

На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС“, бр. 94/2016) и члана 32. став 1. тачка 1. Статута „Дома ученика средњих школа Патријарх Павле – Београд“, Управни одбор „Дома ученика средњих школа Патријарх Павле – Београд“ на седници одржаној дана 25.12.2019.године, донео је



ДОМ УЧЕНИКА
СРЕДЊИХ ШКОЛА ПАТРИЈАРХ ПАВЛЕ
БЕОГРАД

ПРАВИЛНИК
о безбедности информационо - комуникационог система
„Дома ученика средњих школа Патријарх Павле – Београд“

01/1696

25.12.2019 год.

БЕОГРАД, ЗДРАВКА ЧЕДАРА 14

I. Уводне одредбе

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности 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 „Дома ученика средњих школа Патријарх Павле – Београд“ (у даљем тексту: ИКТ систем).

Члан 2.

Мере прописане овим правилником се односе на све радне јединице „Дома ученика средњих школа Патријарх Павле – Београд“, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Дома ученика средњих школа Патријарх Павле – Београд“ (у даљем тексту: Дом).

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса „Дома ученика средњих школа Патријарх Павле – Београд“.

За праћење примене овог правилника обавезује се референт на рачунару.

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

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

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

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

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

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

2) *информациона безбедност* представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

3) *тајност* је својство које значи да податак није доступан неовлашћеним лицима;

4) *интегритет* значи очуваност изворног садржаја и комплетности податка;

5) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) *аутентичност* је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

7) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

8) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

9) *управљање ризиком* је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

10) *инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

11) *мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

12) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

13) *ИКТ систем за рад са тајним подацима* је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

14) *компромићујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

15) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

16) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

17) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;

18) *криptomатеријали* 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 правилнике, процедуре и слично;

- 21) VPN (Virtual Private Network)-je „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
- 22) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
- 23) Backup је резервна копија података;
- 24) Download је трансфер података са централног рачунара или web презентације на локални рачунар;
- 25) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
- 26) Freeware је бесплатан софтвер;
- 27) Opensource софтвер отвореног кода;
- 28) Firewall је „заштитни зид“ односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
- 29) USB или флеш меморија је спољшњи медијум за складиштење података;
- 30) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;
- 31) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података.

II. Мере заштите

Члан 4.

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

1.Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у „ Дому ученика средњих школа Патријарх Павле – Београд“.

Члан 5.

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

Запослени у „ Дому ученика средњих школа Патријарх Павле – Београд“ 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.

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 „ Дома ученика средњих школ Патријарх Павле – Београд“ надлежан је референт на рачунару у складу са систематизацијом радних места у Дому.

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава и 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 Дома ученика средњих школа, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента референт на рачунару, обавештава директора Дома, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Дом не дозвољава рад на даљину.

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.

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.)

Референт на рачунару свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава директора Дома ученика средњих школа, а та MAC адреса се уноси у «block» листу софтвера који се користи за контролу приступа. Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен, осим ако је уређај у Дому, оштећен и није обезбеђена замена.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води референт на рачунару, а по одобрењу директора Дома. Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране референта на рачунару, могу се користити само за обављање

послова у надлежности корисника-запосленог и то само у периоду када није могуће користити уређај у власништву Дома .

Референт на рачунару је дужан да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради *backup* података који се налазе у мобилном уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати податке у мобилни уређај.

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

Члан 8.

ИКТ системом управљају запослени у складу са важећом Актом о систематизацији и организацији послова Дома.

Референт на рачунару је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ Дома, да га упозна са правилима коришћења ресурса ИКТ система.

Радно ангажовани појединци којима је по другим основама додељен приступ поверљивим информацијама морају потписати споразум о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Свако коришћење ИКТ ресурса Дома од стране запосленог-корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог.

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.

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

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

О престанку радног односа или радног ангажовања, као и промени радног места, референт на рачунару референт за кадровске и опште послове у сарадњи са непосредним руководиоцем, је дужан да обавести референт на рачунару ради укидања, односно измену приступних привилегија тог запосленог-корисника.

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

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра Дома су сви ресурси који садрже пословне информације Дома ученика средњих школа, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем и сл.)

Евиденцију о информационим добрима води референт на рачунару, у електронској форми.

Предмет заштите су:

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

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

Члан 11.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебним прописима¹.

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

Опис информација, носача информација и доступности података налази се у Информатору о раду Дома.

7. Заштита носача података

Члан 12.

Референт на рачунару ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да:

¹Закон о слободном приступу информацијама од јавног значаја („Сл. Гласник РС“, бр.120/04, 54/07, 104/09 I 36/10), Закон о заштити података о личности („Сл. Гласник РС“, бр.97/08,104/09-ДР. Закон 68/12,-ОДЛУКА УС И 107/2012), Закон о тајности података („Сл. Гласник РС“, 104/2009), као и Уредба о начину и поступку означавања тајности података, односно докумената („Сл. Гласник РС“, бр. 8/2011)

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

Евиденцију носача на којима су снимљени подаци, води референт на рачунару и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, директор Дома ће одредити одговорну особу и начин транспорта.

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

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

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

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

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

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

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

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

Члан 14.

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

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

Администраторски налог може да користи само запослени на пословима референт на рачунару.

Администраторски налог за управљање доменом може да користе само запослени на пословима референт на рачунару.

Администраторски налог за управљање базом података може да користе само запослени на пословима референт на рачунару.

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

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

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 6 месеци.

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.

Пријављивање у ИКТ систем Дома се врши убацивањем медија са електронским сертификатом у читач картица.

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 Дома не захтева посебну криптозаштиту.

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

Запослени на пословима ИКТ 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 се 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 референт на рачунару.

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 само администратору ИКТ система. Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу директора Дома, и уз присуство надлежног лица референта на рачунару.

Приступ административној зони може имати и запослени на пословима одржавања хигијене уз присуство надлежног лица референта на рачунару.

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

Прозори и врата на овој просторији морају увек бити затворени.

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

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

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

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

Ако се опрема износи ради сервисирања, поред одобрења директора Дома, 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 Дома.

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 директору Дома 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 приметне битне недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

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

Члан 20.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен и неумрежен рачуна.

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 12 сати врши допуна антивирусних дефиниција.

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

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

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

У циљу заштите, односно упада у ИКТ систем Дома са интернета, референт на рачунару 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 прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему референт на рачунару 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 прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши референт на рачунару.

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 референту на рачунару.

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 нарушавају безбедност мреже може се одузети право приступа.

16. Заштита од губитка података

Члан 21.

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

Остали фајлови-документи се архивирају најмање месечно и годишње.

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

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

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).

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 једној од радних јединица Дома.

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

За заштиту од губитка података одговоран је референт на рачунару.

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

Члан 22.

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

Средства за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене. У оквиру ИКТ система записују се активности администратора и корисника и редовно преиспитују у циљу заштите.

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 Дома, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само референт на рачунару, 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.

У циљу заштите ИКТ система од злоупотребе безбедносних слабости, референт на рачунару врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и, у складу са тим, предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену других врста заштите ИКТ систем.

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

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 директора Дома.

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.

Референт на рачунару 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 Дома, мора бити одвојена од интерне мреже коју користе корисници запослени у Дому 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 ИКТ система Дома контролише се и надзире од стране одговорног лица.

Када се пренос података врши између ИКТ система Дома и лица ван ИКТ система Дома, могу се закључити споразуми о преносу података и споразуми о поверљивости или неоткривању који садрже одредбе о безбедности преноса података.

23. *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 пројектовања, тестирања, имплементације коришћења одржавања и на крају повлачења из употребе, Дом је у обавези да обезбеди безбедност информација у свакој фази.

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

Референт на рачунару 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 референт на рачунару користи податке који нису осетљиви, које штити, чува и контролише на одговарајући

начин. Ако се за потребе тестирања користе поверљиве информације, односно лични подаци, потребно их је употребљавати и штитити у складу са прописима и овлашћењима.

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.

Референт на рачунару 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.

У циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, референт на рачунару задужен је за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности.

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 референта на рачунару.

По пријему пријаве референт на рачунару је дужан да одмах обавести директора Дома 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 инцидента и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, „Сл. Гласник РС“, бр, 94/2016), референт на рачунару, је дужан да поред директора Дома обавести и надлежни орган дефинисан овом уредбом.

Референт на рачунару 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.

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 Дома, референт на рачунару 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.

Референт на рачунару је дужан да редовно врши проверу безбедности информација како би оне биле важеће и ефективне и током ванредних ситуација.

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, референт на рачунару је дужан да обавести директора Дома, 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.

I. Провера ИКТ система

Члан 35.

Проверу ИКТ система врши референт на рачунару.

Провера се врши тако што се:

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

О извршеној провери сачињава се извештај, који се доставља директору Дома.

I. 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.

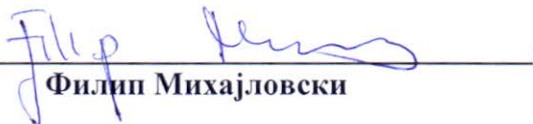
Прелазне и завршне одредбе

Члан 37.

Овај правилник ступа на снагу 8-ог дана од објављивања на огласној табли Дома.



ПРЕДСЕДНИК УПРАВНОГ ОДБОРА


Филип Михајловски