На основу члана 8. Закона о информационој безбедности („Сл. гласник РС”, бр.6/2016, 94/2017 и 77/2019), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Сл. гласник РС”, бр. 94/2016) и чл. 14. Статута Грађевинско-архитектонског факултета у Нишу, бр.7/15 од 11.05.2018.године, бр.7/20 од 26.02.2019.године и бр.7/25 од 29.12.2021.године, Савет Грађевинско-архитектонског у Нишу, на седници одржаној 7. октобра 2024. године, донео је

П Р А В И Л Н И К
о безбедности информационо - комуникационог система Грађевинско-архитектонског факултета Универзитета у Нишу

I. УВОДНЕ ОДРЕДБЕ

Члан 1.

Правилник о безбедности информационо - комуникационог система Грађевинско-архитектонског факултета у Нишу (у даљем тексту: Правилник) утврђује, у складу са законским и подзаконским прописима, мере заштите, принципе, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо - комуникационог система Грађевинско-архитектонског факултета Универзитета у Нишу.

.

Члан 2.

Мере прописане овим Правилником односе се на све организационе јединице **Грађевинско-архитектонског факултета Универзитета у Нишу** (у даљем тексту: Факултет) и на све кориснике информатичких ресурса.

Члан 3.

Поједини термини у смислу овог Правилника имају следеће значење:
1) *Информационо-комуникациони систем* (у даљем тексту: ИКТ систем) је техничко-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 и пренос података коришћењем рачунарског програма;
(3) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из тачке (1) и (2) овог става, 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) *Корисници информатичких ресурса* (регистровани корисници) су запослени, студенти, као и трећа лица која користе информатичке ресурсе Факултета са регистрацијом одобреном од стране Факултета;
4) *Привремено регистровани корисници* су корисници који се на мрежу региструју у ограниченом временском периоду;
5) *Тајност* је својство које значи да податак није доступан неовлашћеним лицима;

6) *Интегритет* значи очуваност изворног садржаја и комплетности податка;
7) *Расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
8) *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;
9) *Непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
10) *Ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
11) *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;
12) *Инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
13) *Мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
14) *Тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
15) *Компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
16) *Криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини нечитљивим неовлашћеним лицима;
17) VPN (Virtual Private Network) је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
18) Backup је резервна копија података;
19) Download је трансфер података са централног рачунара или web презентације на локални рачунар;
20) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
21) Freeware је бесплатан софтвер;
22) Opensource је софтвер чији је изворни код јавно доступан;
23) Firewall је „заштитни зид“, односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
24) USB или флеш меморија је спољашњи медијум за складиштење података;
25) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;
26) DVD је оптички диск већег капацитета који се користи као медијум за складиштење података.

II. МЕРЕ ЗАШТИТЕ

Члан 4.

Мерама заштите ИКТ система Факултета, обезбеђује се превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Факултета

Члан 5.

Сваки корисник ресурса ИКТ система Факултета је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности.
За контролу и надзор над обављањем послова корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Факултета надлежан је руководилац послова информационих система и технологија Факултета.

Члан 6.

Под пословима из области безбедности утврђују 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 информационих добара ИКТ система Факултета, као и приступ, измене 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 Факултета, у складу са прописима.
У случају инцидента руководилац послова информационих система и технологија, обавештава декана Факултета, који у складу са прописима обавештава надлежне органе Факултета у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Привремено регистровани корисници, путем мобилних уређаја, могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ интернету, али не и деловима мреже кроз коју се обавља службена комуникација. О техничкој реализацији брине се администратор мреже.
Регистровани корисници могу уз одговарајуће креденцијале приступити и деловима мреже намењеним јавној употреби.

Члан 8.

Због отворености ка академским ресурсима треба обезбедити раздвајање мреже одговарајућим уређајима на део мреже са кључним уређајима неопходним за пословање Факултета и јавну инфраструктуру. Ти уређаји морају имати активне антивирус, антиспам мере, као и мере против изношења интерних докумената, мере против употребе нестандардизованих апликација и напредно логовање.
Приступ ресурсима ИКТ система Факултета са удаљених локација, од стране корисника, у циљу обављања радних задатака, треба омогућити путем заштићене VPN интернет конекције.

Члан 9.

Проактивне мере за заштиту мреже обезбеђују се употребом одговарајућег софтвера за надгледање мреже. Софтвер треба да поседује систем обавештавања када год се региструје неки догађај који може бити малициозног типа. Такође је потребно извршити и корелацију логова са различитих мрежних уређаја.

Члан 10.

За вођење евиденције приватних уређаја са којих ће бити омогућен приступ одговоран је руководилац послова информационих система и технологија.
Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране администратора информационих система и технологија и могу се користити само за обављање послова у надлежности запосленог и то само у периоду када није могуће користити уређај у власништву Факултета.

3. Одговорност коришћења ИКТ система Факултета

Члан 11.

ИКТ системом Факултета управљају запослени у складу са важећом систематизацијом радних места.
Руководилац послова информационих система и технологија је дужан да сваког новозапосленог ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Факултета, да га упозна са правилима коришћења ресурса ИКТ система Факултета, као и да води евиденцију о изјавама новозапослених да су упознати са правилима коришћења ИКТ ресурса Факултета.

Члан 12.

Свако коришћење ИКТ ресурса Факултета од стране запосленог, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

4. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених на Факултету

Члан 13.

У случају промене послова, односно надлежности запосленог, администратор информационих система и технологија одговоран је за промену привилегија које је запослени имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.
У случају престанка радног ангажовања запосленог, кориснички налог се укида.

Члан 14.

О престанку радног односа или радног ангажовања, као и промени радног места, овлашћени запослени у Служби за опште и административно-правне послове у сарадњи са непосредним руководиоцем обавештава администратора информационих система и технологија, ради укидања, односно измене приступних привилегија тог запосленог.

Члан 15.

Корисник ИКТ ресурса, након престанка радног ангажовања, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 16.

Информациона добра Факултета су сви ресурси који садрже пословне информације Факултета, односно путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему Факултета, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем Факултета и сл.)

Члан 17.

За вођење евиденције о информационим добрима одговоран је руководилац послова информационих система и технологија.

Члан 18.

Предмет заштите су:
1) Хардверске и софтверске компоненте ИКТ система Факултета;
2) Подаци који се обрађују или чувају на компонентама ИКТ система Факултета;
3) Кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система Факултета.

6. Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности

Члан 19.

Подаци који се налазе у ИКТ систему Факултета представљају тајну, уколико је тако дефинисано посебним законским прописима који уређују ову материју.
Подаци који се означе као тајни, морају бити заштићени у складу са одредбама посебних законских прописа који уређују ову материју.
Детаљан опис информација, носача информација и доступности података налази се у Упутству о раду Рачунарско-информационог центра Факултета.

7. Заштита носача података

Члан 20.

Руководилац послова информационих система и технологија ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да:
1) Подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени којима је то право обезбеђено одлуком декана;

2) Подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране администратора информационих система и технологија, у сврху архивирања.
За вођење евиденције носача на којима су снимљени подаци одговоран је руководилац послова информационих система и технологија и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

Члан 21.

У случају транспорта медија са подацима, руководилац послова информационих система и технологија ће одредити одговорну особу и начин транспорта.
У случају истека рокова чувања података који се налазе на медијима, подаци морају бити неповратно обрисани, а ако то није могуће, такви медији морају бити физички оштећени, односно уништени.

Члан 22.

Администратор информационих система и технологија је дужан да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради *backup* података који се налазе у уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати податке у уређај.

8. Ограничење приступа подацима и средствима за обраду података

Члан 23.

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

Члан 24.

Корисник може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, сем администратору за подешавање корисничког профила и радне станице.
Корисник који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.

Члан 25.

Корисник је дужан да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система Факултета, 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, уколико није другачије регулисано уговорима закљученим са трећим лицима, као и да сви подаци могу бити предмет аутоматизованог надгледања и прегледања, у циљу очувања безбедности ИКТ система Факултета;
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, односно закључа радну станицу;
7) Захтев за инсталацију специфичног 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) На радној станици не сме да 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;
14) Прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, 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 технике сигурности (анти вирус 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 који је инсталиран од стране надлежне службе.

9. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Члан 26.

Право приступа ИКТ систему и услугама које ИКТ систем пружа имају само корисници који имају корисничке налоге.
Администраторски налог је налог којим је омогућен приступ и администрација свих ресурса ИКТ система Факултета, као и отварање нових и измена постојећих налога.

Члан 27.

Администраторске налоге за управљање доменом могу да користе само запослени који су овлашћени за обављање ових послова од стране руководиоца послова информационих система и технологија.
Право приступа за управљање базом података имају само запослени који су овлашћени за обављање ових послова од стране декана Факултета. Руководилац послова информационих система и технологија обезбеђује приступ, у складу са одлуком декана Факултета.

Члан 28.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу уносити са тастатуре или читати са медија на коме постоји електронски сертификат, на основу кога/јих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог.

Члан 29.

Кориснички налог додељује администратор, на основу захтева овлашћеног запосленог у Служби за опште и административно-правне послове у сарадњи са непосредним руководиоцем и то тек након уноса података о запосленом у софтвер за

управљање људским ресурсима, а у складу са потребама обављања пословних задатака од стране запосленог.
Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева овлашћеног запосленог у Служби за опште и административно-правне послове, односно надлежног руководиоца.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 30.

Кориснички налог се састоји од корисничког имена и лозинке. Корисничко име се креира по моделу име.презиме, латиничним писмом без употребе слова ђ,ж,љ, њ, ћ, ч, џ, ш.
Уместо ових слова користити слова из табеле.

Ћирилична слова	Латинична слова
ђ	dj
ж	z
љ	lj
њ	nj
ћ, ч	c
ш	s
џ	dz

Лозинка мора да садржи минимум осам 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 посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.
Корисник је дужан да мења лозинку у периоду који одреди руководилац послова информационих система и технологија.
Кориснички налог може да се се креира и на основу података који се налазе на медијуму са квалификованим електронским сертификатом (нпр. лична карта са чипом и уписаним сертификатом).

Члан 31.

Пријављивање у ИКТ систем Факултета за све послове финансијске природе, врши се електронским сертификатом.
Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

11. Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Члан 32.

Руководилац послова информационих система и технологија је задужен за формирање листе критичних ресурса за које се захтева посебна криптозаштита.
За приступ ресурсима из става 1. овог члана посебним правилником ће бити дефинисана употреба одговарајућих мера криптозаштите узимајући у обзир осетљивост информација које треба да се штите, пословне процесе који се спроводе, ниво захтеване заштите, имплементацију примењених криптографских техника и управљање криптографским кључевима.

Члан 33.

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

12. Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система Факултета и обрађују подаци у ИКТ систему Факултета

Члан 34.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система Факултета, организује са као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система Факултета у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом, видео надзором и биометријским мерама.
Простор мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор).
За вођење евиденције о уласку у ову зону одговоран је руководилац послова информационих система и технологија.

13. Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем Факултета

Члан 35.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само надлежним лицима које одреди руководилац послова информационих система и технологија.
Осим лица из става 1. овог члана, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу руководиоца послова информационих система и технологија и уз присуство надлежног лица.
Приступ административној зони може имати и запослени на пословима одржавања хигијене уз присуство надлежног лица из става 1. овог члана.
Просторија мора бити видљиво обележена и у њој се мора налазити противпожарна опрема.
Прозори и врата на овој просторији морају увек бити затворени.
Сервери и активна мрежна опрема (switch, modem, router, firewall), морају стално бити прикључени на уређаје за непрекидно напајање – UPS.

Члан 36.

У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, овлашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.
ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења руководиоца послова информационих система и технологија.
У случају изношења опреме ради селидбе или сервисирања, неопходно је одобрење руководиоца послова информационих система и технологија, који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења руководиоца послова информационих система и технологија, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.
Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Факултета.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података кључних за функционисање Факултета

Члан 37.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система Факултета и, у складу са тим, планирају, односно предлажу руководиоцу послова информационих система и технологија Факултета одговарајуће мере.
Руководилац послова информационих система и технологија је задужен за формирање листе софтвера и рачунарских ресурса кључних за функционисање Факултета, коју доставља декану Факултета на сагласност.

Члан 38.

Пре увођења у рад новог софтвера који је кључан за функционисање Факултета неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију.
Инсталирање новог софтвера из става 1. овог члана, као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад корисника.
У случају да се на новој верзији софтвера који је уведен у оперативни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

Члан 39.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем Факултета морају се користити сервери и подаци који су намењени тестирању и развоју.
При тестирању софтвера је потребно обезбедити неометано функционисање ИКТ система Факултета. Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера, на начин који може да заустави нормално функционисање ИКТ система.

15. Заштита података и средства за обраду података од злонамерног софтвера

Члан 40.

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, електронском поштом, зараженим преносним медијумима (USB меморија, CD итд.), инсталацијом нелегалног софтвера и сл.
Корисник је дужан да у циљу заштите од вируса на рачунару који користи у обављању својих послова има инсталиран антивирусни програм и редовно га ажурира. Руководилац послова информационих система и технологија је одговоран за испуњење услова и контролу из става 2. овог члана.

Члан 41.

Запослени су дужни да редовно врше скенирање рачунара из става 2. члана 39. на вирусе, као и чишћење медија антивирусним софтвером. Запослени су дужни да пријаве присуство малициозног софтвера руководиоцу послова информационих система и технологија.
Преносиви медији, пре коришћења, морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером.
Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносивих медија.
Ризик од евентуалног губитка података приликом чишћења медија од вируса сноси доносилац медија.

Члан 42.

У циљу заштите, односно превенције упада у ИКТ систем Факултета са интернета администратор информационих система и технологија је дужан да одржава систем за спречавање упада.
Руководиоци организационих јединица одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Члан 43.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема). Администратор информационих система и технологија укида приступ за сваки неовлашћено прикључени уређај.

Члан 44.

Корисници ИКТ система Факултета који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем Факултета, а сваки рачунар чији се запослени прикључује на интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши администратор информационих система и технологија.
Приликом коришћења интернета треба избегавати сумњиве WEB странице, с обзиром да то може проузроковати проблеме - неприметно инсталирање шпијунских програма и слично.
У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Рачунарско-информационом центру.

Члан 45.

За дефинисање политике филтрирања садржаја на интернету одговоран је руководилац послова информационих система и технологија.
Није дозвољено:
1) Инсталирање, дистрибуција, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
2) Нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
3) Намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
4) Недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;

5) Гледање видео садржаја са илегалних стриминг сервиса на рачунарима и приступ WEB страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.
6) Нелегално преузимање (download) материјала заштићених ауторским правима;
7) Коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
8) Недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета;
9) Коришћење инфраструктуре Факултета за рударење крипто валуте.
Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже може се одузети право приступа.

16. Заштита од губитка података

Члан 46.

Базе података које се односе на званичне евиденције Факултета обавезно се архивирају на мрежне дискове за ову намену једном дневно уз употребу специјализованог софтвера.
Остали критични фајлови-документи се архивирају најмање једном недељно, месечно и годишње.
Подаци о корисницима, архивирају се најмање једном месечно.
Дневно копирање-архивирање врши се за сваки радни дан у седмици, од 20 часова сваког радног дана.
Недељно копирање-архивирање врши се последњег радног дана у недељи, од 20 часова.
Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно, од 20 часова.
Годишње копирање-архивирање врши се последњег радног дана у години.

Члан 47.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе.
Сваки примерак преносног информатичког медија са копијама-архивама, мора бити означен бројем, врстом (дневна, недељна, месечна, годишња), датумом израде копије-архиве, као и именом запосленог-корисника који је извршио копирање-архивирање.
Дневне, недељне и месечне копије-архиве се чувају у просторији која је обезбеђена физички и у складу са мерама заштите од пожара.
Годишње копије-архиве се израђују у два примерка, од којих се један чува у просторији у којој се чувају дневне, недељне и месечне копије-архиве а други примерак на географски истуреној локацији, са одговарајућом криптографском заштитом.
Исправност копија-архива проверава се најмање на шест месеци и то тако што се изврши повраћај база података које се налазе на медију, при чему враћени подаци након повраћаја треба да буду исправни и спремни за употребу.

17. Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Члан 48.

О активностима администратора и корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др).
Сваког последњег радног дана у недељи датотеке у којима се налази дневник активности се архивирају по процедури за израду копија-архива осталих података у ИКТсистему, у складу са чланом 46.- 47. овог Правилника.

Члан 49.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и др., треба бити подешен тако да одмах обавештава администратора и руководиоца послова информационих система и технологија о свим нерегуларним активностима корисника, покушајима упада и упадима у систем. У случају безбедносних инцидената руководилац послова информационих система и технологија обавештава декана.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 50.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Факултета, односно Freeware и Opensource верзије.
Инсталацију и подешавање софтвера који захтева лиценцирање може да врши само администратор информационих система и технологија, односно запослени који има овлашћење за то.
Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера.

Члан 51.

Пре сваке инсталације нове верзије софтвера, односно подешавања, неопходно је направити копију постојећег, како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система Факултета

Члан 52.

Администратор информационих система и технологија најмање једном месечно а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.
Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, администратор информационих система и технологија је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

20. Обезбеђивање да активности на ревизији ИКТ система Факултета имају што мањи утицај на функционисање система

Члан 53.

Ревизија ИКТ система Факултета се мора вршити тако да има што мањи утицај на пословне процесе запослених. Уколико то није могуће у радно време, онда се врши након завршетка радног времена запослених, чији би пословни процес био ометан, уз претходну сагласност декана.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 54.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, router, firewall) се мора налазити у закључаном rack орману.

Члан 55.

Техничар за одржавање хардвера и софтвера је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Члан 56.

Бежична мрежа коју могу да користе посетиоци објеката у надлежности Факултета, мора бити одвојена од интерне мреже коју користе запослени на Факултету и кроз коју се врши размена службених података и мора да поседује одговарајући систем аутентификације, као минимални ниво заштите. Потпуно отворене мреже се не смеју постављати и инсталирати.

22. Безбедност података који се директно размењују између ИКТ система Факултета и академских и комерцијалних провајдера

Члан 57.

Размена података са академским и комерцијалним интернет провајдерима врши у складу са потписаним Уговорима о пословно техничкој сарадњи.

23. Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система Факултета, односно делова система

Члан 58.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена на Факултету, биће дефинисан уговором који ће бити склопљен са тим лицима.
Техничар за одржавање хардвера и софтвера је/су задужен/и за технички надзор над реализацијом уговорених обавеза од стране трећих лица.
О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система Факултета техничар за одржавање хардвера и софтвера води документацију.
Документација из претходног става мора да садржи описе свих процедура а посебно процедура које се односе на безбедност ИКТ система.

24. Заштита података који се користе за потребе тестирања ИКТ система Факултета односно делова система

Члан 59.

За потребе тестирања ИКТ система односно делова система пројектант информатичке инфраструктуре система може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

25. Заштита средстава оператора ИКТ система Факултета која су доступна пружаоцима услуга

Члан 60.

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ.

Пројектант информатичке инфраструктуре је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог Правилника којима су такве активности дефинисане.

26. Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система Факултета, инцидентима и претњама

Члан 61.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени је дужан да одмах обавести руководиоца послова информационих система и технологија.
По пријему пријаве руководилац послова информационих система и технологија је дужан да одмах обавести декана и предузме мере у циљу заштите ресурса ИКТ система Факултета.

Члан 62.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Сл.гласник РС“, бр, 94/2016), роководилац послова информационих система и технологија, је дужан да поред декана обавести и надлежни орган дефинисан овом Уредбом.

Члан 63.

Руководилац послова информационих система и технологија води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са Уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

27. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 64.

У случају ванредних околности, које могу да доведу до измештања ИКТ система Факултета из зграде Факултета, руководилац послова информационих система и технологија, је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.
Спецификацију делова ИКТ система Факултета који су неопходни за функционисање у ванредним ситуацијама израђује руководилац послова информационих система и технологија.
Делове ИКТ система Факултета који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди руководилац послова информационих система и технологија. Складиштење делова ИКТ система Факултета који нису неопходни врши се тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води.

III. ПРОВЕРА ИКТ СИСТЕМА ФАКУЛТЕТА

Члан 65.

За проверу ИКТ система Факултета одговоран је руководилац послова информационих система и технологија.

IV. САДРЖАЈ ИЗВЕШТАЈА О ПРОВЕРИ ИКТ СИСТЕМА ФАКУЛТЕТА

Члан 66.

Извештај о провери ИКТ система Факултета садржи:
1) Назив оператора ИКТ система Факултета који се проверава;
2) Време провере;
3) Подаци о лицима која су вршила проверу;
4) Извештај о спроведеним радњама провере;
5) Закључке по питању усклађености Правилника о безбедности ИКТ система Факултета са прописаним условима;
6) Закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
7) Закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система Факултета;
8) Оцена укупног нивоа информационе безбедности;
9) Предлог евентуалних корективних мера;
10) Потпис одговорног лица које је спровело проверу ИКТ система Факултета.

V. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 67.

За праћење примене овог Правилника обавезује се руководилац послова информационих система и технологија Рачунарско-информационог центра Факултета.
Непоштовање одредби овог Правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса Факултета.

Члан 68.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, Рачунарско-информационог центра Факултета и радних места за послове ИКТ, руководилац послова информационих система и технологија на Факултету је дужан да обавести декана, како би се покренула процедура измене овог Правилника, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система Факултета, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система Факултета.

Члан 69.

Овај Правилник се мења по поступку који је предвиђен за његово доношење.

Члан 70.

Овај Правилник ступа на снагу осмог дана од дана објављивања на Интернет презентацији Факултета.

Бр. 7/ 35-1 – 07.10.2024. године

САВЕТ
ГРАЂЕВИНСКО-АРХИТЕКТОНСКОГ ФАКУЛТЕТА У НИШУ
ПРЕДСЕДНИК,
Проф.др Александар Милојковић