

На основу одредби члана 2. тачка 15, члана 6, 7 и 8. Закона о информационој безбедности ("Сл. гласник РС", бр. 6/2016 и 94/2017) 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), као и одредби Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја ("Сл. гласник РС", бр.94/2016), члана 59. Статута Библиотеке града Београда бр. 1410 од 15.03.2013. године, Управни одбор Библиотеке града Београда доноси дана 1. 11. 2017. године следећи:

## ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА БИБЛИОТЕКЕ ГРАДА БЕОГРАДА

### I. УВОДНЕ ОДРЕДБЕ

#### Члан 1.

Овим правилником, у складу са Законом о информационој безбедности и Уредбом о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационог система од посебног значаја, 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 Библиотеке града Београда (у даљем тексту: ИКТ систем).

#### Члан 2.

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.) **Оператор** је Библиотека града Београда која у оквиру обављања своје делатности, односно за обављање послова из своје надлежности, користи ИКТ систем;
- 4.) **Корисник ИКТ система** је запослени у Библиотеци града Београда и сваки други корисник ресурса ИКТ система;
- 5.) **Надлежни субјект ИКТ система** је организациона јединица у Библиотеци града Београда у чијој су надлежности послови планирања развоја, одржавања и функционисања рачунарско-комуникационе инфраструктуре и развој информационих технологија.
- 3.) **Интегритет** је очуваност изворног садржаја и комплетности податка;
- 4.) **Расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
- 5.) **Тајност** је обезбеђивање доступности информација само овлашћеним корисницима информатичких ресурса, као и немогућност приступа информацијама лицима која немају таква овлашћења;
- 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.) **Администраторско овлашћење** је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;
- 14.) **Кориснички налог** јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно овлашћењакорисника);
- 15.) **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.
- 16.) **VPN (Virtual Private Network)**-је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају

- заштићену комуникацију;
- 17.) **Backup** је резервна копија података;
  - 18.) **Download** је трансфер података са централног рачунара или web презентације на локални рачунар;
  - 19.) **Freeware** је бесплатан софтвер;
  - 20.) **Opensource** софтвер отвореног кода;
  - 21.) **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;
  - 22.) **USB** или флеш меморија је спољшњи медијум за складиштење података;
  - 23.) **CD-ROM** (Compact disk - read only memory) се користи као медијум за снимање података;
  - 24.) **DVD** је оптички диск високог капацитета који се користи као медијум за складиштење података;

### Члан 3.

#### 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.

### Члан 4.

Мере прописане овим правилником се односе на све организационе јединице у мрежи Библиотеке града Београда, на све кориснике информатичких ресурса Библиотеке града Београда.

Непоштовање одредби овог правилника повлачи дисциплинску одговорност корисника информатичких ресурса Библиотеке града Београда.

### Члан 5.

За обављање послова из области безбедности ИКТ система, праћење примене овог правилника, надлежно је Одељење за развој дигиталне библиотеке и информатичку подршку (у даљем тексту: Надлежни субјект ИКТ система).

Под пословима из области безбедности ИКТ система сматрају се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност;
- послови управљања 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, 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.

## **II. МЕРЕ ЗАШТИТЕ**

### **Члан 6.**

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

Мерама заштите штите се податоци садржани у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не сме бити компромитован.

### **1. Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених**

#### **Члан 7.**

Запослени-корисници ресурса ИКТ система су одговорни да у оквиру обављања послова из своје надлежности штите ресурсе ИКТ система.

За контролу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система надлежни су запослени у Одељењу за развој дигиталне библиотеке и информатичке подршке (надлежни субјекти ИКТ система)

За надзор над обављањем послова у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система надлежан је помоћник директора за библиотечку делатност.

У случају инцидента надлежни субјекти ИКТ система обавештавају директора који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

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

#### **Члан 8.**

Нерегистровани корисници, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ Интернету, имејлу, веб-сајту.

Запослени као и лица која по било ком правном основу обављају послове за БГБ, корисници ресурса ИКТ система, могу путем мобилних уређаја или рачунара који су у

власништву БГБ и који су подешени од стране надлежног субјекта ИКТ система, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њиховог описа посла - надлежности.

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

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

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

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

#### **Члан 9.**

Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен, осим ако је уређај у власништву Библиотеке града Београда оштећен и није обезбеђена замена.

Сагласност на коришћење приватног уређаја у случају из става 1. овог члана даје надлежни субјект ИКТ система.

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

#### **Члан 10.**

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

Приватни уређаји са којих се може приступати ресурсима ИКТ система могу се користити само за обављање послова у надлежности корисника ИКТ система и то само у периоду када није могуће користити уређај у власништву БГБ-а.

Надлежни субјект ИКТ система је дужан да пре предаје уређаја овлашћеном сервису, уради back-up 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 11.**

ИКТ системом управља надлежни субјект ИКТ система, запослени у складу са важећом систематизацијом радних места.

Запослени у Одељењу за развој дигиталне библиотеке и информатичке подршке су дужни да сваког новозапосленог-корисника ИКТ ресурса упознају са одговорностима и правилима коришћења ИКТ ресурса Библиотеке града Београда, да упознају са правилима

коришћења ресурса ИКТ система, као и да воде евиденцију о изјавама новозапослених корисника да су упознати са правилима коришћења ИКТ ресурса.

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

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

##### **Члан 12.**

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

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

Непосредни руководиоца запосленог-корисника коме престане радни однос/радно ангажовање или дође до промене радног места, је дужан да пријави промену надлежној служби за ИКТ систем.

Корисник ИКТ ресурса, након престанка радног ангажовања по било ком основу у Библиотеци, не сме да открива податке који су од значаја за информациону безбедност ИКТ система Библиотеке.

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

##### **Члан 13.**

Информациона добра Библиотеке града Београда су сви ресурси који садрже пословне информације Библиотеке града Београда, 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.

О информационим добрима води се посебна евиденција.

Евиденцију из става 1. овог члана води унутрашња организациона јединица Одељења за развој дигиталне библиотеке и информатичку подршку и Одељење за рачуноводствене послове у папирној или електронској форми.

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

#### **Члан 14.**

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

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 15.**

Евиденцију носача на којима су снимљени подаци, води Одељење за развој дигиталне библиотеке и информатичку подршку 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 Библиотеке града Београда 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 16.**

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

Запослени као и сваки корисник ИКТ ресурса Библиотеке је дужан да поштује 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 града Београда и да могу бити предмет надгледања и прегледања;
- 3.) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
- 4.) безбедно чува своје лозинке, односно да их не одаје другим лицима;
- 5.) мења лозинке сагласно утврђеним правилима;

- 6.) пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу
- 7.) захтев за инсталацију софтвера или хардвера подноси у писаној форми;
- 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 складу са прописаним процедурама у Библиотеци града Београда;
- 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 17.**

Право приступа имају само запослени, односно корисници који имају администраторске и 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.

Искључиво запослени у Одељењу за развој дигиталне библиотеке и информатичку подршку (администратори/надлежни субјекат ИКТ система) имају приступ администраторском налогу и налогу за управљање базом података.

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 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 ИКТ система 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 18.

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира по матрици име.презиме, латиничним писмом без употребе слова: ђ, ж, љ, њ, ћ, ч, ц, ш.

Уместо ових слова користити слова из табеле:

Ћирилична слова	Латинична слова
ђ	dj
ж	z
љ	lj
њ	nj
ћ, ч	c
ш	S
ц	dz

Лозинка мора да садржи минимум шест до 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 ИКТ система посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Запослени-корисник дужан је да мења лозинку у складу са потребама.

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

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

## 11. Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

### Члан 19.

Приступ ресурсима ИКТ система Библиотеке града Београда не захтева посебну криптозаштиту.

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

**Члан 20.**

Простор у коме се налазе рачунари за вођење база података и централни рачунар (сервер), мрежна или комуникациона опрема ИКТ система, организује са као видљиво означен и контролисан простор који је обезбеђен механичком бравом.

Евиденцију о уласку у ову зону води надлежни субјект ИКТ система.

**Члан 21.**

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само запосленима ИКТ систему.

Осим лица из става 1. овог члана, приступ просторији у којој се налази ИКТ опрема, могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу начелника Одељења.

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

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

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

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.

У случају изношења опреме из просторије из става 1. овог члана ради селидбе или сервисирања, неопходно је одобрење начелника Одељења који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења начелника Одељења, потребно је сачинити записник у коме се наводи назив, тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Уговором са сервисером обавезно се дефинише обавеза заштите података који се налазе на медијима који су део ИКТ система.

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

**Члан 22.**

Запослени у Одељењу за развој дигиталне библиотеке и информатичку подршку воде рачуна о заштити средстава ИКТ система од губитка, оштећења, крађе или другог облика угрожавања безбедности.

У циљу заштите средстава ИКТ система води се рачуна о постављању средстава на безбедна места, елиминише непотребан приступ у простор у коме се налазе, врши редовне провере заштићености средстава од крађе, пожара и других претњи и прате се услови околине (температура, влажност и др.) који би могли негативно да утичу на рад средстава.

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

##### **Члан 23.**

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система, у складу са тим, планирају, односно предлажу начелнику 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 24.**

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 тачно одређено време врши допуна антивирусних дефиниција.

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.

## Члан 25.

У циљу заштите, односно упада у ИКТ систем са интернета запослени у Одељењу за развој дигиталне библиотеке и информатичку подршку су дужни да одржавају систем за спречавање упада.

Сви корисници ИКТ система који користе интернет у Библиотеци морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар који се прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врше запослени у Одељењу за развој дигиталне библиотеке и информатичку подршку.

Приликом коришћења интернета треба избегавати сумњиве WEB странице, с обзиром да то може проузроковати проблеме - не приметно инсталирање шпијунских програма и слично.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави запосленима у Одељењу за развој дигиталне библиотеке и информатичку подршку.

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 26.**

Базе података обавезно се архивирају на преносиве медије (CDROM, DVD, USB, екстерни хард диск), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

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

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

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

Недељно копирање-архивирање врши се последњег радног дана у недељи, до 20 часова, у онолико недељних примерака колико има последњих радних дана у месецу.

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

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 Библиотеке града Београда.

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

Дневне, недељне и месечне копије-архиве се чувају у просторији која је 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 седишту Библиотеке града Београда.

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 27.**

О активностима администратора и запослених-корисника воде се дневници активности.

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. 20. овог правилника.

## **18. Обезбеђивање интегритета софтвера и оперативних система**

### **Члан 28.**

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Библиотеке града Београда, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само запослени из Одељења за развој дигиталне библиотеке и информатичку подршку 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 безбедносних слабости ИКТ система**

### **Члан 29.**

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

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, надлежни субјект ИКТ система је дужан 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 30.**

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених.

Надлежни субјект ИКТ система одредиће време обављања ревизије у зависности од врсте послова и радних задатака корисника ИКТ система.

## **21. Заштита података у комуникационим мрежама укључујући уређаје и водове**

### **Члан 31.**

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, router, firewall) се мора налазити у закључаном rack орману.

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

Бежична мрежа коју могу да користе посетиоци објеката Библиотеке, мора бити одвојена од интерне мреже коју користе запослени и кроз коју се врши размена службених података.

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

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

### **Члан 32.**

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

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

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

### **Члан 33.**

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

Начелник Одељења је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система надлежни субјекти ИКТ система воде 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 34.**

За потребе тестирања ИКТ система односно делова система надлежни субјекат ИКТ система 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 35.**

Трећа лица-пужаоци 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.

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

У случају непоштовања уговорених обавеза, надлежни субјект ИКТ система је дужан да одмах обавести директора Библиотеке, ради предузимања мера у циљу откањања неправилности.

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

#### **Члан 36.**

Библиотека града Београда нема склопљен уговор са трећим лицима за пружање услуга информационе безбедности

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

### **Члан 37.**

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести надлежне субјекте ИКТ система у Библиотеци.

По пријему пријаве надлежни субјекти ИКТ система су дужани да одмах обавесте помоћника директора и предузму 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), Начелник Одељења за развој дигиталне библиотеке и информатичку подршку, је дужан да обавести надлежни орган дефинисан овом уредбом.

Начелник Одељења за развој дигиталне библиотеке и информатичку подршку 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 38.**

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Библиотеке надлежни субјекти ИКТ система су дужани да у најкраћем року пренесу делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Надлежна служба ИКТ система формира спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама, и то у три примерка, од којих се један налази код службе ИКТ система, други код запосленог надлежног за послове одбране и ванредне ситуације а трећи примерак код директора Библиотеке.

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

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

## **III. ИЗМЕНА ПРАВИЛНИКА О БЕЗБЕДНОСТИ**

### **Члан 39.**

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, Начелник Одељења за

развој дигиталне библиотеке и информатичку подршку је дужан да обавести директора Библиотеке, како би се могло приступити 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.

#### **IV. ПРОВЕРА ИКТ СИСТЕМА**

##### **Члан 40.**

Проверу ИКТ система врши надлежни субјект ИКТ система.

Провера ИКТ система се тако што се:

- 1.) Проверава усклађеност овог правилника, узимајући у обзир и акта на који се врши упућивање, са прописаним условима, односно проверава да ли су Правилником адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;
- 2.) Проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима;
- 3.) Провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система.

О извршеној провери сачињава се извештај, који се доставља начелнику Одељења.

#### **V. САДРЖАЈ ИЗВЕШТАЈА О ПРОВЕРИ ИКТ СИСТЕМА**

##### **Члан 41.**

О извршеној провери сачињава се извештај, који се доставља начелнику Одељења. 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.

## **VI. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ**

### **Члан 42.**

Овај правилник ступа на снагу у року од осам дана од дана усвајања.

**Управни одбор  
Библиотеке града Београда  
Председник**

*Мирољуб Стојановић*

