

На основу члана 94. Статута Медицинског факултета у Београду и члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16), Декан Универзитета у Београду, Медицинског факултета доноси

АКТ

О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА УНИВЕРЗИТЕТА У БЕОГРАДУ, МЕДИЦИНСКОГ ФАКУЛТЕТА

Предмет акта

Члан 1.

Овим актом ближе се дефинишу мере заштите информационо-комуникационих система на Медицинском факултету Универзитета у Београду (у даљем тексту: Факултет), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса на Факултету.

Циљеви акта

Члан 2.

Циљеви доношења овог акта су:

- 1) допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
- 2) минимизација безбедоносних инцидената;
- 3) допринос развоју одговарајућих безбедоносних апликација и обезбеђивање конзистентне контроле свих компонената информационо- комуникационог система (у даљем тексту: ИКТ систем).

Обавезност акта

Члан 3.

Овај акт је обавезујући за све организационе јединице Факултета и за све кориснике информатичких ресурса, као и за трећа лица која користе информатичке ресурсе Факултета.

Непоштовање овог акта повлачи дисциплинску одговорност корисника информатичких ресурса уз суспензију корисничких налога.

За суспензије корисничких налога предвиђених овим актом надлежан је Центар за информационе и комуникационе технологије (у даљем тексту: Центар).

Појмови

Члан 4.

Поједини изрази употребљени у овм акту имају следеће значење:

- 1) *интегритет* је немогућност неовлашћене измене информација;
- 2) *расположивост* је доступност информација корисницима информатичких ресурса у обиму корисничког овлашћења;
- 3) *администраторско овлашћење* је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;

4) *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);

5) *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.

Мере заштите

Члан 5.

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

Информатички ресурси Факултета

Члан 6.

Информатички ресурси Факултета су сви ресурси који садрже пословне информације Факултета у електронском облику или служе за приступ корисника ИКТ систему укључујући све електронске записе, рачунарску, серверску и мрежну опрему, мобилне уређаје, базе података, пословне апликације и слично.

Предмет заштите

Члан 7.

Предмет заштите обухвата:

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

Корисник информатичких ресурса

Члан 8.

Корисник информатичких ресурса јесте постављено лице, запослено лице на неодређено или одређено време, лице ангажовано по основу уговора, консултант, сарадник, друго радно ангажовано лице коме је одобрен приступ неком информатичком ресурсу Факултета и студенти Медицинског факултета Универзитета у Београду.

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

Корисник информатичких ресурса нема имовинска права над информатичким ресурсима Факултета.

Дужности корисника информатичких ресурса

Члан 9.

Корисник не сме да спроводи активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система Факултета.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне сврхе, а Факултет задржава право да информатичке ресурсе повуче у било ком тренутку и у потпуности задржи све податке, без обавезе да их накнадно преда кориснику.

Студент Факултета може на лични захтев, који мора бити заведен у писарници Факултета, добити податке који се налазе у његовом личном досијеу.

Запослено, односно ангажовано лице у Центру и у службама Факултета је дужно да обезбеди прављење копије података у дефинисаним интервалима.

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

- 1) користи информатичке ресурсе искључиво у пословне сврхе;
- 2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Факултета и да могу бити предмет надгледања и прегледања;
- 3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
- 4) безбедно чува своје лозинке, односно да их не одаје другим лицима;
- 5) мења лозинке сагласно утврђеним правилима;
- 6) пре сваког удаљавања од радне станице, одјави се са система („излогује“), односно закључа радну станицу (CTRL+ALT+DEL+LOCK или WINDOWS+L)

- 7) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;

- 8) обезбеди сигурност података у складу са важећим прописима;
- 9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
- 10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
- 11) не сме да на радној станици складишти садржај који не служи у пословне сврхе;
- 12) израђује заштитне копије (backup) података у складу са прописаним процедурама;
- 13) користи интернет и електронску пошту Факултета у складу са прописаним процедурама детаљније дефинисаним у Правилнику о коришћењу сервиса Медицинског факултета Универзитета у Београду;
- 14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, upgrade firmware-а, покретање антивирусног програма и сл.) обављају у утврђено време;
- 15) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
- 16) прихвати да техничке мере сигурности (антивирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему.
- 17) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

Безбедоносни профил корисника информатичких ресурса

Члан 10.

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 Факултета.

Администраторска овлашћења могу добити само лица која су задужена за одржавање информатичких ресурса на Факултету.

Креирање лозинке

Члан 11.

Лозинка мора да садржи минимум седам карактера комбинованих од малих и великих слова, цифара и специјалних знакова.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке.

Ако корисник информатичких ресурса посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Корисник информатичких ресурса дужан је да мења лозинку најмање једном у три месеца. Иста лозинка се не сме понављати у временском периоду од годину дана.

Употреба корисничког налога

Члан 12.

Кориснички налог може да употребљава 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.

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 администраторског налога

Члан 13.

Администраторски налози свих пословних апликација, сервера база података и системских апликација за управљање мрежном опремом и уређајима за складиштење података чувају се у затвореним, непровидним ковертама на обезбеђеном месту у оквиру Центра.

Право коришћења администраторског налога имају само администратори за потребе информатичких интервенција.

Поступци у случајевима сигурносних инцидената

Члан 14.

Корисник информатичких ресурса дужан је да, без одлагања, пријави непосредном руководиоцу свако уочавање или сумњу о наступању инцидента којим се угрожава сигурност

ИКТ система.

Информацију о инциденту руководиоца из става 1. овог члана дужан је да одмах проследи администратору, као и Центру.

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

- 1) нарушавања поверљивости информација,
- 2) откривања вируса или грешака у функционисању апликација,
- 3) вишеструких покушаја неауторизованог приступа,
- 4) системских падова и престанка рада сервиса.

Центар је дужан да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести надлежни орган, у складу са законом којим се уређује информациона безбедност.

Заштита од малициозног софтвера

Члан 15.

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 и сл.).

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

Ако се утврди да је 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.

Сигурност електронске поште

Члан 16.

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

- 1) електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;
- 2) забрањено је коришћење службене електронске поште у приватне сврхе;
- 3) не смеју се користити приватни налози електронске поште у пословне сврхе;
- 4) програми који користе сервисе електронске поште морају се искључити када се рачунар не користи;

Поред правила из става 1. овог акта, приликом коришћења електронске поште морају се поштовати и правила наведена у Правилнику о коришћењу сервиса Медицинског факултета Универзитета у Београду.

Физичка сигурност информатичких ресурса

Члан 17.

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

- 1) сервери, складишта података (storage-и) и комуникационо чвориште у седишту Факултета морају бити смештени у посебној просторији (сервер сала) која испуњава стандарде противпожарне заштите и поседује редувантно напајање електричном струјом и адекватну климатизацију;
- 2) сервери, складишта података (storage-и) и комуникационо чвориште у службама у другим објектима Факултета морају бити смештени у адекватним просторијама, у којима је забрањен приступ неовлашћеним лицима;
- 3) приступ сервер сали, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење координатора Центра;
- 4) радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;
- 5) обезбеђивање се врши и видео надзором уз обавезна обавештења о постојању видео надзора на свим улазима у објекат у коме се оно врши;
- 6) просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
- 7) штампачи, копијер машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;
- 8) медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

Приступ ИКТ систему Факултета

Члан 18.

Приступ свим компонентама ИКТ система мора бити аутентификован.

Администратор, на основу прецизног писаног захтева непосредног руководиоца, додељује кориснику информационог ресурса корисничко име, лозинку и привилегије, као и налог за електронску пошту.

Кориснику информатичких ресурса додељују се само привилегије које су неопходне за реализацију његових радних обавеза.

У случају престанка радног односа или радног ангажовања на Факултету кориснику информатичких ресурса укида се право приступа ИКТ систему сем у случају електронске поште чије је даље ограничено коришћење дефинисано у Правилнику о коришћењу сервиса Медицинског факултета Универзитета у Београд.

О престанку радног односа или радног ангажовања, као и о промени радног места корисника информатичких ресурса, непосредни руководиоца је дужан да обавести Центар ради укидања, односно измена приступних привилегија тог корисника.

Корисник информатичких ресурса, након престанка радног ангажовања на Факултету, не сме да открива поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система.

Трећем лицу могу се одобрити права приступа ИКТ систему уз претходно склапање одговарајућег уговора, којим се прецизно дефинишу услови и обим права приступа, укључујући и све релевантне безбедносне захтеве.

Изузетно од става 7. овог члана, у случају неопходних и хитних послова могу се одобрити права приступа ИКТ систему трећем лицу по усменом налогу управе Факултета, односно овлашћеног лица, о чему ће се накнадно, по завршетку посла, сачинити записник о оствареном приступу.

Ако се установи повреда уговорне обавезе или прекорачење овлашћења по основу уговара, одобрени приступ се одмах укида.

Инсталација и одржавање софтвера

Члан 19.

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

Факултет обезбеђује запосленом, односно радно ангажованом лицу, коришћење радне станице (десктоп или лаптоп) са преинсталираним системом или без њега док је Центар одговоран за правилно и потпуно конфигурирање софтвера (оперативни систем, сви управљачки програми (драјвери), пословно и развојно окружење, софтвер за вирусну заштиту, разне помоћне апликације), који је типски за све радне станице и који представља минимум потребан за обављање стандардних послова.

Администратор врши оцену конзистентности траженог софтвера са постојећим инсталираним софтверима на предметној радној станици и уколико оцени да тражени софтвер неће угрозити и ометати рад или прекршити ауторска права, инсталираће захтевани софтвер.

Основна подешавања из става 2. овог члана су:

- 1) додељивање имена и TCP/IP адреса или подешавање приступа DHCP-у и ргоху серверу;
- 2) подешавање мејл-клијента;
- 3) подешавање интернет претраживача (TCP/IP адреса прокси сервера);
- 4) инсталација антивирусног софтвера одобреног од стране Центра;
- 5) инсталација званичног апликативног софтвера који одређене организационе јединице Факултета користе у свом раду.

У случају да је кориснику потребно да се изврши инсталација одређеног специфичног софтвера на радној станици, непосредни руководиоца подноси захтев електронским путем Центру.

Корисник информатичких ресурса дужан је да сваки проблем у функционисању оперативног система, имејл клијента, интернет претраживача, пословног софтвера и апликативног софтвера, пријави непосредном руководиоцу, који ову информацију прослеђује електронским путем Центру.

Проблем у функционисању антивирусног и антиспајвер софтвера мора се пријавити Центру без одлагања електронским путем.

Администратор је дужан да проблеме из ст. 6. и 7. овог члана отклони у најкраћем могућем року на локацији корисника, даљинском конекцијом ка радној станици или тражењем да се радна јединица достави у сервис Центра.

Детаљно регулисање употребе сервиса Факултета

Члан 21.

Даље, прецизније регулисање коришћења информационих система и ресурса Факултета регулисано је:

1. Правилником о раду и коришћењу услуга Центра за информационе и комуникационе технологије Медицинског факултета Универзитета у Београду
2. Правилником о садржају интернет портала Медицинског портала у Београду

Завршна одредба

Члан 22.

Овај акт ступа на снагу осмог дана од дана објављивања на огласној табли, односно на интернет страници Факултета.

ДЕКАН
МЕДИЦИНСКОГ ФАКУЛТЕТА
Проф. др Небојша Лалић