УНИВЕРЗИТЕТСКИ
КЛИНИЧКИ ЦЕНТАР НИШ
БРОЈ: 31167/12а
ДАТУМ: 18.10.2022.год.

На основу члана 8. Закона о информационој безбедности („Сл. гласник РС“, бр. 6/16, 94/17, 77/19), 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. 94/16) и члана 27. статута Универзитетског клиничког центра Ниш, Управни одбор Универзитетског клиничког центра Ниш на седници одржаној дана 18.10.2022. доноси

П Р А В И Л Н И К
о информационо-комуникационој безбедности Универзитетског клиничког центра Ниш

I Уводне одредбе

Члан 1.

Овим правилником се, 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-комуникационих система од посебног значаја утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и у вези са безбедношћу и ресурсима информационо-комуникационог система УКЦ Ниш (у даљем тексту: ИКТ систем).

Члан 2.

Мере прописане овим правилником се односе на све организационе јединице УКЦ Ниш и на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе УКЦ Ниш.

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог корисника информатичких ресурса УКЦ Ниш.

За праћење примене овог правилника обавезује се руководилац послова информационих система и технологија - Одељења информационих система, технологија и телекомоникационих система - Службе за техничке и друге сличне послове, УКЦ Ниш.

Члан 3.

Поједини термини информационог система, технологија и телекомуникационих система (ИКТ систем УКЦ Ниш), у смислу овог правилника, представљају технолошко-организациону целину која обухвата следећа значења:

1. информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата:
   - електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
   - 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;
   - податке који се воде, похрањују, обрађују, претражују или преносе помоћу средстава из претходне две подтачке у сврху њиховог рада, употребе, заштите или одржавања;
   - организациону структуру путем које се управља ИКТ системом;
   - све типове системског и апликативног софтвера и сифтверске развојне алате;
2. оператор ИКТ система је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3. информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ систем 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;
4. тајност је својство које значи да податак није доступан неовлашћеним лицима;
5. интегритет значи очуваност изворног садржаја и комплетности податка;
6. расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
7. 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;
8. непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
9. ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
10. 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;
11. инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
12. мере заштите ИКТ система су техничке и организационе мере за управљање безбедоносним ризицима ИКТ система;
13. тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
14. ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
15. компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
16. криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
17. криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
18. криптографски производ је софтвер или уређај путем кога се врши криптозаштита;
19. криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
20. безбедоносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
21. информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
22. VPN (Vfrtual Private Netyyork) је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
23. MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
24. Backup је резервна копија података;
25. Download је трансфер података са централног рачунара или web презентације на локални рачунар;
26. UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
27. Freeware је бесплатан софтвер;
28. Opensource је софтвер отвореног кода;
29. 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;

30. USB или флеш меморија је спољашни медијум за складиштење података;
31. CD-ROM (Compact Disk Read - Only Memory) се користи као медијум за читање података;
32. DVD-RW (Digital Versatile Disk - Rewriteable) је оптички диск високог капацитета који се користи као медијум за складиштење и/или читање података;

II Мере заштите

Члан 4.

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

1. Правилник о организацији и систематизацији послова Универзитетског клиничког центра Ниш, којим се остварује управљање ИКТ системом и безбедношћу у оквиру УКЦ Ниш.

Члан 5.

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 УКЦ Ниш, надлежан је руководилац послова информационих система и технологија, Службе за техничке и друге сличне послове, УКЦ Ниш.

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност,
- послови 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 УКЦ Ниш, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе,
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу,
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента руководилац послова информационих система и технологија, обавештава руководиоца Службе за техничке и друге сличне послове и директора УКЦ Ниш, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Запослени - корисници ресурса ИКТ система, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ Интернету, али не и деловима мреже кроз које се обавља службена комуникација.

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 важећим Правилником о организацији и систематизацији послова Универзитетског клиничког центра Ниш.

Руководилац послова информационих система и технологија је дужан да сваког новозапосленог - корисника ИКТ система ресурса УКЦ Ниш, упозна са одговормостима и правилима коришћења ресурса ИКТ система УКЦ Ниш, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденцију о изјавама новозапослених - корисника да су упознати са правилима коришћења ресурса ИКТ система.

Свако коришћење ресурса ИКТ система УКЦ Ниш 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 код оператора ИКТ система

Члан 9.

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

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

О престанку радног односа или радног ангажовања, као и промени радног места, начелник одељења за правне, кадровске и административне послове, а у сарадњи са непосредним руководиоцем, је дужан да обавести руководиоца послова информационих система и технологија ради укидања, односно измену приступних привилегија тог запосленог - корисника.

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

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

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

Евиденцију о информационим добрима води Одељење информационих система, технологија и телекомуникационих система, у папирној или електронској форми, уз помоћ запосленог у одсеку задуженом за материјално књиговодство.

Предмети заштите су:

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

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

Члан 11.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебним прописима (Законом о слободном приступу информацијамз од јавног значаја - „Сл. Гласник РС", бр. 120/04, 54/07, 104/09, 36/10, 105/21, Законом о заштити података о личности - „Сл. Гласник РС", бр. 87/18, Законом о тајности података - „Сл. Гласник РС", 104/09),

као и Уредбаом о начину и поступку означавања тајности података, односно докумената - „Сл. Гласник РС", бр. 8/11).

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

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

7. Заштита носача података

Члан 12.

Руководилац послова информационих система и технологија 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 руководиоца,
- подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених - корисника у Одељењу информационих система, технологија и телекомуникационих система.

Евиденцију носача на којима су снимљени подаци, води Одељење информационих система, технологија и телекомуникационих система 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, руководилац послова информационих система и технологија ће одредити одговорну особу и начин транспорта.

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

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

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

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

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

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

Запослени - корисник дужан је да поштује и следећа 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 процесуирају у оквиру информатичких ресурса власништво УКЦ Ниш и да могу бити предмет надгледања и прегледања;
3. поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. безбедно чува своје лозинке, односно да их не одаје другим лицима;
5. мења лозинке сагласно утврђеним правилима;
6. пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну

станицу;

7. захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8. обезбеди сигурност података у складу са важећим прописима;
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 УКЦ Ниш у складу са прописаним процедурама;
14. прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање 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 шифровање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ сустему;
17. не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 14.

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

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

Администраторски налог могу да користе само запослени на пословима у Одељењу информационих система, технологија и телекомуникационих система.

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

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

Лозинка мора да садржи минимум осам карактера комбинованих од слова, цифара и специјалних знакова.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке.

Ако запослени - корисник посумња да је друго лице открило његову лозинку дужан је да

исту одмах измени.

Запослени - корисник дужан је да мења лозинку најмање једном у шест месеци.

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

Неовлашћено уступање крисничког налога другом лицу подлеже дисциплинској одговорности.

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

Члан 16.

Приступ ресурсима ИКТ система УКЦ Ниш не захтева посебну криптозаштиту.

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

Члан 17.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује се као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом.

Простор мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода и у њему треба да буде одговарајућа температура (климатизован прострр).

Контролу о уласку у ову зону врши руководилац послова информационих система и технологија.

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

Члан 18.

Улаз у просторију у којој се налази опрема ИКТ система, дозвољен је само руководиоцу послова информационих система и технологија и администраторима у Одељењу информационих система, технологија и телекомуникационих система.

Осим администратора система, приступ административној зони мбгу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу руководиоца Службе за техничке и друге сличне послове и уз присуство руководиоца послова информационих система и технологија.

Приступ административној зони може имати и запослени/а на пословима одржавања хигијене уз присуство запосленог у одељењу информационих система, технологија и телекомуникационих система.

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

Прозори и врата на овој просторији морају увек бити затворени.

Сервери и активна мрежна опрема (swltch, modem, router, firewali), морају стално бити прикључени на уређаје за непрекидно напајање - UPS.

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

Опрема ИКТ система из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења било ког непосредног руководиоца.

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

Ако се опрема износи ради сервисирања, поред одобрења руководиоца Службе за техничке и друге сличне послове, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервиса, име и презиме овлашћеног лица/сервисера задуженог

сервиса.

Уговором са сервисом или сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ресурса ИКТ система УКЦ Ниш.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Запослени на пословима ИКТ система 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 руководиоцу послова информационих система и технологија 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 срфтвера.

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, електронском поштом (e-mail), 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, једном дневно, врши допуна антивирусних дефиниција.

Сваког петка у недељи је потребно оставити укључене и закључане рачунаре ради скенирања на вирусе.

Забрањено је заустављање искључивање антивирусног софтвера током скенирања преносивих медија.

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

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

У циљу заштите, односно упада у ИКТ систем УКЦ Ниш са интернета, руководилац послова информационих система и технологија је дужан да одржава систем за спречавање упада.

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

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему руководилац послова информационих система и технологија може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени - корисник прикључује на интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врше запослени у одељењу информационих послова.

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

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави одељењу информационих система, технологија и телекомуникационих система.

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" WEB страницама које садрже недоличан садржај, као и самбвољно 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 одговајрајући начин;
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, 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 видеостриминг и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

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

16. Заштита од губитка података

Члан 21.

Базе података обавезно се архивирају на хард диску (HD) једном дневно или једном недељно, а на преносиве медије (CD-ROM, DVD, USB, „strimer" трака, екстерни хард диск) најмање једном недељно, месечно и годишње, за потребе обнове базе података.

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

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

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

Недељно копирање - архивирање врши се последњег радног дана у недељи, после 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, после 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 органа државне управе („Сл. Гласник РС", бр. 10/93, 14/93-испр., 67/16, 3/17).

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, месечне и годишње копије-архиве података се чувају у просторији која је физички обезбеђена и у складу је са мерама заштите против-пожарног обезбеђења.

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 при процедури за израду копија-архива осталих података у ИКТ систему, у складу са чланом 20. овог правилника.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

Инсталацију и подешавање софтвера могу да врше само запослени у одељењу информационих система, технологија и телекомуникационих система, 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 злоупотрвбе техничких безбедоносних слабости ИКТ система

Члан 24.

Руководилац послова информационих система и технологија 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, руководилац послова информационих система и технологија 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 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 руководиоца Службе за техничке и друге сличне послове

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.

Запослени у одељењу информационих система, технологија и телекомуникационих система су дужни да стално врше контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коју могу да користе посетиоци и/или корисници свих објеката у саставу УКЦ Ниш, мора бити одвојена од интерне мреже коју користе корисници - запослени у УКЦ Ниш, а

кроз коју се врши размена службених података.

Та мрежа треба да буде посебно означена (ССИД).

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

Члан 27.

Размена података са другим државним органима врши се према закону и подзаконским актима којима се предвиђа ова врста размене података.

Протокол размене поменутих података уређен је од стране надлежних органа којима се подаци достављају.

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 УКЦ Ниш, биће дефинисан уговором који ће бити склопљен са тим лицима.

Одељење информационих система, технологија и телекомуникационих система је задужено 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, руководилац послова информационих система и технологија води документацију.

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

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

Члан 29.

Приликом тестирања система у раду са подацима који су означени ознаком тајности, односно службености као информационих послова као поверљиви подаци, или су лични подаци, руководилац послова информационих система и технологија одговара за податке у складу са прописима којима је дефинисана употреба и заштита такве врсте података).

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

Члан 30.

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

Одељење информационих система, технологија и телекомуникационих система је одговорно за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

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

Члан 31.

УКЦ Ниш нема склопљен уговор са трећим лицима за пружање услуга информационе безбедности.

27. Превенција и реаговање на безбедоносне инциденте, што подразумева адекватну размену информација о безбедоносним 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 одељење информационих система, технологија и телекомуникационих система.

По пријему пријаве запосдени у одељењу информационих система, технологија и телекомуникационих система је дужан/а да одмах обавести руководилац послова информационих система и технологија, а он руководиоца Службе за техничке и друге сличне послове и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку обавештавања и инцидентима у информационо-комуникационим системима од посебног значаја, („Сл. Гласник РС", бр. 11/2020), руководилац послова информационих система и технологија је дужан да поред руководиоца Службе за техничке и друге сличне послове обавести надлежни орган дефинисан овом уредбом.

Руководилац послова информационих система и технологија води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

У случају ванредних околнокти, које могу да доведу до измештања ИКТ систем из зграде УКЦ Ниш, одељење информационих система, технологија и телекомуникационих система је дужно да у најкраћем року пренесе делове ИКТ система (или обезбеди функционисање редудантних компоненти на резервној локацији уколико постоје) неопходних за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама, уз потпуну сарадњу одељења безбедности, одбране и ванредних ситуација, службе за техничке и друге сличне послове УКЦНиш.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђују руководилац послова информационих система и технологија у сарадњи са начелником одељења безбедности, одбране и ванредних ситуација и то у три примерка, од којих се један налази код њега/е, други код запосленог надлежног за послове безбедности, одбране и ванредних ситуација, а трећи примерак код руководиоца службе за техничке и друге сличне послове.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервној локацију, коју одреди руководиоц службе за техничке и друге сличне послове.

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 информавионо-информатичкој безбедности

Члан 34.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информационо-информатичку безбедност, руководилац послова информационих система и технологија је дужан да обавести руководиоца Службе за техничке и друге сличне послове, како би он могао да приступи измени 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 одељење информационих система, технологија и телекомуникационих система.

О извршеној провери сачињава се извештај, који се доставља руководиоцу службе за техничке и друге сличне послове.

V Садржај извештаја о провери ИКТ система

Члан 36.

Извештај о провери ИКТ система садржи:

1. назив оператора ИКТ система који се проверава;
2. време провере;
3. подаци о лицима која су вршила проверу;
4. извештај о спроведеним радњама провере;
5. закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;
6. закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
7. закључке по питању ревентуалних безбедоносних 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 37.

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

ПРЕДСЕДНИК
УПРАВНОГ ОДБОРА,

Проф. др Ивана Милошевић

Овај Правилник је објављен на огласној табли Универзитетског клиничког центра Ниш дана 8.10. 2022. године.