На основу члана 8. Закона о информационој безбедности („Службени гласник Републике Србије", број 6/16 и 94/17), чланова 1-8 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, Владе Републике Србије ("Службени гласник Републике Србије", број 94/16) и члана 34. став 1. алинеја 3. Статута Народне библиотеке Смедерево („Службени лист града Смедерева", број 2/2013, 9/2016 и 12/2017 – пречишћен текст), Управни одбор Народне библиотеке Смедерево, на седници одржаној дана 24.06.2019. године, донео је

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНИХ СИСТЕМА НАРОДНЕ БИБЛИОТЕКЕ СМЕДЕРЕВО

I Уводне одредбе

Члан 1.

Овим правилником ближе се дефинишу мере заштите информационо-комуникационих система у Народној библиотеци Смедерево (у даљем тексту Библиотека), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса у Библиотеци.

Члан 2.

Циљеви доношења овог правилника су:
- допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
- минимизација безбедносних инцидената;
- допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистентне контроле свих компонената информационо - комуникационог система (у даљем тексту: ИКТ систем).

Члан 3.

Овај правилник је обавезујући за све унутрашње организационе јединице Библиотеке и за све кориснике информатичких ресурса, као и за сва трећа лица која користе информатичке ресурсе Библиотеке.

Непоштовање овог правилника повлачи дисциплинску одговорност корисника информатичких ресурса.

За праћење примене овог правилника надлежна је Служба општих послова Библиотеке.

Члан 4.

Поједини појмови 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 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) информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
13) VPN (Virtual Private Network) је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
14) MAC адреса (Media Acces Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
15) Администратор ІКТ система – лице које има администраторски налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога;
16) Backup је резервна копија података;
17) Лице задужено за информационе технологије је запослени у Библиотеци чији је задатак управљање ИКТ Библиотеке.

II Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Библиотеке, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у Библиотеци

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 Библиотеке надлежно је лице задужено за информационе технологије.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Уређаји у централном објекту Библиотеке и у огранцима морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Лице задужено за информационе технологије 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 писаним путем одмах, а најкасније сутрадан обавештава директор Библиотеке, а та MAC адреса се уноси у „block“ листу софтвера који се користи за контролу приступа.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води лице задужено за информационе технологије, а по одобрењу директора Библиотеке.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране лица задуженог за информационе технологије и могу се користити само за обављање послова у надлежности корисника-запосленог и то само у периоду када није могуће користити уређај у власништву Библиотеке.

Употреба мобилних уређаја у ИКТ систему није омогућена.

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

Члан 8.

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места.

Лице задужено за информационе технологије је дужно да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Библиотеке, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденцију о изјавама новозапослених – корисника да су упознати са правилима коришћења ИКТ ресурса.

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

4. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених у Библиотеци

Члан 9.

У случају промене послова, односно надлежности корисника-запосленог, администратор система 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.

Корисник ИКТ ресурса, након престанка радног ангажовања у Библиотеци, 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 Библиотеке су сви ресурси који садрже пословне информације Библиотеке, 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 лице задужено за информационе технологије, у папирној или електронској форми.

Предмет заштите су:

1) хардверске и софтверске компоненте ИКТ система;

2) подаци који се обрађују или чувају на компонентама ИКТ система;

3) 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 посебних прописа.

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).

7. Заштита носача података

Члан 12.

Лице задужено за информационе технологије 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:

- 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 одлуком директора овлашћених запослених – корисника.

Евиденцију носача на којима су снимљени подаци води лице задужено за информационе технологије и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

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

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

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

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

Запослени-корисник дужан је да поштује 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 Библиотеке;

3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;

4) безбедно чува своје лозинке, односно да их не одаје другим лицима;

5) мења лозинке сагласно утврђеним правилима;
6) пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу;
7) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8) обезбеди сигурност података у складу са важећим прописима;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
12) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
13) прихвати да технике сигурности (антивирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;
14) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер;
15) израђује заштитне копије (backup) података у складу са прописаним процедурама;
16) користи интернет и електронску пошту у Библиотеци у складу са прописаним процедурама.

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 могу да користе само запослени са овлашћењем директора.

Кориснички налог се састоји од корисничког имена и лозинке, 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 запосленог-корисника.

Кориснички налог додељује администратор, на основу захтева запосленог задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем 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 шест карактера.

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 шест месеци.

Кориснички налог може да се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом. Пријављивање у ИКТ систем Библиотеке врши се 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.

У Библиотеци није предвиђена употреба криптозаштите података.

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.

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови:

1. сервери, сторици и комуникационо чвориште у Библиотеци морају бити смештени у посебној просторији (сервер соби), која испуњава стандарде противпожарне заштите и поседује редудантно напајање електричном струјом и адекватну климатизацију и којој је забрањен приступ незапосленим лицима;
2. приступ сервер соби, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење директора;
3. радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;
4. просторије у којима се треунутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
5. штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;
6. медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

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

Члан 18.

Просторије у којима се налази ИКТ опрема морају бити обезбеђене видео надзором. Осим видео надзора, обезбеђење ових просторија у току радног времена врши се сталним присуством најмање једног запосленог у просторији (одељењу) у којој се налази ИКТ опрема.

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

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

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

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 одговарајуће мере.

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

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

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

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

Члан 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.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена лиценцираног софтвера, односно забрана коришћења неауторизованог софтвера.

Преносиви медији пре коришћења морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, врши се чишћење медија од вируса, уз сагласност доносиоца медија.

Ризик од евентуалног губитка података приликом чишћења медија антивирусним софтвером сноси доносилац медија.

У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

- електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;
- забрањено је коришћење електонске поште у приватне сврхе;
- не смеју се користити приватни налози електронске поште у пословне сврхе.

Приликом коришћења интернета треба избегавати сумњиве WEB странице. 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.

16. Заштита од губитка података

Члан 21.

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

Дневно копирање-архивирање врши се за сваки радни дан у седмици, од 20 часова сваког радног дана.

Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно, од 20 часова.

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

Дневне и месечне копије-архиве се чувају у просторији која је физички и у складу са мерама заштите од пожара обезбеђена.

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

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

Члан 22.

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

Сваког последњег радног дана у недељи датотеке у којима се налази дневник активности се архивирају по процедури за израду копија-архива осталих података у ИКТ систему, у складу са чл. 21. овог правилника.

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 Библиотеке, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само лице задужено за информационе технологије и лице ангажовано за послове одржавања информационог и аудио-визуелног система у Библиотеци.

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.

Лице задужено за информационе технологије најмање једном месечно, а по потреби и чешће, врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, лице задужено за информационе технологије је дужно да одмах 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.

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.

Лице задужено за информационе технологије је дужно да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Мрежа коју могу да користе корисници и посетиоци објеката у надлежности Библиотеке, мора бити одвојена од интерне мреже коју користе корисници-запослени у Библиотеци и кроз коју се врши размена службених података.

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

Члан 27.

Преносиви медији који садрже податке морају да буду прописно обележени и пописани.

Преносиви медији пре стављања ван употребе морају бити физички уништени.

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

Члан 28.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Библиотеци дефинише се уговором који се закључује са тим лицима.

Лице задужено за информационе технологије у обавези је да врши технички надзор над реализацијом уговорних обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система, лице задужено за информационе технологије мора да води документацију.

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

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

Члан 29.

За потребе тестирања ИКТ система, односно делова система лице задужено за информационе технологије може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

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

Члан 30.

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима Библиотеке који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ.

Лице задужено за информационе технологије је одговорно за контролу приступа и надзор над извршењем уговорних 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.

Лице задужено за информационе технологије је одговорно за надзор над поштовањем уговорних обавеза од стране трећих лица – пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система. У случају непоштовања уговорних обавеза, лице задужено за информационе технологије је дужно да одмах обавести директора, како би директор могао да предузме мере у циљу отклањања неправилности.

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

Члан 32.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести лице задужено за информационе технологије.

По пријему пријаве лице задужено за информационе технологије је дужно да одмах обавести директора и предузме мере у циљу заштите ресурса ИКТ система.

Лице задужено за информационе технологије води евиденцију о свим инцидентима, као и пријавама инцидената на основу којих против одговорних 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 објекта Библиотеке, лице задужено за информационе технологије је дужно 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 лице задужено за информационе технологије и то у три примерка, од којих се један налази код тог лица, други код запосленог надлежног за послове одбране и ванредне ситуације, а трећи примерак код директора.

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

У случају немогућности функционисања ИКТ система у ванредним околностима, запослени су дужни да након поновног успостављања функционисања сачине извештај о свим процедурама које су предузимали у току отказа система.

III Измена Правилника о безбедности

Члан 34.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских или организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, лице задужено за информационе технологије је дужно да обавести директора, како би директор могао да покрене процедуру измене овог правилника, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IV Провера ИКТ система

Члан 35.

Проверу ИКТ система врши лице задужено за информационе технологије у сарадњи са лицем коме су уговором поверени послови одржавања информационог и аудио-визуелног система.

Провера се врши последњег месеца у години.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на које 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, 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.

V Садржај извештаја о провери ИКТ система

Члан 36.

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава (Народна библиотека Смедерево);
2) време провере;
3) податке 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) оцену укупног нивоа информационе безбедности;
9) предлог евентуалних корективних мера;
10) потпис одговорног лица које је спровело проверу ИКТ система.

VI Прелазне и завршне одредбе

Члан 37.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли Библиотеке.

Број 350
У Смедереву, 24.06.2019. године

Председник Управног одбора
Народне библиотеке Смедерево
Марија Огаревић

Марија Огаревић

НАРОДНА БИБЛИОТЕКА СМЕДЕРЕВО

Правилник објављен
на огласној табли Библиотеке

24.06.2019.

Правилник ступио на снагу

02.07.2019.