сатови свих одговарајућих система за обраду информација заштите морају бити синхронизовани по Гриничком средњем времену.

За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужени су надлежни запослени.

## *Обезбеђивање интегритета софтвера и оперативних система*

### Члан 23.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву ЈП за склоништа односно Freeware и Open source верзије.

Инсталацију и подешавање софтвера може да врши само надлежни запослени, 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.

## *Заштита од злоупотребе техничких безбедносних слабости ИКТ система*

### Члан 24.

Надлежни запослени најмање једном месечно а по потреби и чешће врши анализу дневника активности (activity log, history, security log, transaction log и др. ) у циљу идентификације потенцијалних слабости ИКТ система.

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

Надлежни запослени треба да подешавањем корисничких полиса, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

## *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 шефа надлежне службе и непосредног руководиоца запосленог - корисника.

## ***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. Надлежни запослени је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

## ***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 ЈП за склоништа између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила, процедуре, потписивањем уговора и споразума, као и применом адекватних контрола.

Употреба електронске поште мора бити у складу са правилима поступка, сигурна и у складу са позитивним прописима, интерним актима 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.

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.

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.

Изјаве о поверљивости штите информације ЈП за склоништа и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

Рзмена података са државним органима, правним и физичким лицима се врши у складу са важећим прописима, интерним актима и потписаним уговорима.

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

**Члан 28.**

У оквиру животног циклуса ИКТ система који укључује фазе концепирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, ЈП за склоништа је у обавези да обезбеди безбедност информација у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система, јер такво разматрање доводи до ефективнијих и рационалнијих решења.

Директор одређује лица задужена за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

Шеф надлежне службе води документацију о успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова.

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

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

**Члан 29.**

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредила актуелна и очекивана понашања.

Приликом тестирања система, за податке који су означени ознаком тајности, односно службености као поверљиви или лични подаци, одговарају запослени који користе наведене податке у свом раду, у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

***Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга***

**Члан 30.**

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација ЈП за склоништа морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

Пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са ЈП за склоништа.

Пре потписивања уговора, пружалац услуга у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, која садржи обавезу за пружаоца услуга да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране ЈП за склоништа и за потребе извршења предмета уговора, или да наведена одредба буде саставни део уговора о пружању услуга.

Изјава о поверљивости, односно уговор о пружању услуга, морају садржати одредбе са јасно утврђеном обавезом и одговорношћу пружаоца услуге уз претњу једностраног раскида уговора и накнаду штете у корист ЈП за склоништа у случају повреде поверљивости.

Пружаоци услуга дужни су да захтеве ЈП за склоништа у погледу безбедности информација пренесу и на заједничке понуђаче илиподуговараче.

Комисија, или лице одговорно за реализацију предметног уговора је одговорна/о за контролу приступа и поштовање одредби уговора о поверљивости.

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

Члан 31.

Комисија, или лице одговорно за реализацију уговора је одговоран/а за надзор над поштовањем уговорених обавеза од стране пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система.

У случају непоштовања уговорених обавеза, лица из претходног става су дужна да одмах обавесте надлежног запосленог, који након извршене провере, обавештава директора, у циљу предузимања мера и отклањања неправилности.

***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 надлежног запосленог.

По пријему пријаве надлежни запослени је дужан да одмах обавести помоћника директора надлеженог сектора 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 („Сл. гласник РС“ бр. 94/2016), помоћник директора надлеженог сектора је дужан да обавести директора, у циљу пријаве инцидента надлежним органима дефинисаним уредбом.

Шеф надлежне службе води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом.

#### *Мере које обезбеђују континуитет обављања посла у ванредним околностима*

##### Члан 33.

У случају ванредне ситуације, које могу да доведу до измештања ИКТ система из ЈП за склоништа, шеф надлежне службе је дужан да у најкраћем року пренесе делове ИКТ система, неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује шеф надлежне службе и то у три примерка, од којих се један налази у надлежној служби, други код помоћника директора надлежног сектора, а трећи примерак код запосленог надлежног за послове одбране.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди помоћник директора надлежног сектора. 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.

#### *Измена Правилника о безбедности информационо - комуникационих система Јавног предузећа за склоништа*

##### Члан 34.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ЈП за склоништа, као ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, као и у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система и преиспитивања овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система, помоћник директора надлежног сектора је дужан да обавести директора, ради подношења предлога за измену овог правилника.

## *Провера ИКТ система*

### Члан 35.

Проверу ИКТ система врши шеф надлежне службе.

Проверу ИКТ система може да врши и изабрани понуђач у складу са одредбама Закона о јавним набавкама.

Провера се врши последњег месеца у години.

Провера се врши тако што се:

- 1) проверава усклађеност Правилника о безбедности ИКТ система са прописаним условима, тј. да ли су адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему, узимајући у обзир интерна акта повезана са Правилником;
- 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 помоћнику директора надлежног сектора.

## *Садржај извештаја о провери ИКТ система*

### Члан 36.

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.

*Прелазне и завршне одредбе*

Члан 37.

Овај правилник ступа на снагу даном доношења и објављује се на интернет страници Јавног предузећа за склоништа.

