На основу члана 8. Закона о информационој безбедности ("Сл. гласник РС", бр. 6/2016) у даљем тексту: Закон, 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), на основу одредби Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја ("Сл. гласник РС", бр.94/2016), као и на основу члана 51. став 1. тачка 4. Статута Народне библиотеке Србије-установе културе од националног значаја 0101 број 123/1 од 11.02.2011. године и Одлука о изменама и допунама Статута Народне библиотеке Србије-установе културе од националног значаја 0101 бр. 80/3 од 30.03. 2012. године и 0101 бр. 110/3-1 од 05.04.2013. године, 0101 бр. 110/6 од 24.09.2013. године, 0101 бр. 78/4 од 14.03. 2015. године, управник Народне Библиотеке Србије-установе културе од националног значаја, дана 28.03.2017. године, доноси

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА НАРОДНЕ БИБЛИОТЕКЕ СРБИЈЕ-УСТАНОВЕ КУЛТУРЕ ОД НАЦИОНАЛНОГ ЗНАЧАЈА

Предмет

Члан 1.

Овим Правилником о безбедности информационо-комуникационих система Народне библиотеке Србије-установе културе од националног значаја (у даљем тексту: Правилник) утврђују се и ближе дефинишу мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности, овлашћења и одговорности корисника информатичких ресурса у Народној Библиотеци Србије-установи културе од националног значаја (у даљем тексту: Библиотека).

Циљеви

Члан 2.

Циљеви за доношење Правилника су:

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

Примена

Члан 3.

Примена Правилника је обавезујућа за све организационе јединице Библиотеке и за све запослене - кориснике информатичких ресурса, као и за трећа лица која користе информатичке ресурсе Библиотеке.

Непоштовање одредби овог Правилника повлачи дисциплинску одговорност корисника информатичких ресурса.

За праћење примене овог Правилника надлежно је Одељење за одржавање и развој рачунарско-информатичког система.

Појмови

Члан 4.

Поједини изрази употребљени у овом Правилнику имају следеће значење:

1. **информационо-комуникациони систем** (ИКТ систем) је технолошко-организациона целина која обухвата:
   a) електронске комуникационе мреже у смислу закона који уређује електронске комуникације
   b) 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;
   c) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачке (а) и (б) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
   d) 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. **интегритет** је немогућност неовлашћене измене информација;
4. **расположивост** је доступност информација корисницима информатичких ресурса у обиму корисничког овлашћења;
5. **тајност** је обезбеђивање доступности информација само овлашћеним корисницима информатичких ресурса, као и немогућност приступа информацијама лицима која немају таква овлашћења;
6. **администраторско овлашћење** је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;
7. **кориснички налог** јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно овлашћења корисника);
8. **администраторски налог** јесте јединствен налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога.
9. **мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
10. **инцидент** је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
11. **VPN (Virtual Private Network)**-је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;

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.

Информатички ресурси Библиотеке

Члан 6.

Информатички ресурси Библиотеке су сви ресурси који садрже пословне информације Библиотеке у електронском облику или служе за приступ корисника ИКТ систему укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и слично.

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

Предмет заштите

Члан 7.

Предмет заштите обухвата:

1. хардверске и софтверске компоненте информатичких ресурса;
2. податке који се обрађују или чувају на информатичким ресурсима;
3. корисничке налоге и друге податке о корисницима информатичких ресурса у Библиотеци.

Корисник информатичких ресурса

Члан 8.

Корисник информатичких ресурса јесте постављено лице, запослено лице на неодређено или одређено време, лице ангажовано по основу уговора, консултант или друго радно ангажовано лице коме је одобрен приступ неком информатичком ресурсу Библиотеке, као и корисници ІКТ услуга – чланови Библиотеке.

Корисник информатичких ресурса одговоран је за правилну употребу, тачност и сигурност података приликом коришћења информатичких ресурса Библиотеке, односно лично је одговоран за остваривање својстава података у ИКТ систему Библиотеке.

Корисник информатичких ресурса нема имовинска права над информатичким ресурсима Библиотека.

Администратор, на основу прецизног писаног захтева непосредног руководиоца, додељује кориснику информационог ресурса корисничко име, лозинку и привилегије, као и налог за електронску пошту.

Кориснику информатичких ресурса додељују се само привилегије које су неопходне за реализацију његових радних обавеза.

У случају престанка радног односа или радног ангажовања у Библиотеци кориснику информатичких ресурса укида се право приступа ИКТ систему.

У случају одсуства са посла дуже од месец дана, кориснику информатичких ресурса се привремено укида право приступа ИКТ систему, до повратка на посао.

О престанку радног односа или радног ангажовања, одсуству са посла дуже од месец дана, као и о промени радног места корисника информатичких ресурса, непосредни руководилац је дужан да обавести Одељење за одржавање и развој рачунарско-информатичког система ради укидања, односно измена приступних привилегија тог корисника.

Корисник информатичких ресурса, након престанка радног ангажовања у Библиотеци, не сме да открива поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система.

Трећем лицу могу се одобрити права приступа ИКТ систему уз претходно склапање одговарајућег уговора, којим се прецизно дефинишу услови и обим права приступа, укључујући и све релевантне безбедоносне захтеве.

Ако се установи повреда уговорне обавезе или прекорачење овлашћења по основу уговара, одобрени приступ се одмах укида.

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.

Дужности корисника информатичких ресурса

Члан 9.

Корисник не сме да спроводи активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система Библиотеке.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне сврхе, а Библиотека задржава право да информатичке ресурсе повуче у било ком тренутку и у потпуности задржи све податке, без обавезе да их накнадно преда кориснику.

Корисник непреносиве радне станице је дужан да пословне податке смешта на одређене мрежне дискове, односно портале Библиотеке.

Изузетно од става 3. овог члана, због потребе посла, подаци се могу привремено сместити на локални диск непреносиве радне станице, ако се са тим сагласи непосредни руководилац корисника.

Корисник преносиве радне станице има право да привремено смешта пословне податке на локални диск преносиве радне станице, као и обавезу да уради копију докумената са локалног диска на мрежни, односно портале Библиотеке.

Запослено, односно ангажовано лице у Одељењу за одржавање и развој рачунарско-информатичког система, дужни су да дневно израђују резервне копије података са мрежних дискова и портала.

Корисник информатичких ресурса дужан је да поштује и следећа правила безбедног и примереног коришћења информатичких ресурса, 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 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 („излогује“), односно закључа радну станицу (CTRL+ALT+DEL+LOCK или WINDOWS L);
7. користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење Одељења за одржавање и развој рачунарско-информатичког система, а на основу образложеног предлога непосредног руководиоца;
8. захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
9. обезбеди сигурност података у складу са важећим прописима;
10. приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
11. не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
12. не сме да на радној станици складишти садржај који не служи у пословне сврхе;
13. израђује заштитне копије (backup) података у складу са прописаним процедурама;
14. користи Internet и Internet e-mail сервис у Библиотеци у складу са прописаним процедурама;
15. прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, upgrade firmware, покретање антивирусног програма и сл.) обављају у утврђено време;
16. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
17. 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.
18. не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

Безбедоносни профил корисника информатичких ресурса

Члан 10.

У зависности од описа задатака и послова радног места на које је распоређен, корисник информатичких ресурса, на предлог непосредног руководиоца, стиче одређена права приступа ИКТ систему Библиотеке.

Администраторска овлашћења могу добити само лица која су задужена за одржавање информатичких ресурса у Библиотеци, уз претходну сагласност руководиоца Одељења за одржавање и развој рачунарско-информатичког система

Креирање лозинке

Члан 11.

Лозинка мора да садржи минимум седам 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 корисник информатичких ресурса посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Корисник информатичких ресурса дужан је да мења лозинку најмање једном у три месеца.

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

Употреба корисничког налога

Члан 12.

Кориснички налог може да употребљава само корисник информатичких ресурса коме је исти издат.

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору у случају подешавања радне станице.

Корисник информатичких ресурса је непосредно одговоран за активности које су реализоване на основу његовог корисничког налога.

Кориснички налози са администраторским овлашћењима користе се само за потребе неопходних интервенција којима се обезбеђује несметан рад информатичких ресурса (у даљем тексту: информатичке интервенције).

Употреба администраторског налога

Члан 13.

Администраторски налози свих пословних апликација, сервера база података и системских апликација за управљање мрежном опремом и уређајима за складиштење података чувају се у фајлу који је заштићен, криптован и доступан само запосленима у Одељењу за одржавање и развој рачунарско-информатичког система и Заменику управника - руководиоцу Сектора Виртуелне библиотеке Србије.

Право коришћења администраторског налога имају само администратори за потребе информатичких интервенција који по потреби врше промену административних налога.

Поступци у случајевима сигурносних инцидената

Члан 14.

Корисник информатичких ресурса дужан је да, без одлагања, пријави непосредном руководиоцу свако уочавање или сумњу о наступању инцидента којим се угрожава сигурност ИКТ система.

Информацију о инциденту руководилац из става 1. овог члана дужан је да одмах проследи администратору, као и Одељењу за одржавање и развој рачунарско-информатичког система.

По пријави инцидента мора се поступати адекватно и ефикасно, а по хитном поступку у случајевима:

1. нарушавања поверљивости информација,
2. откривања вируса или грешака у функционисању апликација,
3. вишеструких покушаја неауторизованог приступа,
4. системских падова и престанка рада сервиса.

Одељења за одржавање и развој рачунарско-информатичког система је дужно да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести надлежни орган, у складу са законом којим се уређује информациона безбедност.

Заштита од малициозног софтвера

Члан 15.

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.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена:

1. лиценцираног софтвера, односно забрана коришћења неауторизованог софтвера;
2. правила за заштиту од ризика приликом преузимања фајлова из екстерних извора (података, апликација и сл.)

Приликом преузимања фајлова из става 1. тачка 2. овог члана преносиви медији пре коришћења морају бити проверени на присуство вируса.

Ако се утврди да је 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.

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.

Сигурност електронске поште

Члан 16.

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

1. електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;
2. забрањено је коришћење електронске поште у приватне сврхе;
3. не смеју се користити приватни налози електронске поште у пословне сврхе;
4. програми који користе сервисе електронске поште морају се искључити када се рачунар не користи;

Поступање са преносивим медијима

Члан 17.

Преносиви медији који садрже податке морају да буду прописно обележени и пописани и да се чувају у заштићеној библиотеци магнетних или електронских медија.

У случају брисања података који се налазе на преносивим медијима, потребно је обезбедити њихово неповратно брисање.

Преносиви медији из става 1. овог члана, пре стављања ван употребе, морају бити физички уништени.

Физичка сигурност информатичких ресурса

Члан 18.

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

1. сервери, сторици (storage) и комуникационо чвориште у седишту Библиотеке морају бити смештени у посебној просторији (сервер сала) која испуњава стандарде противпожарне заштите и поседује редундантно напајање електричном струјом и адекватну климатизацију;
2. сервери, сторици (storage) и комуникационо чвориште у службама морају бити смештени у адекватним просторијама, у којима је забрањен приступ незапосленим лицима;
3. приступ сервер сали, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење руководиоца Одељења за одржавање и развој рачунарско-информатичког система;

4. радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;
5. просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
6. штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;
7. медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

Приступ ИКТ систему Библиотеке

Члан 19.

Приступ свим компонентама ИКТ система мора бити аутентификован.

Инсталација и одржавање софтвера

Члан 20.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужени су администратори, који су дужни да поступају у складу са прописаним процедурама и упутствима.

Одељења за одржавање и развој рачунарско-информатичког система обезбеђује запосленом, односно радно ангажованом лицу, коришћење радне станице (десктоп или лап-топ) са преинсталираним и правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачки програми (драјвери), пословно и развојно окружење, софтвер за вирусну заштиту, разне помоћне апликације), који је типски за све радне станице и који представља минимум потребан за обављање стандардних послова.

Администратор врши оцену конзистентности траженог софтвера са постојећим инсталираним софтверима на предметној радној станици и уколико оцени да тражени софтвер неће угрозити или ометати рад, инсталираће захтевани софтвер.

Основна подешавања из става 2. овог члана су:

1. додељивање имена и TCP/IP адреса радној станици и њено придруживање домену или радној групи;
2. подешавање mail-клијента;
3. подешавање Web-претраживача (TCP/IP-адреса прокси сервера);
4. инсталација антивирусног софтвера одобреног од стране Одељења за одржавање и развој рачунарско-информатичког система,
5. инсталација лиценцираног апликативног софтвера који одређене унутрашње јединице Библиотеке користе у свом раду.

У случају да је кориснику потребно да се изврши инсталација одређеног специфичног софтвера на радној станици, непосредни руководилац подноси захтев електронским путем Одељењу за одржавање и развој рачунарско-информатичког система, односно руководиоцу наведеног одељења.

Корисник информатичких ресурса дужан је да сваки проблем у функционисању оперативног система, mail-клијента, Web-претраживача, пословног софтвера (MS Office

ili Open Office) и апликативног софтвера, пријави непосредном руководиоцу, који ову информацију прослеђује електронским путем Одељењу за одржавање и развој рачунарско-информатичког система, односно руководиоцу наведеног одељења.

Проблем у функционисању антивирусног и антиспајвер софтвера мора се пријавити без одлагања.

Администратор је дужан да проблеме из става 6. и 7. овог члана отклони у најкраћем могућем року на локацији корисника, даљинском конекцијом ка радној станици, одласком на место где је настао проблем или доношењем радне станице у Одељење за одржавање и развој рачунарско-информатичког система.

Бежичне мреже (WiFi)

Član 21.

За бежичну мрежу и њено одржавање, као и начин безбедног приступа задужен је AMPEC – Академска мрежа Србије (***eduroam®*** *– **edu**cation **roam**ing).*

Обавезе Корисника ИКТ услуга које Библиотека нуди

Члан 22.

Корисници ИКТ услуга су дужни да се придржавају прописаних правила и процедура садржаних у општим актима Библиотеке по питању коришћења ИКТ ресурса.

Корисници ИКТ услуга, сваки захтев за коришћење ИКТ услуга и ресурса у библиотеци морају најавити корисничком сервису односно дежурном библиотекару који по потреби консултује Одељења за одржавање и развој рачунарско-информатичког система.

Измена Правилника

Члан 23.

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, извршиће се измена 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.

Члан 24.

Провера ИКТ система

Проверу ИКТ система врши Одељење за одржавање и развој рачунарско-информатичког система.

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.

Библиотека је дужна да проверу ИКТ система врши најмање једном годишње и да о томе сачини извештај.

Садржај извештаја о провери ИКТ система

Члан 25.

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 26.

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

УПРАВНИК
ЛАСЛО БЛАШКОВИЋ

Објављено на огласној табли Библиотеке

28. 03. 2017. године