На основу члана 63. Закона о високом образовању („Службени гласник РС“, бр. 88/2017, 27/18 др.закон, 73/18, 67/19, 6/20 др.закони, 11/21 аутентично тумачење, 67/21, 67/21 др.закон и 76/23), члана 14. Статута Факултета спорта и физичког васпитања у Нишу, Савет Факултета спорта и физичког васпитања у Нишу, на седници одржаној дана 28.11.2023. године, донео је следећу

ОДЛУКУ

ДОНОСИ СЕ Одлука о усвајању Правилника о безбедности информационо-комуникационог система Факултета спорта и физичког васпитања у Нишу.

Правилник о безбедности информационо-комуникационог система Факултета спорта и физичког васпитања у Нишу је саставни део ове одлуке.

Образложење

Наставно- научно веће Факултета спорта и физичког васпитања у Нишу, на седници одржаној дана 06.10.2023.године, разматрало је Правилник о безбедности информационо-комуникационог система Факултета и исти упутило Савету Факултета. Након разматрања Предлога, Савет Факултета спорта и физичког васпитања у Нишу, донео је одлуку као у диспозитиву.

Одлуку доставити: Одељењу за рачунарско-информационе послове, општој служби и писарници Факултета спорта и физичког васпитања у Нишу.

САВЕТ ФАКУЛТЕТА СПОРТА И ФИЗИЧКОГ ВАСПИТАЊА У НИШУ

Број: 04- 1850/6

У Нишу, 28.11.2023. године

Председник Савета

Проф. др Саша Миленковић

На основу члана 63. Закона о високом образовању („Службени гласник РС" бр. 88/2017, 27/2018 - други закон, 73/2018, 67/2019, 6/2020 др. закони, 11/2021 аутентично тумачење, 67/2021, 67/2021 др. закон, 76/23), а у вези примене Закона о информационој безбедности („Сл. гласник РС", број 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), члана 14. Статута Факултета спорта и физичког васпитања у Нишу, Савет Факултета спорта и физичког васпитања у Нишу, на својој седници одржаној дана 28.11.2023.године донео је следећи

ПРАВИЛНИК

О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ФАКУЛТЕТА СПОРТА И ФИЗИЧКОГ ВАСПИТАЊА У НИШУ

Уводне одредбе

Члан 1.

Правилником о безбедности информационо-комуникационог система Факултета спорта и физичког васпитања у Нишу (у даљем тексту: Правилник), у складу са Законом о информационој безбедности и Уредбом 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), 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 ИКТ система на Факултету спорта и физичког васпитања у Нишу, (у даљем тексту: Факултет).

Члан 2.

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

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

За праћење примене овог Правилника надлежни су запослени у Одељењу за рачунарско-информационе послове (у даљем тексту: Одељење).

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 воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКТ системом;
- све типове системског и апликативног софтвера и софтверске развојне алате.

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; инцидент је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система
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. ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
14. компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
15. криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
16. криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
17. криптографски производ је софтвер или уређај путем кога се врши криптозаштита;
18. криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
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;

информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, технички и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично

21. Download је трансфер података са централног рачунара или web презентације на локални рачунар;
22. UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
23. Freeware је бесплатан софтвер;
24. Opensource софтвер отвореног кода;
25. 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;
26. USB или флеш меморија је спољашњи медијум за складиштење података;
27. CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;
28. DVD је оптички диск високог капацитета који се користи као медијум за складиштење података.

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.

Утврђени послови и одговорност запослених којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

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 обављање послова из области целокупног ИКТ система Факултета, надлежани су запослени у Одељењу.

Кршење безбедносних процедура у ИКТ систему запослени-корисник је дужан да пријави запосленима Одељења, а они су дужни да предузму одговарајуће мере.

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 средстава без овлашћења и без евиденције о томе,

- бекап података неопходних за обављање делатности,
- спречавање изношења тајних података изван ИКТ система Факулетета,
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу,
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

Члан 7.

У случају промене послова, односно надлежности корисника-запосленог, лице задужено за послове одржавања ИКТ система ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу налога декана Факултета.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида, декан Факултета је обавезан да именује другог запосленог као корисника корисничког налога и да о томе обавести лице које је задужено за одржавање ИКТ система и технологија и новог корисника налога.

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

Безбедност рада на даљину и употреба мобилних уређаја

Члан 8.

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.

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја који су у власништву Факултета и који су подешени од стране запослених из Одељења, да приступају деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Запосленом-кориснику, забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима.

Приватни уређаји са којих ће се приступити ресурсима ИКТ система морају бити подешени - сертификовани од стране запослених Одељења, и могу се користити само за обављање послова у надлежности запосленог-корисника.

Запослени Одељења су дужни да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава,ураде backup података који се налазе у мобилном уређају, а потом их обришу са уређаја и по повратку из сервиса поновно врате податке у мобилни уређај.

Размена електронске поште

Члан 9.

Размена електронске поште на Факултету дозвољена је искључиво преко система за размену електронске поште и докумената.

Систем за размену електронске поште не сме да се користи или дистрибуцију нежељених порука.

Електронске поруке или други електронски подаци, који покушавају да сакрију идентитет пошиљаоца или да представе пошиљаоца као неког другог, нису дозвољени.

Члан 10.

Забрањена је употреба службене адресе електронске поште за размену порука:

- чији је садржај увредљив, клеветнички или застрашујући према било коме, као и поруке које су погрдне за било ког појединца или групу;
- које својим садржајем дискриминишу по било ком основу;
- којима се открива пословна тајна Факултета или пословног партнера, те лични подаци корисника услуга Факултета који могу да нанесу штету Факултету било које врсте;
- које служе за политичку или другу пропаганду;
- које својим садржајем ометају запослене у раду и онемогућавају редовну размену пословних садржаја („тзв. ланчане поруке“ и сл).

Члан 11.

Нежељена пошта се смешта у карантин. Корисник се обавештава о порукама које су смештене у карантин и омогућава му се приступ карантину.

Није дозвољено слање електронских порука без наслова или порука већих од прописане величине. О свакој промени у коришћењу система за размену електронске поште корисник се обавештава електронским путем.

Обезбеђење да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност

Члан 12.

ИКТ системом управљају запослени Одељења, а користе запослени према својим радним обавезама и додељеним овлашћењима.

Сваки новозапослени - корисник ИКТ ресурса треба да се упозна са одговорностима и правилима коришћења ИКТ ресурса Факултета.

Свако коришћење ИКТ ресурса Факултета од стане запосленог-корисника 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 код оператора ИКТ система

Члан 13.

У случају промене послова, односно надлежности корисника-запосленог, запослени Одељења 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.

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

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 14.

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 информационом систему, укључујући све елетронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, кофигурацију хардверских компонената, техничку и корисничку документацију и сл.

Предмет заштите су: хардверске и софтверске компоненете ИКТ система, подаци који се не обрађују или чувају на компонентама ИКТ система, кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система.

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

Члан 15.

Избор и ниво примене мера заштите података се заснива на процени ризика, потреби за превенцијом ризика и отклањању последица ризика који се остварио, укључујући све врсте ванредних околности.

Заштита носача података

Члан 16.

Ангажовани запослени Одељења Факултета 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-корисници којима је то право обезбеђено,

- подаци и документи могу да се сниме на друге носаче (екстерни хард диск, USB, SC, DVD), само од стране овлашћених запослених- корисника. Евиденцију носача на којима су снимљени подаци, воде запослени Одељења и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

Ограничење приступа подацима и средствима за обраду података

Члан 17.

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 кривичној и дисциплинској одговорности.

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

- користи информатичке ресурсе искључиво у пословне сврхе;
- прихвати да су сви подаци који се складиште, преносе или процесуирају у оквиру информатичких ресурса власништво Факултета и да могу бити предмет надгледања и прегледања од законом овлашћених лица;
- поступа са поверљивим подацима у складу са законским прописима, а посебно приликом копирања и преноса података;
- безбедно чува све лозинке сагласно утврђеним правилима;
- захтев за инсталацију софтвера или хардвера подноси запосленом у Одељењу;
- обезбеди сигурност падатака у складу са важећим прописима;
- приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
- не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
- на радној станици не сме да складишти садржај који не служи у пословне сврхе;
- израђује заштитне копије (backup) података у складу са прописаним процедурама;
- користи интернет и електронску пошту Факултета у складу са прописаним процедурама;

- прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
- прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
- 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;
- не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 18.

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 радници Одељења.

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/којих се врши аутентификација- провера идентитета и ауторизација- провера права приступа, односно права коршћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налог додељује администратор, у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева надлежног руководица.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 19.

Кориснички налог састоји се од корисничког имена и лозинке.

Лозинка мора да садржи:

- број карактера лозинке мора бити од 8
- најмање једно велико слово
- најмање један специјални знак („#$%&/!+ и сл.)
- најмање један број

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 креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр.лична карта са чипом и уписаним сертификатом).

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 20.

Запослени - корисници користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама.

Запослени Одељења 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.

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

Члан 21.

Рачунарска опрема од виталног значаја за Факултет (мрежно чвориште, мрежна опрема, сервери) се налази у просторији Одељења и њој могу приступити само запослени Одељења и налази се под сталним видео надзором.

Трећа лица могу имати приступ овој опреми само у циљу инсталације и сервисирања, по одобрењу декана, а уз присуство радника Одељења.

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

Члан 22.

Сервери и активна мрежна опрема морају стално бити прикључени на уређаје за непрекидно напајење UPS.

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.

У случају опасности (пожар, временска непогода...) ИКТ опрема се може изнети и без одобрења декана.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 23.

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 одговарајуће мере.

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

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије, може се извршити 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.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 24.

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, имајлом, зараженим преносним медијима (USB меморија, CD итд), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефиниција.

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.

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

Приликом коришћења интернета треба избегавати сумљиве веб странице, с обзиром да то може проузроковати проблеме- неприметно исталирање шпијунских програма и сл.

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:

- самостално инсталирање и дистрибуција софтверских производа који нису лиценцирани на одговарајући начин,

- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет конекције,
- намерно ширење деструктивних и опструктивних програма на 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 материјала заштићених ауторским правима.

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

Заштита од губитка података

Члан 25.

Документи у електронском облику сматрају се службеним документима на исти начин као и документи у папирном облику па је сходно томе потребно осигурати њихово чување и приступ само овлашћеним особама.

Сви запослени су дужни да самостално праве и на безбедан начин чувају резервну копију података за које су задужени.

Податке који су од виталног значаја за Факултет архивира и чува администратор система, коме је додељена та обавеза.

За чување одређених података могу бити именовани различити администратори.

Израда резервних копија података о запосленима-корисницима се врши на дневном нивоу.

Факултет може да користи спољне сервисе (као што је хостовање система ван рачунарске мреже Факултета или извршавање апликација од виталног значаја) и у том случају фирма/институција који обавља хостовање тог сервиса или администрирање апликације, дужна је да обезбеди правилан рад сервиса, његову безбедност као и прављење резервних копија.

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

Члан 26.

Неопходно је обезбедити евидентирање свих активности корисника, администратора, оператера, порука о процесима, грешкама, промени конфигурације система и сл.

Средстава за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене. Записи се редовно преиспитују у циљу заштите.

За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужени су запослени Одељења.

Обезбеђивање интегритета софтвера и оперативних система

Члан 27.

У ИКТ систему може да се инстлира само софтвер за који постоји важећа лиценца, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера могу да врше само запослени Одељења. 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.

Заштита од злопупотребе техничких безбедоносних слабости ИКТ система

Члан 28.

У циљу правовременог и ефикасног реаговања на објављене и уочене слабе тачке софтвера предузимају се мере за контролу заштићености средстава за обраду, чување и предају информација.

Контрола заштићености се врши на следећи начин:

-периодичном анализом заштићености помоћу скенирања безбедносним алатима/софтверима,

- мониторингом заштићености,

-анализом конфигурационих фајлова средстава за обраду, чување и пренос информација.

Подаци о слабим тачкама софтврерских решења редовно се обнављају са сајтова произвођача конкретних решења. Уочене слабе тачке средстава за обраду, чување и пренос информација отклањају се помоћу нових верзија софтвера (update“) или применом препоручених конфигурација које нуде произвођачи софтвера.

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

Члан 29.

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

Заштиту података у комуникационим мрежама укључујући уређаје и водове

Члан 30.

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

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

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

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

Члан 31.

Размена података са државним органима и институцијама (нпр. Министарством просвете, Министарством финансија, Трезором, Пореском управом, Централним регистром социјалног и здравственог осигурања, Управом за јавне набавке и сличним институцијама), правним и физичким лицима се врше у складу са важећим прописима и унапред дефинисаним и потписаним уговорима.

Испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 32.

О успостављању новог ИКТ система, односно увођења нових делова и изменама постојећих делова ИКТ система запослени Одељења воде документацију. Документација мора да садржи описе свих процедура које се односе на безбедност ИКТ система.

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

Члан 33.

За потребе тестирања ИКТ система односно делова система запослени Одељења могу користити податке који нису осетљиви, које штите, чувају и контролишу на одговарајући начин.

Заштита средстава операторта ИКТ система која су доступна пружаоцима услуга

Члан 34.

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.

Запослени Одељења су одговорни за контролу приступа и надзор над извршењем уговорних обавеза.

Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са прижаоцем услуга

Члан 35.

Запослени Одељења су одговорни за надзор над поштовањем уговорених обавеза од стране трећих лица - пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система.

У случају непоштовања уговорених обавеза запослени Одељења су дужни да одмах обавесте секретара и декана Факултета.

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

Члан 36.

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

По пријему пријаве запослени Одељења су дужни да одмах обавесте декана Факултета и предузму мере у циљу заштите ресурса ИКТ система.

Запослени Одељења воде евиденцију о свим инцидентима, као и пријавама инцидента.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 37.

У случају ванредних околности, које могу да доведу до измештања ИКТ система, запослени Одељења су дужни да у најкраћем року понесу делове ИКТ система неопходних за функционисање у ванредној ситуацији на резервну локацију.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште на резервну локацију који одреди декан Факултета. Складиштење делова ИКТ система који нису неопходни, се врши тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води.

Прелазне и завршне одредбе

Члан 38.

Даном ступања на снагу овог Правилника престаје да важи Правилник о ИТ безбедности Факултета спорта и физичког васпитања у Нишу (бр. 04-532/3 од 19.03.2014.године).

Члан 39.

Овај Правилник ступа на снагу осам дана по објављивању на интернет страници Факултета.

САВЕТ ФАКУЛТЕТА СПОРТА И ФИЗИЧКОГ ВАСПИТАЊА У НИШУ

Број: 04-1850/6

У Нишу, 28.112023. године

ПРЕДСЕДНИК САВЕТА

Проф. др Саша Миленковић