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

РЕПУБЛИКА СРБИЈА
ИНСТИТУТ ЗА ОНКОЛОГИЈУ И РАДИОЛОГИЈУ СРБИЈЕ
Бр. 01-1/625/3494-16
26 DEC 2023
Београд, Пастерова 14

ПРОЦЕДУРА ЗА ОБЕЗБЕЂИВАЊЕ КОНТИНУИТЕТА РАДА ТОКОМ И НАКОН ИНЦИДЕНТА

Ознака процедуре	**П.ДТЦ.17**
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;

Радна станица је персонални рачунар сачињен од хардвеских и софверких компоненти са монитором, тастатуром и мишем или мобилни рачунар (лаптоп, таблет), намењен обављању пословних активности.

2.0 ПРЕДМЕТ

Ова процедура утврђује активности, носиоце активности и одговорности које се спроводе приликом у циљу обезбеђивања континутитета рада ИОРС-а током и након безбедоносног инцидента.

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

Институт примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, као и мере које би омогућиле да ИКТ систем у што краћем року буде у функционалном стању.

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. проваљивање 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 (denial of service);
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 Активности у случају безбедносног инцидента

Поступак у случају безбедносног инцидента има неколико фаза. Почетна фаза укључује успостављање и образовање тима за решавање инцидента, у чијем саставу је Инжињер за ИТ безбедност ДЦ, као и прибављање потребних алата и ресурса. Током припреме, ИОРС покушава да ограничи број потенцијалних безбедносних инцидената правилним одабиром и применом низа безбедносних мера које почивају на резултатима континуиране процене ризика.

Процена ризика и планирање потребних активности укључује перманентно:

- откривање општих претњи,
- откривање специфичних претњи,
- процена адекватности постојећег нивоа заштите и откривање безбедносних слабости или пропуста
- процена потребног нивоа заштите и
- усклађивање постојећег са потребним нивоом заштите.

У случају појаве безбедносног инцидента, потребно је (1) откривање безбедносног пропуста и (2) пријављивање инцидента надлежним органима и лицима.

У зависности од тежине, обима и озбиљности инцидента, ИОРС може предузети одговарајуће мере ради смањивања последица и опоравка од инцидента међу којима је и замена креденцијала на нападнитим ресурсима.

За безбедносне инциденте мањег обима, нису нужне опсежне анализе, осим инцидената код којих су коришћене нове методе напада како би се слични напади избегли или брже и ефикасније санирали у будућности.

5.4 Континуитет пословања током безбедносног инцидента

5.4.1 Инциденти који узрокују прекид у функционисању система или дела система

Уколико се деси ицидент који отежава или онемогућава рад запослених ИОРС-а, тада се спроводи његова анализа**.** Уколико је инцидент проузроковао прекид у функционисању система или дела система, у зависности од обима прекида, спроводе активности које су описане у наставку овог документа.

1) *Прекид рада једне радне станце једног Корисника (тј. једно радно место)*

Активност: Администратор ДЦ спроводи проверу и поправку те радне станице. Уколико на тој радној станици постоје витални подаци које је Корисник чувао на резервним копијама у складу са *Процедуром за израду резервних копија,* тада се након поправке радне станице ради и повраћај података. Уколико процес рада у коме Корисник учествује не дозвољава прекид у раду, тада Администратор ДЦ даје кориснику на употребу заменски рачунар док је његова радна станица на сервисирању или другој интервенцији.

2) *Прекид рада рачунарске мреже (више радних места) или сервера*

Активност: Администратор ДЦ процењује ситуацију и зависно од разлога прекида рада мреже или сервера, планира даље активности и о томе, уколико је у могућности,

обавештава о планираним активностима надлежне руководиоце ОЈ ИОРС-а: (1) постављањем одговарајућег обавештења на главну страну ИС Хелиант; (2) слањем циркуларне поруке путем е-маил; (3) слањем писаног обавештења или (4) усменим путем, уколико нема других могућности. Руководиоци ОЈ су дужни да обавесте запослене своје ОЈ о планираним активностима Администратора ДЦ. Администратори ДЦ ангажују одговарајућег вендора и у најкраћем року раде поправку. Уколико је дошло до губитка података на серверима, тада се повраћај података спроводи у складу са *Процедуром за израду резервних копија*. Док су мрежа и/или сервери ван функције, Корисници евидентирају податке и медицинску документацију у Word-у или у папирној форми. Запослени на шалтерима ИОРС-а евидентирају у Word-у или у папирној форми списак пацијента (идентификациони подаци; дијагнозе; услуге које су спроведене и остали релевантни подаци). Након оспособљавања мреже и/или сервера, Администратор ДЦ, обавештава надлежне руководиоце ОЈ ИОРС-а а корисници уносе податке у одговарајући ИС.

3) *Прекид рада ИС у коме се генерише медицинса документација*

Активност: Администратор ДЦ процењује ситуацију и зависно од разлога прекида рада ИС, планира даље активности и о томе, уколико је у могућности, обавештава о надлежне руководиоце ОЈ ИОРС-а: (1) постављањем одговарајућег обавештења на главну страну ИС Хелиант; (2) слањем циркуларне поруке путем е-маил; (3) слањем писаног обавештења или (4) усменим путем, уколико нема других могућности. Руководиоци ОЈ су дужни да обавесте запослене своје ОЈ о планираним активностима Администратора ДЦ. Администратори ДЦ ангажују вендора за ИС и у најкраћем року раде на његовом оспособљавању. Уколико је дошло до губитка података ИС који су на серверима, тада се повраћај података спроводи у складу са *Процедуром за израду резервних копија*. Док је ИС ван функције, Корисници евидентирају податке и медицинску документацију у Word-у или у папирној форми. Запослени на шалтерима ИОРС-а евидентирају у Word-у или у папирној форми списак пацијента (идентификациони подаци; дијагнозе; услуге које су спроведене и остали релевантни подаци). Након оспособљавања ИС, Администратор ДЦ, обавештава надлежне руководиоце ОЈ ИОРС-а а корисници уносе податке у одговарајући ИС Када се оспособи ИС.

4) *Прекид рада ИЗИС-а*

Активност: Уколико је прекид рада ИЗИС-а настао или је најављен (у трајању дужем од 60 минута), тада Администратор ДЦ уз сагласност Помоћника директора за здравствену делатност, у Хелианту привремено искључује везу ИС Хелиант-ИЗИС (тј. прекид размене података између наведених ИС). Администратор ДЦ обавештава о

насталом стању надлежне руководиоце ОЈ ИОРС-а: (1) постављањем одговарајућег обавештења на главну страну ИС Хелиант; (2) слањем циркуларне поруке путем е-маил; (3) слањем писаног обавештења или (4) усменим путем, уколико нема других могућности. Руководиоци ОЈ су дужни да обавесте запослене своје ОЈ о насталом стању. По нормализовању рада ИЗИС-а, Администратора ДЦ активира у Хелианту везу ИС Хелиант-ИЗИС (тј. успостављање размене података између наведених ИС) и ажурира податке за размену кроз опцију „Администрирање ИЗИС-а“ и обавештава надлежне руководиоце ОЈ ИОРС-а.

5) Прекид рада услед нестанка електричне енергије

Уколико се планира прекид електричне енергије или до њега долази непланирано или услед хаварије (поплава; пожар; земљотрес или друге елементарне непогоде; квар клима уређаја; итд), неопходно је да надлежни из Техничке службе ИОРС-а у најкраћем року обавесте начелника Дата центра и/или администратора ДЦ о томе.

А) Планиран нестанак електричне енергије у Дата центру или у целом ИОРС-у

Активност: Након добијања обавештења о планираном искључењу електричне енергије, Администратор ДЦ процењује будуће активности, када и на колико је потребно искључити сервере у сервер сали Дата центра и, уколико је у могућности, обавештава о планираним активностима надлежне руководиоце ОЈ ИОРС-а: (1) постављањем одговарајућег обавештења на главну страну ИС Хелиант; (2) слањем циркуларне поруке путем е-маил; (3) слањем писаног обавештења или (4) усменим путем, уколико нема других могућности. Руководиоци ОЈ су дужни да обавесте запослене своје ОЈ о планираним активностима Администратора ДЦ. Уколико је потребно, Администратор ДЦ у складу са планираним активностима, искључује сервере по *Процедури за укључивање и искључивање сервера.* У периоду искључених сервера у сервер сали ДЦ (у трајању дужем од 60 минута), Корисници евидентирају све податке и документацију, у зависности од могућности, у одговарајућем ИС, у Word-у или у папирној форми. Запослени на шалтерима ИОРС-а евидентирају у Word-у или у папирној форми списак пацијента (идентификациони подаци; дијагнозе; услуге које су спроведене и остали релевантни подаци). По доласку електричне енергије, администратор ДЦ укључује сервере у складу са *Процедуром за укључивање и искључивање сервера*, обавештава надлежне руководиоце ОЈ ИОРС-а а корисници уносе податке у одговарајући ИС након његовог оспособљавања.

Б) Хаварија или непланиран нестанак електричне енергије у Дата центру или у целом ИОРС-у

Активност: Након самосталног утврђивања или добијања обавештења о непланираном искључењу електричне енергије или хаварије, Администратор ДЦ

процењује ситуацију и зависно од трајања нестанка електричне енергије или обима хаварије, планира даље активности и о томе, уколико је у могућности, обавештава о планираним активностима надлежне руководиоце ОЈ ИОРС-а: (1) постављањем одговарајућег обавештења на главну страну ИС Хелиант; (2) слањем циркуларне поруке путем е-маил; (3) слањем писаног обавештења или (4) усменим путем, уколико нема других могућности. Руководиоци ОЈ су дужни да обавесте запослене своје ОЈ о планираним активностима Администратора ДЦ. У периоду искључених сервера у сервер сали ДЦ, у трајању дужем од 60 минута, Корисници евидентирају све податке и документацију, у зависности од могућности, у одговарајућем ИС, у Word-у или у папирној форми. Запослени на шалтерима ИОРС-а евидентирају у Word-у или у папирној форми списак пацијента (идентификациони подаци; дијагнозе; услуге које су спроведене и остали релевантни подаци). По доласку електричне енергије или санирања хаварије, администратор ДЦ, када је постигнута потребна сигурност и безбедност сервер сале ДЦ и опреме у њој, укључује сервере у складу са *Процедуром за укључивање и искључивање сервера,* обавештава надлежне руководиоце ОЈ ИОРС-а а корисници уносе податке у одговарајући ИС након његовог оспособљавања.

5.4.2 Инциденти у вези неовлашћеног приступа, губитка, измене или отицања података

Уколико дође до проваљивања у ИКТ систем и неовлашћеног приступа, губитка, измене или отицања података, 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). Ако је нападач познат и ако је корисник ИКТ система, тада се најкраћем могућем року ради промена креденцијала и иницира дисциплински поступак.

5.4.3 Инциденти у вези проваљивања у ИКТ систем

Уколико се догоди напад на рачунарску мрежу и серверску инфраструктуру у оквиру кога је, кршењем мера заштите, остварен приступ који омогућава неовлашћен утицај на рад ИКТ система, 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).

5.5 Активности након инцидента

Битан део решавања инцидента су учење и побољшавање како би могли што боље деловати у будућности која доноси нове претње и префињеније нападе. Стога, након

инцидента, тим за решавање инцидента треба да продискутује и да пружи одговоре на следећа питања:

- Шта се тачно догодило и у које време?
- Да ли су запослени и управа добро извели свој задатак и носили се с инцидентом?
- Да ли су процедуре биле јасне и добро документоване и јесу ли биле одговарајуће?
- Које је информације требало дознати раније?
- Јесу ли предузети сви кораци или акције које могу убрзати опоравак?
- Које је мере потребно предузети за спречавање сличних инцидената у будућности?
- Који су додатни ресурси и алати потребни за откривање, анализу и ублажавање посљедица будућих инцидената?
- Што би требало запослени и управа да учине другачије идући пут када се догоди сличан инцидент?

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 за израду резервних копија*
3. *Процедуром за укључивање и искључивање сервера*
4. *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)*