



Број: 01-7844/9-1

Датум: 17.06.2025. године

На основу члана 8. Закона о информационој безбедности („Службени гласник РС“, број 6/16, 94/2017 и 77/19), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационих система од посебног значаја Владе РС („Службени гласник РС“, број 94/16) и члана 28. став 1. тачка 2. Статута, Управни одбор Универзитетског клиничког центра Крагујевац на седници одржаној дана 17.06.2025. године донео је

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА УНИВЕРЗИТЕТСКОГ КЛИНИЧКОГ ЦЕНТРА КРАГУЈЕВАЦ

Опште одредбе

Члан 1.

Овим Актом ближе се дефинишу мере заштите информационо-комуникационих система Универзитетског клиничког центра Крагујевац (у даљем тексту: Установа), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система као и овлашћења и одговорности корисника информатичких ресурса у Установи.

Члан 2.

Мере прописане овим Правилником односе се на све организационе јединице Установе, на све запослене кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Установе.

Непоштовање одредби овог Правилника од стране корисника информатичких ресурса представља повреду радне обавезе.

За праћење примене овог Правилника надлежно је Одељење информационо технолошког одржавања.

Члан 3.

Под пословима из области безбедности ИКТ система, сматрају се:

1. послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност;
2. послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности;
3. послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно добара ИКТ система Оператора, као и приступ, измена или коришћење средстава без овлашћења и без евиденције о томе;
4. праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу;
5. обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента Одељење информационо технолошког одржавања обавештава помоћника директора за техничке послове и директора Установе, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедносног инцидента.

Члан 4.

Поједини термини у смислу овог правилника имају следеће значење:

- 1) информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина 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 података коришћењем рачунарског програма;
- (3) 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;
- 2) информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;
- 3) тајност је својство које значи да податак није доступан неовлашћеним лицима;
- 4) интегритет значи очуваност изворног садржаја и комплетности податка;
- 5) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
- 6) аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
- 7) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
- 8) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
- 9) управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
- 10) инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
- 11) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
- 12) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
- 13) администраторско овлашћење је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;
- 14) кориснички налог јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно овлашћења корисника);
- 15) администраторски налог јесте јединствен налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога.

Коришћење ИКТ система

Члан 5.

Запослени који управљају ИКТ системом, у складу са важећом систематизацијом радних места, обавезно ће се оспособљавати и усавршавати, између осталог и упућивањем на обуке из области безбедности ИКТ система, управљања ИКТ системима и других области ИКТ, најмање једном на сваких шест месеци.



Одељење информационо технолошког одржавања је дужно да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Оператора, да га обучи за коришћење ресурса ИКТ система, да по завршетку обуке од запосленог узме изјаву о обучености за коришћење ИКТ ресурса и да о истима води евиденцију.

У случају промене радног места, односно надлежности корисника-запосленог надлежни субјект ИКТ система ће извршити промену права у коришћењу ИКТ система које је корисник запослени имао у складу са описом радних задатака.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида. Корисник ИКТ ресурса, коме је престало радно ангажовање по било ком основу код Оператора, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

Свако коришћење ИКТ ресурса Установе, запосленог-корисника, ван додељених овлашћење, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

Мере заштите

Члан 6.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Установе, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Сваки запослени-корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система, које користи ради обављања послова из своје надлежности.

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система надлежан је директор Установе и помоћник директора за техничке послове и Одељење информационо технолошког одржавања, у складу са важећом систематизацијом радних места у Установи.

Информатички ресурси Установе

Члан 7.

Информатички ресурси Установе су сви ресурси који садрже пословне информације Установе у електронском облику или служе за приступ корисника ИКТ систему укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, и слично.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебним прописима.

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо - телекомуникационим системима („Сл. Гласник РС“, бр. 53/2011).

Предмет заштите

Члан 8.

Предмет заштите обухвата:

1. хардверске и софтверске компоненте информатичких ресурса;
2. податке који се обрађују или чувају на информатичким ресурсима;
3. корисничке налоге за друге податке о корисницима информатичких ресурса Установе.



Корисник информатичких ресурса

Члан 9.

Корисник информатичких ресурса јесте постављено лице, запослено лице на неодређено или одређено време, лице ангажовано по основу уговора, консултант или друго радно ангажовано лице коме је одобрен приступ неком информатичком ресурсу Установе.

Корисник информатичких ресурса одговоран је за правилну употребу, тачност и сигурност података приликом коришћења информатичких ресурса Установе, односно лично је одговоран за остваривање својстава података у ИКТ систему Установе.

Дужност корисника информатичких ресурса

Члан 10.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне сврхе, а Установа задржава право да информатичке ресурсе повуче у одређеном тренутку и у потпуности задржи податке, с тим да ће у том случају Установа податке учинити доступним кориснику само уз претходну сагласност директора Установе.

Корисник не сме спроводити активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система Установе.

Корисник радне станице је дужан да пословне податке смешта на локалне дискове непреносиве радне станице или мрежне дискове.

Запослено, односно ангажовано лице у Одељењу информационо технолошког одржавања, са администраторским овлашћењима (у даљем тексту администратор) је дужно да повремено израђује резервне копије података са сервера, а док су лица која су задужила поједине радне станице дужна да израђују резервне копије локалних дискова радних станица Установе.

Корисник информатичких ресурса дужан је да поштује следећа правила безбедности примереног коришћења информатичких ресурса и то:

1. да користи информатичке ресурсе искључиво у пословне сврхе;
2. прихвати да су сви подаци који се складиште, преносе или процесуирају у оквиру информатичких ресурса власништво Установе и да могу бити предмет надгледња и прегледања;
3. поступа се поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. безбедно чува своје лозинке, односно да их не даје другим лицима;
5. мења лозинке сагласно утврђеним правилима;
6. пре сваког удаљавања од радне станице одјави се са система („log out“ односно „излогује“);
7. обезбеди сигурност података у складу са важећим прописима;
8. приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
9. не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
10. не сме да на радној станици складишти садржај који не служи у пословне сврхе;
11. израђује заштитне копије (backup) података у складу са прописаним процедурама;
12. користи Internet и Internet e-mail сервис у Установи у складу са приписаним процедурама;
13. прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, upgrade firmware, покретање антивирусног програма и сл.) обавља у утврђено време;
14. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;



15. прихвати да технике сигурности (антивирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалну претњу ИКТ систему;
16. не сме да инсталира, модификује, искључује из рада или брише, заштитни, системски или апликативни софтвер;
17. да се уздржи од активности којима се изазива неоправдано оптерећење информатичких ресурса Установе, као и повећано ангажовање особља на одржавању тих ресурса;
18. не сме неовлашћено да објављује или преноси личне податке до којих је дошао коришћењем информатичких ресурса Установе, као што су лозинке, бројеви платних картица, медицински подаци, приватни телефонски бројеви итд. и да тиме повреди приватност појединца;
19. да се уздржи од неубичајно и неоправдано великог коришћења информатичких ресурса Установе.

Безбедоносни профил корисника информатичких ресурса

Члан 11.

Право приступа имају само запослени/корисници који имају администраторске или корисничке налоге.

У зависности од описа задатака и послова радног места на које је распоређен, корисник информатичких ресурса, на предлог непосредног руководиоца, стиче одређена права приступа ИКТ систему Установе.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени корисник има. запослени који има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Креирање лозинке

Члан 12.

Лозинка може да садржи комбиноване карактере од малих и великих слова и цифара.

Лозинка не сме да садржи препознатљиве податке.

Ако корисник информатичких ресурса посумња да је друго лице открило његову лозинку, дужан је да исту одмах измени или, уколико нема приступ, да се писмено обрати администратору који ће лозинку променити.

Употреба корисничких налога

Члан 13.

Кориснички налог може употребљавати само корисник информатичких ресурса коме је исти издат.

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору у случају подешавања радне станице.

Корисник информатичких ресурса је непосредно одговоран за активности које су реализоване на основу његовог корисничког налога.

Запослени-корисник који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.



Кориснички налози са администраторским овлашћењима користе се само за потребе неопходних интервенција којима се обезбеђује несметан рад информатичких ресурса (у даљем тексту информатичке интервенције).

Употреба електронског сертификата

Члан 14.

Запослени-корисници користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама.

Запослени на пословима ИКТ су задужени за инсталацију потребног софтвера и хардвера за коришћење сертификата.

Запослени-корисници су дужни да чувају своје квалификоване електронске сертификате како не би дошли у посед других лица.

Употреба администраторског налога

Члан 15.

Право коришћења администраторског налога имају администратори за потребе информатичких интервенција.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Администраторска овлашћења могу добити само лица која су задужена за одржавање информатичких ресурса у Установи, уз претходну сагласност директора Установе.

Поступци у случајевима сигурносних инцидената

Члан 16.

Корисник информатичких ресурса дужан је да, без одлагања, пријави непосредном руководиоцу свако учовање или сумњу о наступању инцидената којим се угрожава сигурност ИКТ система.

Информације о инциденту руководиоца из става 1. овог члана дужан је да одмах проследи администратору, као и Одељење информационо технолошког одржавања.

По пријави инцидента мора се поступати адекватно и ефикасно, а по хитном поступку у случајевима:

1. нарушавање поверљивости информација,
2. откривање вируса или грешака у функционисању апликација,
3. вишеструки покушај неауторизованог приступа,
4. системских падова и престанка рада сервиса.

Одељење информационо технолошког одржавања је дужно да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести директора Установе, у складу са Законом којим се утврђује информационо безбедност.

Заштита од малициозног софтвера

Члан 17.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.



За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена:

1. лиценцираног софтвера, односно забрана коришћења неауторизованог софтвера;
2. правила за заштиту од ризика приликом преузимања фајлова из екстерних извора (података, апликација итд.).

Приликом преузимања фајлова из става 1. тачка 2) овог члана преносиви медији пре коришћења морају бити проверени на присуство вируса.

Ако се утврди да преносиви медиј садржи вирусе, врши се чишћење медија од вируса, уз сагласност доносиоца медија.

Ризик од евентуалног губитка података приликом чишћења медија антивирусним софтвером, сноси доносилац медија.

Заштита од губитка података

Члан 18.

Базе података обавезно се архивирају на преносиве медије (CDROM, DVD, USB, „strimer“ трака, екстерни харддиск), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

Остали фајлови-документи се архивирају најмање једном недељно, месечно и годишње.

Сигурност електронске поште

Члан 19.

У циљу коришћења сервиса електронске поште морају се поштовати следећа правила:

1. електронска пошта са прилозима не сме се отворати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;
2. забрањено је коришћење електронске поште у приватне сврхе.

Поступање са преносивим медијима

Члан 20.

У случају брисања података који се налазе на преносивим медијима, потребно је обезбедити њихово неповратно брисање. Преносив медији из става 1. овог члана, пре стављања ван употребе, морају бити физички уништени.

Физичка сигурност информатичких ресурса

Члан 21.

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови:

1. сервери и рачунари са посебним апликативним софтвером морају бити смештени у посебним просторијама (припадају одговарајућим службама Установе), које испуњавају стандарде противпожарне заштите, обезбеђене су механичком бравом и у којима је ограничен приступ другим лицима;
2. приступ просторијама из тачке 1., поред лица која су задужена за одржавање ИКТ система и лица која су запослена у тим службама, могу имати и друга лица, уз претходну сагласност директора Установе;
3. радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;



4. просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
5. штампачи, копиер машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих инфорамција;
6. медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

Инсталација и одржавање софтвера

Члан 22.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужени су администратори, који су дужни да поступају у складу са прописаним процедурама и упутствима.

Одељење информационо технолошког одржавања обезбеђује запосленом, односно ангажованом лицу, коришћење радне станице са преинсталираним и правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачи програми (drivers), пословно и развојно окружење, софтвер за вирусну заштиту, разне помоћне апликације), који је типски за све радне станице који представља минимум потребан за обављање стандардних послова.

Члан 23.

Запослени у Установи и друга релевантна лица су дужни да се у свему придржавају одредаба овог Правилника

Члан 24.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли Установе.

ПРЕДСЕДНИК УПРАВНОГ ОДБОРА
Проф. др Александар Стефановић