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. 01-1/2023/3949/10
26 DEC 2023
БЕОГРАД, Пастерова 14

ПРОЦЕДУРА О БЕЗБЕДНОСТИ У РАЗМЕНИ ЕЛЕКТРОНСКИХ ПОРУКА

Ознака процедуре	**П.ДТЦ.11**
Верзија	01
Датум усвајања	08.03.2018./15.12.2023.
Аутор процедуре	Душица Гавриловић, маст мат Зорана Бизетић, маст мат Душко Стојановски инг
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

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;

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).

Е-пошта – електронска порука

2.0 ПРЕДМЕТ

Овом процедуром утврђују се активности, носиоци активности и одговорности приликом размене електронских порука у циљу и заштите информација и информационих добара ИОРС-а од злоупотребе или непажњом изазване штете.

3.0 ПОДРУЧЈЕ ПРИМЕНЕ

Примењује се за све запослене који користе радне станице ИКТ система ИОРС-а за потребе електронске комуникације.

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 ИОРС-а је да све запослене и све новозапослене упозна са процедуром, било да су у сталном или радном односу на одређено време.

За контролу спровођења процедуре одговорни су одговарајући руководиоци организационих јединица.

5.0 ОПИС ПРОЦЕДУРЕ

Као средство унапређивања продуктивности, ИОРС подстиче пословну употребу електронских комуникација (електронска пошта, интернет, видеоконференције, *online* chat, портали за учење на даљину итд.).

5.1 Доступност службене електронске поште

Корисник може добити службену е-маил адресу само уколико је потписао Изјаву о поверљивости. Захтев за доделу, измену, блокирање, деблокирање или укидање е-маил адресе Корисника као и додељивање његових креденцијала за приступ истој, врши се у складу са *Процедуром о правима приступа ИКТ систему.*

Подешавања параметара за приступ електронској пошти запосленог на радној станици коју користи, врши Администратор ДЦ у складу са *Процедуром о инсталацији и конфигурацији система*.

Приступ електронској пошти ИОРС-а Корисник може остварити на два начина:

- коришћењем интернета, преко сајта ИОРС-а *http://www.ncrc.ac.rs*, где је приступ е-пошти на *webmail* серверу Дата центра омогућен путем апликације *roundcube*. Прочитана, започета или послата е-пошта у том случају остаје доступна запосленом на webmail серверу Дата центра.
- коришћењем *outlook* апликације на радној станици. У том случају прочитана, започета или послата електронска пошта остаје доступна запосленом искључиво на његовој радној станици.

5.2 Одговорност Корисника

- Корисник који има службену е-мејл адресу дужан је да је користи у свакодневном раду.
- Сваки Корисник је одговоран за садржај, архивирање и брисање електронских порука које шаље путем своје службене е-мејл адресе.
- Корисник је дужан да чува тајност лозинке и не открива је другим особама, како би се спречила злоупотреба његове е-мејл адресе. Уколико посумња да је његова лозинка компромитована, Корисник треба хитно да обавести Администратора ДЦ ради њене измене. Откривање лозинке другој особи повлачи са собом одговорност Корисника за акције које та особа може предузети коришћењем његове лозинке.
- Забрањено је слање поверљивих података (креденцијала и лозинки) путем електронске поште.
- Забрањено је уступање е-мејл адреса трећим лицима, осим уколико не постоји уговор између ИОРС-а и трећих лица који садржи клаузулу о поверљивости података.

5.3 Употреба службене електронске поште

Свака порука електронске поште може се сматрати ауторским делом, дакле припада особи која ју је послала. Прилози који се шаљу уз електронске поруке могу садржати ауторски заштићене информације (напр. музику, филмове, чланке итд). Примајући и шаљући такве садржаје корисници морају бити свесни да не представљају само себе, већ

и установу за коју раде. Стога, при слању електронске поште користећи службену е-маил адресу, Корисник мора да се придржава следећег:

- Електронска пошта ИОРС-а се користи само у циљу обављања послова за потребе ИОРС-а (тј. за пословне, научне, истраживачке или наставне потребе). Приватне поруке су дозвољене у умереној количини, уколико то не ометају рад и уколико се придржавају правила пристојног понашања на интернету;
- Свака написана порука сматра се документом, те на тај начин подлеже прописима о ауторском праву и интелектуалном власништву. Поруке које су послате лично једном Кориснику, тај Корисник нема право проследити даље без дозволе аутора, односно пошиљаоца;
- Придржавајући се правила пристојног понашања на интернету, корисници службену е-маил адресу не смеју користити за слање увредљивих, омаловажавајућих порука, сексуално или било какво друго узнемиравање;
- Није дозвољено слање ланчаних порука којима се оптерећују мрежни ресурси и људима одузима радно време;
- Све поруке аутоматски ће прегледати апликација која открива вирусе. Ако пошиљка садржи вирус, неће бити испоручена. Порука ће неко време провести у карантину;
- Поруке које су део пословног процеса треба архивирати и чувати прописани временски период као и документе на папиру;
- Корисницима није допуштено пресретање и прегледање, нити помагање у пресретању и прегледању садржаја електронске поште других Корисника;
- Корисник је дужан да води рачуна о исправном адресирању електронске поште.

5.4 Слање интерних и/или пословних података

Слање интерних и/или пословних података путем порука електронске поште подлеже прописима о заштити података о личности или пословној тајни, те може бити учињено од стране Корисника само уз:
- сагласност непосредног руководиоца и
- са службене е-маил адресе пошиљаоца (Корисника).

Интерне и/или пословне податке путем порука електронске поште, Корисник може упутити на:
- службену е-маил адресу примаоца који је као запослен у ИОРС-у;
- службену е-маил адресу надлежних државних органа;
- на службени е-маил вендора, као потписника клаузуле о поверљивости информација која је део њиховог уговора са ИОРС-ом

- на службени маил трећих лица када је обавезно да подаци који подлежу прописима о заштити података о личности или пословној тајни, пре слања буду трансформисани у агрегарну или анонимизирану форму, осим у случајевима када уговором, који садржи клаузулу о поверљивости информација, није другачије прецизирано.

Уколико коресподенција путем порука електронске поште у којој би анонимизацијом било онемогућило прибављање важних података (нпр. подаци о смрти пацијената за потребе научноистраживачког рада), тада је потребно спроводи неке од других методе заштите (нпр. шифровано отварање документа који је у прилогу електронске поште) или користити размену података са криптозаштитом. У таквим ситуацијама се корисници могу обратити Администратору ДЦ.

5.5 Слање порука свим или већем броју корисника ИКТ система (циркуларни мејл)

Директор ИОРС-а, помоћници директора, руководиоци клиника и самосталних служби могу послати циркуларни е-мејл са обавештењем, наредбом или друге садржине свим Корисницима којима је намењен.

Запослени Дата центра могу послати циркуларни мејл:

- у случају постојања опасности по информациону безбедност;

- у случају постојања важних е-мејл порука упућених од стране државних институција, вендора или трећих лица;

- у случају постојања важних информација које се тичу рада ИКТ система и/или су од значаја за рад ИОРС-а.

Остали Корисници могу да пошаљу циркуларни е-мејл само уз претходно одобрења руководиоца ОЈ.

5.6 Поштовање права приватности

- ИОРС поштује право својих Корисника укључујући и право приватности.
- Администратор ДЦ не сме прегледати садржај електронске поште других Корисника из личне радозналости, нити допустити увид у садржај електронске поште трећим лицима које за то немају потребна овлашћења Корисника.
- Уз сагласност Корисника, а у случају решавања проблема комуникације, Администратор ДЦ ће имати право на увид у садржај порука електронске поште појединачног Корисника.

- ИОРС задржава право филтрирања порука с намером да се зауставе непожељне поруке е-поште (тзв. Спам).
- У посебним случајевима, кад постоји оправдана сумња у кршење одредби ове процедуре, ради заштите електронске поште и по захтеву овлашћених државних установа и/или Директора ИОРС-а, ИОРС може допустити повремено пресретање и прегледање садржаја електронске поште својих Корисника.
- И поред мера заштите кое ИОРС спроводи, а због претходно наведених разлога, ИОРС не може гарантовати приватност садржаја е-поште. Корисници треба да буду свесни да поруке е-поште могу без њихова знања, зависно од технологије, бити прослеђиване, пресретане, штампане или сачуване од стране других особа.

5.7 Брисање електронских порука

- Корисник је одговоран за архивирање и брисање електронских порука свог службеног мејла. Поруке које више нису битне за пословне потребе Корисник треба да премести у локалну архиву е-поште на радној станици или обрише из свог електронског поштанског сандучета на серверу е-поште. Динамику архивирања и брисања одређује Корисник.
- Уколико је у току нека истражна акција узрокована могућим безбдносним инцидентом, покренута од Руководства ИОРС-а или од стране овлашћених државних установа, све поруке електронске поште релевантне за ту истражну акцију неће бити брисане до изричите наредбе Руководства ИОРС-а.

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. *Процедура о правима приступа ИКТ систему*
3. *Процедура о инсталацији и конфигурацији система*
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)*
- *Правилник о анонимизацији података о личности*