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

01-1/2023/3494-1
26 DEC 2023

ПРОЦЕДУРА
О ПРАВИМА ПРИСТУПА
ИКТ СИСТЕМУ

Ознака процедуре	**П.ДТЦ.02**
Верзија	03
Датум усвајања	15.12.2023.
Аутор процедуре	Душица Гавриловић, маст мат Зорана Бизетић, маст мат Будимир Јуришић, маст.инг ИТ Душко Стојановски, инг Јертец Александра, маг ИТ Александар Ђуричић, Спец.струк.инж.
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;

База ИКТ ресурса и услуга ДЦ је електронска база евиденција ИКТ ресурса и услуга које Дата центар пружа у ИОРС-у;

ИКТ Захтев је документ под називом *Захтев за задужење/раздужење ИКТ опреме и администрирање налога за ИКТ системе Института* (у Прилогу).

Вендор је треће лице са којим Институт сарађује по основу уговора о пружању услуга одржавању ИКТ система или његових делова; Поред основне опреме ИС може

садржати и додатну опрему која је неопходна за реализацију унапред уговорених послова.

2.0 ПРЕДМЕТ

Овом процедуром утврђују се активности, носиоци активности и одговорности приликом додељивања, промене или укидања права приступа ИКТ и ИС системима ИОРС-а као и задужење/раздужење *ИКТ опреме* од стране корисника и Администратора ДЦ.

Правилном применом утврђеног поступка и начина приступа, ИОРС своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа ИКТ систему.

3.0 ПОДРУЧЈЕ ПРИМЕНЕ

Примењује се на све запослене ИОРС-а који приступају ИКТ и ИС ИОРС-а 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 ИОРС-а 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 одговорни су одговарајући руководиоци организационих јединица.

5.0 ОПИС ПРОЦЕДУРЕ

5.1 Кориснички креденцијали

Кориснички креденцијали (име и лозинка; картица; ПИН-код и сл.) су идентификатори корисника помоћу којег је кориснику омогућен приступ ИКТ или ИС системима ИОРС-а који садрже пословне и/или интерне податке. Они служе за додељивање, ограничавање, измену или укидање права приступа ИКТ и ИС системима.Право приступа ИКТ и ИС системима ИОРС-а имају само запослени који имају корисничке

кредeнцијале и одговарајући вендори са којима ИОРС има уговором дефинисану сарадњу.

Кориснички кредeнцијали су поверљиви подаци који се евидентирају у електронској форми само у склопу ИС и то у енкриптованом облику.

Уколико кориснички кредeнцијал чини *Корисничко име* и *Лозинка* (шифра) тада се он дефинише на следећи начин:

- *Корисничко име* се састоји од алфанумеричких, латиничних карактера.
- *Лозинка* се састоји од алфанумеричких, латиничних карактера и у себи:
  - не сме да садржи слова: đ, Đ, ž, Ž, ć, Ć, č, Č, š и Š;
  - не сме да садржи више од 3 узастопна идентична словна или бројчана знака
  - пожељно је да има најмање 9 карактера
  - пожељно је да има најмање једно велико и једно мало слово
  - пожељно је да има најмање једну цифру (0-9)
  - пожељно је да има бар један специјалан знак ($,& и сл.)

Лозинка не сме бити заснована на препознатљивим или личним подацима запосленог (име, датум рођења, број телефона, и сл.). Један (корисник) запослени може имати *више различитих корисничких кредeнцијала.

5.2 Обавезе корисника према корисничким кредeнцијалима које користи

Сваки запослени (сваки корисник) је, из безбедносних разлога, у обавези да:

- чува корисничке кредeнцијале који су му додељени тј. своје лозинке држи у тајности, не открива их другим лицима, укључујући и надређене особе;
- не злоупотребљава лозинку заједничког налога;
- избегава чување у писаном облику ПИН-кода као и лозинке личног и/или заједничког налога;
- онемогући злоупотребу својих кредeнцијала тако што ће изаћи (излоговати се) из ИС по завршетку својих радних задатака;
- промени лозинку личног налога увек када постоји било какав наговештај могућег компромитовања или злоупотребе;
- чува картицу и тражи замену када постоји било какав наговештај злоупотребе или могућег компромитовања;
- промени привремену лозинку приликом првог пријављивања на систем, уколико је тако предвиђено.

5.3 Права приступа ИКТ систему ИОРС-а

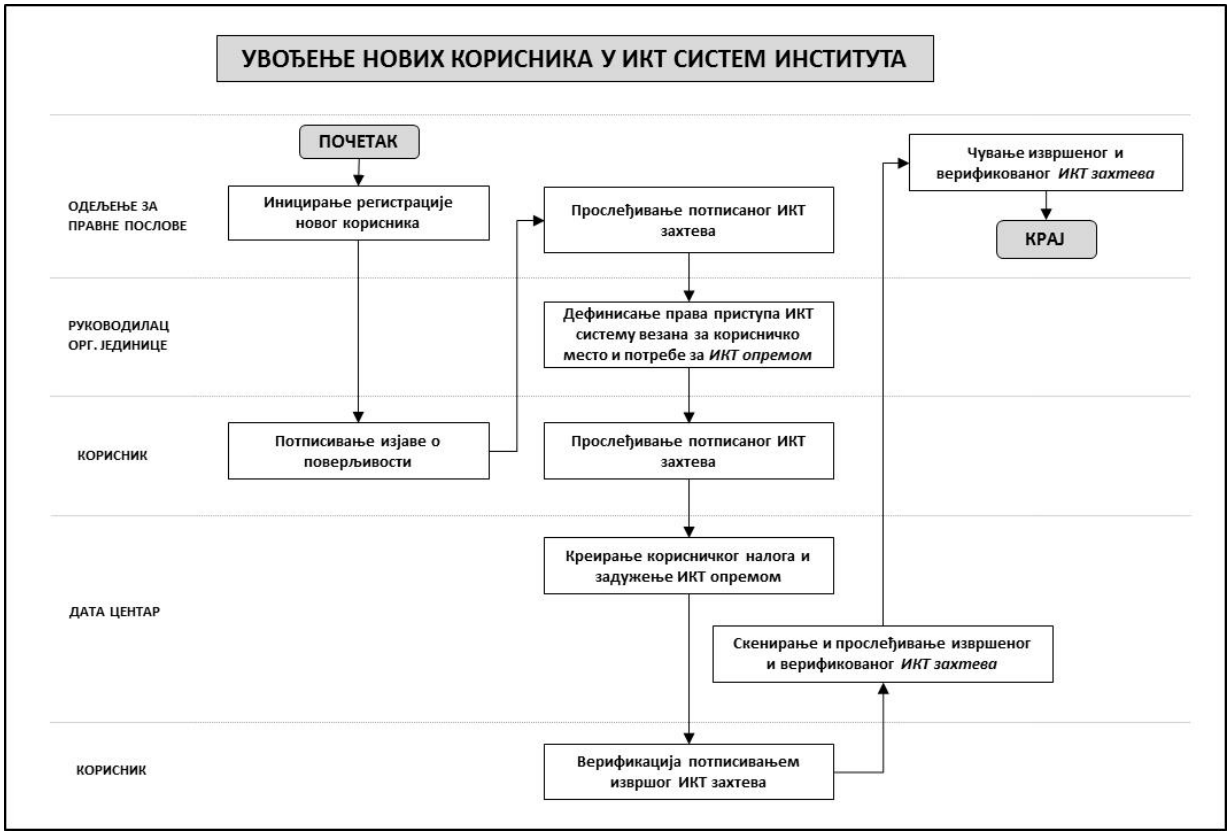
Право приступа ИКТ и ИС системима, које се остварује корисничким креденцијалима, може бити администраторско и корисничко:

- *Администраторско право приступа* се додељује кроз *Администраторски налог* кога чине креденцијали помоћу кога се омогућава администрирање ИКТ или ИС система. Администраторска права се додељују посебно за сваки систем. Забрањено је неовлашћено коришћење Администраторских права.
- *Корисничко право приступа* се додељује кроз *Кориснички налог* кога чине креденцијали помоћу кога је кориснику омогућен ограничен приступ ИКТ или ИС систему, у складу са пословима које обавља на ИОРС-у.

Кориснику се додељује право приступа ИКТ и ИС системима у складу са радним задацима које обавља. Иницирање, администрирање или укидање права приступа ИКТ и ИС системима покреће Одељење за правне послове, путем *ИКТ Захтева*.

5.3.1 Додељивање права приступа ИКТ систему ИОРС-а на почетку радног ангажовања запосленог

Увођење нових корисника у ИКТ систем је приказано на следећој шеми:



Шема: Увођења нових корисника у систем

Као што је види на шеми Увођења нових корисника у систем, на почетку радног ангажовања запосленог, Одељење за правне послове:

- од корисника прибавља потписану *Изјаву о поверљивости*
- прибавља кориснички креденцијал потребан за Систем за евиденцију присуства на раду TimeWorks3 који је у форми идентификационе картице;
- попуњава и потписује део који је обележен „Попуњава Правна служба“ на *ИКТ Захтеву* (у Прилогу) и предаје га кориснику који га доставља свом руководиоцу.

Руководилац ОЈ којој корисник припада, попуњава и потписује *ИКТ Захтев*, део који је обележен „Попуњава руководилац организационе јединице у којој запослени почиње да ради или у коју долази“, и предаје га кориснику који га доставља Дата центру.

Администратор ДЦ на основу потписане ~~*Изјаве о поверљивости*~~ и *ИКТ Захтева*:

- додељује Кориснички/Администраторски налог у присуству корисника који сам уноси лозинку;

- попуњава и потписује на *ИКТ Захтеву* део који је обележен „Попуњава Дата центар“;

- евидентира новог корисника у *Бази ИКТ ресурса и услуга ДЦ;*

Корисник се упознаје са основним концептима информационе безбедности, са својим обавезама и дужностима по питању приступа ИКТ систему ИОРС-а и потписом даје сагласност са подацима наведеним у *ИКТ Захтеву*.

По завршетку *ИКТ Захтева*, администратор ДЦ га скенира а папирну верзију документа доставља Одељењу за правне послове која га архивира и које, у случају потребе, обавештава шефа Одсека књиговодства о промени задужења ИКТ опреме.

5.3.2 Укидање права приступа ИКТ систему ИОРС-а услед престанка радног односа/отказа уговора о раду

Приликом престанка радног ангажовања корисника, Одељење за правне послове предузима следеће активности:

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату;
- утврђује начин контакта са бившим корисником након одласка;
- попуњава и потписује део који је обележен „Попуњава Правна служба“ на *ИКТ Захтеву,* предаје га кориснику који га доставља свом руководиоцу.

Руководилац ОЈ у којој корисник ради потписује *ИКТ Захтев*, део који је обележен „Попуњава руководилац организационе јединице у којој запослени већ ради или из које одлази“, и предаје га кориснику који га доставља Дата центру.

По пријему *ИКТ Захтева*, Администратор ДЦ предузима следеће активности:

- укида све корисничке налоге за приступ ИКТ систему, почев од дана престанка радног ангажовања корисника;
- проверава и преузима сву доступну рачунарску опрему која је евидентирана у *Бази ИКТ ресурса и услуга ДЦ* на име Корисника;
- попуњава и потписује на *ИКТ Захтеву* део који је обележен „Попуњава Дата центар“;
- у *Бази ИКТ ресурса и услуга ДЦ* евидентира промену задужења ІКТ опреме која је била евидентирана на име Корисника.

Корисник потписом даје сагласност са подацима наведеним у *ИКТ Захтеву*.

По завршетку *ИКТ Захтева*, администратор ДЦ га скенира, а папирну верзију документа доставља Одељењу за правне послове које обавештава шефа Одсека књиговодства о промени задужења ІКТ опреме.

5.3.3 Привремено укидање (блокирање) права приступа ИКТ систему ИОРС-а у случају одласка на дуже одсуство

У случају дужег одсуствовања, Кориснику је потребно блокирати његов Кориснички налог тј. тј. спречити коришћење његових креденцијала и права приступа ИКТ систему ИОРСа током дужег одсуства. Потребно је да Одељење за правне послове у делу ИКТ *Захтева* под насловом „Попуњава Одељење за правне послове“ означава да налог треба „блокирати“ избором опције „Одлазак на дуже одсуство“ као основа за администрирања налога.

ИКТ Захтев потом Корисник доставља руководиоцу ОЈ у којој корисник ради. Руководилац попуњава и потписује *ИКТ Захтев* (део који је обележен „Попуњава руководилац организационе јединице у којој запослени већ ради или из које одлази“), и предаје га кориснику који га доставља Дата центру.

Администратор ДЦ на основу *ИКТ Захтева* спроводи тражену измену, попуњава и потписује на *ИКТ Захтеву* део који је обележен „Попуњава Дата центар“, евидентира у *Бази ИКТ ресурса и услуга ДЦ*.

Корисник потписом даје сагласност са подацима наведеним у *ИКТ Захтеву*.

По завршетку *ИКТ Захтева*, администратор ДЦ га скенира, а папирну верзију документа доставља Одељењу за правне послове које обавештава шефа Одсека књиговодства о промени задужења ІКТ опреме.

5.3.4 Деблокирање права приступа ИКТ систему ИОРС-а у случају повратка са дужег одсуства

Уколико је Кориснику блокиран Кориснички налог (тј. спречено коришћење његових креденцијала и права приступа ИКТ систему ИОРСа током одсуства) и потребно је да се исти одблокира ради обављања редовних радних задужења Корисника, тада Одељење за правне послове у делу ИКТ *Захтева* у сегменту „Попуњава Одељење за правне послове“ означава да налог треба „деблокирати“ избором опци „Повратак са дужег одсуства“ као основа за администрирања налога.

ИКТ *Захтев* потом Корисник доставља руководиоцу ОЈ у којој корисник ради. Руководилац попуњава и потписује *ИКТ Захтев* (део који је обележен „Попуњава руководилац организационе јединице у којој запослени већ ради или из које одлази“), и предаје га кориснику који га доставља Дата центру.

Администратор ДЦ на основу *ИКТ Захтева* спроводи тражену измену, попуњава и потписује на *ИКТ Захтеву* део који је обележен „Попуњава Дата центар“, евидентира у *Бази ИКТ ресурса и услуга ДЦ*.

Корисник потписом даје сагласност са подацима наведеним у *ИКТ Захтеву*.

По завршетку *ИКТ Захтева*, администратор ДЦ га скенира, а папирну верзију документа доставља Одељењу за правне послове које обавештава шефа Одсека књиговодства о промени задужења ИКТ опреме.

5.3.5 Измена права приступа ИКТ систему ИОРС-а у случају Анекса уговора о раду

У случају да Анекс уговора о раду узрокује промене због којих је потребна измена права или обима приступа ИКТ систему, тада Одељење за правне послове у делу ИКТ *Захтева* у сегменту „Попуњава Одељење за правне послове“ означава да налог треба „изменити“ избором опци „Анекс уговора“ као основа за администрирања налога. Попуњен ИКТ *Захтев* се доставља Кориснику који га прослеђује свом непосредном руководиоцу.

Руководилац ОЈ у којој Корисник већ ради, попуњава и потписује *ИКТ Захтев*, део који је обележен „Попуњава руководилац организационе јединице у којој запослени већ ради или из које одлази“ и предаје га Кориснику.

У случају миграције запосленог у другу ОЈ, Корисник доставља *ИКТ Захтев* руководиоцу организационе јединице у коју Корисник прелази који попуњава део *ИКТ Захтева*, који је обележен „Попуњава руководилац организационе јединице у којој запослени почиње да ради или у коју долази“. Потписан ИКТ Захтев предаје Кориснику.

Попуњени *ИКТ Захтев* Корисник доставља Дата центру. По пријему *ИКТ Захтева*, Администратор ДЦ спроводи тражене активности и уколико је потребно:

- прилагођава корисничке налоге за приступ ИКТ систему и/или ИС ИОРС-а, у складу са његовим новим радним ангажовањем или промењеним радним статусом;
- у случају потребе, проверава и преузима сву доступну рачунарску опрему која је евидентирана на име корисника и о исходу провере и преузимања обавештава у писаној форми Одељење за правне послове;
- промену евидентира у *Бази ИКТ ресурса и услуга ДЦ.*

Корисник потписом даје сагласност са подацима наведеним у *ИКТ Захтеву*.

По завршетку *ИКТ Захтева*, Администратор ДЦ га скенира, а папирну верзију документа доставља Одељењу за правне послове које обавештава шефа Одсека књиговодства о промени задужења ІКТ опреме.

5.3.6 Промена личних података корисника

Приликом промене личних података корисника због којих је потребна измена Корисничког налога, Одељење за правне послове попуњава део ИКТ *Захтева:* у сегменту „Попуњава Одељење за правне послове“ означава да налог треба „изменити“ избором опције „Измена личних података“ као основа за администрирање налога. Попуњен ИКТ *Захтев* се доставља Кориснику који га прослеђује свом непосредном руководиоцу.

Руководилац ОЈ у којој корисник већ ради потписује *ИКТ Захтев*, део који је обележен „Попуњава руководилац организационе јединице у којој запослени већ ради или из које одлази“, и предаје га кориснику који га доставља Дата центру.

Администратор ДЦ на основу *ИКТ Захтева* спроводи тражену измену корисничког креденцијала, попуњава и потписује на *ИКТ Захтеву* део који је обележен „Попуњава Дата центар“, евидентира у *Бази ИКТ ресурса и услуга ДЦ.*

Корисник потписом даје сагласност са подацима наведеним у *ИКТ Захтеву*.

По завршетку *ИКТ Захтева*, администратор ДЦ га скенира, а папирну верзију документа доставља Одељењу за правне послове које обавештава шефа Одсека књиговодства о промени задужења ИКТ опреме.

5.4 Задужење/раздужење Корисника ИКТ опремом

Задужење ИКТ опреме у власништву ИОРС-а (тј. са инвентарским бројем), врши се на име Корисника, а од стране администратора ДЦ.

Раздужење ИКТ опреме у власништву ИОРС-а (тј. са инвентарским бројем), врши се на име Дата центра, преузимањем од стране администратора ДЦ опреме којом је Корисник задужен.

Корисници са правом приступа ИКТ систему ИОРСа се задужују/раздужују рачунарском и другом ИКТ опремом путем *ИКТ Захтева*, истовремено са додељивањем, изменом, укидањем, блокирањем иил деблокирањем Корисничких налога описаних у претходној тачки 5.3. **Права приступа ИКТ систему ИОРС-а.**

У ситуацијама када се не мења статус Корисничког налога а потребно је Корисника задужити/раздужити са ИКТ опремом, *ИКТ захтев* не попуњава Одељење за правне послове већ само Корисник, одговарајући руководилац ОЈ и администратор ДЦ.

5.4.1 Задужење Корисника ИКТ опремом

Корисник или његов непосредни руководилац тражи од Дата центра усмену информацију да ли има за Корисника расположиве и потребне ИКТ опреме на стању. Након добијања потврдне информације од Дата центра, Корисник или руководилац ОЈ у којој корисник већ ради, у Напомени дела који је обележен „Попуњава руководилац организационе јединице у којој запослени већ ради или из које одлази“ наводи шта је од ИКТ опреме потребно Кориснику, руководилац ОЈ потписује *ИКТ Захтев* и предаје га Кориснику који га доставља Дата центру.

Администратор ДЦ на основу *ИКТ Захтева* спроводи задужење корисника ИКТ опремом, која је претходно конфигурисана у складу са *Процедуром о инсталацији и конфигурацији система.* Администратор ДЦ попуњава и потписује на *ИКТ Захтеву* део који је обележен „Попуњава Дата центар“ и евидентира промене у *Бази ИКТ ресурса и услуга ДЦ.*

Корисник потписом даје сагласност са подацима наведеним у *ИКТ Захтеву*.

По завршетку *ИКТ Захтева,* Администратор ДЦ га скенира, папирну верзију документа доставља Одељењу за правне послове, а електронску верзију шаље шефу Одсека књиговодства чиме га обавештава о промени задужења ІКТ опреме.

5.4.2 Раздужење Корисника ИКТ опремом

Корисник обавештава непосредног руководиоца да је потребно раздужити га ИКТ опремом. Тада Корисник или Руководилац ОЈ у којој корисник већ ради, у Напомени дела који је обележен „Попуњава руководилац организационе јединице у којој запослени већ ради или из које одлази“ наводи коју ИКТ опрему Корисник раздужује (списак инвентарских бројева опреме), Руководилац ОЈ потписује *ИКТ Захтев* и предаје га Кориснику који га доставља Дата центру.

Администратор ДЦ на основу *ИКТ Захтева,* спроводи проверу и раздуживање опреме Корисника којом је задужен, попуњава и потписује се на *ИКТ Захтеву (*део који је обележен „Попуњава Дата центар“) и евидентира промене у *Бази ИКТ ресурса и услуга ДЦ.* У случају постојања неправилности, исте евидентира у *ИКТ захтеву* и у *Бази ИКТ ресурса и услуга ДЦ.*

Корисник се потписује у *ИКТ Захтеву, ради потврде о примопредаји ИКТ опреме.*

По завршетку *ИКТ Захтева,* Администратор ДЦ га скенира, а папирну верзију документа доставља Одељењу за правне послове које обавештава шефа Одсека књиговодства о промени задужења ІКТ опреме.

5.5 Резервна Администраторска права

Администрирање сервера или неког ИС ИОРС-а може да врши само један изабрани Администратор ДЦ помоћу јединственог Администраторског налога. У таквим ситуацијама постоји резервни Администраторски креденцијал који се ковертира од стране надлежног Администратора ДЦ, затворена коверта се предаје начелнику ДЦ који коверту чува на безебедном месту.

У случају паланираних или непланираних одсуствовања изабраног Администратора ДЦ, начелник ДЦ именује заменика коме предаје коверат са резервним Администраторским креденцијалима. Заменик потом врши администрирање ИС.

По повратку са одсуства, изабрани Администратор ДЦ укида искоришћене резервне креденцијале, и генерише нове резервне Администраторске креденцијале које ковертира и доставља начелник ДЦ.

5.6 Заборављање, губитак или крађа корисничког креденцијала

- **Картица као кориснички креденцијал**

У случају заборављања идентификационе картице за TimeWorks3, запослени се јавља надлежном Администратору ДЦ на почеку и на крају радног времена тога дана на основу чега Администратор ДЦ то евидентира.

Ако дође до оштећења, губитка или крађе идентификационе картице за TimeWorks3, запослени је дужан да у најкраћем року то пријави Одељењу за правне послове које иницира добијање нове идентификационе картице и обавештава Администратора ДЦ. Администратор ДЦ додељује запосленом ПИН код који запослени користи до добијања идентификационе картице.

- **Име и лозинка као кориснички креденцијал**

У случају заборављања лозинке, запослени се јавља надлежном Администратору ДЦ који у његовом присуству изврши промену лозинке, без увида у исту.

Ако дође до губитка или крађе лозинке запослени је дужан да у најкраћем року то пријави Администратору ДЦ који:

- спречава могућу или даљу злоупотребу спорних креденцијала њиховим укидањем;
- омогућава даљи рад корисника отварањем нових креденцијала;
- о инциденту обавештава Одељење за правне послове;
- евидентира инцидент у *Бази ИКТ ресурса и услуга ДЦ*.

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. *Захтев за администрирање корисничког налога ИКТ система ИОРС-а* (у Прилогу)
3. *Процедуром 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)*

8.0 ПРИЛОГ

8.1 ПРИЛОГ: *Захтев за задужење/раздужење ИКТ опреме и администрирање налога за ИКТ система Института*

Захтев за задужење/раздужење ИКТ опреме и администрирање налога ИКТ система Института бр. _____

Име и презиме запосленог: [[IME_RADNIKA]] **Орг.јединица:** [[NAZIV_SLUZBE]] **Радно место:** [[RADNO_MESTO]]	**ЈМБГ:** [[JMBG]]	**ЛБО:** ID број (за TimeWORX3): [[MBROJ]]

Попуњава Одељење за правне послове

Основ за администрирање налога за ИКТ системе Института:

1. **Потписан уговор о раду** [[DATUM_ZAPOSLENJA]]
2. **Престанак радног односа**
3. **Одлазак на дуже одсуство**
4. **Повратак са дужег одсуства**
5. **Анекс уговора о раду**
   којим се запослени премешта из организационе јединице: _____
   у организациону јединицу: _____
   на послове: _____
6. **Промена личних података (имена и презимена, титуле и др.):**
   Из _____ у _____

Потребно је налоге за приступ ИКТ систему Института:
☐ отворити ☐ блокирати ☐ деблокирати ☐ укинути ☐ изменити

Напомена: _____

Потпис одговорног лица
Бранка Кривић, дипл.правник

Датум _____

Попуњава руководилац организационе јединице у којој запослени ПОЧИЊЕ да ради или у коју ДОЛАЗИ

Запосленом су потребни креденцијали за:
☐ лични email ☐ групни email
☐ Хелиант, за послове, тј. надлежности (навести):
- _____
- За лекаре специјализанте, навести име и презиме лекара за фактурисање: _____
- За лекаре специјалисте, навести назив специјалности: _____

☐ ИЗИС, email: _____ тел. _____

☐ ЛИС
☐ ТимДМС ☐ NextBIZ
☐ TimeWORX ☐ Е-досије
☐ ОпИС ☐ еПоС

Напомена: _____

Потпис руковидиоца: _____
Датум _____

Попуњава Администратор Дата Центра за запослене којима је ПОЧЕО/ПРЕСТАО радни однос

Запосленом су почели/престали да важе креденцијали:
лични email _____
групни email _____
Хелиант, корисничко име _____
ИЗИС, корисничко име _____
ЛИС, корисничко име _____
NexTBIZ, корисничко име _____
ТимДМС, корисничко име _____
Е-Досије, корисничко име _____
TimeWORX, корисничко име _____
ОпИС, корисничко име _____
еПоС, корисничко име _____
☐ _____

НАПОМЕНА: _____

Потпис Администратора ДЦ: _____
Датум _____

8.2 ПРИЛОГ: *Изјава о поверљивости*

ИЗЈАВА О ПОВЕРЉИВОСТИ

Име и презиме корисника

_____

ЈМБГ: | | | | | | | | | | | | | **ИД број корисника:** | | | | |

Сви подаци садржани у ИКТ систему ИОРС-а који нису јавни се сматрају поверљивим пословним или интерним подацима који не смеју бити саопштени или на други начин учињени доступним трећим лицима. Због тога је Корисник ИКТ система дужан да поштује следећа правила безбедног и примереног коришћења ресурса ИКТ система ИОРСа:

1. да обезбеди сигурност података и да се понаша сагласно утврђеним процедурама у складу са важећим процедурама и другим интерним прописима;
2. да користи информатичке ресурсе искључиво у пословне сврхе;
3. да током свог радног ангажовања у ИОРС-у и 10 година након његовог престанка поступа са поверљивим, интерним и пословним подацима у складу са прописима који уређују заштиту података о личности, а посебно приликом копирања и преноса података;
4. да током свог радног ангажовања у ИОРС-у и 10 година након његовог престанка не сме да износи, преноси или на други начин учини доступним трећим лицима, све поверљиве, интерне или пословне податке и информације, без одговарајућег одобрења;
5. да сви подаци који се генеришу, складиште, преносе или обрађују у оквиру ИКТ система ИОРС-а представљају власништво ИОРСа и да могу бити предмет надгледања и прегледања;
6. да приступа информатичким ресурсима само на основу додељених корисничких права од стране Дата центра и да иста не злоупотребљава;
7. да безбедно чува своје креденцијале од других лица и не дели их са другима (осим у случају заједничких или групних креденцијала);
8. да мења лозинке сагласно утврђеним правилима;
9. да одговорно и безбедно користи Internet, Intranet и e-mail сервис ИОРСа, у складу са прописаним процедурама и другим интерним правилима;
10. да се, пре сваког удаљавања од радне станице, одјави са система, односно закључа радну станицу;
11. да не сме да инсталира друге софтвере или модификује подешене опције, као ни да искључује из рада или брише заштитни, системски, апликативни или било који други софтвер инсталиран од стране Дата центра;
12. да не сме да инсталира, модификује, деинсталира, искључује из рада или мења хардверске компоненте рачунарске опреме, конфигурисане и инсталиране од стране Дата центра;
13. да не сме самоиницијативно да премешта, сервисира, мења са другим корисницима или на други начин располаже рачунарима или рачунарском опремом којом је задужен;
14. да не сме прикључује на рачунарску мрежу ИОРСа опрему која није власништво ИОРСа или која није проверена, инсталирана или конфигурисана од стране Дата центра;
15. да не сме да укључује или искључује мрежну конекцију без знања Дата центра;
16. да прихвати да се одређене врсте информатичких интервенција обављају у утврђено време;
17. да прихвати инсталацију техника и програма у циљу сигурности ИКТ система.

Корисник је упознат са основним концептима информатичке и сајбер безбедности и:

1. **прихвата правила безбедног и примереног коришћења ресурса ИКТ система ИОРСа;**
2. **сагласан је да се његови лични подаци, у контексту његовог рада на ИОРС-у, јавно објаве на сајту ИОРС-а, у публикацијама ИОРС-а, у часописима, медијима или другим облицима и формама јавног, научног или стручног обавештавања.**

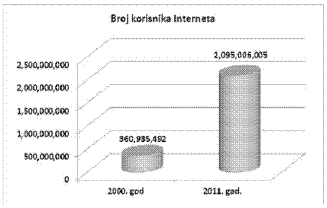
Датум: _____ **Потпис корисника**: _____

8.3 ПРИЛОГ: *Информатичка и сајбер безбедност: основни концепти и како се заштитити*

Информатичка и сајбер безбедност: основни концепти и како се заштити

Сајбер безбедност

- Интеграцијом Интернета у скоро све облике људске делатности доводи до повећане рањивости од сајбер напада.
- Сајбер безбедност је у жижи интересовања савременог друштва јер не може да се посматра одвојено од безбедности у реалном свету.



Сајбер безбедности се може разматрати према три критеријума:

Врста акције	Врста починиоца	Врста циља
▪ Пресретање података ▪ Ометање пријема података ▪ Илегални приступ/Шпијунирање ▪ Уништавање података ▪ Саботаже /Ускраћивање услуга ▪ Крађа идентитета...	▪ Хакери ▪ Сајбер криминалци ▪ Сајбер ратници ▪ Сајбер терористи...	▪ Појединци ▪ Компаније ▪ Јавне институције ▪ Државни органи ▪ Критична инфраструктура...

Најчешћи облици нарушавања безбедности:

- Крађа идентитета: крађа личних података, лозинки, пин-ова, итд.
- *Cyber шпијунажа*: неовлашћено прислушкивање, надгледања и прегледања
- *Haking:* приступ компјутерском или комуникационом систему за које не постоји дозвола његовог коришћења
- *Cyber саботажа*: саботажа је прикривено и подмукло деловање којим се наноси штета другима, а *Cyber* саботажа подразумева уништење или оштећење компјутера и других уређаја; брисање, мењање информација; спречавање коришћења информација садржаних у меморији информатичких уређаја, итд.
- *Cyber тероризам* обично подразумева нападе на компјутерске системе или мреже иза којих стоје неки политички циљеви)
- *Cyber ратовање* је подврста информационог ратовања, која се одвија у *Cyber* простору. Одликује га дејство у групи.
- *Крађа Интернет услуга* (крађа wifi-a)
- *Индустријска шпијунажа*
- *Надгледање е-поште и праћење е-конференција*
- *Phishing*: израда лажних WEB страница које су скоро идентичне оригиналној, са циљем да кроз унос података на лажној страници битне информације (лозинке, ПИН кодови,...) заврше код особа који могу да их искористити и злоупотребити. **ПАЖЊА: Сви сервиси са рад са осетљивим подацима имају протокол https** /**H**ypertext **T**ransfer **P**rotocol **S**ecure/ док лажне странице немају„**s**“ већ само **http**.

Подаци о Сајбер криминалу:

- Губици које наноси Сајбер криминал у 2017 години премашили су **1 трилион $**.
- Детектовано је око **300 милиона нових малвера** (злонамерних или штетних софтвера) у 2017 години, што је око 900 хиљада нових малвера сваког дана.
- Забележено је **10 пута више Ransomware** (злонамерни или штетни софтвер који угрожава рад рачунара) напада него у 2016 години. Ransomwape су софистицираније па је и број успешних напада налеко већи.
- Зарада од Сајбер криминала у 2017 години била је **дупло већа од зараде стечене трговином наркотицима**.

Слабости у Србији

- Јако ниска свест о значају Cyber-безбедности у јавном и приватном сектору.
- Треба знати да **једна Ваша грешка и један погрешан клик мишем може нарушити читав безбедносни концепт Вашег рачунара и целе мреже!**

Како се заштитити?

- ✓ Едукацијом о Cyber безбедности, као најефикаснијом мером заштите од свих врста претњи.
- ✓ Коришћењем легалних софтвера и њиховим редовним ажурирањем (*update*)
- ✓ Коришћењем одговарајућих антивирус-програма
- ✓ Избегавањем сумњивих email-ова, написаних „чудним“ писмом као и отварање линкова или attachment-а тих email-ова. **ПАЖЊА: увек избегавати email-ове којима се тражи одавање Ваших података и прослеђивање непознатом лицу.**
- ✓ Избегавањем сумњивих сајтова са игрицама, филмовима или музиком
- ✓ Провером адресне линије browser-а пре уноса важних података (лозинки, ПИН кодова или других личних података). **ПАЖЊА: Не уносити важне податке на порталима који нису https.**
- ✓ Редовном израдом копија електронских података (тј. редован Backup података)
- ✓ Прописним уништавањем папирних извора Ваших личних података (нпр. слипова са банкомата, сваког папира који садржи неки Ваш лични податак) како Ваши подаци не би случајно доспели у нежељене руке.

Коме се обратити?

За све информације у вези ИТ-безбедности или постојања било какве недоумице, обратите се Дата Центру (локали: **264, 116 и 123**)