УНИВЕРЗИТЕТ У БЕОГРАДУ
ФИЛОЗОФСКИ ФАКУЛТЕТ
05/2-7 бр. 1646/1
У Београду, 07.10.24. године

На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/2016, 94/2017 и 77/2019), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС", бр. 94/2016) и члана 202. Статута Универзитета у Београду – Филозофског факултета, Декан Факултета доноси следећи

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНОГ СИСТЕМА

I Уводне одредбе

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности и Уредбом о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начин провере информационо-комуникационих система од посебног значаја и садржај извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС", бр. 94/2016), утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационих система (даље: ИКТ систем) Универзитета у Београду — Филозофског факултета (даље: Факултет).

Члан 2.

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

За праћење примене овог правилника обавезује се Рачунско документациони центар Факултета (даље: РДЦ).

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

1. информационо-комуникациони систем (ИКТ систем) је техполошко-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 подтачке (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. *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

14. *информациона добра* обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонента, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

15. VPN (Virtual Private Network)-је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;

16. MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;

17. Backup је резервна копија података;

18. Download је трансфер података са централног рачунара или web презентације на локални рачунар;

19. UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;

20. Freeware је бесплатан софтвер;

21. Opensource је софтвер отвореног кода;

22. 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;

23. USB или флеш меморија је спољашњи медијум за складиштење података;

24. CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;

25. DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

II Мере заштите

Члан 4.

Мерама заштите ИКТ система се обезбеђује 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 безбедности у оквиру Факултета

Члан 5.

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 Факултета надлежан је РДЦ.

Члан 6.

Под пословима из области безбедности утврђују се:

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

У случају инцидента РДЦ обавештава декана, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системам буду оспособљена за посао који раде и разумеју своју одговорност

Члан 7.

ИКТ системом управља РДЦ у складу са важећом систематизацијом радних места.

РДЦ 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, као и да води евиденцију о изјавама новозапослених — корисника да су упознати са правилима коришћења ИКТ ресурса.

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

3. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Члан 8.

У случају промене послова, односно надлежности корисника-запосленог, РДЦ ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида на захтев корисника или службе Факултета која се бави кадровским пословима.

О престанку радпог односа или радног ангажовања, као и промени радног места Одсек за правне, кадровске и административне послове је дужан да обавести РДЦ ради укидања, односно измене приступних привилегија тог запосленог-корисника.

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

4. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 9.

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, 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 и сл.

Евиденцију о информационим добрима Факултета води РДЦ у сарадњи са Одсеком за материјално финансијско пословање у папирној или електронској форми.

Предмет заштите су:

- хардверске и софтверске компоненте ИКТ система;
- подаци који се обрађују или чувају на компонентама ИКТ система;
- кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система.

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

Члан 10.

Подаци који се налазе у ИКТ систему представљају тајну, у складу са одредбама: Закона о слободном приступу информацијама од јавног значаја ("Сл. гласник РС", бр. 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021), Закона о заштити података о личности („Сл, Гласник РС“, бр. 87/18), Закона о тајности података („Сл.

Гласник РС", 104/2009), као и Уредбе о начину и поступку означавања тајности података, односно докумената („Сл. Гласник РС“ бр. 8/2011).

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).

6. Заштита носача података

Члан 11.

РДЦ ће успоставити организацију приступа и рада са подацима, тако да:

- подаци и документи могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени,
- подаци и документи могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених — корисника.

Евиденцију носача на којима су снимљени подаци, води РДЦ и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

7. Ограничење приступа подацима и средствима за обраду података

Члан 12.

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.

Запослени - 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.

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

Запослени-корисник дужан је да поштује и следећа правила безбедног и примереног коришћегьа ресурса ИКТ система, и то да:

1. користи информатичке ресурсе искључиво у пословне и академске сврхе;
2. прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво 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. обезбеди сигурност података у складу са важећим прописима;
8. приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
9. на радној станици не сме да складишти садржај који не служи у пословне сврхе;
10. израђује заштитне копије (backup) података у складу са прописаним процедурама;

11. користи интернет и електронску пошту у складу са прописаним процедурама;
12. прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
13. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
14. 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;
15. не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 13.

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

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

Администраторски налог могу да користе само овлашћени запослени РДЦ-а.

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

Кориснички налог додељује запослени на пословима ИКТ, на основу захтева непосредног руководиоца и то тек након уноса података о запосленом-кориснику у софтвер, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Запослени на пословима ИКТ води евиденцију о корисничким налозима, проверава њихово коришћење, мењају права приступа и укидају корисничке налоге на основу захтева надлежног руководиоца организационе јединице Факултета.

9. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 14.

Кориснички налог се састоји од корисничког имена и лозинке.

Лозинка мора да садржи препоручено 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 запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Кориснички налог може да се се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр. лична карта са чипом и уписаним сертификатом) уколико је предвиђено описом рада.

Пријављивање у ИКТ систем Факултета се врши убацивањем медија са електронским сертификатом у читач картица.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 15.

Приступ ресурсима ИКТ система Факултета не захтева посебну криптозаштиту.

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.

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

Члан 16.

Простор у коме се налазе сервери, мрежна или комуникациопа опрсма ИКТ система, организује са као административна зона.

Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом, и физичким надзором.

Простор мора да буде обезбеђен од пожара и других елемснтарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор).

Евиденцију о уласку у ову зону води РДЦ.

12. Заштипш од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем

Члан 17.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само запосленима на пословима ИКТ.

Осим запосленима на пословима ИКТ, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, уз присуство надлежног лица, руководиоца РДЦ или запослених.

Просторија мора бити видљиво обележена а у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима.

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.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети од стране запослених.

У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење или реверс који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, потребно је сачинити записник-реверс у коме се наводи назив и тип опреме, назив сервисера, име и презиме овлашћсног лица сервисера.

13. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 18.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим, планирају, односно предлажу декану Факултета одговарајуће мере.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије, може се вршити па начин који не омета оперативни рад запослених-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.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери и подаци који су намењени тестирању и развоју.

При тестирању софтвера је потребно обезбедити неометано функционисање ИКТ система. Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера, на начин који може да заустави нормално функционисање ИКТ система.

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

Члан 19.

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 нелиценцирапог софтвера и сл.

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

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

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.

Ризик од евентуалног губитка података приликом чишћења медија од вируса сноси доносилац медија.

У циљу заштите, односно упада у ИКТ систем Факултета са интернета, РДЦ је дужан да одржава систем за спречавање упада.

Корисницима који су прикључсни на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему РДЦ може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се

запослени-корисник прикључује на интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши РДЦ.

Приликом коришћења интернета треба избегавати сумњиве веб странице, с обзиром на то 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 РДЦ-у.

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" веб страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

Недозвољена употреба интернета обухвата:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских" или других софтверских производа који нису лиценцирани на одговарајући начин;
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивпих програма па интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимање (download) података велике "тежине" које проузрокује "загушење" на мрежи;
- преузимање (download) материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже може се одузети право приступа.

15. Заштита од губитка података

Члан 20.

Базе података обавезно се архивирају на препосиве медије (CDROM, DVD, USB, „strimer" трака, екстерни хард диск), дневно, недељно, месечно и годишње, за потребе обнове базе података у складу са потребама и карактером података.

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

Подаци о запосленима-корисницима, архивирају се најмање једном месечно.

Дневно копирање-архивирање врши се за сваки радни дан у седмици, након радног времена запослених.

Недељно копирање-архивирање врши се последњег радног дана у недељи, након радног времена запослених.

Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно, након радног времена запослених.

Све актуелне копије-архиве се износе са факултета и чувају ван зграде.

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

Члан 21.

О активностима администратора и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др).

17. Обезбеђивање интегритета софтвера и оперативних система

Члан 22.

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 може да врши само РДЦ, 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.

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.

18. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 23.

РДЦ по потреби, у односу на актуелне ризике 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, РДЦ је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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

Члан 24.

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

20. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 25.

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

РДЦ је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

21. Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 26.

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.

РДЦ је задужен и за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

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

Члан 27.

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

23. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 28.

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.

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

24. Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга

Члан 29.

Факултет нема склопљен уговор са трећим лицима за пружање услуга информационе безбедности.

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

Члан 30.

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

По пријему озбиљније пријаве о претњи по безбедност РДЦ је дужан да одмах обавести декана Факултета и предузме мере у циљу заштите ресурса ИКТ система.

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), РДЦ је дужан да поред декана Факултета обавести и надлежни орган дефинисан овом уредбом.

26. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 31.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Факултета, РДЦ је дужан да у најкраћем року пренесе делове ИКТ система (или обезбеди функционисање редудантних компоненти на резервној локацији уколико постоје) неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

III. Измена Правилнника о безбедности

Члан 32.

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 бсзбедност, РДЦ је дужан да обавести декана Факултета, како би он могао да приступи измени овог Правилника, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IV. Провера ИКТ система

Члан 33.

Проверу ИКТ система врши РДЦ.

Провера се врши тако што се:

1. проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на која се врши упућивање, са прописаним условима, односно проверава да ли су правилником адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;
2. проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама интервјуа, симулације, посматрања, увида у предвиђене евиденције и другу документацију;
3. врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

О извршеној провери сачињава се извештај, који се може доставити декану Факултета уколико за тим постоји потреба.

V. Садржај извештаја о провери ИКТ система

Члан 34.

РДЦ спроводи безбедносну анализу система једном годишње, на чега спроводи мере заштите.

VI. Прелазне и завршне одредбе

Члан 35.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли и сајту Факултета.

Декан Факултета

проф. др Данијел Синани