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 и садржају извештаја о провери информационо-комуникационих система од посебног значаја („Службени гласник РС", број 94/2016) и члана 38. Статута Универзитета у Београду – Факултета за специјалну едукацију и рехабилитацију, Деканка Универзитета у Београду – Факултета за специјалну едукацију и рехабилитацију дана 7. 8. 2025. године доноси следећи

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

I Уводне одредбе

Члан 1.

Овим Правилником, у складу са Законом о информационој безбедности и Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери информационо-комуникационих система од посебног значаја („Службени гласник РС", број 94/2016), утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационих система (даље: ИКТ систем) Универзитета у Београду – Факултета за специјалну едукацију и рехабилитацију (даље: Факултет).

Изрази употребљени у овом Правилнику у граматичком мушком роду, подразумевају природни мушки и женски род лица на које се односе.

Члан 2.

Мере прописане овим правилником односе се 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 Одсек за ИТ послове.

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

1. информационо-комуникациони систем (ИКТ систем) је технолошко-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 података коришћењем рачунарског програма;
   - 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;
   - организациону структуру путем које се управља ИКТ системом;
2. имовина – све што за одређену организацију има вредност;
3. администраторско овлашћење је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;
4. корисник – свака особа (запослени или спољни партнер Факултета) који има приступ ИКТ систму, сходно својој улози у пословним процесима;

5. кориснички налог јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно овлашћења корисника);
6. администраторски налог јесте јединствени налог који омогућава приступ и администрацију информатичких ресурса, као и уношење и измену свих осталих корисничких налога;
7. 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;
8. трећа страна (third party) – особа или тело признато да је независно од страна ангажовнаих на проблему о којем се ради;
9. тајност је својство које значи да податак није доступан неовлашћеним лицима;
10. интегритет значи очуваност изворног садржаја и комплетности податка;
11. расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
12. 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;
13. непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
14. ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
15. 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;
16. инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
17. мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
18. тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
19. безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
20. информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
21. VPN (Virtual Private Network) је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
22. MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
23. backup је резервна копија података;
24. download је трансфер података са централног рачунара или web локације на локални рачунар;
25. UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
26. freeware је бесплатан софтвер;
27. opensource је софтвер отвореног кода;

28. 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;
29. контрола (control) – средства за управљање ризиком, укључујући политике, процедуре, смернице, праксе или организациону структуру која може бити административне, техничке, руководне или законске природе; овај термин се користи и као синоним за заштиту или противмеру;
30. догађај у вези са сигурношћу информација (information security event) – свака идентификована појава у систему, услузи или стању на мрежи која указује на могуће нарушавање политике сигурности или на отказ заштите, или ситуација која претходно није била позната и која се може односити на сигурност;
31. инцидент нарушавања сигурности информација (information security incident) – састоји се од појединачног догађаја или низа нежељених/неочекиваних догађаја нарушавања сигурсноти информација за које постоје знатни изгледи да компромитују пословне активности и да запрете сигурности информација;
32. претња (threat) – потенцијални узрок неког нежељеног инцидента, који може довести до штете на систему или у организацији;
33. рањивост (vulnerability) – слабост неке имовине или групе добара коју нека претња може да искористи;
34. ризик (risk) – комбинација вероватноће неког догађаја и његових (негативних) последица;
35. USB или флеш меморија је спољашњи медијум за складиштење података;
36. CD-ROM (Compact disk – read only memory) се користи као медијум за снимање података;
37. DVD је оптички диск високог капацитета који се користи као медијум за складиштење података.

Уређаји из става 1 овог члана подразумевају уређаје у власништву Факултета, као и личне уређаје запослених који се користе за приступ ИКТ ресурсима Факултета.

Члан 4.

Информационо-комуникациони систем Факултета представља уређен скуп који чине:

- методе, процеси и операције за прикупљање, чување, обраду, преношење и дистрибуцију података у оквиру Факултета;
- опрема која се у те сврхе користи;
- рачунарска мрежа са свим просторима који се користе за складиштење података;
- људски ресурси који тај ИКТ систем користе.

II Мере заштите

Члан 5.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају обављање делатности Факултета.

1. Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедности у оквиру Факултета

Члан 6.

За управљање безбедношћу ИКТ система одговоран је декан Факултета који именује лице задужено за информациону безбедност (у даљем тексту: ЛИЗБ).

ЛИЗБ је, по правилу, руководилац Одсека за ИТ послове, осим ако околности не налажу другачије.

ЛЗИБ је одговорно за планирање, спровођење и надзор мера информационе безбедности, као и за координацију активности у случају инцидената.

Сви запослени, сарадници и студенти који користе ИКТ ресурсе Факултета дужни су да поштују прописане мере и процедуре информационе безбедности.

Члан 7.

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 Одсек за ИТ послове и његов руководилац, именован за ЛИЗБ.

ЛЗИБ има следеће надлежности:

- израда и ажурирање документације о информационој безбедности;
- спровођење процене ризика и предлагање мера за њихово ублажавање;
- надзор над применом мера заштите;
- организација обука и подизање свести корисника;
- извештавање руководства о стању информационе безбедности;
- сарадња са надлежним органима и спољним ревизорима.

Члан 8.

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

Сви корисници ИКТ система имају обавезу да:

- користе ресурсе у складу са својим овлашћењима;
- чувају поверљивост приступних података (лозинки, токена и сл.);
- одмах пријаве сваки уочени безбедносни инцидент или сумњу на злоупотребу;
- присуствују обукама и придржавају се интерних политика и процедура.

Члан 9.

Под пословима из области безбедности сматрају се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност;
- послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности;
- послови онемогућавања, односно спречавања неовлашћене или (не)намерне 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 систсму, у складу са прописима.

У случају инцидента Одсек за ИТ послове обавештава декана који, у складу са прописима, обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 10.

Факултет не додељује мобилне уређаје запосленима.

Приликом приступа ИКТ ресурсима Факултета, лични уређаји запослених се користе у складу са одредбама овог Правилника.

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

Члан 11.

ИКТ системом управља Одсек за ИТ послове у складу са важећом систематизацијом радних места.

Одсек за ИТ послове је дужан да сваког новозапосленог-корисника ИКТ система упозна са одговорностима и правилима коришћења ресурса ИКТ система Факултета, као и да води евиденцију о изјавама новозапослених–корисника да су упознати са правилима коришћења ИКТ ресурса.
Обуке за коришћење ИКТ ресурса и у сврху информисања корисника организују се најмање једном годишње, а по потреби и чешће.
Свако коришћење ИКТ ресурса Факултета од стране запосленог-корисника 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 код оператора ИКТ система

Члан 12.

Корисници ИКТ система су запослени и студенти који се корисничким налогом и шифром пријављују на рачунарску мрежу Факултета.
Сваки запослени-корисник ИКТ система је одговоран за безбедност ресурса система које користи ради обављања послова из своје надлежности.
У случају промене послова, односно надлежности корисника – запосленог, Одсек за ИТ послове ће извршити промену права у коришћењу које је запослени-корисник 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 службе Факултета која се бави кадровским пословима.
О престанку радног односа или радног ангажовања, као и промени радног места Служба за правне, кадровске, административне послове и послове јавних набавки је дужна да обавести Одсек за ИТ послове ради укидања, односно измене приступних привилегија тог запосленог-корисника.
Након престанка радног ангажовања на Факултету не престаје обавеза чувања поверљивих података/информација у складу са законом коју ту област уређује.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 13.

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 Одсек за ИТ послове у сарадњи са Финансијско рачуноводственом службом 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.

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

Члан 14.

Поверљивост, интегритет и расположивост информација мора бити заштићена, без обзира на облик у којем се подаци појављују и система на којем се подаци обрађују, прослеђују или похрањују.

Члан 15.

Руководство и власници информација одговорни су за класификацију информационих ресурса, у складу са системом класификације информација наведеним у Правилнику.

Сви запослени носе свој део одговорности у процесима заштите информација, како би се обезбедило да информациони ресурси Факултета имају одговарајући ниво заштите у складу са Правилником.

Сви запослени биће упућени на који начин, на основу информационе категорије, треба да управљају информацијама. Корисници су дужни користити информације на начин примерен класификацији. Обавеза чувања тајности примењује се и након престанка радног или другог уговорног односа.

Члан 16.

Информације имају различите степене осетљивости и критичности.

Подаци се класификују с обзиром на њихову поверљивост, поузданост и расположивост.

Рачунарски системи, рачунарска мрежа и друге компоненте информационог система које садрже информације, морају бити заштићени примерено класификационом разреду информације који се на датом систему налазе.

Ако одређени систем садржи податке који припадају различитим нивоима сигурности онда мора бити третиран сходно захтевима највишег класификационог разреда присутног на реченом систему.

Спољни сарадници који долазе у додир са поверљивим подацима обавезују се на чување тајности писаном изјавом или на други примерен начин.

Члан 17.

У зависности од осетљивости и критичности информације, врше се њихова класификација и груписање у неку од следећих категорија:

- јавне;
- интерне (само за интерну употребу);
- поверљиве;
- строго поверљиве.

Члан 18.

Јавне информације, у папирном или електронском облику, су оне информације које нису поверљиве и могу бити објављене без импликације предузећа.

У ову категорију спадају документа која чине генералне и јавно доступне информације о самој компанији и као таква се посебно не обележавају. Доступна су свим запосленима у компанији као и свим ентитетима ван компаније. Компанија нема директну контролу над дистрибуцијом истих.

Могу бити јавно истакнута су на огласној табли компаније.

Пре него што се информација учини јавно доступном (нпр. објављивањем на web сите-у) потребно све улазне податке проверити и верификовати, утврдити да је њихово објављивање у складу са законском регулативом, и коначно добити одобрење за објављивање.

Примери:

- политика сигурности информационих система, политика квалитета, изјава о применљивости;
- информације широко доступне у јавном домену, укључујући јавно доступне информације на сајту Факултета;
- рекламни материјал у виду брошура, флајера;
- рекламни материјал у електронском облику;
- финансијски извештаји које захтевају државни органи.

Члан 19.

Интерне информације су оне информације чија се употреба ограничава на примену унутар организације, тј. унутар организације се не захтева поверљивост, али су заштићене од

приступа споља. Могу бити у папирном, електронском или усменом облику, оријентисане ка корисницима или ка предузећу.
Обележавање ових средстава је дефинисано локацијом и доступна су свим запосленима у компанији. Као таква не носе посебну ознаку. Компанија има директну контролу приступа истима која је дефинисана правима приступа организованих по организационим јединицама унутар саме компаније као и Уговором о раду сваког појединца.
Примери

- деловодници, књига поште;
- вести и писма обавештења интерно;
- вести и писма обавештења ка корисницима/добављачима;
- стандардне оперативне процедуре;
- упутства за управљање информацијама о корисницима;
- тренинг материјали;
- интерни извештаји са састанка;
- понуде/предрачуни/поруџбенице;
- фактуре ка корисницима /од добављача;
- уговори и споразуми о поверљивости са корисницима/добављачима;
- контакт информације;
- знање (интелектуална својина) и Business Intelligence.

Члан 20.

Поверљиве информације су информације чија је доступност ограничена на овлашћене запослене унутар организације и контролисане. Могу бити у електронском или папирном облику, оријентисане ка корисницима или ка предузећу.
Средства која припадају категорији поверљиво, тамо где је то применљиво, означена су речју: ПОВЕРЉИВО. Уколико су у питању папирна документа, реч ПОВЕРЉИВО је обавезно истакнута на регистраторима или фасциклама у којима се поменута документа чувају. Приступ тако обележеним средствима је ограничен на приступ кључу којим се иста закључавају. Такође, сва остала средства која нису документа или информације а која се сматрају ПОВЕРЉИВИМ се такође одлажу у посебан простор намењен за чување поверљивих средстава који је закључан. Простор који се закључава је обавезно означен речју ПОВЕРЉИВО.
Информације сврстане у ову категорију су од великог значаја за пословање организације, а њихово одавање или губитак интегритета може значајно угрозити пословање фирме, конкурентност и углед. Губитак расположивости такође може имати велики утицај на пословање.
Примери

- backup fajlovi;
- електронске трансмисије корисника;
- поверљиви пословни подаци корисника;
- плате и други лични подаци о запосленима.

Члан 21.

Строго поверљиве информације су информације чија је доступност строго ограничена на овлашћене запослене унутар организације и најстроже контролисана. Могу бити у електронском или папирном облику, оријентисане ка корисницима или ка предузећу.
Информације које подлежу важећој законској регулативи, у смислу да је организација у законској обавези очувања тајност и интегритета, сврстане су у ову категорију.
Строго поверљиви подаци о клијентима су оне информације које су, током продуктивних процеса предузећа, добијене од клијената у било којој форми за процесирање, а чију тајност Факултет гарантује.
Строго поверљиви подаци предузећа су оне информације, прикупљене и коришћене од стране предузећа за потребе пословања, бележења и испуњавање захтева клијената, као и

управљања финансијама предузећа, чији евентуални губитак би на најозбиљнији Строго поверљиви подаци предузећа су оне информације, прикупљене и коришћене од стране предузећа за потребе пословања, бележења и испуњавање захтева клијената, као и управљања финансијама предузећа, чији евентуални губитак би на најозбиљнији начин утицао на пословање. Лични подаци о запосленима такође сврстани су у ову категорију. Приступ овим информацијама строго је ограничен.
Када више нису потребне поверљиве и строго поверљиве информације се морају уништити на безбедан начин. Папирне поверљиве информације морају бити физички шредоване уз коришћење минимум CrossCut шредера.
Примери

- лозинке;
- интерни финансијски и рачуноводствени извештаји;
- строго поверљиви пословни подаци клијената;
- планови пословања предузећа.

Члан 22.

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).

7. Заштита носача података

Члан 23.

Одсек за ИТ послове ће успоставити организацију приступа и рада са подацима, тако да:

- подаци и документи могу да се сниме (архивирају) 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 Одсек за ИТ послове и ти медији морају бити прописно обележени и одложени на место на којем ће бити заштићени од неовлашћеног приступа.

Члан 24.

Медији који садрже поверљиве информације (меморије, екстерни дискови, папирна документација...) не бацају се, већ се уништавају методом која осигурава да се трајно и поуздано уништи садржај спаљивањем, уситњавањем, уништавањем медија.
Уколико се застарела и расходована рачунарска опрема даје на коришћење трећој страни, обавезно је уништавање података са дискова посебним програмима који неповратно бришу садржаје.
Оператор ИКТ система одређује за које податке, у складу са шемом класификације података, треба водити евиденцију о коришћењу носача података и предузетим поступцима у вези са заштитом података и носача података.

8. Ограничење приступа подацима и средствима за обраду података

Члан 25.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има.

Запослени који има администраторски налог има право 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 властитог корисничког налога.
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 коришћења 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.

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

Члан 26.

Право приступа ИКТ система Факултета имају само запослени-корисници који имају администраторске или корисничке налоге.
Администраторски налог је налог којем 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 у Одсеку за ИТ послове, распоређени на пословима/радним задацима администратора.
Кориснички налог додељује администратор, 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.
Администратори воде евиденцију о корисничким налозима, проверавају њихово коришћење, на основу захтева надлежног руководиоца организационе јединице Факултета мењају права приступа и обезбеђују механизам за укидање права приступа у случају промене радног места, престанка радног односа и, по потреби, у другим случајевима.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 27.

Кориснички налог се састоји од корисничког имена и лозинке.
Када је одобрен приступ систему/апликацији, корисник ће бити обавештен о својој (уколико је применљиво) привременој лозинци на безбедан начин.
Привремена лозинка мора бити промењена након првог логовања, а где је применљиво, систем ће аутоматски од корисника тражити да промени лозинку.
Лозинка мора да задовољи минималне захтеве комплексности дефинисане у оквиру доменске политике Факултета.
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.
Запослени-корисник је дужан да мења лозинку периодично (најмање једном у шест месеци, а по потреби и чешће).
Иста лозинка се не сме понављати у временском периоду од годину дана.
Запослени-корисник се обавезује да корисничко име и лозинку не сме давати другим лицима на коришћење.
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.
Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 28.

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.

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

Члан 29.

Ресурси ИКТ система Факултета налазе се у посебној канцеларији која се закључава, односно у обезбеђеном, закључаном rack-у од којег кључ има одговорна особа.

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

Члан 30.

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.
На важним тачкама на Факултету налазе се противпожарни апарати чиме се обезбеђује правовремена реакција у случају пожара.
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 наводе назив и тип опреме, назив сервисера, име и презиме овлашћеног лица сервисера.
Осим запосленима на пословима ИКТ, приступ ресурсима ИКТ система могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, уз присуство надлежног лица, руководиоца Одсека за ИТ послове или запослених.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 31.

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 на 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.
Оператор ИКТ система континуирано надзире и проверава функционисање средстава за обраду података и предвиђа будуће промене које могу утицати на безбедност ИКТ система и, у складу са тим, планира одговарајуће мере.
Оператор ИКТ система међусобно раздваја окружења за развој, тестирање и оперативан рад да би се смањили ризици од неовлашћеног приступа или промена у радном окружењу.
Одсек за ИТ послове је надлежан за дефинисање оперативних процедура, управљање променама и за континуирани надзор система.

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

Члан 32.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.
За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм.
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, Одсек за ИТ послове је дужан да одржава систем за спречавање упада.
Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему Одсек за ИТ послове 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 Одсек за ИТ послове.
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 Одсеку за ИТ послове .
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 опструктивних програма па интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја;
- 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 видеостриминг 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.

16. Заштита од губитка података

Члан 33.

Базе података обавезно се архивирају на преносивим медијима (CDROM, DVD, USB, екстерни хард диск, различити cloud сервиси) 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.

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

Члан 34.

Одсек за ИТ послове, обезбеђује заштиту средстава за записивање и записа од неовлашћеног приступа и промене.
У циљу обезбеђивања поузданости записа, времена у свим подсистемима ИКТ система морају бити синхронизована међусобно, као и са референтним тачним временом.
О активностима администратора и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др) и исти се редовно преиспитују у циљу заштите.

Оператор ИКТ система треба да осигура постојање података о времену када су одређени log-ови урађени.
Брисање историје log-ова није дозовољено.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 35.

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 Одсек за ИТ послове, 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.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 36.

Одсек за ИТ послове 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, Одсек за ИТ послове је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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

Члан 37.

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.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 38.

Мрежна опрема (switch, router, firewall) се мора налазити у закључаном „rack“ орману.
Одсек за ИТ послове је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

22. Безбедност података који се преносе унутар оператора икт система, као и између оператора ИКТ система и лица ван оператора ИКТ система

Члан 39.

За потребе преноса података унутар ИКТ система факултета, као и у комуникацији са спољним странама, Одсек за ИТ послове је дужан да успостави процедуре и контроле које обезбеђују безбедан пренос података.
Ове процедуре морају да укључују:

- заштиту комуникације од прислушкивања, модификовања, погрешног усмеравања и уништења, применом криптографских техника (нпр. TLS/SSL за веб апликације, VPN за удаљени приступ);
- коришћење дигиталних потписа за осетљиве документе и поруке;
- примена антивирусних и анти-malware алата ради откривања и спречавања злонамерног софтвера;

- успостављање споразума о преносу података и поверљивости (NDA) са спољним партнерима, који садрже јасне клаузуле о безбедности комуникације;
- у случају преноса личних података, обрада мора бити усклађена са Законом о заштити података о личности, уз претходну процену ризика и примену одговарајућих техничких и организационих мера.

Када се пренос података врши између оператора ИКТ система и лица ван оператора ИКТ система, закључују се споразуми о преносу података и споразуми о поверљивости или неоткривању који садрже одредбе о безбедности преноса података.
У случају из става 3. овог члана, за пренос података о личности испуњавају се услови предвиђени законом којим се уређује заштита податка о личности.

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

Члан 40.

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.
Одсек за ИТ послове је задужен и за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

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

Члан 41.

За потребе тестирања ИКТ система, односно делова система, Одсек за ИТ послове може да користи податке који нису осетљиви, уз примену одговарајућих мера заштите, чувања и контроле.
Уколико је за тестирање неопходно коришћење поверљивих информација или личних података, њихова обрада мора бити усклађена са важећим прописима и уз одговарајућа овлашћења, уз примену анонимизације или псеудонимизације података, где год је то могуће.

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

Члан 42.

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.
Одсек за ИТ послове је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог Правилника којима су такве активности дефинисане.
Одсек за ИТ послове је дужан да, у оквиру својих процедура, дефинише ниво доступности, врсту информација и средстава којима могу да приступе пружаоци услуга, као и начине приступа и надзор над тим приступом.
У том смислу, потребно је:

- идентификовати средства и информације којима пружаоци услуга могу приступити, уз јасну класификацију по нивоу осетљивости;
- успоставити процедуре безбедности које регулишу приступ пружалаца услуга информацијама и средствима унутар организације;
- закључити споразуме са пружаоцима услуга који садрже одредбе о безбедности, поверљивости и начину коришћења доступних ресурса, у складу са важећим прописима и техничким стандардима;

– обезбедити да пружаоци услуга обављају поверене активности у складу са актом о безбедности ИКТ система факултета, као и другим релевантним актима који уређују безбедност информационог система.

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

Члан 43.

Факултет може да склопи уговор са трећим лицима за пружање услуга информационе безбедности.

Члан 44.

У циљу очувања уговореног нивоа информационе безбедности и квалитета пружених услуга, Одсек за ИТ послове је дужан да успостави механизме надзора над радом пружалаца услуга, у складу са условима дефинисаним уговором.

У том смислу, потребно је:

– именовати одговорно лице за праћење реализације пружања услуга, као и за контролу испуњености безбедносних захтева;
– успоставити процедуре за редовну проверу и евиденцију нивоа услуга;
– обезбедити да пружалац услуга поступа у складу са уговореним обавезама, техничким стандардима и прописима који регулишу безбедност информационог система.

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

Члан 45.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-кориспик је дужан да одмах обавести Одсек за ИТ послове.

По пријему озбиљније пријаве о претњи по безбедност Одсек за ИТ послове 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), Одсек за ИТ послове је дужан да поред декана Факултета обавести и надлежни орган дефинисан овом уредбом.

Члан 46.

Безбедносни инцидент је сваки догађај који:

– угрожава поверљивост, интегритет или доступност информација или ИКТ система;
– указује на покушај или успешно нарушавање безбедности (нпр. вирус, неовлашћени приступ, крађа података, DoS/DDoS напад, фишинг, цурење података).

Инцидент се без одлагања пријављује одговорном лицу у Одсеку за ИТ послове.

Пријава треба да садржи:

– опис инцидента;
– време и начин уочавања;
– потенцијални утицај;
– предузете мере (ако их има).

Пријава се врши путем службене е-поште, телефона или, уколико постоји, преко унутрашњег система за пријаву инцидената.

Члан 47.

Обавезе запослених и пружалаца услуга:

– обавезна пријава сваког уоченог инцидента, претње или слабости у систему;
– сарадња са одговорним лицем током истраге и отклањања последица;

- чување релевантних информација и доказа (логови, скриншоти, поруке);
- поштовање процедура за реаговање и обавештавање, укључујући поверљивост података;
- учествовање у обукама и симулацијама за реаговање на инциденте.

Члан 48.

Превенција и реаговање на безбедносне инциденте подразумева дужност Одсека за ИТ послове да утврди процедуре за превенцију и реаговање на безбедносне инциденте, укључујући дефинисање одговорних лица и плана поступања у случају опасности или настанка инцидента.

Поменуте процедуре треба да обухвате:

- именовање лица задуженог за пријем и обраду пријава безбедносних слабости, претњи и инцидената;
- обавезу свих запослених и пружалаца услуга да без одлагања пријаве уочене безбедносне слабости, претње и инциденте;
- вођење евиденције о свим активностима у вези са инцидентима;
- размену информација о безбедносним слабостима, инцидентима и претњама;
- именовање лица задуженог за обавештавање надлежних органа у случају инцидената који могу имати значајан утицај на информациону безбедност;
- успостављање регулативе за идентификацију, прикупљање и чување информација које могу послужити као доказ у дисциплинском, прекршајном или кривичном поступку.

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 49.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Факултета, Одсек за ИТ послове 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 Правилника о безбедности

Члан 50.

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, Одсек за ИТ послове 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 51.

Проверу ИКТ система врши Одсек за ИТ послове, најмање једном годишње, а по потреби и чешће.

Провера се врши тако што се:

- 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;

- 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;
- 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 52.

Одсек за ИТ послове спроводи безбедносну анализу система једном годишње, на основу чега израђује извештај и спроводи мере заштите. Извештај о провери ИКТ система садржи:

1. назив оператора ИКТ система 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 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;
8. оцена укупног нивоа информационе безбедности;
9. предлог евентуалних корективних мера;
10. потпис одговорног лица које је спровело проверу ИКТ система.

На основу поднетог Извештаја планирају се будућа побољшања система.

VI. Прелазне и завршне одредбе

Члан 53.

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

Деканка Факултета

Проф. др Сања Ђоковић