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/g-23/ 3499-14
26 DEC 2023
БЕОГРАД

ПРОЦЕДУРА О БЕЗБЕДНОСТИ ИНФОРМАЦИЈА КОЈЕ СУ ДОСТУПНЕ ПРУЖАОЦИМА УСЛУГА

Ознака процедуре	**II.ДТЦ.18**
Верзија	01
Датум усвајања	08.03.2018./15.12.2023.
Аутор процедуре	Зорана Бизетић, маст мат Душица Гавриловић, 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;

Инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

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 Институт сарађује по основу уговора о одржавању ИКТ система или његових делова.

2.0 ПРЕДМЕТ

Ова процедура утврђује активности, носиоце активности и одговорности у циљу заштите информација које су доступне пружаоција услуга ИОРС-у.

3.0 ПОДРУЧЈЕ ПРИМЕНЕ

Примењује се у Дата центру.

4.0 ОДГОВОРНОСТИ

Сваки запослени је дужан да се понаша у складу са процедуром и у складу са својим задужењима ће сносити одговорност.

Обавеза руководиоца сваке организационе јединице је да све запослене упозна са процедуром и све новозапослене, било да су у сталном или радном односу на одређено време.

За контролу спровођења процедуре одговоран је начелник Дата центра.

5.0 ОПИС ПРОЦЕДУРЕ

Институт успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга (вендори).

5.1 Идентификовање врсте пружаоца услуга (вендора) којима ће дозволити да приступ информацијама

За потребе одржавања, унапређења и развоја ИКТ система, ИОРС успоставља сарадњу са трећим лицима који пружају услуга одржавања:

- болничког информационог система Хелиант
- пословног информационог система NextBiz
- лабораторијског информационог система ЛИС
- система за пословну документацију ТимДМС
- Linux сервера
- рачунарске мреже
- рачунарске опреме

5.2 Обавезе пружаоца ИКТ услуга (вендора) према ИОРС-у

Односи и обавезе ИОРС-а и вендора су дефинисани одговарајућим уговором о одржавању за чије праћење је надлежан начелник Дата центра. Уколико стање ИКТ система ИОРС-а намеће сарадњу два или више вендора, тада начелник Дата центра врши координацију и праћење реализације њиховог рада.

5.2 Врсте информација које су доступне пружаоцима услуга (вендорима)

За потребе испуњавања својих уговорних обавеза, вендорима је дозвољен приступ одређеним информацијама. Услоге које пружају одређују и врсту информација којима имају приступ.

Вендори који одржавају информационе системе имају приступ информацијама које се чувају у тим системима. Приступ информацијама је најчешће иницран од стране администратора ДЦ. Инжињер за ИТ безбедност ДЦ свакодневно прати логове болничког информационог система Хелиант који у себи чува виталне податке о пацијентима и запосленима. Такође се прате и активности које су рађене (у случају да је долазило до измене података/докумената) чиме се осигурава интегритет информација.

Вендор који одржава Linux сервера има приступ серверима који раде под оперативним системом Linux, а вендори који одржавају рачунарску мрежу имају приступ само рачунарској мрежи и то искључиво у пратњи администратора ДЦ.

Вендори који одржавају рачунарску опрему немају приступ подацима који су на носачима података јер се у Дата центру врши склапање рачунара.

5.3 Минимални захтеви за безбедност информација

Минимални захтеви за безбедност података су дефинисани уговором који у себи има клаузулу о поверљивости података која је у складу са *Упутством за клаузулу о поверљивости податка*.

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*
2. *Упутство за клаузулу о поверљивости податка*

3. *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)*