

ИНСТИТУТ ЗА ОНКОЛОГИЈУ И РАДИОЛОГИЈУ СРБИЈЕ

Београд, Пастерова број 14.

Број: 25-33 од 28.12. 2017. године

На основу члана 22. Статута Института за онкологију и радиологију Србије, Управни одбор Института је на седници одржаној дана 28. децембра 2017. године, донео следећу

### ОДЛУКУ

Усваја се Правилник о безбедности информационо-комуникационог система Института за онкологију и радиологију Србије.

Саставни део ове одлуке је Правилник из става 1. одлуке.



ПРЕДСЕДНИК УПРАВНОГ ОДБОРА  
Проф. др Радисав Шћепановић

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16), чл. 2. и 3. 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) и члана 25 Статута Института за онкологију и радиологију Србије, Управни одбор Института је на седници одржаној дана 28. децембра 2017. године, донео

## ПРАВИЛНИК

### о безбедности информационо-комуникационог система Института за онкологију и радиологију Србије

#### І. ОСНОВНЕ ОДРЕДБЕ

РЕПУБЛИКА СРБИЈА  
ИНСТИТУТ ЗА ОНКОЛОГИЈУ И РАДИОЛОГИЈУ СРБИЈЕ

Бр. 25-33/1

Члан 1.

28.12.2017

БЕОГРАД, Пастерова 14

Овим Правилником се ближе уређују мере заштите информационо-комуникационог система, нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења, дужности и одговорности корисника информатичких ресурса Института за онкологију и радиологију Србије (у даљем тексту: Институт).

#### Значење појединих термина

Члан 2.

Поједини термини у смислу овог Правилника имају следеће значење:

- 1) **информационо-комуникациони систем (ИКТ систем)** је технолошко-организациона целина која обухвата:
  1. електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
  2. уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада електронских података коришћењем рачунарског програма;
  3. електронске 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) **информациони систем (ИС)** је део ИКТ система, који је формализован и намењен планском прикупљању, складиштењу, обради, размени и испоруци информација од

значаја за рад, тако да су информације доступне и употребљиве свима који су овлашћени да их користе;

- 3) **информациона безбедност** представља скуп мера које омогућавају да електронски подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити тајност, интегритет, расположивост, аутентичност и непорецивост тих података, да би ИКТ систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;
- 4) **ризик** значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
- 5) **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;
- 6) **инцидент** је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
- 7) **мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
- 8) **надлежни орган** је Министарство надлежно за послове информационе безбедности (у складу са Чланом 4 Закона о информационој безбедности)
- 9) **информациона добра** обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и слично;
- 10) **корисник** је запослени Института који има приступ ИКТ систему ради обављања својих пословних активности;
- 11) **ДЦ** је одељење Дата центар;
- 12) **администратор ДЦ** је запослени Дата центра коме је дозвољено администрирање ИКТ система;
- 13) **инџињер за ИТ безбедност ДЦ** је запослени који ради на праћењу, откривању, спречавању, превенирању и заштити од безбедоносних ризика ИКТ система; унапређењу мера заштите од безбедоносних ризика; опоравку ИКТ система и обавештавању Надлежног органа и/или ЦЕРТ након безбедоносних инцидената; едукацији и подизању свести запослених о безбедоносним ризицима и мерама за њихово спречавање;
- 14) **вендор** је треће лице са којим Институт сарађује по основу уговора о одржавању ИКТ система или његових делова;
- 15) **креденцијал** је идентификатор (корисничко име и лозинка; картица; ПИН код; IP адреса и сл.) на основу кога се врши аутентикација (провера права приступа) и ауторизација (провера обима приступа ИКТ сиситему). Може се односити на личност, групу Корисника, групу Администратора ДЦ, уређај итд.;

- 16) **кориснички налог** чине креденцијали Корисника помоћу кога је Кориснику омогућен обим приступа ИКТ систему, у складу са пословима које обавља на Институту;
- 17) **администраторски налог** чине креденцијали Администратора ДЦ или Администратора вендора помоћу кога се омогућава администрирање ИКТ система или његових делова;
- 18) **IP адреса** (енгл. Internet Protocol address) је јединствени број који користи машина (најчешће рачунар) у међусобном саобраћају путем интернета/интранета уз коришћење интернет/интранет протокола;
- 19) **ВПН (Virtual Private Network)** је сигурна криптована интернет веза која омогућава повезаном рачунару прступ институтској мрежи као да се рачунар физички налази у Институту;
- 20) **База ИКТ ресурса и услуга ДЦ** је електронска база евиденција ИКТ ресурса и услуга које Дата центар пружа у Институту;
- 21) **мобилни уређај** је преносиви рачунар, таблет, SMART-мобилни телефон, PDA и сл. који се повезује са институтском мрежом;
- 22) **медијум** – диск, УСБ меморија, преносиви хард диск, ЦД, ДВД, као и остали предмети и компоненте који имају могућност чувања и преноса података;
- 23) **радна станица** – рачунар или мобилни рачунар који је умрежен у мрежу Института са циљем да запослени могу обављати своје редовне пословне активности.

### Циљеви Правилника о безбедности

#### Члан 3.

Циљеви доношења овог Правилника су:

- 1) одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности ИКТ система;
- 2) прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
- 3) спречавање и минимизација безбедносних инцидената којим се угрожава или нарушава информациона безбедност;
- 4) свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите;
- 5) подизање свести код запослених о значају информационе безбедности, опасностима, ризицима и мерама заштите приликом коришћења ИКТ система;
- 6) ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност.

## **Обавеза примене одредби Правилника о безбедности**

### **Члан 4.**

За све запослене је обавезна примена мера заштите ИКТ система које су ближе уређене овим Правилником и које служе превенцији од настанка и минимизацији штете од инцидентата. Мере заштите се примењују у свим организационим нивоима и свим радним местима.

Запослени у Институту морају бити упознати са садржином овог Правилника и дужни су да поступају у складу са њим, као и другим интерним процедурама којима се регулише информациона безбедност.

### **Одговорност запослених**

#### **Члан 5.**

Запослени су дужни да приступају информацијама и ресурсима ИКТ система Института само ради обављања редовних пословних активности.

Запослени су дужни да све безбедносне инциденте или проблеме пријаве Одељењу Дата центар у најкраћем року.

Непоштовање одредби овог Правилника, као и свако угрожавање или нарушавање информационе безбедности, представља повреду радних обавеза и повлачи одговорност запосленог.

Руководиоци организационих јединица су одговорни за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим Правилником и интерним процедурама.

### **Предмет заштите**

#### **Члан 6.**

Предмет заштите ИКТ система су:

- хардверске и софтверске компоненте ИКТ система;
- подаци који се чувају, обрађују, претражују или преносе помоћу електронских уређаја;
- организациону структуру путем које се управља ИКТ системом;
- техничку и корисничку документацију;
- општи акти и процедуре.

## II. МЕРЕ ЗАШТИТЕ

Мерама заштите се обезбеђује превенција од настанка инцидената и минимизација штете од инцидента који угрожавају обављање делатности Института. Ови мерама се врши заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

### 1. Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Института

#### Члан 7.

Организациона структура Института се рефлектује у ИКТ систему. Приступ ИКТ систему је условљен радним задужењима и обавезама које свако од запослених има у опису свог радног места, с циљем да се смањи ризик од злоупотреба, неовлашћених приступа, нарушавања интегритета података у ИКТ систему и људске грешке. Институт у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

Општим актима, појединачним актима и процедурама уређују се обавезе и одговорности запослених, правних и физичких лица у вези са управљањем информационом безбедношћу.

Институт утврђује начин доделе овлашћења за приступ ИКТ систему, начин промене и укидања права приступа у случају када дође до промене радног статуса као и поступак заштите ИКТ система у случају губитка или крађе креденцијала Процедуром о правима приступа ИКТ систему.

Уговором о раду утврђује се и одговорност сваког запосленог и одговорног лица и прописује одговорност запосленог, у случају непоштовања одредби које уређују информациону безбедност.

### 2. Постизање безбедности рада на даљину и употребе мобилних уређаја

#### Члан 8.

ИКТ систем Института је дистрибуиран и има више корисника, те обухвата више различитих уређаја који су умрежени. Динамика и потребе рада захтевају да се унос, обрада или приказ података у оквиру ИКТ система врши са више локација.

Под мобилним уређајима се подразумевају сви преносиви електронски уређаји намењени за комуникацију на даљину (преносиви рачунари, таблети, мобилни SMART-телефони, PDA, итд).

Институт дозвољава запосленима употребу мобилних уређаја и приступ на даљину, уколико је за потребе обављања радних задатака и уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја. Правилном применом утврђеног поступка и начина приступа, Институт своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи.

### **Рад на даљину**

Приступ ИКТ систему Института са удаљених локација је дозвољен и омогућен путем заштићене ВПН конекције:

- запосленима који обављају рад на даљину на радним станицама које су у власништву Института у складу са Процедуром за ВПН приступ ИС;
- вендорима са којима се ВПН приступ дефинише уговором;
- надлежним државним органима/институцијама.

### **Коришћење мобилних уређаја**

Приступ ИКТ систему Института путем мобилних уређаја је дозвољен и омогућен у складу са Процедуром о коришћењу мобилних уређаја чија је примена обавезна од стране свих запослених који користе мобилне уређаје у власништву Института укључујући и вендоре са којима се употреба мобилних уређаја дефинише уговором.

За мобилне уређаје важе све мере заштите које се примењују за уређаје у оквиру централног ИКТ система, а подешавање мобилних уређаја спроводи Администратор ДЦ.

Дата центар је одговоран за вођење евиденције о свим мобилним уређајима у власништву Института.

### **Праћење приступа ресурсима ИКТ система**

Инжењер за ИТ безбедност ДЦ, контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC-адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава начелника ДЦ који обавештава Директора Института, а та MAC 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 обављају и у потпуности разумеју своју одговорност**

#### **Члан 9.**

Институт се стара да запослени који администрирају или користе ИКТ систем имају адекватан степен образовања, способности и одговорности које су утврђене Правилником о унутрашњој организацији и истематизацији послова.

Заснивање радног односа у Институту врши се у складу са Процедуром заснивања радног односа. Сви запослени и радно ангажовани појединци по другом основу којима је додељен приступ ИКТ систему, морају потписати изјаву односно уговор у коме су садржане одредбе о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Институт се стара да запослени ДЦ који долазе у контакт са поверљивим, пословним и/или интерним подацима периодично похађају екстерну едукацију из области безбедности ИКТ система.

Запослени су обавезни да путем едукације редовно стичу нова и обнављају постојећа знања о безбедносним ризицима који могу угрозити ИКТ систем у складу са Процедуром о едукацији запослених из области безбедности ИКТ система.

Руководиоци ОЈ Института су одговорни да сви запослени и на други начин радно ангажована лица у њиховој ОЈ, примењују мере заштите ИКТ безбедности у складу са овим Правилником и важећим процедурама.

Инжењер за ИТ безбедност ДЦ је:

- надлежан за интерну појединачну или групни едукацију запослених из области ИКТ безбедности.
- надлежан за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура ИТ безбедности;
- ауторизован за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Запослени у Дата центру су дужни су да се континуирано обучавају у циљу унапређења техничких, технолошких и других знања везаних за област ИКТ безбедности и да периодично похађају и екстерну едукацију која ће та њихова знања унапредити.

У случају одговорности запосленог за нарушавање безбедности ИКТ система, Институт покреће одговарајући поступак у складу са законским прописима.

#### **4. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених у Институту**

##### **Члан 10.**

Променама послова или престанка радног ангажовања лица запослених у Институту представља ризик за информациону безбедност. Стога, ИНСТИТУТ прецизно уређује дужности и обавезе запосленог или на други начин ангажованог лица које ради у ИКТ систему на следећи начин:

- Након престанка радног ангажовања, сваком Кориснику се укида право приступа ИКТ систему Института у складу са Процедуром о правима приступа ИКТ систему.
- Сваки Корисник је дужан да чува поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система током радног ангажовања и 10 година након престанка или промене радног ангажовања, што се уређује уговорима и изјавом о поверљивости.

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

##### **Члан 11.**

Информациона добра у власништву Института обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Институт поседује *Базу ИКТ ресурса и услуга ДЦ* која одражава реално стање ИКТ система Института и у којој се:

- евидентирају сва информациона добра, опрема и софтвери који се користе за израду, обраду, чување, пренос, брисање и уношење података у оквиру ИКТ система Института;
- за свако информационо добро, опрему и софтвере је назначена запослена особа која је одговорна за његову безбедност, односно интегритет;
- евидентирају све интервенције на рачунарској опреми изражене кроз пружену услугу ДЦ

#### **Класификација информационих добара Института и одговорност за њихову заштиту**

Информациона добра Института класификована су на:

- (1) хардверске компоненте,
- (2) софтверске компоненте,
- (3) компоненте ИС,

- (4) остале е-податке,
- (5) ИКТ документацију.

### **(1) Хардверске компоненте**

Хардверске компоненте чине: сервери; УПС-еви; мрежа, мрежни уређаји и мрежна опрема; рачунари; штампачи; скенери; мобилни уређаји у власништву Института и преносиви носачи података у власништву Института.

Задужена лица за заштиту хардверских компоненти:

1. За заштиту сервера, УПС-ева, мреже и мрежне опреме задужен је надлежни Инжењер за ИТ безбедност ДЦ и/или надлежни вендор у складу са уговором.
2. За заштиту осталих хардверских компоненти задужен је Корисник који на њима обавља своја радна задужења.
3. За заштиту осталих хардверских компоненти које користи више Корисника задужен је непосредни руководилац организационе јединице.

Евиденција хардверских компоненти и задужених лица за њихову заштиту се води кроз *Базу ИКТ ресурса и услуга ДЦ*.

### **(2) Софтверске компоненте**

Софтверске компоненте чине: оперативни системи (лиценцирани оперативни системи Windows; Open source оперативни систем Linux); апликативни софтвери (лиценцирани MS Office пакети; лиценцирани антивирус програм; остали Open source програми /browser-и други програми специфичне намене/)

Задужена лица за заштиту софтверских компоненти:

1. Софтверских компоненти које се налазе на радним станицама задужен је запослени који дужи радну станицу.
2. За заштиту софтверских компоненти које се налазе на северима задужен је Инжењер за ИТ безбедност ДЦ и/или надлежни вендор у складу са уговором.

Евиденција софтверских компоненти и задужених лица за њихову заштиту се води кроз *Базу ИКТ ресурса и услуга ДЦ* у склопу хардверских компоненти на којима се налазе.

### **(3) Компоненте ИС**

Компоненте ИС чине: програмски кодови ИС; систем за управљање базама података ИС и е-подаци ИС.

Задужена лица за заштиту компоненти ИС:

1. За заштиту програмских кодова, система за управљање базама података ИС и е-података информационих система који се налазе на серверима, задужен је надлежни вендор у складу са уговором.

2. За садржај е-података ИКТ система и ИС, задужен је Корисник, у складу са његовим корисничким налогом.

Евиденција информационих система води се кроз *Базу ИКТ ресурса и услуга ДЦ* у склопу хардверских компоненти на којима се налазе.

#### **(4) Остали е-подаци**

Остали е-подаци су сви е-подаци који се налазе на серверима и радним станицама као и мобилним уређајима или преносним носачима података који су у власништву Института.

Задужена лица за заштиту осталих е-података

1. За заштиту осталих е-података који се налазе на серверима, задужен је надлежни Инжењер за ИТ безбедност ДЦ и/или надлежни вендор у складу са уговором.
2. За заштиту осталих е-података на осталим хардверским компонентама задужен је Корисник који на њима обавља своја радна задужења

#### **(5) ИКТ документација**

Техничка и корисничка документација ИКТ система, као и унутрашње опште акте и процедуре које се односе на ИКТ системе, чувају се на серверу Дата центра и за њу је задужен начелник Дата центра.

#### **Пописивање имовине**

Институт једном годишње, у складу са законом и подзаконским актима, врши попис, у оквиру чега се води и евиденција хардверских компоненти.

#### **Власништво над имовином, прихватљиво коришћење имовине и њен повраћај**

Правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација, уређују се Процедуром о коришћењу имовине.

6. **Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности**

#### **Члан 12.**

Ниво заштите података у оквиру ИКТ система Института:

- одговара осетљивости и важности података,

- одговара штети која може настати услед неовлашћеног откривања, измене, брисања или уништења података,
- у складу је са законским прописима које уређују питања заштите података као што су пословна тајна, тајни подаци и подаци о личности.

*Класификациона шема поверљивости података Института* базира на следећа четири нивоа поверљивости података:

- *Поверљиви подаци* су они чије откривање има озбиљан утицај на дугорочне стратешке циљеве или угрожава опстанак. То су креденцијали Администратора ДЦ, креденцијали групе Администратора ДЦ, кориснички креденцијали, креденцијали групе Корисника.
- *Пословни подаци* су сви подаци на које се односи Закон о заштити пословне тајне ("Сл. Гласник РС", бр. 72/2011)
- *Интерни подаци* су сви подаци из медицинске документације пацијената Института као и подаци о запосленима Института на које се односи Закон о заштити података о личности ("Сл. Гласник РС", бр. 97/2008, 104/2009 - др. Закон, 68/2012 - одлука ус и 107/2012).
- *Јавни подаци* су они чије откривање не изазива никакву штету. То су подаци који су доступни на WEB сајту Института, подаци који се јавно презентују и остали подаци на које се односи Закон о слободном приступу информацијама од јавног значаја ("Сл. гласник РС", бр. 120/2004, 54/2007, 104/2009 и 36/2010)

Приступ поверљивим подацима имају само одређени запослени који су истовремено и одговорни за њихову безбедност. Поверљиви подаци не смеју да се складиште ван ИС система где се иначе налазе у енкриптованом облику, као ни да се преносе путем мобилних уређаја или путем електронске поште.

Руковање пословним и интерним подацима ИКТ система Института се спроводи у складу Процедуром за поступање, обраду, складиштење и пренос података. Право и обим приступа пословним и/или интерним подацима ИКТ и ИС система Института остварују запослени путем својих креденцијала, који се додељује, мењају или укидају у складу са Процедуром о правима приступа ИКТ систему.

Приступ јавним подацима имају сви. Обрада, складиштење и пренос јавних података је дозвољена.

## 7. Заштита носача података

### Члан 13.

Носачи података су све врсте меморијских предмета и уређаја који се користе за складиштење и пренос података. Овај сегмент опреме обухвата дискове који су фиксни део ИКТ система, али и уређаје и носаче који се користе за пренос података (УСБ-Flash

меморије, екстерни дискови, ЦД, ДВД, као и остали предмети и компоненте који имају могућност чувања и преноса података).

Сем на серверима ДЦ, на осталим носачима података се не смеју налазити поверљиви подаци, већ само пословни, интерни или јавни подаци.

### **Употреба носача података**

У оквиру ИКТ система Института дозвољено је коришћење свих носача података који су власништво Института и који се користе на следећи начин:

- Дискови сервера, као носачи података поверљивих, пословних и интерних података се користе искључиво у просторијама ДЦ и за њихову безбедност задужен је Инжењер за ИТ безбедност ДЦ.
- Дискови рачунара, као носачи пословних и интерних података, се користе искључиво у просторијама Института и за њихову безбедност су задужени запослени који користе радне станице за обављање пословних активности или запослени који је задужен за ту радну станицу.
- Дискови мобилних рачунара или екстерна меморија орталих мобилних уређаја, као носачи пословних и интерних података, се може користити на безбедном месту које је и ван просторија Института. За њихову безбедност су задужени запослени који користи и дужи мобилни уређај за обављање пословних активности.
- Покретни носачи података се користе за пренос пословних, интерних или јавних података. Запослени који их користе у пословне сврхе, дужни су да поступају у складу са Процедуром за управљање преносним носачима података и задужени су за њихову безбедност.

У оквиру *Базе ИКТ ресурса и услуга ДЦ*, Дата центар води евиденцију о рачунарима, серверима и покретним носачима податка који су власништво Института.

Употреба носача података на којима су пословни, интерни или јавни подаци је у складу са Процедуром за поступање, обраду, складиштење и пренос података.

Носачи података који су фиксни део ИКТ система Института (дискови сервера и радних станица) не могу да се користе у другим ИКТ системима док се подаци који су записани на њима трајно не униште.

### **Сервисирање и расхоровање носача података**

Сервисирање радних станица, сервера, мобилних уређаја који су у власништву Института се обавља у Дата центру у складу са Процедуром о одржавању рачунарске опреме и ажурирања система. Уколико је носач података неисправан тада се од сервисера наручује нови носач података који се у Дата центру уграђује у радну станицу, сервер или мобилни уређај. Тиме се ризик од доласка пословних и интерних података до неовлашћених особа своди на минимум.

Уколико се процени да је носач података неисправан и да се не може користити, тада се они расходују у складу са Процедуром за безбедно расхоровање носача података.

Исправност и процену потребе за расходовањем преносних носача података, врши спроводи Корисник.

#### **Физички пренос носача података**

Дискови сервера и радних станица се сервисирањем у Дата центру не износе из просторија Института.

Мобилни уређаји се транспортују у складу са Процедуром о коришћењу мобилних уређаја.

Преносни носачи податка се транспортују у складу са Процедуром за управљање преносним носачима података.

### **8. Ограничење приступа подацима и средствима за обраду података**

#### **Члан 14.**

Приступ подацима у ИКТ систему Института је дозвољен само лицима која за то имају правни основ, у складу са уговором.

Приступ поверљивим подацима ИКТ система Института имају само одговарајући запослени који су истовремено и одговорни за њихову безбедност.

Приступ пословним и интерним подацима ИКТ система Института је ограничен тако да је Кориснику ИКТ система омогућен приступ само оним подацима и деловима ИКТ система који су му потребни за реализацију активности за које је надлежни на основу важећег Правилника о унутрашњој организацији и систематизацији послова или одговарајућег уговора. Сваком Кориснику се додељује, мења или укида право приступа пословним и интерним подацима у складу са Процедуром о правима приступа ИКТ систему и Процедуром о приступу мрежи и мрежним уређајима.

Приступ јавним подацима имају сви запослени.

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

#### **Члан 15.**

Одобравање овлашћеног и спречавање неовлашћеног приступа ИКТ систему Института се врши:

- хардверски, где се приступ додељује и укида у складу са Процедуром о приступу мрежи и мрежним уређајима
- корисничким крeденцијалима.

Кориснички крeденцијали који се састоје од корисничког имена и лозинке, где се лозинке сматрају поверљивим подацима. Кориснички крeденцијали могу имати форму администраторског или корисничког налога који се додељују, евидентирају, мењају или укидају у складу са Процедуром о правима приступа ИКТ систему.

Овлашћен приступ ИКТ систему Института је одобрен само лицима са администраторским или корисничким налогом.

Додела и коришћење администраторских налога је контролисана и ограничена само на Администраторе ДЦ или вендоре, у складу са уговором. Додела и коришћење корисничких налога је контролисана и ограничена само на запослене Института који користе ИКТ систем за обављање својих послова.

## **10. Утврђивање одговорности Корисника за заштиту сопствених средстава за аутентикацију**

### **Члан 16.**

Приступ ИКТ систему Института базиран је на корисничким крeденцијалима те су корисници ИКТ система дужни да поштују следећа правила:

1. Администратори ДЦ генеришу корисничке крeденцијале уз присуство Корисника који самостално и тајно генерише своју лозинку;
2. уколико приликом развоја ИКТ система Администратор аутоматски креира корисничке налоге са иницијалном лозинком Корисника, потребно је да Корисник измени иницијалну лозинку приликом прве пријаве у систем;
3. све лозинке Корисника се чувају у базама или датотекама ИС система које се налазе на серверима ДЦ, у енкриптованој форми, тако да нико па ни систем Администратор не може да их прочита;
4. у случају појаве безбедносног ризика, Администратор ДЦ има могућност да ресетује лозинке Корисника.

Како лозинке Корисника имају статус поверљивих података, ради спречавања безбедносних претњи и ризика услед откривања података за аутентификацију запослених, корисници ИКТ система Института су у обавези да:

- држе у тајности и чувају своје лозинке;
- не деле лозинке са другим Корисницима;
- избегавају чување лозинки у писаном облику;
- лозинке не шаљу електронском поштом;

- онемогућавају злоупотребу својих креденцијала обавезним изласком из ИКТ система Института по завршетку радних задатака;
- мењају лозинке увек када постоји наговештај злоупотребе, могућег компромитовања или другог безбедносног ризика.

За заштиту лозинки и других сопствених средстава за аутентикацију одговорни су сви корисници ИКТ система и то:

- (1) запослени, у складу са овим правилником, и
- (2) вендори, у складу са одговарајућим уговором.

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

### Члан 17.

Институт користи криптозаштиту (енкрипцију) за пренос пословних и интерних података преко ИС приликом комуникације са државним институцијама (РФЗО, Министарство здравља-ИЗИС, Управа за трезор, и сл), или са запосленима Института који раде у просторијама које Институт користи и налазе се ван његове зграде. Систем за управљање криптографским кључевима спроводи државна институција или одговарајући вендор.

Криптозаштитом се обезбеђује:

- Аутентикација (идентификацију Корисника и других системских ентитета који захтевају приступ или одобрење трансакције);
- Непоречиност (примена криптографских техника како би се добила потврда о извршавању или неизвршавању неке трансакције од стране појединачног Корисника);
- Поверљивост (применом шифровања врши се заштита осетљивих података који се складиште или се преносе);
- Интегритет (непроменљивост података који се преносе).

У оквиру ИКТ система, криптозаштита се користи уз поштовање следећих правила:

- Енкрипција се користи за заштиту лозинки Корисника на серверима Дата центра као и осетљиве и поверљиве ИКТ системе којима се приступа споља.
- Енкрипција било којих других информација или ресурса организације мора претходно бити одобрена.
- Минимална дужина енкрипционог кључа је 128-бит. Сигурност енкрипционог

система веома зависи од тајности коришћених енкрипционих кључева.

- Енкрипциони кључеви се не смеју слати путем *e-mail*-а.
- Коришћење технологије јавних кључева захтева да се креира и одржава јавни и приватни кључ за сваког Корисника.
- Јавни кључеви се морају дистрибуирати или складиштити на такав начин који ће омогућити приступ само одређеним корисницима.

У оквиру система се користе следеће механизме енкрипције:

1. **SSL (Secure Socket Layer)**, који користи асиметричну енкрипцију за аутентификацију и симетричну енкрипцију за заштиту комуникационих сесија. *SSL* се у Институту користи за енкрипцију комуникације веб сервиса.
2. **IPSec** који се у организацији користи за успостављање *VPN* тунела за спољне конекције на системе организације.
3. **L2TP (Layer 2 Tunneling Protocol)**, протокол за успостављање тунела који се користи за подржавање *VPN*-а и служи за успостављање спољних конекција на системе.
4. **SSH (Secure Shell)** успоставља енкриптовани тунел између *SSH* клијента и сервера, и користи се за удаљену администрацију сервиса и пренос података приликом спољних конекција.
5. **WPA2- PSK (AES) (WPA2: Wi-Fi Protected Access 2; PSK: Pre-Shared Key; AES: Advanced Encryption Standard)** протокол за успостављање спољних конекција на системе путем *wireless* мреже

Управљање криптографским кључевима има следеће карактеристике:

- потпуно је аутоматизовано те запослени немају могућност утицаја на креирање кључа;
- подаци су заштићени јер се ниједан податак никада не појављује као чист текст када је енкриптован коришћењем кључа за енкрипцију кључева (кључ за енкрипцију кључева се користи за енкриптовање других кључева, што их штити од откривања);
- у зависности од потребе, кључеви се мењају најмање једном у три године.

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

### Члан 18.

У служби надзора новлашћеног приступа, просторије Института су физички заштићене на више начина: стандардним физичким препрекама којима се спречава неовлашћени

приступ (решетке, врата са сигурносним бравама, итд) и обезбеђењем Института (пријавница са службеницима обезбеђења задуженим за праћење приступа).

Приступ Институту се контролише употребом идентификационих картица запослених, картицама за приступ појединим зонама Института, као и непрекидним видео-надзором.

Сва потребна опрема за безбедност физичког окружења се редовно одржава.

### **Зона раздвајања и успостављање система физичке безбедности**

Институт предузема додатне мере ради спречавања неовлашћеног физичког приступа свим службеним просторијама у којима се налази ИКТ опрема. Опрема за обраду информација се штити закључавањем просторија у којима се налази. У складу са проценом ризика на Институту постоје следеће зоне:

- (1) Дата центар,
- (2) серверска сала Дата центра и
- (3) Службене просторије са радним станицама и осталом ИКТ опремом.

#### **(1) Дата центар**

Просторије Дата центра, у којима се налази серверска сала и документа која су саставни део ИКТ система Института, представљају безбедну зону у оквиру објекта Института. Карактеристике простора Дата центра су следеће: налазе се у згради Института, на спрату те нису лако доступне неовлашћеном приступу; зидови и подови су од чврстог материјала; простор Дата центра је видно обележен; не поседују спољна врата, већ централни улаз са механичком бравом, који је доступан из унутрашњости зграде Института (ходник, коме је приступ обезбеђен видео-надзором); сва унутрашња врата су заштићена од неовлашћеног приступа помоћу врата са механичком бравом; врата и прозори су закључани у свим случајевима када су без надзора; централни кључ простора Дата центра је јединствен, без копије, и приступ њему имају само запослени Дата центра, обезбеђења Института и спремачица; свака канцеларија Дата центра има посебан кључ који се чува у Дата центру, а приступ овим кључевима имају само запослени Дата центра и спремачица; приступ просторијама Дата центра имају само запослени Института, вендори и трећа лица уз одобрење начелника Дата центра.

#### **(2) Серверска сала Дата центра**

Сервери ИКТ система Института су смештени у серверској сали Дата центра која има следеће карактеристике: налази се у згради Института, на спрату, унутар Дата центра, са подовима и зидовима од чврстог материјала; серверска сала је видно обележена; ради спречавања загађења из околине, просторија је без прозора и без спољних врата, већ се у њу улази из канцеларије Дата центра од које је деле посебна врата са механичком бравом; поседује електропроводни под и клима уређај који обезбеђује потребну температуру, влажност и вентилира ваздух; под непрекидним је видео-надзором; ради спречавања неовлашћеног физичког приступа, серверска сала поседује тростепену физичку препреку у

виду забрављених врата са сигурносним бравама – централна врата просторија Дата центра са механичким кључем, врата канцеларије са механичком бравом из које је улаз у серверску собу и врата серверске сале са механичком бравом; приступ кључу серверске сале имају само Администратори ДЦ; приступ серверској сали је ограничен само на овлашћене појединце – запослене ДЦ, вендоре или трећа лица, уз одобрење начелника Дата центра; приступ сервер сали је под обавезним надзором од стране Администратора ДЦ. У циљу контроле уласка у серверску салу, у Дата центру се води евиденција приступа серверској сали од стране вендора или, уз одобрење начелника Дата центра, трећих лица: име лица, датум и време улазака и излазака из серверске собе.

### **(3) Службене просторије са радним станицама и осталом ИКТ опремом**

Физички су заштићене и све службене просторије са радним станицама: налазе се у просторијама чији је Института власник или корисник, са кровом, подовима и зидовима од чврстог материјала; сва просторије су заштићене од неовлашћеног приступа помоћу врата са сигурносним бравама, видео надзором ходника и улаза у зграду као и обезбеђењем Института; врата и прозори су закључани у свим случајевима када су без надзора.

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

### **Члан 19.**

#### **Постављање и заштита опреме**

ИКТ опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења. Поред обезбеђења, непрекидног видео-надзора и физичких заштита (решетке, врата са механичким и електронским бравама) Институт има и систем за противпожарну заштиту и усвојена документа: План евакуације и упутство за поступање у случају пожара; Правила заштите од пожара. Серверска сала располаже и противпожарним апаратом.

Редовну контролу система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, електричну енергију врше Служба за техничке и друге сличне послове Инжењери заштите.

Сервери су заштићени од свих врста удара и физичких оштећења, од претерано високих или ниских температура, електромагнетних зрачења, као и од сувише високе или ниске влажности ваздуха. Сервери се налазе на гаск орманима изнад патоса како би се избегла оштећења у случају поплаве.

У серверској сали се редовно прате температура, влажност и други услови околине који би могли негативно да утичу на рад опреме за обраду информација.

### **Помоћне функције за подршку**

Сервери користе уређаје за непрекидно напајање електричном енергијом (Uninterruptible Power Supplies - UPS) чији се рад прати а уређаји се благовремено сервисирају.

У случају прекида електричног напајања ван радног времена Дата центра, службеници обезбеђења Института су дужни да у најкраћем року о престанку електричног напајања обавесте начелника Дата центра. У случају да је прекид електричног напајања дужи од капацитета УПС-а, начелник Дата центра ангажује Администратора ДЦ да искључи сервере Дата центра у складу са Процедуром за укључивање и искључивање сервера.

### **Безбедносни елементи приликом постављања каблова**

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се оштећења и неовлашћеног приступа постављањем истих у зид или каналице на безбедној или оптималној висини.

### **Одржавање опреме**

Одржавање рачунарске опреме врши се у складу са Процедуром о одржавању рачунарске опреме и ажурирања система како би се осигурали њихова непрекидна расположивост и неповредивост.

### **Безбедност током измештања и премештања имовине**

Измештање и премештање рачунара са носачима података могу да врше:

- Администратори ДЦ унутар просторија Института у складу са Процедуром о приступу мрежи и мрежним услугама којом се омогућавају безбедносни механизми заштите измештене опреме
- корисници изван просторија Института, у складу са Процедуром о коришћењу мобилних уређаја којом се омогућавају безбедносни механизми заштите измештене опреме

Измештање и премештање рачунарске опреме која нема носаче података врши:

- Администратор ДЦ унутар просторија Института у складу са Процедуром о приступу мрежи и мрежним услугама
- одговарајући вендор за сервисирање за потребе поправке, у складу са уговором којим се омогућавају безбедносни механизми заштите измештене опреме

Измештање и премештање софтвера и података врше Администратори ДЦ и/или надлежни вендори, у складу са уговором којим се омогућавају безбедносни механизми заштите софтвера и података.

### **Безбедно расходовање или поновно коришћење опреме**

Администратор ДЦ проверава и процењује употребљивост коришћене опреме. У случају да је треба расходовати тада се делови опреме који садрже носаче података се расходују у складу са Процедуром за безбедно расходовање носача података. Остала ИКТ опрема се расходује у складу са Процедуром за расход.

У случају да се опрема може поново користити, поступа се у складу са Процедуром о приступу мрежи и мрежним уређајима. Ако се делови опреме могу поново користити онда

се они уграђују у другу опрему и поступа се у складу са Процедуром о инсталацији и конфигурацији система.

#### **Остављање осетљивих и поверљивих докумената и материјала**

Сва осетљива и поверљива документа и материјали се уклањају са радне површине и одлажу на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе. У раду са осетљивим, поверљивим документима и материјалима (електронским или папирним), Корисник је дужан да поступа у складу са Процедуром за остављање осетљивих и поверљивих докумената и материјала.

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

#### **Члан 20.**

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, ИНСТИТУТ је дефинисао процедуре за руковање средствима за обраду података које које садрже инструкције за детаљно извршење следећих послова:

- а) инсталација и конфигурација система се ради униформно у складу са Процедуром о инсталацији и конфигурацији система;
- б) обрада и поступање са информацијама се ради у складу са Процедуром за поступање, обраду, складиштење и пренос података;
- в) руковање са преносним носачима података се ради у складу са Процедуром за управљање преносним носачима података;
- г) одржавање опреме се ради у складу са Процедуром о одржавању рачунарске опреме и ажурирања система;
- д) израда резервних копија се ради у складу са Процедуром за израду резервних копија;
- ђ) инструкције за поступање према грешкама или другим ванредним стањима која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција су дефинисане Процедуром за рад Дата Центра (опција Измена е-података и е-докумената);
- е) контакти за подршку, у случају неочекиваних оперативних или техничких потешкоћа су контакти са Одељењем Дата центар складу са Процедуром за рад Дата Центра;
- ж) инструкције за поступања према поверљивим подацима су дефинисане уговорима и изјавом о поверљивости;
- з) процедуре за поновно покретање система и опоравак, које се користе у случају отказа система се ради у складу са Процедуром за укључивање и искључивање сервера.

У случају промене у организацији, пословним процесима и средствима за обраду информација и на системима које имају утицај на безбедност информација поступа се у складу са Процедуром о правима приступа ИКТ систему.

Свакога јутра начелник Дата центра извештава Стручни колегијум о стању ИКТ система и оперативном функционисању свих информационих система.

#### **Управљање расположивим капацитетима**

Коришћење ресурса се надгледа, подешава и пројектује у складу са захтеваним капацитетима у наредном периоду, како би се осигурале захтеване перформансе система. Потребне за одржавањем и унапређењем система се исказују у оквиру Плана рада, Плана јавних набавки и Плана стручног усавршавања.

У циљу оптимизације расположивих капацитета, периодично се спроводе следе активности:

- а) брисање застарелих података које спроводе Администратори ДЦ (ако су подаци на серверима ДЦ и не подлежу трајном чувању) и корисници (ако су подаци на радним станицама и не подлежу трајном чувању);
- б) повлачење из употребе апликација, система, база података или окружења и њихово архивирање;
- в) оптимизација серије процеса и распореда;
- г) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису критичне за пословање.

#### **Раздвајање окружења за развој, испитивање и рад**

У циљу смањења ризика од промена у радном окружењу или неовлашћеног приступа, окружење за развој и испитивање система је доступно само запосленима Дата центра и/или одговарајућим вендорима. Када год је то могуће, прави се тестно окружење које је одвојено од оперативног и не садржи осетљиве податке из ИКТ система Института.

Одговарајући вендори обавештавају и документују правила за преношење софтвера из развојног или модификованог статуса у оперативни статус. Вендори се старају:

- да се развојни и радни софтвери извршавају на различитим системима или рачунарским процесорима, као и у различитим доменима или директоријумима;
- да се промене у радним системима и апликацијама испитују у окружењу за испитивање или режиму одржавања пре него што се примене на радним системе;
- да се испитивање не ради на радним верзијама система, осим у изузетним околностима;
- да компајлери, едитори и други развојни алати или системски помоћни програми не буду доступни из радних верзија система, ако се то не захтева;
- да се осетљиви подаци не копирају у системско испитно окружење, осим ако нису обезбеђене еквивалентне контроле за систем за испитивање.

## **15. Заштита података и средстава за обраду података од злонамерног софтвера**

### **Члан 21.**

Злонамерни софтвер (енгл. malware) јесте сваки програм направљен у намери да (1) оштети неки умрежен или неумрежен рачунар; (2) да компромитује поверљивост, интегритет или доступност жртвиних података; (3) да злоупотреби апликације или оперативни систем; (4) да на неки од начина омете, успори, угрози или онемогући рад жртве на рачунару. Злонамерни софтвер се најчешће тајно убацује у ИКТ систем или његов део, а обухвата вирусе, црве, spyware, adware, nagware, backdoors, exploits, тројанаци, rootkits, keyloggers итд.

У циљу заштите свог ИКТ система од злонамерног софтвера, Институт примењује и унапређује мере које обухватају: праћење и контролу података, софтвера и хардвера; спречавање и откривање напада злонамерним софтвером; опоравак ИКТ система након напарад злонамерног софтвера а све у складу са Процедуром о заштити од злонамерног софтвера.

Институт користи искључиво лиценцирани антивирусни софтвер који штити ИКТ систем од злонамерног софтвера. Корисницима је сторго забрањено искључивање антивирусног софтвера.

## **16. Заштита од губитка података**

### **Члан 22.**

Стварање резервне копије (backup) не утиче на степен безбедности самог система, али је од кључног значаја ако се после безбедносне кризе јави потреба да се изгубљени подаци поврате. У Институту се врши израда резервних копија које обухватају податке који су од виталног значаја у складу са Процедуром за израду резервних копија.

Резервне копије сервера се налазе у закључаним просторијама и штите се од свих врста физичких повреда.

## **17. Чување података о догађајима који могу бити од значаја за безбедност ИКТ система**

### **Члан 23.**

У оквиру ИКТ система Института, болнички ИС Хелиант садржи медицинску документацију свих пацијента те је пројектован тако да се формирају и памте записи о

свим активностима Корисника (логови) унутар тог ИС. Логови Хелианта садрже податке о следећим активностима:

- идентификаторе Корисника који је приступао систему;
- име и презиме Корисника;
- име и презиме пацијента чијој медицинској документацији је Корисник приступао;
- разлог приступа медицинској документацији;
- датум и време пријављивања и одјављивања;
- идентитет уређаја (кроз ИП адресу) са ког је приступао систему;
- назив документа коме је приступао;
- активнос коју је спроводио над документом: креирање, измена, брисање;
- назив податка коме је приступао;
- активност коју је спроводио над податком креирање, измена (са садржајем измене), брисање.

Логови Хелианта се чувају 2 месеца и служе за потребе претраге по: имену и презимену Корисника; имену и презимену пацијента; разлогу приступа; времену приступа и опису приступа.

Хелиант пржа и могућност увида у тренутно пријављене Кориснике као и у време пријаве.

#### **Заштита информација у записима**

Логови Хелианта су заштићени од неовлашћеног мењања и приступа. За потребе контроле приступа подацима, Администратори ДЦ имају право приступа логовима Хелианта у циљу прегледа и увида у активности Корисника, али без могућности измене, брисања или деактивирања дневника о било чијим активностима. Администратори ДЦ добијају право приступа помоћу администраторског налога, а штити администраторским креденцијалима.

Запослени који користе ИКТ систем Института немају приступ логовима Хелианта.

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

### **Члан 24.**

У ИКТ систему може да се инсталира само софтвер и оперативни систем за који постоји важећа лиценца у власништву Института, односно Freeware и Open source верзије.

Инсталацију и подешавање софтвера може да врши само Администратор ДЦ и вендори и то за портребе ИС који одржавају у складу са уговором. На Институту је обезбеђено униформно конфигурирање радних станица и њихових оперативних система у складу са

Процедуром о инсталацији и конфигурацији система од стране оспособљених Администратора ДЦ.

Одржавање рачунарске опреме и ажурирање оперативних система спроводе Администратори ДЦ у складу са Процедуром о одржавању рачунарске опреме и ажурирања оперативних система.

Тестирање безбедности система спроводи Инжињер за ИТ безбедност.

У договору са вендором, плански се спроводи имплементација нових верзија ИС тек након обимног и успешног тестирања. У случају неуспешне имплементације нове верзије спроводи се враћања на претходну верзију ИС.

## **19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система**

### **Члан 25.**

Институт 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.

#### **(1) Управљање техничким рањивостима**

Институт прикупља информације о техничким рањивостима ИС који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимањем у обзир припадајуће ризике.

#### **Прикупљање информација о техничким рањивостима ИС**

Прикупљање информација о техничким рањивостима ИС је у складу са могућностима ИС-а. Инжињер за ИТ безбедност ДЦ прати рад ИКТ система и врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др ) у циљу идентификације потенцијалних слабости ИКТ система.

Инжињер за ИТ безбедност ДЦ врши периодичне тестове безбедности ИКТ система (penetration testing) како би идентификовао слабости у безбедносним процедурама ИКТ система. Ови тестови обухватају све сегменте ИКТ система, а пре свега приступ споља кроз "brute force" нападе. Приликом спровођења тестирања, Инжињер за ИТ безбедност ДЦ води рачуна да ове активности не утичу на нормално функционисање система, или да њихов утицај буде минимализован. Практично, најбоље је да обим тестова буде ограничен, или да се они спроводе ван радног времена или током викенда, кад је то могуће.

#### **Вредновање рањивости**

Техничке рањивости се вреднују према прекиду у функционисању система који може бити на:

- једној радној станици
- више радних станица и/или делу рачунарске мреже
- целом једном информационом систему
- целом ИКТ систему

Техничке рањивости се вреднују и према степену угрожености вршења послова и/или пружања услуга Института. У складу са тим, послови се групишу према следећем критеријуму:

- послове свих запослених чиме је угрожено пружања услуга Института па самим тим и лечење свих пацијената који су у том тренутку у Институту (узрокована угроженошћу сервера, мреже, и др.)
- послове дела запослених због које је угрожено лечење амбулантних пацијената који су у том тренутку у Институту (узрокована угроженошћу дела мреже или система који на пример ради на конзилијуму, у амбуланти на пријему, у дневним болницама, на радиолошкој дијагностици, на шалтерима, и др.)
- послове дела запослених због које је угрожено лечење стационарних пацијената који су у том тренутку у Институту (узрокована угроженошћу дела мреже или система који на пример ради на стационару или у лабораторији и др.)
- послове са дефинисаним роковима (напр. послови запослених у Одсеку за план, анализу и обрачун реализације непосредно пре пуштања фактуре; послови запослених у Одсеку финансијске оперативе непосредно пре пуштања плата; послови запослених у Одсеку књиговодства непосредно пре израде биланса и др.)
- остали послови због којих је отежан рад запослених у Институту (напр. запослених у Одељењу за правне послове, Служби за техничке и друге сличне послове послови којима је потребан инетернет и сл.)

### **Предузимање одговарајућих мера**

У складу са процењеним рањивостима и у договору са одговарајућим вендорима, Дата центар предузима мере и акције у циљу исправке рањивих делова ИКТ система, а све у циљу смањивања безбедносних ризика и спречавања злоупотребе техничких безбедносних слабости ИКТ система. Акције које се могу спровести су: едукација; измена процедура рада; измена постојећих верзија ИС, измена ИС кроз нове верзије или набавка (хардвера, софтвера, услуга, система и сл.).

Дата центар процењује и у зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, предузима активност које су везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности.

Управљање техничким рањивостима се усклађује са активностима које се односе на управљање инцидентима, тако да обезбеди процедуре које треба спровести ако се догоди неки инцидент.

### **(2) Ограничења у погледу инсталације софтвера**

Инсталирање софтвера врше Администратори ДЦ, као овлашћена лица са адекватним образовањем, и одговарајући вендори у складу са уговором. Осталим лицима је забрањена инсталација софтвера у ИКТ систему Института.

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

### Члан 26.

Институт планира адекватно време спровођења ревизије и редослед активности који не ометају пословне процесе Института. У зависности од потреба, ревизије она може бити на:

- Радној станици – тада, у договору са Корисником, ревизија се ради у периодима када се неће ометати процес рада. Уколико то није могуће, Кориснику се даје заменска радна станица у трајању до краја сервисирања.
- Делу мреже – тада, у договору са руководиоцима организационих јединица чији запослени раде на том делу мреже, ревизија се ради у периодима када се неће значајно ометати процес рада.
- Мрежу, серверима или ИС – у договору са вендором, ревизија се ради у периодима када је смањена потреба за коришћење ИКТ система (током поподнева или викендом) уз обавезно претходно обавештавање Корисника.

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

### Члан 27.

У Институту постоји више интерних мрежа (*ОНКОЛОГИЈА, ИМПАК, PACS*), а користи се и *Телеком WiFi* мрежа за бежични приступ интернету.

Комуникациони каблови и каблови за напајање електричном енергијом, постављени су у зидовима или каналицама а мрежна опрема (switch, router) се налази у закључаним rack орманима. На тај начин је обезбеђена њихова изолација, физичка заштита и заштита од неовлашћеног приступа. Приступ мрежи и мрежној опреми имају Администратори ДЦ са или без одговарајућих вендора, у циљу измене или контроле мрежне инфраструктуре. У случају потребе, Администратори ДЦ са или без одговарајућих вендора благовремено предузимају мере у циљу отклањања евентуалних неправилности.

Бежична мрежа *Телеком WiFi* за приступ интернету је одвојена од интерних мрежа ИКТ система кроз које се врши размена пословних и интерних података. *Телеком WiFi* бежичну мрежу могу да користе запослени као и сви посетиоци објекта Института.

На Институту је омогућен и ВПН приступ ИКТ систему Института у складу са Процедуром за ВПН приступ ИС. Подаци, који се преносе оваквим путем, се енкриптују како не би били јасно видљиви приликом преноса.

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

### **Члан 28.**

Заштита података који се размењују комуникационим средствима унутар ИКТ система Института, или са другим ИКТ системима организација или трећих лица, обезбеђена је интерним процедурама, уговорима и споразумима са организацијама и трећим лицима, као и применом адекватних контрола.

Информације Института се штите, користе или објављу на одговоран и ауторизован начин од стране запослених или трећих лица, у складу са уговорима и изјавом о поверљивости, који су обавезујући за све потписнике

#### **Правила коришћења електронске поште**

Као средство унапређивања продуктивности, Институт подстиче пословну употребу електронских комуникација (електронска пошта, интернет, видеоконференције, *online chat*, портали за учење на даљину итд.). Стога се Електронска пошта Института користи у складу са Процедуром о безбедности у размени електронских порука.

#### **Правила коришћења интернета**

Приступ садржајима на интернету је дозвољен искључиво за пословне намене. Инжињер за ИТ безбедност периодично надзире и контролише коришћење интернета и у случају злоупотребе или угрожавања безбедности он задржава право да укине могућност приступа о чему извештава начелника ДЦ који обавештава Директора Института.

Приступ садржајима на интернету је дозвољен искључиво за пословне намене. Објављивање садржаја на интернету који се тичу Института се обавља у складу са Процедуром за односе са јавношћу.

#### **Правила коришћења информационих ресурса**

ИКТ ресурси Института се користе искључиво у пословне сврхе, на раду или у вези са радом у складу са процедуром Процедуром за поступање, обраду, складиштење и пренос података.

Размена података са ИКТ системима институција (РФЗО, Министарство здравља, Трезор Народне банке, Институт за јавно здравље, Завод за јавно здравље и др.) базирана је на поштовању истих стандарда безбедности података као и одредбама *Закона о заштити података о личности* када су предмет преноса подаци о личности, а врши се у складу са уговорима, протоколима и интерним упутствима између Института и тих субјеката за текућу годину.

Безбедан пренос пословних и интерних информација између Института и организација, установа, правних лица и др. обезбеђују су у складу са законом и уговорима.

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

#### **Члан 29.**

Стандарди информационе безбедности постављају се у оквиру сваке фазе развоја ИКТ система Института: фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе. Развој новог или замена постојећег дела ИКТ система се увек реализује у складу са планом набавки или у оквиру пројектата.

#### **Анализа и спецификација захтева за безбедност информација**

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

Захтеви за безбедност информација укључују:

- проверу идентитета Корисника;
- доступност, поверљивост, непорецивост и интегритет података и имовине;
- надгледање пословних процеса;
- омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке Кориснике.

Спецификација захтева мора узети у обзир аутоматску контролу која ће бити уведена у информациони систем и потребу да такође постоји и ручна контрола, која мора бити примењена при вредновању пакета софтвера, развијених или купљених, за пословне апликације.

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

Формално тестирање и процес имплементације се примењује за нове као и за модификоване делове ИКТ система. У уговору са вендором се дефинишу се захтеви безбедности.

#### **Обезбеђивање апликативних услуга у јавним мрежама**

Информације обухваћене апликативним услугама које пролазе кроз јавне мреже се штите од малверзација, неовлашћеног откривања података и модификовања, у складу са

интерним правилима и процедурама, уговорима и споразумима са организацијама и трећим лицима, као и применом адекватних контрола.

Потврда идентитета Корисника, подела овлашћења и одговорности за постављање садржаја, електронског потписивања или обављања трансакција јесу у складу са радним задацима запосленог и садржани су у креденцијалима Корисника који су му додељени.

#### **Заштита трансакција апликативних услуга**

Информације укључене у трансакције апликативних услуга се штите да би се спречио непотпун пренос, погрешно усмеравање, неовлашћено мењање порука, неовлашћено разоткривање, неовлашћено копирање порука или поновно емитовање.

Енкриптовање података се користи приликом коришћења ВПН приступа или комуникације преко портала институција, док се безбедност у размени електронских порука постиже Процедуром о безбедности у размени електронских порука.

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

### **Члан 30.**

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

Тестирање могу да врше одговарајући вендори у складу са уговором који има клаузулу о поверљивости података, запослени Дата центра или други запослени, именовани од стране руководиоца одговарајуће организационе јединице.

За потребе испитивања и тестирања ИКТ система, односно делова система, Институт избегава коришћење оперативних (пословних и интерних) података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачну личност (пацијента, запосленог или др.).

Уколико је за тестирање неопходно користити оперативне податке, тада се примењују следеће мере безбедности:

- за потребе тестирања ИКТ система односно делова система, се користе подаци који нису осетљиви
- уколико се за сврху испитивања користе лични подаци или неке друге поверљиве или осетљиве информације, онда се користи метода „измишљене особе“ (тзв. „тест пацијент“) чији подаци нису стварни али симулирају стварне.
- уколико се за сврху испитивања морају користити лични подаци тада се свако копирање оперативних података у тестно окружење врши се под надзором Дата центра а у складу са уговором.

- Дата центар, одговарајући вендори или други запослени, именовани од стране руководиоца одговарајуће организационе јединице, дужни су да штите, чувају и контролишу податке у тестном окружењу на одговарајући начин
- оперативне информације се одмах по завршетку испитивања бришу из тестног окружења

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

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

### **Члан 31.**

Ниво приступа и безбедносни стандарди који су неопходни како би се одговарајућим вендорима омогућио приступ подацима, информацијама, средствима или опреми за обраду информација ИКТ система Института, регулишу се уговорима између Института и вендора. Такви уговори садрже уговорну клаузулу о заштити и чувању поверљивости информација, података и документације која је у складу са Упутством за клаузулу о поверљивости податка.

Институт успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга у складу са Процедуром о безбедности информација које су доступне пружаоцима услуга.

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

### **Члан 32.**

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, Институт успоставља мере надзора и заштите за време пружања услуга и након извршеног посла. Дата центар је одговоран за праћење и надзор вендора током извршавања обавеза из уговора.

### **Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга**

Дата центар редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

- Надгледање и преиспитивање услуга се може вршити преко трећег лица;
- Неопходно је да се поштују сви услови из споразума у вези са безбедношћу

информација, као и да се спрече сви инциденти и проблеми нарушавања безбедности, те омогући управљање на одговарајући начин;

- Врши се оцена квалитета извршења и саобразности уговорене услуге;
- Пружалац услуге има уговорну обавезу да организује и припреми периодичне састанке који ће обезбедити редовно извештавање Дата центра и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;
- Дата центар одржава максималну контролу над спровођењем услуга и осигурава увид у осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа страна приступа, процесира или којима управља;
- Дата центар одржава максимални увид у безбедносне активности кроз јасно дефинисан процес извештавања;
- Дата центар преиспитује трагове провере и записа о догађајима у вези са безбедношћу код пружаоцем услуга, оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.

#### **Управљање променама уговорених услуга од стране пружаоца услуга**

Уговором са пружаоцем услуга се обезбеђује могућност континуираног управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контролу безбедности информација. Промене које се узимају у обзир су промене у споразумима са пружаоцима услуга, повећање обима текућих услуга које се нуде, као и промене које уводи Институт ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

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

#### **Члан 33.**

Инциденти су унутрашње или спољне околности или догађаји којима се угрожава или нарушава информациона безбедност. Могу се поделити на следеће групе:

- инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга Института;
- инциденти који утичу на велики број Корисника услуга Института;
- инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;
- инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;

- инциденти који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе.

Процедуром за управљање безбедносним инцидентима у ИКТ систем се уређује начин одговора на инциденте нарушавања безбедности информација, и Инжињер за ИТ безбедност ДЦ је особа за контакт у случајевима нарушавања безбедности, као и контакте са овлашћеним телима. Инжињер за ИТ безбедност ДЦ би требало да поседује одговарајућа техничка знања како би на најбржи и одговарајућу начин могао да одговори на безбедносне инциденте.

## **28. Мере које обезбеђују континуитет обављања посла у ванредним околностима**

### **Члан 34.**

Институт примењује мере које обезбеђују континуитет обављања посла у ванредним околностима у складу са Процедуром обезбеђивање континуитета пословања током и након инцидента, како би ИКТ систем у што краћем року био у функционалном стању.

Дата центар редовно врши проверу усвојених процедура контроле континуитета безбедности информација, како би оне биле важеће и ефективне током ванредних ситуација.

Провера се врши вежбањем и испитивањем знања и рутине приликом руковања процесима, процедурама и контролама, као и преиспитивањем ефективности мера безбедности информација у случају промене информационих система, процеса, процедуре и контроле безбедности информација.

## **III.**

### **IV. ПРЕЛАЗНА И ЗАВРШНА ОДРЕДБА**

#### **Посебна обавеза Института за онкологију и радиологију Србије**

### **Члан 35.**

Обавеза Института за онкологију и радиологију Србије је да најмање једном годишње изврши проверу ИКТ система.

Измене и допуне Правилника о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Института за онкологију и радиологију Србије, врше се на начин на који је донесен овај правилник.

## Ступање на снагу Правилника о безбедности

Члан 36.

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



**ПРЕДСЕДНИК УПРАВНОГ ОДБОРА**

**Проф.др Радисав Шћепановић**

Правилник објављен на огласној табли Института \_\_\_\_\_ 2018. године и ступио је на снагу \_\_\_\_\_ 2018 године.

ОВЕРАВА

Начелник Одељења за правне послове

Бранка Кривић, дипл.правник