Клиника за неурологију и психијатрију
за децу и омладину

Др Суботића старијег 6а, 11000 Београд
ПИБ: 100269185; мат. бр: 07035802
Тел: 011/2658-355; тел/факс 011/2645-064
e-mail: npk.zmaj@gmail.com

На основу члана 33. Статута Клинике за неурологију и психијатрију за децу и омладину, Београд, Управни одбор Клинике, на Првој редовној седници одржаној дана 21.10.2022. године, усвојио је следећу:

Република Србија
Клиника за неурологију и психијатрију
за децу и омладину
Бр. 3472/1
21.10. 2022 године
Београд

О Д Л У К У

Усваја се Правилник о безбедности информационо комуникационих система у Клиници за неурологију и психијатрију за децу и омладину, како је дато у материјалу, који је у прилогу Одлуке и чини њен саставни део.

Председник Управног одбора
Проф. др Предраг Станковић

Република Србија
Клиника за неурологију и психијатрију
за децу и омладину
Бр. 3472/2
21.10. 20 22 године
Београд

На основу члана 8. Закона о информационој безбедности ("Службени гласник РС", број 6/2016, 94/2017 и 77/2019), члана 119. став 1. тачка 1. Закона о здравственој заштити („Службени гласник РС" број 25/19), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја ("Сл. гласник РС", бр. 94/2016) и члана 33. Статута Клинике за неурологију и психијатрију за децу и омладину, Управни одбор Клинике за неурологију и психијатрију за децу и омладину, на Првој редовној седници одржаној дана 21.10.2022. године, доноси

ПРАВИЛНИК
о безбедности информационо - комуникационог система

I. УВОДНЕ ОДРЕДБЕ

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности ("Службени гласник РС", број 6/2016, 94/2017 и 77/2019) и Уредбом о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начин провере информационо-комуникационих система од посебног значаја и садржај извештаја о провери информационо-комуникационог система од посебног значаја ("Сл. гласник РС", бр. 94/2016), 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 Клинике за неурологију и психијатрију за децу и омладину, др Суботића 6а, Београд (у даљем тексту: Клиника).

Члан 2.

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

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

Члан 3.

За праћење примене овог правилника обавезује се лице које обавља послове инфоматичара у Клиници, у складу са Правилником о организацији и систематизацији послова у Клиници (у даљем тексту: Администратор).

Члан 4.

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) **уређаји или групе међусобно повезаних уређаја**, су такви уређаји у оквиру којих се, 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) **тајност** је својство које значи да податак није доступан неовлашћеним лицима;

4) **интегритет** значи очуваност изворног садржаја и комплетности податка;

5) **расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) **аутентичност** је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

7) **непорецивост** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

8) **ризик** значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

9) **управљање ризиком** је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

10) **безбедоносни 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) **тестирање ИКТ система и тестирање делова истог**, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама,

13) **процес тестирања ИКТ система** подразумева процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

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) **безбедносна зона** је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

21) **информациона добра** су сви ресурси који садрже пословне информације, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе који обухватају податке у датотекама и базама података, програмски кôд, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем који обухватају податке у датотекама и базама података, процедуре и слично;

22) **VPN (*Virtual Private Network*)** 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" односносистем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

30) **Мобилни уређаји** су сви преносни електронски уређаји намењени за комуникацију на даљину, и то преносиви рачунари, таблети, мобилни телефони, PDA и сви други мобилни уређаји који садрже податке и имају могућност повезивања на мрежу;

31) **USB или флеш меморија** је спољашњи медијум за складиштење података;

32) **CD - ROM (Compact disk - read only memory)** се користи као медијум за снимање података;

33) **DVD** је оптички диск високог капацитета који се користи као медијум за складиштење података;

34) **Запослени-корисник** је лице које је запослено у Клиници, на неодређено или на одређено време, као и лице које је радно ангажовано по основу уговора ван радног односа, а које има приступ информационим добрима Клинике или користи информациона добра Клинике;

35) **Трајно брисање** подразумева процедуру брисања података на тај начин да се искључује могућност накнадног повраћаја тих података, а у складу са препоруком *NIST 800-88 Revision 1*.

II. МЕРЕ ЗАШТИТЕ

Члан 5.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски код, податке који се чувају, обрађују, претражују или

преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Члан 6.

Мерама заштите ИКТ система се обезбеђује 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.

Члан 7.

Сви запослени и радно ангажовани по основу уговора ван радног односа, којима је додељен приступ поверљивим информацијама, морају потписати споразум о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Члан 8.

Директор Клинике и Администратор су дужни да предузму мере ради спречавања неовлашћеног физичког приступа просторијама, у којима се налазе уређаји, као и спречавање оштећења и ометања информација.

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

Члан 9.

Директор Клинике је дужан да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

Директор Клинике, у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

- обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;

- обезбеди заштиту информација и податка са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама Клинике;

- обезбеди спровођење програма заштите на конзистентан и уједначен начин у свим организационим јединицама Клинике.

Члан 10.

Додељивање администраторских права на приступ врши се на основу одлуке директора Клинике.

Администраторска права на приступ која треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности.

Редовне пословне активности не могу се вршити из администраторских корисничких идентификатора.

Компетенције корисника са администраторским правима на приступ се редовно преиспитују ради провере да ли су у складу са обавезама истог.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора и исто представља непоштовање радне дисциплине.

Члан 11.

Шифре за приступ општим корисничким идентификаторима администратора мењају се променом Администратора.

Члан 12.

Администратор је дужан да се континуирано обучава у циљу унапређења техничког и технолошког знања, а нарочито да континуирано стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, у складу са пословима које обавља.

Клиника је дужна да Администратору обезбеди обуку из става 1. овог члана.

Члан 13.

Сваки запослени-корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности.

Сваки запослени-корисник ИКТ система је дужан да приступа информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информише Администратора о свим сигурносним инцидентима и проблемима.

Члан 14.

Сваком запосленом-кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља.

Запосленом-кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим запосленим-корисницима.

Члан 15.

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 Клинике надлежан је Администратор.

Администратор је дужан да обавештава директора Клинике, односно овлашћено лице о животном циклусу информационих добара.

Члан 16.

Под пословима из области безбедности утврђују се:

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

- послови управљање 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 Клинике, 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 Администратор одмах обавештава директора Клинике, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 17.

Рад на даљину и употреба мобилних уређаја у ИКТ систему је могућ само уз сагласност директора Клинике.

2.1. Рад на даљину

Члан 18.

Обављање послова ван просторија послодавца обухвата:

- Рад на даљину;
- Рад од куће;
- Виртуелно радно окружење.

Такође, рад на даљину у смислу овог Правилника подразумева и случајеве када је запослени и други радно ангажовани обавезан да изврши одређене послове на мрежи Клинике, а налази се ван просторија Клинике.

Рад на даљину може се остварити коришћењем мобилних уређаја, али и уређаја који нису мобилни (на пример, десктоп рачунари). Уређаји који нису мобилни морају имати примењене најмање исте безбедносне мере као и сродни уређаји који се налазе у оквиру мреже, док се за заштиту комуникације морају применити исте мере као и за заштиту комуникације мобилних уређаја.

Члан 19.

Обављање задатих и неопходних послова на даљину уређује се путем Процедуре за VPN приступ информационом систему (у даљем тексту: VPN процедура).

VPN процедура дефинише правила и услове за повезивање на мрежу Клинике са удаљене локације.

VPN процедура се примењује на све запослене-кориснике, који користе рачунаре или мобилне уређаје за повезивање на мрежу Клинике, и уређује приступ са удаљених локација у сврху обављања посла у име и за рачун Клинике, укључујући коришћење електронске поште и мрежних ресурса, као и начин приступа мрежи Клинике са удаљених локација.

Члан 20.

Захтеви који морају бити испуњени у VPN процедури су следећи:

- приступ са удаљених локација мора бити заштићен коришћењем криптозаштите
- регистровани корисници морају чувати лозинке својих налога и не смеју омогућити приступ било ком трећем лицу
- приликом коришћења службеног рачунара за приступ са удаљене локације мрежи Клинике, регистровани корисник не сме истовремено бити повезан и на неку другу мрежу која може угрозити безбедност комуникације
- приступ са удаљене локације мора бити одобрен од стране Администратора
- сви уређаји који су повезани на интерну мрежу Клинике преко удаљених локација мора имати инсталирану заштиту у виду антивирусне заштите

- сви пословни подаци који се креирају приликом рада на даљину складиште се у информационом систему Клинике

- пословни подаци се, ради безбедности истих, не могу складиштити на мобилним уређајима

Члан 21.

Рад на даљину запослених или радно ангажованих лица одобрава Администратор.

2.2. Коришћење мобилних уређаја

Члан 22.

Процедуром коришћења мобилних уређаја дефинише се начин физичке заштитите од крађе и активности које је неопходно предузети у случају крађе или губитка мобилних уређаја, односно безбедносног инцидента, како не би била нарушена безбедност података Клинике.

Члан 23.

Право на коришћење мобилних уређаја ван седишта Клинике се стиче на основу писаног захтева запосленог-корисника мобилног уређаја упућеног Администратору.

Запослени-корисници ресурса ИКТ система, могу само путем мобилних уређаја, који су у власништву Клинике, и који су подешени од стране Администратора да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности, а на основу писане сагласности директора Клинике.

Мобилни уређаји из става 1. овог члана, морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и листе MAC адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Члан 24.

Администратор је одговоран је за вођење евиденције о свим уређајима намењеним за рад на даљину.

Евиденција о уређајима треба да садржи податке који су неопходни да би се уређај и/или корисник недвосмислено идентификовали, као што су произвођач, модел, серијски број, инвентарски број, MAC адреса, IMSI, IMEI, корисник који је задужио уређај и његов јединствени матични број и слично.

Администратор је дужан да, одмах по пријави о нестанка мобилног уређаја, блокира приступ истог мрежи ИКТ система и кориснику промени шифру за приступ истој.

Члан 25.

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

Члан 26.

Запосленима-корисницима није дозвољено да користе мрежу Клинике за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада појединачног запосленог.

Члан 27.

Нерегистровани корисници, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ Интернету али не и деловима мреже кроз коју се обавља службена комуникација.

Члан 28.

Приступ ресурсима ИКТ система, са приватног мобилног уређаја, није дозвољен, осим ако је мобилни уређај у власништву Клинике, оштећен и није обезбеђена замена истог, а на основу писане сагласности директора Клинике.

Евиденцију приватних мобилних уређаја, из става 1. овог члана, води Администратор.

Члан 29.

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

Члан 30.

Администратор је дужан да пре предаје мобилног уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради *„backup“* података који се налазе у мобилном уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати податке у мобилни уређај.

Члан 31.

У случају крађе, губитка мобилног уређаја или било ког другог догађаја који доводи до нарушавања тајности и интегритета података који се налазе на мобилном уређају Администратор је дужан да, одмах по пријави безбедносног инцидента, блокира несталом мобилном уређају приступ ИКТ систему и кориснику промени шифре за приступ.

У случају да се пронађе мобилни уређај чији нестанак је пријављен, Администратор ће извршити трајно брисање комплетног медијума за смештање оперативног система, апликација и података и поновну инсталацију оперативног система и потребних апликација.

Члан 32.

Администратор свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих мобилних уређаја (са непознатих МАС адреса).

Уколико се установи неовлашћен приступ из става 1. овог члана, Администратор одмах о томе, путем електронске поште, обавештава директора Клинике, а та МАС адреса се уноси у "*block*" листу софтвера који се користи за контролу приступа.

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

Члан 33.

ИКТ системом управља Администратор.

Администратор је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Клинике, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденцију о изјавама новозапослених - корисника да су упознати са правилима коришћења ИКТ ресурса.

Члан 34.

Свако коришћење ИКТ ресурса Клинике од стране запосленог-корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог као, одговорност запосленог-корисника за неовлашћено коришћење имовине.

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

Члан 35.

У случају промене послова, односно надлежности запосленог-корисник, Администратор 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 односа, односно радног ангажовања запосленог-корисника, кориснички налог се укида.

Запослени-корисници су обавезни да врате сва информациона добра коју користе у свом раду након престанка радног односа, односно радног ангажовања.

Током отказног рока запослених, Администратор је дужан да контролише да ли исти неовлашћено копирају, умножавају или преузимају заштићене информације Клинике.

Запослени-корисник, након престанка радног односа, односно радног ангажовања у Клиници, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 36.

Информациона добра Клинике су она која су дефинисана у члану 4. став 1. тачка 20) овог Правилника.

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.

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

Члан 37.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебних прописа (Закона о слободном приступу информацијама од јавног значаја ("Сл. гласник РС", бр.120/04, 54/07, 104/09, 36/10 и 105/21), Закона о заштити података о личности ("Сл. гласник РС", бр. 87/2018), Закона о тајности података ("Сл. гласник РС", 104/2009), као и Уредбом о начину и поступку означавања тајности података, односно докумената ("Сл. гласник РС", бр. 8/2011).

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 38.

Администратор ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да:

- подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено одлуком директора Клинике,

- 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.

Евиденцију носача на којима су снимљени подаци, води оператор ИКТ 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, директор Клинике ће одредити одговорну особу и начин транспорта.

Члан 39.

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 40.

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

Члан 41.

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

Члан 42.

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.

Члан 43.

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) разуме и прихвата да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Клинике 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, укључујући и надређене;

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 начелника службе у којој је запослени распоређен на послове;

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 Клиници у складу са прописаним процедурама;

14) разуме и прихвата да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;

15) разуме и прихвата да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;

16) разуме и прихвата 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;

18) разуме и прихвата да му је забрањено давање уређаја другим лицима (на услугу, сервисирање и сл.);

19) прихвата усвојену оперативну процедуру за потпуно брисање података када престане потреба за чувањем истих у уређају;

20) крађу или губитак урађаја мора без одлагања да пријави Администратору, који затим спроводи активности у смислу очувања безбедности података Клинике. Уколико се уређај накнадно пронађе, исти је потребно предати Администратору;

21) у циљу заштите података на мобилним уређајима, прихвата да Администратор евидентира коришћење истих у одговарајућим логовима, који ће се у слушају потребе користити за утврђивање евентуалних злоупотреба.

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

Члан 44.

Право приступа ИКТ систему имају само запослени/корисници који имају администраторске или корисничке налоге.

Члан 45.

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 може да користи само оператор ИКТ система.

Члан 46.

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 оператор ИКТ система , на основу захтева начелника службе у којој је запослени распоређен на послове 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.

Члан 47.

Оператор ИКТ система води евиденцију о корисничким налозима, проверавју њихово коришћење, мењају права приступа и укидају корисничке налоге на основу захтева начелника службе.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 48.

Кориснички налог се састоји од корисничког имена и лозинке.

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

Лозинка не сме да садржи личне податке корисника, као што су лично име, телефонски број или датум рођења и не смеју садржати више од 3 узастопна идентична бројчана или словна знака.

Запослени-корисници су дужни да привремене шифре промене приликом првог пријављивања.

Члан 49.

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 годину дана.

Иста лозинка се не сме понављати у временском периоду од две године.

Члан 50.

Пријављивање у ИКТ систем Клинике се врши уношењем корисничог имена и лозинке на страници за пријаву.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 51.

Приступ ресурсима ИКТ система Клинике захтева посебну криптозаштиту.

Администратор је задужен за инсталацију потребног софтвера и хардвера за коришћење сертификата.

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

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

Члан 52.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује са као административна зона.

Администраторска зона мора бити видљиво обележена.

Администраторска зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом и видео надзором.

Администраторска зона мора да буде обезбеђена од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор), и влажност ваздуха и поседовати систем за обезбеђење.

Прозори и врата у администраторској зони морају бити стално затворени.

Администраторску зону треба редовно чистити од прашине.

Сервери, мрежна или комуникациона опрема ИКТ система мора бити заштићена од атмосферских падавина;

Администратор врши редовну контролу система за обезбеђење, електромагнетног зрачења, противпожарне заштите, температуре, влажности ваздуха као и инсталација за воду, струју, централно грејање, електронске комуникације, као и других услова који морају бити испуњени у администраторској зони.

Евиденцију о уласку у административну зону води Администратор.

Члан 53.

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

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

Уређаји за непрекидно напајање – UPS:

1) се одржавају у складу са спецификацијама опреме произвођача и прописима;

2) редовно процењује капацитет истих;

3) редовно прегледају и испитују у погледу правилног функционисања и врши поправка кварова;

4) обезбеђује вишеструко напајање са различитих траса;

Администатор редовно прати да ли су испуњени услови из става 2. овог члана.

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

Члан 54.

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

Осим администратора система, приступ Администраторској зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу директора Клинике, и уз присуство Администратора.

Приступ Администраторској зони могу имати и запослени распоређени на послове одржавања хигијене уз присуство Администратора.

Члан 55.

ИКТ опрема, информације или софтвер се измештају само уз одобрење директора Клинике, а током измештања се примењују следећа правила:

1) директор Клинике треба да одреди запослене или друга лица која ће извршити измештање исте;

2) директор Клинике треба да одреди временски период за измештање и да се проверава усклађеност приликом повратка исте;

3) треба документовати идентитет и улогу лица која користе или поступају са истом приликом премештања и ова документација треба да буде враћена са ИКТ опремом, информацијама или софтвером

Члан 56.

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

Члан 57.

Поправке и сервисирање ИКТ опреме може обављати само особље овлашћено за одржавање.

Приликом сервисирања ИКТ опреме осетљиве информације треба избрисати из исте, односно Уговором закљученим са сервисером опреме мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Клинике.

Администратор о свим сумњивим или стварним неисправностима ИКТ опреме, као и о целокупном превентивном и корективном одржавању исте се чувају записи.

Пре враћања ИКТ опреме у рад након одржавања, потребно је да Администратор прегледа исту како би се проверило да није неовлашћено коришћена или оштећена.

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

Члан 58.

У циљу обезбеђивања исправног и безбедног функционисања ИКТ система, дефинишу се процедуре за руковање средствима, које се односе на отпочињање и завршетак приступа

информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевивма измештања делова ИКТ система.

Директор Клинике, посебним актом, на предлог Администратора, успоставља радне процедуре које садрже инструкције за детаљно извршење следећих послова:

1) инсталација и конфигурација система;

2) обраду и поступање са информацијама (аутоматски и мануелно);

3) израда резервних копија;

4) обрада захтева за временски распоред активности;

5) израда инструкција за поступање у случају грешке или у другим ванредним ситуацијама која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција;

6) утврђивање листе контаката за подршку и есклацију (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;

7) израда инструкција за управљање поверљивим подацима;

8) процедуре за поновно покретање система и опоравак, које се користе у случају отказа система;
9) управљање системским записима (логовима); и) процедуре за надгледање.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 59.

Администратор континуирано надзире и проверава функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим, планира, односно предлаже директору Клинике одговарајуће мере.

Члан 60.

Пре увођења у рад новог софтвера неопходно је да Администратор направи 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 софтвера, 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.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери и подаци који су намењени тестирању и развоју.

При тестирању софтвера, потребно је да Администратор обезбеди неометано функционисање ИКТ система.

Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера, на начин који може да заустави нормално функционисање ИКТ система.

Члан 61.

Администратор континуирано надгледа коришћење ресурса ИКТ система, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе система.

Периодично, Администратор спроводи следеће активности:

1) брисање застарелих података;

2) повлачење из употребе апликација, система, база података или окружења;

3) оптимизација серије процеса и распореда;

4) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису критичне за пословање

Члан 62.

Уређаји морају бити закључани у току одсуства запосленог са рада и угашени на крају радног дана.

USB или флеш меморија, CD – ROM и DVD медијуми морају бити одложени и закључани.

Шифре за приступ уређајима не смеју бити записане и оставене на месту које је приступачно.

Приликом штампања, штампани материјал који садржи осетљиве информације мора се одмах преузети са штампача приликом штампања.

Штампани материјал који је намењен за бацање, без одлагања, треба уништити, односно одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

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

Члан 63.

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 се инсталира антивирусни програм.

Члан 64.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних 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.

Члан 65.

У циљу заштите, односно упада у ИКТ систем Клинике са интернета, Администратор је дужан да одржава систем за спречавање упада.

Запосленима-корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема).

Администратор, по налогу директора Клинике, може укинути приступ интернету у случају доказане злоупотребе истог од стране запосленог-корисника.

Запослени- 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 врши Администратор.

Члан 66.

Приликом коришћења интернета, запослени-корисник треба избегавати сумњиве WEB странице, с обзиром да приступање истим може проузроковати неприметно инсталирање шпијунских програма и слично.

У случају да запослени-корисник примети неуобичајено понашање рачунара, исто, без одлагања, треба да пријави Администратору.

Члан 67.

Директор Клинике, посебним актом, на предлог Администратора, у циљу заштите од злонамерног софтвера успоставља следеће процедуре:

1) забрана коришћења неауторизованих софтвера;

2) имплементација контрола које спречавају или откривају коришћење неовлашћених софтвера;

3) имплементација контрола које спречавају или откривају коришћење познатих или сумнивих компромитованих *web* сајтова;

4) успостављање формалне процедуре заштите од ризика повезаних са добијањем датотека и софтвера са или преко интернет мреже или на неком медијуму, указујући на заштитне мере које треба предузети

5) смањење ризика које може да произведе непријатељски софтвер

6) спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају ризичне пословне процесе

7) испитивање присуства било каквих неодобрених датотека или неауторизованих допуна

8) инсталирање и редовно ажурирање софтвера за откривање злонамерног софтвера

Члан 68.

Запосленима-корисницима је забрањено гледање филмова и играње игара на рачунарима и "крстарење" WEB страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

Недозвољена употреба интернета обухвата и:

- 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*) 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.

Уколико Запослени предузимају радње које су забрањене овим чланом, чине непоштовање радне дисциплине.

Члан 69.

Запосленима-корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност интернет мреже Клинике може се, по налогу директора Клинике, одузети право приступа интернет мрежи.

Администратор је дужан да о неадекватном коришћењу интернета, одмах по сазнању, обавести директора Клинике.

16. Заштита од губитка података

Члан 70.

Администратор врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог ИКТ система у случају наступања последица изазваних ванредним околностима.

Члан 71.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Заштитне копије запосленима-корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака запосленог-корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се израђивање резервних копија корисничких података, конфигурационих и log фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и исте треба израђивати у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система

Члан 72.

За чување заштитних копија користе се преносиви информатички медији (CD ROM, DVD, USB, екстерни хард диск и сл.).

Израђивање заштитних копија врши се у складу са посебним актом, који, на предлог Администратора, доноси директор Клинике, уз сагласност Управног одбора Клинике

Члан 73.

Актом из члана 72. овог Правилника прописују се:

1) обим и учесталост израда заштитних копија

2) начин складиштења заштитних копија у циљу избегавања оштећења истих

3) медијуме са заштитним копијама треба редовно проверавати ради сигурности података у истим

4) у случајевима нарочите важности података на медијумима који садрже заштитне копије, исте треба заштитити помоћу шифровања

5) и друге процедуре које су од значаја за чување заштитних копија

Члан 74.

У ИКТ систему Клинике формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Члан 75.

Администратор води дневнике о догађајима и бележи активности корисника, грешке и догађаје у вези са безбедношћу ИКТ система, који се морају чувати и редовно преиспитивати.

Дневници Администратора о догађајима садрже:

1) идентификаторе корисника;

2) активности ИКТ система;

3) датуме, време и детаље кључних догађаја, нпр. пријављивања и одјављивања;

4) идентитет или локацију уређаја, ако је могуће, и идентификатор система;

5) записе о успешним и одбијеним покушајима приступа ИКТ систему;

6) записе о успешним и одбијеним покушајима приступа подацима и другим ресурсима;

7) промене у конфигурацији ИКТ система;

8) коришћење привилегија;

9) коришћење системских помоћних функција и апликација;

10) датотеке којима се приступало и врсте приступа;

11) мрежне адресе и протоколе;

12) аларме које је побудио систем за контролу приступа;

13) активирање и деактивирање система заштите, као што су антивирусни системи и системи за откривање упада.

Администратор не сме да брише или деактивира дневнике о сопственим активностима.

Члан 76.

Средства за записивање и записане информације морају бити заштићени од неовлашћеног мењања и приступа.

Забрањено је неовлашћено уношење следећих измена:

1) мењање типова порука које се записују;

2) уношење измена у датотеке са записима или њихово брисање;

3) препуњавање медијума за записе, што доводи до отказа записивања догађаја или уписивања преко већ раније записаног

Члан 77.

Активности администратора и оператора ИКТ система се записују, а записи штите и редовно преиспитују.

Корисници привилегованих корисничких налога да управљају записима на опреми за обраду информација која је под њиховом директном контролом, на који начин се штите и прегледају записи да би се одржала одговорност за привилеговане кориснике.

Сатови свих одговарајућих система за обраду информација заштите морају бити синхронизовани по Гриничком средњем времену.

За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужен је Администратор.

Члан 78.

Администратор спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за контролу промена и инсталацију софтвера.

Смернице за контролу промена и иснсталацију софтвера су следеће:

1) ажурирање оперативног софтвера, апликација, и програмских библиотека може да обавља искључиво Администратор, на основу овлашћења директора Клинике, односно овлашћеног лица.

2) оперативни системи могу да садрже само одобрене извршне кодове, односно не смеју садржати развојне кодове или компилаторе

3) оперативни системски софтвер и апликације се могу имплементирати тек по обављеном спроведеном испитивању, које обухвата испитивање применљивости, безбедности, утицаја на друге системе и погодности за коришћење и морају се спроводити на засебним системима, односно тестним окружењима;

4) морају се обезбедити азурирање свих одговарајућих библиотека изворних програма;

5) пре имплементације било каквих промена, мора се успоставити стратегија повретка на претходно стање;

6) морају се одржавати записи за проверуприликом ажурирања на библиотекама оперативних програма;

7) морају се сачувати претходне верзије апликативног софтвера као меру предострожности за непредвиђене ситуације

8) морају се архивирати старије верзије софтвера, заједно са свим потребним информацијама и параметрима, процедурама, детаљима конфигурације и софтвером за подршку, све док се подаци чувају на заштитним копијама – архиви.

Инсталацију и подешавање софтвера може да врши искључиво Администратор.

Члан 79.

Администратор врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите истог.

Члан 80.

Администратор благовремено прикупља информације о техничким рањивостима ИКТ система који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимањем у обзир припадајућих ризика.

Посебне информације које су потребне за подршку управљања техничким рањивостима ИКТ система обухватају продавца софтвера, бројеве верзија, текуће стање размештаја, као и особе које су одговорне за тај софтвер.

Члан 81.

Администратор обавља послове у вези са управљањем техничким рањивостима ИКТ система, укључујући надзор, оцену ризика услед утврђене рањивости и исправке.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, Администратор је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене рањивости, при чему се прво узимају у разматрање системи са високим ризиком.

Смернице за обављање послова из става 1. овог члана, прописује директор Клинике посебним актом.

Члан 82.

Сваки примерак заштитне копије чува се у року и на начин који је дефинисан законом, другим прописима и општим актима Клинике о уређивању архивске грађе и архивске делатности.

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

Заштитне копије-архиве се чувају у просторији која је физички и у складу са мерама које су предвиђене законом и другим прописима којим уређује архивска грађа и архивска делатност.

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

Члан 83.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и др, мора бити подешен тако да одмах обавештава Администратора, о свим нерегуларним активностима запослених-корисника, покушајима упада и упадима у систем.

18. Обезбеђивање интегритета софтвера и оперативних Система

Члан 84.

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

Инсталацију и подешавање софтвера може да врши само Администратор.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера.

Забрањено је на уређајима инсталирање софтвера који могу довести до изложености ИКТ система безбедоносним ризицима.

Директор Клинике посебним актом прописује које врсте софтвера Администратор сме да инсталира, односно које врсте софтвера исти не сме да инсталира ради одржавања безбедности ИКТ система.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ Система

Члан 85.

Администратор 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, Администратор је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

Администратор треба да подешавањем корисничких налога, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

20. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање истог

Члан 86.

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 писану сагласност директора Клинике.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 87.

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.

Каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње.

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

Администратор је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Администратор контролише неовлашћено прикључење уређаја на каблове техничким претраживањем и физичком провером, као и неовлашћени приступ до разводних табли и у просторије са кабловима.

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

У мрежама у којима су међусобно раздвојене групе информационих услуга, корисника и системи Администратор је одговоран за управљање мрежом и дужан је да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности исте.

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

Члан 88.

У оквиру животног циклуса ИКТ система Клинике, који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и повлачења из употребе, директор Клинике и Администратор су дужни да обезбеде информациону безбедност у свакој фази.

Питање безбедности се анализира у раним фазама пројеката ИКТ система.

Члан 89.

Постојећи ресурси ИКТ система се одржавају како би се осигурали њена непрекидна расположивост и неповредивост, и то тако што се ИКТ систем, односно делови истог одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао произвођач, односно испоручилац истих.

Члан 90.

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

Администратор 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 Администратор води одговарајућу документацију.

Документација из става 3. овог члана, мора да садржи описе свих процедура а посебно процедура које се односе на безбедност ИКТ система.

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

Члан 91.

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

Приликом тестирања система, подаци који су означени ознаком тајности, односно као поверљиви подаци, или су у питању лични подаци, исти морају бити заштићени и Администратор одговара за такве податке у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

25. Анализа и спецификација захтева за информациону безбедност

Члан 92.

У захтеве за нове ИКТ системе или за побољшање постојећих ИКТ система морају бити укључени захтеви који се односе на информациону безбедност и они су саставни део уговора о набавци, модификацији и одржавању истог.

Захтеви за информациону безбедност ИКТ система укључују:

1) Проверу идентитета корисника;

2) Доступност, поверљивост, непорецивост и интегритет података и имовине;

3) Надгледање пословних процеса;

4) Омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке кориснике.

Спецификација захтева обухвата контролу која ће бити уведена у ИКТ систем, која мора бити примењена при вредновању развијених или купљених пакета софтвера, намењених за пословне апликације.

Системски захтеви за информациону безбедност и процеси за увођење безбедности се интегришу у фази дизајнирања ИКТ система.

Формално тестирање и процес имплементације ће се примењивати за све купљене делове ИКТ система, односно производе.

У уговору са извођачем, односно испоручиоцем купљених делова ИКТ система, односно производа, посебно се дефинишу захтеви за информациону безбедност.

У случају да безбедносна функционалност предложеног дела ИКТ система, односно производа не задовољава одређен захтев, ризик и повезане контроле ће бити преиспитане пре куповине истог.

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

Члан 93.

Тестирање ИКТ система може вршити само Администратор, односно трећа лица пружаоци услуга за које постоји уговором дефинисан приступ ИКТ систему (у даљем тексту овог члана заједнички назив: Администратор).

Тестирање ИКТ система, односно делова система, Администратору је дозвољено јпод условом потпуне примене свих безбедносних мера наведених у овом члану.

За потребе испитивања и тестирања ИКТ система, односно делова система, Администратор избегава коришћење оперативних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачног корисника здравствених услуга, његовог законског заступника, запосленог, добављача, запосленог или др.

Уколико се за сврху испитивања ИКТ система користе лични подаци или неке друге поверљиве информације, Администратор је дужан да обезбеди да сви осетљиви подаци и информације пре коришћења штите анонимизацијом личних података, уклањањем садржаја или изменом текста садржаја у предметном делу.

За податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су подаци о личности коришћени приликом тестирања ИКТ система, одговоран је Администратор, односно друго запослено или радно ангажовано лице у Клиници, у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

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

Приликом тестирања апликативних система, Администратор примењује додатне процедуре за контролу приступа путем физичке заштите и применом криптографских мера за заштиту ИКТ система и података од неовлашћених приступа, а које се примењују и на оперативним системима.

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

Члан 94.

Трећа лица-пружаоци услуга, могу приступити подацима који се налазе у базама података ИКТ система само на основу уговором дефинисаног приступа истим, при чему такви уговори морају садржати одредбу о заштити и чувању поверљивости информација, података и документације.

Трећа лица-пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са Клиником.

Администратор успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити трећа лица-пружаоци услуга:

1) идентификовање и документовање врсте трећих лица-пружаоца услуга којима ће Администратор дозволити да приступ информацијама;

2) стандардизовани процес за управљање односима између трећих лица-пружаоца услуга;

3) дефинисање врста информација које ће различитим типовима трећих лица-пружаоца услуга бити дозвољено ради приступања, праћења и контроле приступа;

4) минимални захтеви за безбедност информација за сваку врсту информација и врсту приступа;

5) процеси и процедуре за праћење придржавања утврђених захтева за безбедност за сваку врсту трећих лица-пружаоца услуга и врсту приступа;

6) контроле за осигурање интегритета информација или обраде информација коју обезбеђује било која страна;

7) поступање са инцидентима и непредвиђеним ситуацијама које су у вези са приступом пружаоца услуга, укључујући одговорности и организације и трећих лица-пружаоца услуга;

8) управљање неопходним променама информација, опреме за обраду информација и свега осталог што треба да се премешта и осигурање да се безбедност информација одржава током прелазног периода.

Администратор је одговоран за контролу приступа и надзор над извршењем уговорених обавеза од стране трећих лица-пружаоца услуга, као и за поштовање одредби овог Правилника којима су такве активности дефинисане.

Члан 95.

Уговор са трећим лицем-пружаоцем услуга мора да садржи одредбу о заштити података, информација и документације, као и да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин који је претходно одобрен од стране Администратора, а за потребе извршења предмета уговора.

Уговор са трећим лицем-пружаоцем услуга мора да садржи одредбу о накнаде штете у корист у Клинике у случају повреде одредбе из става 1 овог члана од страна трећег лица-пружаоца услуга.

Трећа лица-пружаоци услуга дужни су да захтеве Клинике у погледу безбедности информација предвиде одредбама уговора који су закључили са својим подуговарачима за додатне услуге или производе.

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

Члан 96.

Администратор је одговоран за надзор над поштовањем уговорених обавеза од стране трећих лица-пружаоца услуга који се односе на ИКТ систем Клинике, а посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система.

Администратор је дужан да редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, што нарочито подразумева прегледање и преиспитивање извршавање услуга у складу са условима из уговора у вези са безбедношћу информација, вршење оцене квалитета извршења и саобразности уговорене услуге; редовно извештавање и

обавештавање директора Клинике о истом, како би директор Клинике могао да предузме мере у циљу отклањања неправилности.

Администратор је дужан да одржава потпуну контролу над спровођењем услуга и осигурава увид у све осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа лица-пружиоци услуга приступају, које процесуирају или којима управљају и др.

Приликом надзора над извршењем квалитета и саобразности уговорене услуге, Администратор проверава да ли треће лице-пружалац услуге задовољава све критеријуме који су били од пресудног значаја приликом избора, укључујући обим и квалитет услуге, као и да се у току поступка извршења услуге може утицати на побољшање квалитета услуге или начина и обима извршења, у складу са утврђеним стварним потребама ИКТ система Клинике.

Члан 97.

У поступку евалуације квалитета и обима пружене услуге у односу на уговорену, Администратор је дужан да прикупи све релевантне чињенице, податке и документацију у вези са извршењем услуге, као и прикупи податке од непосредних, крајњих корисника у вези са предметом услуге. Евалуација се може извршити слањем упитника, разговором са изабраним појединцима или на основу анкетирања путем елетронске поште.

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

Члан 98.

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

По пријему пријаве Администратор је дужан да одмах обавести директора Клинике и предузме 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 инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја ("Сл. гласник РС", бр, 94/2016), Администратор, је дужан да поред директора Клинике обавести надлежни орган дефинисан овом уредбом и Повереника за информације од јавног значаја и заштиту података о личности на основу Закона о заштити података о личности ("Сл. гласник РС", бр. 87/2018).

Администратор води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом из става 3. овог члана, на основу које се, против лица одговорног за инцидент, могу да се воде дисциплински, прекршајни или кривични поступци.

Члан 99.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, Администратор је дужан да се придржава процедура:

1) за припрему и планирање одговора на безбедоносне инциденте

2) за надгледање, детекцију, анализу и извежтавање о безбедоносним инцидентима
3) за записивање активности у оквиру управљања безбедоносним инцидентима
4) за оцењивање и одлучивање о безбедоносним инцидентима у оквиру безбедности информација и оцењивања слабости у погледу безбедности инфрмација
5) за одговарање на безбедоносне инциденте, опоравак од истих

6) у циљу превенције од безбедносних ризика обезбеђује више (различитих и другачијих) мехнизама за комуникацију и координацију у случају нарушавања безбедности, као што су, између осталог, обезбеђивање контакт информација (број телефона, електронска адреса) појединаца у оквиру Клинике и ван ње, систем за праћење проблема, шифровани софтвер који би био коришћен од стране појединаца у оквиру Клинике, посебну осигурану просторију за чување података и складиштење поверљивог материјала.

Директор Клинике дефинише процедуре за идентификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају покретања дисциплинског, прекршајног или кривичног поступка, док Администратор примењује исте.

30. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 100.

Администратор примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању, а које су прописане Планом за обезбеђење континуитета пословања и Планом опоравка од нежељених догађаја ИКТ система.

План за обезбеђење континуитета пословања за хардверске компоненте ИКТ система треба да обухвати следеће:

1) документацију за логички и физички дијаграм и копије пројеката;

2) заштитне копије конфигурисаних фајлова и оперативног система активних уређаја

3) унапред припремљене конфигурације за различите сценарије

4) израду заштитних копија

План опоравка од нежељених догађаја треба да обухвати следеће:

1) процењивање најкритичнијих апликација, података, конфигурационих фајлова и системски софтвер за који треба направити заштитне копије

2) одредити место чувања заштитних копија

3) одредити нову локацију за рад ИКТ система, у случају немогућности рада на основној локацији, као и одређивање рачунара који ће привремено обављати послове сервера до поновног стављања сервера у функцију

4) навести податке о запосленима, односно другим лицима који ће бити ангажовани на отклањању последица нежељених догађаја

5) одредити изворе непрекидног напајања електричном енергијом

6) постојање документације за сервисе, апликације и базе података

7) процедуре инсталације и конфигурисања сервиса, апликација и база података

8) место чувања инсталација сервиса, апликација, база података и заштитних копија података

9) развијене и одобрене документоване планове, одговоре и процедуре за опоравак, а нарочито у погледу организације управљања догађајима који узрокују поремећаје и одржавања безбедности информација Клинике

III. Измена Правилника о безбедности

Члан 101.

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, Администратор је дужан да обавести директора Клинике у писаној форми, 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

Члан102.

Проверу ИКТ система врши Администратор.

Администратор је дужан да најмање једном годишње изврши проверу ИКТ система.

О извршеној провери Администратор сачињава извештај и исти доставља директору Клинике.

V. Садржај извештаја о провери ИКТ Система

Члан 103.

Извештај о провери ИКТ система, из члана 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 104.

Овај правилник ступа на снагу и примењује се од 8 (осмог) дана од дана објављивања на огласној табли Клинике.

Председник Управног одбора
Проф. др Предраг Станковић