**Институт за онкологију и радиологију Србије**
Пастерова 14, Београд, Србија
+381 11 2067 100
iors@nerc.ac.rs www.nerc.ac.rs

РЕПУБЛИКА СРБИЈА
ИНСТИТУТ ЗА ОНКОЛОГИЈУ И РАДИОЛОГИЈУ СРБИЈЕ
Бр. 01-1/2023/3494-8
26 DEC 2023
БЕОГРАД, Пастерова 14

# ПРОЦЕДУРА ЗА УПРАВЉАЊЕ ПРЕНОСНИМ НОСАЧИМА ПОДАТАКА

| | |
|---|---|
| Ознака процедуре | **П.ДТЦ.09** |
| Верзија | 01 |
| Датум усвајања | 08.03.2018./15.12.2023. |
| Аутор процедуре | Душица Гавриловић, маст мат<br>Зорана Бизетић, маст мат |
| Носилац процедуре | Др сци. мед. др Ана Јовићевић |
| Процедуру одобрио | Доц. др Милан Жегарац |

## 1.0 ДЕФИНИЦИЈЕ И СКРАЋЕНИЦЕ

*ИОРС* је Институт за онкологију и радиологију Србије;
*ОЈ* је Организациона јединица ИОРС-а;
*ДЦ* је Дата Центар ИОРС-а;

*ИКТ систем* је информационо-комуникациони систем ИОРС-а у смислу технолошко-организационе целине 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;

*ИС (информациони систем)* је део ИКТ система ИОРС-а 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;

*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;

*Администратор ДЦ* је запослени Дата центра коме је дозвољено администрирање ИКТ и/или ИС система.

*Инжињер за ИТ безбедност* је запослени Дата центра који се бави пословима информационе безбедности;

*Корисник* је запослени ИОРС-а који има приступ ИКТ систему ради обављања својих пословних активности;

*Вендор* је треће лице са којим ИОРС сарађује по основу уговора о одржавању ИКТ система и/или ИС

*Медијум* је диск, УСБ меморија, преносиви хард диск, ЦД, ДВД, као и остали предмети и компоненте који имају могућност чувања и преноса података

*Анонимизација података* представља поступак конверзија података о личности у облик који онемогућава идентификацију личности

*Анонимизирани подаци* су подаци о личности на основу којих се не може идентификовати о којој особи је реч.

*Агрегарни подаци* су подаци који нису изворни (подаци на којима је спроведена обрада података) и из којих се не може идентификовати особа/личност (напр сумарне табеле, графикони)

## 2.0 ПРЕДМЕТ

Овом процедуром утврђују се активности, носиоци активности и одговорности при управљању преносним носачима података. Правилном применом утврђеног поступка, ИОРС своди на минимум потенцијалну изложеност штети која може настати услед недозвољеног приступа подацима.

## 3.0 ПОДРУЧЈЕ ПРИМЕНЕ

Примењује се на све преносне носаче на којима се налазе пословни и/или интерни подаци ИОРС-а.

## 4.0 ОДГОВОРНОСТИ

Сваки запослени је дужан да се понаша у складу са процедуром и у складу са својим задужењима сноси одговорност за чување и пренос пословних или интерних података ИОРС-а. Вендори или други сарадници ИОРС-а су дужни да се понашају у складу са уговором и у складу са њим сносе одговорност.

Обавеза руководиоца сваке ОЈ је да све запослене упозна са процедуром, без обзира да ли су запослени ангажовани по основу рада на одређено време, сталног радног односа или другог облика радног ангажовања.

За контролу спровођења процедуре одговорни су одговарајући руководиоци ОЈ.

## 5.0 ОПИС ПРОЦЕДУРЕ

На преносним носачима података се не смеју налазити поверљиви подаци, већ само пословни, интерни или јавни подаци.

Пословни и интерни подаци се могу налазити на преносним медијума само за Кориснике који својим корисничким налозима имају приступ таквим подацима. О преносу пословних или интерних података по потреби воде евиденцију руководиоци одговарајућих организационих јединица.

### 5.1 Чување пословних или интерних података на преносним носачима података

Пословни и интерни подаци ИОРС-а се чувају на серверима или радним станицама. Инжињер за ИТ безбедност ДЦ је одговоран за чување података на серверима. Сваки Корисник, који на радној станици чува пословне или интерне податке, одговоран је за њих.

За чување пословних или интерних података на преносним носачима података у власништву ИОРС-а задужен је Корисник, који треба да се придржава следећег:

1) Сачинити вишеструке копије вредних података на преносним носачима података.
2) Копије података треба чувати на одвојеним медијумима како би се смањио ризик од случајног оштећења или губитка података.
3) Минимални број медијума (локација за складиштење) је два, а препорука је да то буду три или четири медијума.
4) Локације сачуваних података треба да буду различите (различити делови ИОРС-а) како би подаци били сигурни у случају пожара или сличних непогода.
5) Да би се ограничила могућност губљења података, треба предвидети регистровање покретних медијума од стране одговорних лица – руководиоца ОЈ и Корисника.
6) Све преносне носаче података треба складиштити на безбедном и заштићеном месту, у складу са препорукама произвођача.
7) Треба водити рачуна о трајању преносног носача медијума, у складу са препорукама произвођача.
8) Подаци треба да буду пренети на нови медијум пре него што постану нечитљиви.
9) Све неупотребљиве или оштећене преносне носаче података на којима се налазе пословни или интерни подаци, треба уништити у складу са *Процедуром за безбедно расходовање носача података*.

Употребу приватних носача података за чување пословних или интерних података одобрава и евидентира по потреби руководилац одговарајуће ОЈ.

### 5.2. Изношење пословних или интерних података на преносним носачима података

Изношење интерних и/или пословних података подлеже прописима о заштити података о личности и о пословној тајни те оно може бити само за потребе обављања редовних

радних задатака. За изношење пословних или интерних података од стране Корисника на преносним носачима података, потребно је придржавати се следећег:

1) За све медијуме који се износе из ИОРС-а, онда када је то неопходно и изводљиво, Корисник захтева одобрење руководиоца одговарајуће ОЈ.
2) Уколико постоји потреба за коришћењем преносног медијума, руководилац одговарајуће ОЈ процењује да ли треба пратити пренос информација на такве медијуме.
3) Руководилац одговарајуће ОЈ по потреби води евиденцију о преносном носачу података, његовом садржају и Кориснику, како би се сачувао траг за проверу.
4) Корисник је обавезан да све преносне носаче података складишти на безбедном и заштићеном месту, у складу са препорукама произвођача.
5) Садржај сваког медијума (који ће се износити изван ИОРС-а и који се може поново користити), треба неповратно избрисати када више није потребан. По налогу Корисника, брисање врши Инжињер за ИТ безбедност ДЦ помоћу софтвера предвиђеног за то.
6) Све неупотребљиве или оштећене преносне носаче података на којима се налазе пословни или интерни подаци, треба уништити у складу са *Процедуром за безбедно расходовање носача података.*

Уколико се изношење података врши за потребе трећих лица тј. трећим лицима се даје преносни носач података на коме се они налазе, тада је потребно да:

- ИОРС има уговор са трећим лицима који у себи има клаузулу о поверљивости података.
- Подаци буду агрегарни или бар анонимизирани. Уколико би се депесонализацијом онемогућило прибављање важних података (нпр. ако се траже подаци о смрти) тада се спроводи нека од других методе заштите (нпр. шифровано отварање документа у прилогу) или размена података са криптозаштитом. У вези са тим, корисници се могу обратити администратору ДЦ.

### 5.3. Чување и изношење јавних података на преносним носачима података

Чување и изношење јавних података је дозвољено свим запосленима ИОРС-а. За чување јавних података који се налазе на серверима ДЦ задужен је Инжињер за ИТ безбедност ДЦ. За чување јавних података који се налазе на радним станицама, мобилним уређајима или преносним носачима података задужен је Корисник.

У случају потребе, на захтев Корисника или руководиоца ОЈ, у Дата центру се врши безбедоносна провера преносних носача података.

## 6.0 ВЕЗА СА ДРУГИМ ДОКУМЕНТИМА

Процедура је у вези са документима:

1. *Правилник о безбедности информационо-комуникационог система Института за онкологију и радиологију Србије*

1. *Процедуром за безбедно расходовање носача података*
2. *Процедура за рад Дата центра.*

## 7.0 ПРАВНИ ОСНОВ

- *Закон о информационој безбедности ("Сл. Гласник РС", бр. 6/2016)*
- *Закон о здравственој документацији и евиденцијама у области здравства ("Службени гласник РС", број 123 од 10. новембра 2014)*
- *Закон о заштити података о личности ("Сл. гласник РС", бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012)*