УНИВЕРЗИТЕТ У НИШУ
ФАКУЛТЕТ ЗАШТИТЕ НА РАДУ У НИШУ
UNIVERSITY OF NIŠ
FACULTY OF OCCUPATIONAL SAFETY

РЕПУБЛИКА СРБИЈА, 18106 Ниш, Чарнојевића 10 А, Тел: (018) 529-701, Факс: (018) 249-962, Т.Р. 840-1747666-77, ПИБ 100663853, М.Б. 07226063
E-mail: info@znrfak.ni.ac.rs, www.znrfak.ni.ac.rs

Број	03-175/5
У Нишу	27. 09. 2024. .

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 члана 101. став 1. тачка 14. Статута Факултета заштите на раду у Нишу бр. 03-187/3 од 4. 4. 2018. године, 03-478/5 од 27. 12. 2018. године, 03-77/3 од 1. 3. 2022. године, 03-135/3 од 5. 6. 2023. године, 03-174/3 од 6. 9. 2023. године и 03-265/5 од 27. 12. 2023. године, Савет Факултета заштите на раду у Нишу, на седници одржаној дана 27. 9. 2024. године, донео је

П Р А В И Л Н И К
о безбедности информационо - комуникационог система Факултета заштите на раду у Нишу

I. УВОДНЕ ОДРЕДБЕ

Члан 1.

Правилник о безбедности информационо - комуникационог система Факултета заштите на раду 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 Факултета заштите на раду у Нишу (у даљем тексту: Факултет).

Члан 2.

Мере прописане овим Правилником односе се на све организационе јединице Факултета 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:
   - електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
   - 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;
   - 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;
   - 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) *Компромитујућа електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

14) *Криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини нечитљивим неовлашћеним лицима;
15) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
16) Backup је резервна копија података;
17) Download је трансфер података са централног рачунара или web презентације на локални рачунар;
18) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
19) Freeware је бесплатан софтвер;
20) Opensource је софтвер чији је изворни код јавно доступан;
21) 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;
22) USB или флеш меморија је спољашњи медијум за складиштење података;
23) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;
24) 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.

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 самостални стручнотехнички сарадник за рад у рачунском центру Факултета (у даљем тексту: руководилац послова ИКТ система), у сарадњи са техничарем одржавања информационих система и технологија (у даљем тексту: администратор ИКТ система).

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 ИКТ система, обавештава декана Факултета, који у складу са прописима обавештава надлежне органе Факултета у циљу решавања насталог безбедоносног инцидента.

Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Нерегистровани 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 (дозволе, шифре, лозинке и сл.) 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.

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.

Одговорност коришћења ИКТ система Факултета

Члан 10.

ИКТ системом Факултета управљају запослени у складу са важећом систематизацијом радних места.

Руководилац послова ИКТ система је дужан да сваког новозапосленог корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Факултета, да га упозна са правилима коришћења ресурса ИКТ система Факултета.

Члан 11.

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

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

Члан 12.

У случају промене послова, односно надлежности запосленог, администратор ИКТ система 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 13.

О престанку радног односа или радног ангажовања, као и промени радног места, овлашћени запослени у служби за правне, кадровске и административне послове у сарадњи са непосредним руководиоцем обавештава администратора ИКТ система, ради укидања, односно измене приступних привилегија тог запосленог.

Члан 14.

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

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 15.

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 16.

За вођење евиденције о информационим добрима одговоран је руководилац послова ИКТ система.

Члан 17.

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.

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

Члан 18.

Подаци који се налазе у ИКТ систему Факултета доступни су само овлашћеним лицима и заштићени су у складу са одредбама посебних законских прописа који уређују ову материју.

Заштита носача података

Члан 19.

Руководилац послова ИКТ система успоставља 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 ИКТ система, у сврху архивирања.

За вођење евиденције носача на којима су снимљени подаци одговоран је руководилац послова ИКТ система и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

Члан 20.

У случају транспорта медија са подацима, руководилац послова ИКТ система 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 21.

Администратор ИКТ система је дужан да пре предаје уређаја који садржи осетљиве податке 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.

Ограничење приступа подацима и средствима за обраду података

Члан 22.

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 23.

Корисник може да користи само свој кориснички налог који је добио од администратора ИКТ система 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 24.

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) Обезбеди сигурност података у складу са важећим прописима;
7) Приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
8) Не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
9) Користи интернет и електронску пошту Факултета у складу са прописаним процедурама;

10) Прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
11) Прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
12) 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;
13) Не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер који је инсталиран од стране надлежне службе.

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

Члан 25.

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 26.

Право приступа за управљање базом података имају само запослени који су овлашћени за обављање ових послова од стране декана Факултета. Руководилац послова ИКТ система обезбеђује приступ, у складу са одлуком декана Факултета.

Члан 27.

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 28.

Кориснички налог додељује администратор, на основу захтева надлежног руководиоца, 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 надлежног руководиоца.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 29.

Кориснички налог се састоји од корисничког имена и лозинке. Корисничко име се

креира 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

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 ИКТ система.

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 30.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 31.

Руководилац послова ИКТ система је задужен за формирање листе критичних ресурса за које се захтева посебна криптозаштита.

За приступ ресурсима из става 1. овог члана, посебном одлуком се дефинише 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 32.

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.

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

Члан 33.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само надлежним лицима које одреди декан Факултета, односно руководилац послова ИКТ система.

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 ИКТ система 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 треба да буде видљиво обележена, уз поштовање прописаних мера противпожарне заштите.

Прозори и врата на овој просторији морају увек бити затворени.

Сервери и активна мрежна опрема (switch, modem, router, firewall) највишег приоритета, морају стално бити прикључени на уређаје за непрекидно напајање – UPS.

Члан 34.

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 ИКТ система. У случају изношења опреме ради селидбе или сервисирања, неопходно је одобрење декана Факултета, односно руководиоца послова ИКТ система, који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења декана Факултета, односно руководиоца послова ИКТ система, 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.

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

Члан 35.

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 декану Факултета, односно руководиоцу послова ИКТ система одговарајуће мере.

Члан 36.

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 37.

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.

Заштита података и средства за обраду података од злонамерног софтвера

Члан 38.

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 ИКТ система је одговоран за испуњење услова и контролу из става 2. овог члана.

Члан 39.

Запослени су дужни да редовно врше скенирање рачунара на вирусе, као и чишћење медија антивирусним софтвером. Запослени су дужни да пријаве присуство малициозног софтвера руководиоцу послова ИКТ система.

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 40.

У циљу заштите, односно превенције упада у ИКТ систем Факултета са интернета, руководилац послова ИКТ система и администратор ИКТ система су дужни да одржавају систем за спречавање упада, применом свих прописаних мера заштите.

Члан 41.

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.

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 администратору ИКТ система, односно руководиоцу послова ИКТ система.

Члан 42.

За дефинисање политике филтрирања садржаја на интернету одговоран је руководилац послова ИКТ система.

Није дозвољено:

1) Нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
2) Намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
3) Гледање видео садржаја са илегалних стриминг сервиса на рачунарима и приступ WEB страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета;
4) Нелегално преузимање (download) материјала заштићених ауторским правима;
5) Коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
6) Недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета;
7) 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.

Заштита од губитка података

Члан 43.

Базе података обавезно се архивирају на мрежне дискове за ову намену једном дневно уз употребу специјализованог софтвера.

Остали критични фајлови-документи се архивирају на преносиве медије (CDROM, DVD, ектерни хард диск) најмање два пута годишње.

Дневно копирање-архивирање врши се за сваки радни дан у седмици, од 23 часова сваког радног дана.

Годишње копирање-архивирање врши се последње радне недеље у години и последње радне недеље пре колективног одмора.

Члан 44.

Сваки примерак преносног информатичког медија са копијама-архивама, мора бити означен врстом (дневна, недељна, месечна, годишња) и датумом израде копије - архиве.

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

Члан 45.

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

Обезбеђивање интегритета софтвера и оперативних система

Члан 46.

Инсталацију и подешавање софтвера који захтева лиценцирање може да врши само администратор ИКТ система, 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 47.

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.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 48.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, администратор ИКТ система је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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

Члан 49.

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.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 50.

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 rack орману.

Члан 51.

Запослени на пословима ИКТ система су дужни да стално врше контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалних неправилности.

Члан 52.

Бежична мрежа коју могу да користе посетиоци објеката у надлежности Факултета, мора бити одвојена од дела 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.

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

Члан 53.

Размена података са академским и комерцијалним интернет провајдерима врши се у складу са потписаним уговорима о пословно техничкој сарањи.

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

Члан 54.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена на Факултету, дефинише се одговарајућим уговором.

Запослени на пословима ИКТ система је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

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

Члан 55.

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.

Заштита средстава оператора ИКТ система Факултета која су доступна пружаоцима услуга

Члан 56.

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.

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

Члан 57.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени је дужан да одмах обавести руководиоца послова ИКТ система.

По пријему пријаве руководилац послова ИКТ система је дужан да одмах обавести декана и предузме мере у циљу заштите ресурса ИКТ система Факултета.

Члан 58.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Сл. гласник РС“, бр. 11/2020), руководилац послова ИКТ система, је дужан да поред декана обавести и надлежни орган дефинисан овом Уредбом.

Члан 59.

Руководилац послова ИКТ система 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.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 60.

У случају ванредних околности, које могу да доведу до измештања ИКТ система Факултета из зграде Факултета, руководилац послова ИКТ система, 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 ИКТ система.

Делове ИКТ система Факултета који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди декан Факултета и руководилац послова ИКТ система. 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 61.

За проверу ИКТ система Факултета одговоран је руководилац послова ИКТ система.

IV. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 62.

За праћење примене овог Правилника задужен је руководилац послова ИКТ система и запослени на пословима ИКТ система Факултета.

Непоштовање одредби овог Правилника повлачи дисциплинску одговорност запосленог - корисника информатичких ресурса Факултета.

Члан 63.

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 ИКТ система 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 64.

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

Члан 65.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли и интернет страници Факултета.

ПРЕДСЕДНИК САВЕТА
ФАКУЛТЕТА ЗАШТИТЕ НА РАДУ У НИШУ

Др Иван Мијаиловић, ванр. проф.