Република Србија
Аутономна покрајина Војводина
Специјална болница за психијатријске болести
„др Славољуб Бакаловић“ Вршац
Број: 01-12/33
Датум: 21.10.2019.године

На основу члана 8. Закона о информационој безбедности ("Службени гласник РС", број 6/16), чланова 1-8 Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја ("Службени гласник РС", број 94/16 од 24.11.2016. године), Управни одбор Специјалне болнице за психијатријске болести „ др Славољуб Бакаловић“ Вршцу на својој деветој седници дана 21.10.2019. године доноси:

ПРАВИЛНИК О ПРОЦЕДУРАМА БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНИХ СИСТЕМА У СПЕЦИЈАЛНОЈ БОЛНИЦИ ЗА ПСИХИЈАТРИЈСКЛЕ БОЛЕСТИ „ Др СЛАВОЉУБ БАКАЛОВИЋ“ ВРШАЦ

Члан 1.

Овим правилником ближе се дефинишу мере заштите и дефинисање информационо-комуникационих система (у даљем тексту ИКТ систем) у Специјалној болници за психијатријске болести „ др Славољуб Бакаловић“ Вршац (у даљем тексту: Болница), а нарочито принципи, начин и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информационо-комуникационих система.

Члан 2.

Циљеви доношења овог Правилника су:

- допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
- минимизација безбедносних инцидената;
- допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистентне контроле свих компонената ИКТ система.

Члан 3.

Овај Правилник је обавезујући за све унутрашње организационе јединице Болнице и за све кориснике ИКТ ресурса, као и за сва трећа лица која користе ИКТ ресурсе Болнице.
За праћење примене овог Правилника надлежан је Руководилац послова информационих система и технолногија (у даљем тексту: ИКТ Руководилац) у одсеку за медицинску информатику и статистику (у даље тексту:ИКТ одсек).

Члан 4.

Поједини појмови у смислу овог правилника имају следеће значење:

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 да се у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
- податке који се потхрањују, обрађују, претражују или преносе у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКТ системом;

2. Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;
3. Тајност је својство које значи да податак није доступан неовлашћеним лицима;
4. Интегритет значи очуваност изворног садржаја и комплетности података;
5. Расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
6. Аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
7. Непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
8. Ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
9. Управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
10. Инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
11. Мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
12. Тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одговарајућим степеном тајности;
13. Криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
14. Информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
15. Администраторски налог - омогућава приступ и администрацију икт опреме само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога.
16. Backup је резервна копија података;
17. Download је трансфер података са централног рачунара или web презентације на локални рачунар;
18. UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
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 спољни медијум за складиштење података;
23. CD-ROM (Compact disk - read only memory) користи се као медијум за складиштење података;
24. DVD је оптички диск високог капацитета који се користи за складиштење података.

Мере заштите

Члан 5.

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

Члан 6.

Идентификовање ИКТ добара и одређивање одговорности за њихову заштиту

ИКТ систем су сви ресурси који садрже пословне информације Болници у Вршцу, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података, укључујући све електронске записе, рачунарску опрему, мобилни телефони, видео надзор, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију.
Евиденцију о ИКТ добрима води ИКТ Руководилац у електронској форми.

Предмет заштите обухвата:

1. хардверске и софтверске компоненте ИКТ система
2. податке који се обрађују или чувају на ИКТ системима.
3. корисничке налоге и друге податке о корисницима ИКТ система.
4.

Члан 7.

Организациона структура, са утврђеним пословима и одговорностима запослених, којима се остварује управљање информационом безбедношћу у СБПБ у Вршцу

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, надлежаније ИКТ одсек.

Члан 8.

Обезбеђење да лица која користе ИКТ систем и раде у ИКТ одсеку разумеју своју одговорност

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места.
ИКТ Руководилац је дужан да сваког корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса у Болници.

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

Члан 9.
Заштита од ризика који настају при променама послова или престанка радног ангажовања запосленог-корисника ИКТ система

У случају промене послова, односно надлежности корисника-запосленог, ИКТ Руководилаће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева директора болнице.
У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида.

Корисник ИКТ ресурса, након престанка радног ангажовања у болници, не сме да открива податке који су од значаја за информациону безбедност ИКТ система, у супротном подлаже кривичном и дисциплинском одговорношћу.

Члан 10.
Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Приступ ресурсима ИКТ система болнице не захтева посебну криптозаштиту.

За приступ ресурсима ИКТ система који се односе на послове одбране, односно, за које је надлежно министарство прописало коришћење криптозаштите, посебним правилником ће бити дефинисана употреба одговарајућих мера криптозаштите узимајући у обзир осетљивост информација које треба да се штите, пословне процесе који се спроводе, ниво захтеване заштите, имплементацију примењених криптографских техника и управљање криптографским кључевима.

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

Запослени у ИКТ одсеку задужени су за инсталацију потребног софтвера и хардвера за коришћење сертификата.

Запослени-корисници дужни су да чувају своје квалификоване електронске сертификате како не би дошли у посед других лица.

Члан 11.
Класификовање података тако да ниво заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности

Подаци који се налазе у ИКТ систему представљају пословну тајну и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. Гласник РС", бр. 53/2011).

Члан 12.
Безбедност рада на даљину

Нерегистровани корисници, путем приватних мобилних уређаја, лаптопа могу да приступе само оним деловима мреже који су конфигурисани од стране ИКТ одсека тако да

омогућавају приступ интернету, али не и деловима мреже кроз коју се обавља службена комуникација. Евиденцију приватних уређаја са којих ће бити омогућен приступ води запослени из ИКТ одсека.
Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву болнице и који су подешени од стране запослених у ИКТ одсеку, на основу писане сагласности директора болнице, могу да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности.

Запосленом-кориснику забрањена је самостална инсталација програма, подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима.

У случају квара мобилног уређаја, запослени у ИКТ одсекусу дужни да пре предаје уређаја овлашћеном сервису, уради копију података који се налазе на мобилном уређају, а потом их обрише из уређаја и по повратку из сервиса поново врати податке у мобилни уређај.

Члан 13.

Безбедност и Заштита података преносних медија

Директор ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном тајности у складу са Законом о тајности података („Службени гласник РС“, бр. 104/09).
Подаци и документи који се користе у ИКТ систему (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, УСБ, ЦД, ДВД, сториџ систем), само од стране запослених ИКТ одсеку уз одобрење директора Болнице.

Размена података са државним органима, органима локалних самоуправа, правним и физичким лицима се врше у складу са важећим прописима и унапред дефинисаним и потписаним уговорима.

Подаци који су доступна пружаоцима услуга 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.

Носачи информација морају бити прописано обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.У случају истека рокова чувања података који се налазе на носачима, подаци морају бити трајно обрисани, ако то није могуће, такви носачи морају бити физички оштећени односно уништени.

Члан 14.

Ограничење права приступа подацима и средствима за обраду података у ИКТ систему

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има. У случају три неуспеле пријаве, налог се аутоматски блокира. Поново одблокирање налога врши ИКТ руководилац.

Кориснички налог се састоји од корисничког имена и лозинке 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 ИКТ Руководилац у складу са потребама обављања пословних задатака од стране запосленог-корисника.

ИКТ Руководилац који има администраторски налог, има права приступа свим ресурсима ИКТ система у циљу управљања ресурсима ИКТ система и води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева директора болнице.У случају више неуспелих пријава, ИКТ руководилац врши истраживање и обавештава директора болнице.

Члан 15.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Кориснички налог се састоји од корисничког имена и лозинке.
Корисничко име се креира латиничним писмом по матрици (прво слово имена и цело презиме) као једна реч раздвојено једино тачком и без употребе слова ђ, ж, љ, њ, ћ, ч, џ, ш.
Лозинка мора да садржи минимум осам карактера, састављених комбинацијом латиничних великих и малих слова као и бројева. 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 периодицно, иста лозинка не сме да се понавља у временском периоду од годину дана.
Кориснички налог може да се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр. Лична карта са чипом и уписаним сертификатом).

Члан 16.

Правила запосленог-корисника при корисцењу ИКТ ресурса

Запослени-корисник дужан је да поштује и следећа правила безбедног и примерног коришћења ресурса ИКТ система и то да:

1. коришћење ИКТ ресурса искључиво у пословне сврхе;
2. сви подаци који се складиште, преносе или процесирају у оквиру ИКТ ресурса власништво су болнице;
3. обезбеди сигурност података у складу са важећим прописима;
4. чување сопствених лозинка за приступ ИКТ ресурсима, односно да их не одаје другим лицима;
5. мењање лозинке сагласно утврђеним препорукама;
6. након завршетка рада корисник-запослени је дужан да угаси рачунар;
7. удаљавањем са радне станице је дужан закључа радну станицу;
8. захтев за инсталацију новог софтвера и хардвера подноси у писаној форми руководиоцу;
9. забрањено је да инсталира, зауставља, и мења подесавања на софтверу и хардверу

који подешен искључиво стране ИКТ одсека;

10. забрањено је мењање подесавања видео надзора;
11. забрањено је да прикључивање личних рачунара, стампаца, и wифи уредјања на болничку мрежу;
12. забрањено је корисцење интернета ради преузимања великих количина података који проузрукују загушење мреже;
13. забрањено је коришћење интернета за гледање филмова, аудио и видео стриминг, радио, друштвене мреже, ширење деструктивних и опструктивних програма (вируси, тројански коњи, црви и друге врсте малициозних софтвера)
14. приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
15. користи интернет и електронску пошту у складу са прописаним процедурама;
16. Сваки запослени који приступа ИКТ системима је дузан да потпише изјаву о заштити поверљивих података.

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

Члан 17.

Физичка заштита ИКТ опреме

Сервери су смештени у посебној просторији (сервер зона), која испуњава стандарде противпожарне заштите и поседује непрекидно напајање електричном енергијом (УПС) и адекватну климатизацију, антистатичким подом. Приступ самој просторији обезбеђен је механичком бравом и видео надзором.

Приступ серверској соби поред лица која су запослена у ИКТ одсеку, могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система. Евиденцију о уласку води ИКТ Руководилац.

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 (cwитцх, роутер, фиревалл) мора бити обезбеђена и лоцирана на прописаним местима, доступна запосленима у ИКТ одсеку који су дужни да врше контролу целокупне мрежне опреме и благовремено преузима мере у циљу отклањања евентуалних неправилности.

Штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација.

Преносни медији са поверљивим подацима су заштићени од неауторизованог приступа и прегледа.

У случају изношења ИКТ опреме ради сервисирања, и селидбе. Потребно је да се направи записник у коме се наводи назив и тип опреме, серијски број, назив сервисера и кратак опис квара, и одобрење Руководиоца.

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

Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса болнице.

Несправна ИКТ опрема се расходује у складу са важећим законским нормама.

Члан 18.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

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 директору болнице одговарајуће мере.

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

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

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

Члан 19.

Заштита од губитка података

Заштита од губитка података у Болници се обезбеђује се креирањем дневних резервних копија серверских података на екстерном диску који је прописано обележен и чува се на обезбеђеном месту. Подаци са рачунара се два пут месечно копирају, а поједине имају и конфигурисан секундарни хард диск на коме се копирају подаци.

Члан 20.

Обезбеђење интегритета софтвера и оперативних система

У ИКТ систему инсталира се само софтвер за који постоји важећа лиценца, или Freewere и Opensource верзије.Инсталацију и подешавање софтвера врши ИКТ одсек, или треће лице у складу са уговоромо одржавању софтвера под надзором запослених у ИКТ одсеку. 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.

Члан 21.

Превенција и реаговање на безбедносне инциденте

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

Који је дужан да о томе обавести директора болнице и преузме мере у циљу заштите ресурса ИКТ система.

ИКТ Руководилац 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.

Измена правилника
Члан 22.

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, ИКТ Руководилац је дужан да обавести Директора болнице, 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 ресурса ИКТ система.

Провера ИКТ система
Члан 23.

Проверу ИКТ система врши ИКТ Руководилац или запослени у ИКТ одсеку. По потреби могу вршити трећа лице уз сагласност Руководица и одобрење Директора болнице. Провера ће се вршити последњег месеца у години.

Провера се врши тако што се:

1)проверава усклађеност Правилника о безбедности информационо- комуникационих система у Републичком геодетском заводу, са прописаним условима, односно проверава да ли су 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)врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе. архитектуре решења, техничке конфигурације, техничке податке о статусима. записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

О извршеној провери сачињава се извештај који се доставља Директору болнице.

Садржај извештаја о провери ИКТ система
Члан 24.

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;
5. закључке по питању усклађености Правилника о безбедности ИКТ система Болнице 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.

Члан 25.

Обезбеђење да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника- запослених. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност Директора установе.

Члан 26.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли. Овај Правилник биће објављен на интернет страници Болнице.

Правилник је ступио на снагу 24.10.2019. године.

ЗАМЕНИК ПРЕДСЕДНИКА
УПРАВНОГ ОДБОРА
адвокат Драгослав Алексић