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

РЕПУБЛИКА СРБИЈА
ИНСТИТУТ ЗА ОНКОЛОГИЈУ И РАДИОЛОГИЈУ СРБИЈЕ
Бр. 01-1/2023/3794-18
26 DEC 2023
БЕОГРАД

ПРОЦЕДУРА ЗА УПРАВЉАЊЕ БЕЗБЕДНОСНИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМУ

Ознака процедуре	**П.ДТЦ.19**
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

РЕПУБЛИКА СРБИЈА
ИНСТИТУТ ЗА ОНКОЛОГИЈУ И РАДИОЛОГИЈУ СРБИЈЕ

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 које се спроводе приликом превенције и одговора на безбедносне ициденте.

3.0 ПОДРУЧЈЕ ПРИМЕНЕ

Примењује се на све запослене ИОРС-а који приступају ИКТ и ИС ИОРС ради извршавања својих радних задатака.

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

5.1 Инциденти

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 ИОРС-а;
- инциденти који утичу на велики број корисника услуга ИОРС-а;
- 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.

5.2 Врсте инцидената

Приликом одређивања врсте инцидента треба се придржавати следеће поделе:

1. провађивање у ИКТ систем – напад на рачунарску мрежу и серверску инфраструктуру у оквиру кога је, кршењем мера заштите, остварен приступ који омогућава неовлашћен утицај на рад ИКТ система;
2. отицање података – доступност заштићених података ван круга лица овлашћених за приступ подацима;
3. неовлашћена измена података;
4. губитак података;
5. прекид у функционисању система или дела система;
6. ограничавање доступности услуге (дениал оф сервице);
7. инсталирање злонамерног софтвера у оквиру ИКТ система;
8. неовлашћено прикупљање података путем неовлашћеног надзора над комуникацијом или социјалним инжењерингом;
9. непрестани напад на одређене ресурсе;
10. злоупотреба овлашћења приступа ресурсима ИКТ система;
11. остали инциденти.

5.3 Припрема и планирање одговора на инциденте

Инжињер за ИТ безбедност, запослен у Дата центру, се бави пословима планирања, детектције, анализе и информисања надлежних, у току и након инцидента.

Инжињер за ИТ безбедност треба да поседује одговарајућа техничка знања како би на најбржи и одговарајућу начин могао да одговори на безбедносне инциденте.

Инжињер за ИТ безбедност је такође дужан да припреми детаљан план за превенцију безбедносних ризика и неколико метода комуникације које би могле да се примене у зависности од инцидента. Могуће методе комуникације су: електорнска пошта, веб сајтови (интерни, екстерни, портали), телефонска комуникација, говорна порука, писмено извештавање, директан контакт.

5.4 Поступање у случају безбедносних инцидената

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

5.5 Извештавање о догађајима у вези са безбедношћу информација

Сви запослени су у обавези да извештавају о уоченим и утврђеним слабостима ИКТ система Дата центар, у што краћем року, како би се инциденти нарушавања безбедности информација спречили и спречио настанак штете.

Запослени који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и пријавити га путем електронске поштом Администратору ДЦ и/или позивом локала 264.

Администратор ДЦ врши проверу пријављеног инцидента и уколико посумња да је безбедоносни ицидент обавештава Инжињера за ИТ безбедност.

Догађаји у вези са безбедношћу информација се оцењују и у складу са тим се доноси одлука да ли је потребно да се класификују као инциденти нарушавања безбедности информација.

5.6 Записивање активности у оквиру управљања инцидентима и поступање са судским доказима

Инжињера за ИТ безбедност води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Инжењер ИТ безбедности Дата центра је:

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

Инжињера за ИТ безбедност, применом процедура за идентификацију, сакупљање, набавку и чување информација прикупља сва електронска и папирна документа које могу да служе као доказ у случају покретања казнених мера унутар организације.

ИОРС дефинише и примењује процедуре за идентификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају покретања казнених мера унутар организације.

Прикупљено знање из анализе и решавања инцидената који су нарушили безбедност информација, ИОРС користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

5.7 Одговор на инциденте и комуникација са интерним и екстерним или интерним особама или организацијама

Уколико је догађај калсификован као инцидент, тада се писмено и усмено обавештава Директор ИОРС-а који обавештава Надлежни орган тј је министарство надлежно за послове информационе безбедности (у складу са Чланом 4 Закона о информационој безбедности), а све у циљу прикупљања доказа и размене с осталим организацијама. Обавештење о инциденту мора да има:

- врсту инцидента
- опис инцидента
- време појаве инцидента
- трајање инцидента
- последице које је инцидент изазвао
- предузете активности ради ублажавања инцидента
- додатне релевантне информације.

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. *Процедуром обезбеђивање континуитета пословања током и након инцидента*
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)*