На основу Закона о информационој безбедности („Службени гласник РС“, број 6/16, 94/17, 77/19) и одредби Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС“, број 94/16), члана 65 Закона о високом образовању („Сл. гласник РС“ бр. 88/17, 27/18 – др. закон, 73/18, 67/19, 6/20, 11/21, 67/21, 76/23) и 29. Статута Факултета деканка факултета дана 31. октобра 2024. године доноси следећи

ПРАВИЛНИК
О УПРАВЉАЊУ ИНФОРМАЦИЈАМА И БЕЗБЕДНОСТИ ИНФОРМАЦИОНОГ СИСТЕМА ТЕХНОЛОШКО-МЕТАЛУРШКОГ ФАКУЛТЕТА

Члан 1.

Универзитет у Београду, Технолошко-металуршки факултет (у даљем тексту: Факултет) води прописану евиденцију у папирном и електронском облику, у складу са Законом о високом образовању.

Сви видови прикупљања, обраде, објављивања и коришћења података спроводе се у складу са Законом којим се уређује заштита података о личности и Законом о високом образовању.

Члан 2.

Факултет води: матичну књигу студената, записнике о полагању испита, евиденцију о издатим дипломама и додацима диплома и евиденцију о запосленима.

Члан 3.

У оквиру јединственог информационог система просвете, који успоставља и води ресорно министарство, све акредитоване високошколске установе уносе и ажурирају податке, у оквиру одговарајућег регистра, у електронском облику.

Члан 4.

У складу са Законом о информационој безбедности и Уредбом о ближем садржају акта о безбедности информационог система од посебног значаја, овим Правилником се утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационог система (у даљем тексту: ИС), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИС Факултета.

Члан 5.

Информациона добра Факултета су сви ресурси који садрже пословне информације Факултета, односно сви ресурси путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИС, укључујући све електронске записе, рачунарску опрему, базе података, пословне апликације и сл.

Члан 6.

Информациони систем Факултета представља уређен скуп који чине:

- методи, процеси и операције за прикупљање, чување, обраду, преношење и дистрибуцију података у оквиру зграде Факултета, као и ван Факултета у складу са склопљеним уговорима са трећим лицима,
- опрема која се у те сврхе користи,
- рачунарска мрежа, са свим просторима који се користе за складиштење података,
- људски ресурси који користе ИС факултета.

Члан 7.

Под пословима из области безбедности ИС сматрају се:

- послови заштите информационих добара, односно средстава и 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 ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИС Факултета, као и приступ, измена или коришћење средстава без овлашћења,
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу,
- обавештавање надлежних органа о инцидентима у ИС, у складу са прописима.

Члан 8.

У случају промене радног места, односно надлежности корисника – запосленог, овлашћени администратор ће извршити промену права у коришћењу ИС, које је корисник - запослени имао у складу са описом радних задатака.

Члан 9.

У случају престанка радног односа корисника - запосленог, кориснички налог се укида.

Корисник ИС ресурса, коме је престао радни однос по било ком основу, не сме да открива податке који су од значаја за информациону безбедност ИС, а у складу са Уговором о чувању поверљивих подататка.

Члан 10.

Право приступа ИС Факултета имају само корисници који имају администраторске и корисничке налоге.

Администраторским налогом је омогућен приступ и администрација свих ресурса ИС и отварање нових и измена постојећих налога. Могу да га користе само запослени распоређени на послове и радне задатке администратора у служби за одржавање рачунарске мреже Факултета, односно трећа лица којима Факултет уговором повери послове администрације уз потписивање Уговора о чувању поверљивих подататка.

Кориснички налог је налог који садржи корисничко име и лозинку. Кориснички налог додељује администратор, на основу захтева надлежног руководиоца службе или шефа катедре. На основу послова и радних задатака запосленог - корисника, администратор одређује права приступа 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 руководиоца у организационим јединицима Факултета.

Члан 11.

Кориснички налог се састоји од корисничког имена и лозинке.

Корисник се обавезује да корисничко име и лозинку не сме давати другим лицима на коришћење.

Члан 12.

Запослени у служби за одржавање рачунарске мреже Факултета су задужени за безбедност и функционисање ИС као и да сваког новозапосленог корисника ИС ресурса упознају са одговорностима и правилима коришћења ИС ресурса Факултета, да га обуче за коришћење ресурса ИС које служба администрира и доделе му одговарајућа права у складу са описом радних задатака.

Члан 13.

Обавезе запослених у Служби за опште послове:

– уносе и ажурирају електронску базу података са свим подацима везаним за запослене: општи подаци, промене статуса, избор у звање, промене функција и сл.

Обавезе запослених у Служби за наставно-студентска питања:

- уносе и ажурирају електронску базе података са свим подацима везаним за наставу и студенте: општи подаци, ангажовања наставника, испитни рокови, пријемни испити, упис на студије, дипломирање и сл.,
- администраторима ИС достављају информације о променама статуса студената, ради одређивања одговарајућих права студената за коришћење ИС.

Обавезе запослених у Служби за одржавање рачунарске мреже Факултета:

- обезбеђују континуирано функционисање целокупног информационог система,
- израђују резервне копије које обухватају системске информације, апликације и податке који су неопходни за функционисање система у случају наступања последица изазваних ванредним околностима и чување једне копије на удаљеној локацији, која ће бити изнајмљена у ту сврху, у складу са финансијским могућностима Факултета.

Члан 14.

Информације о запосленима и студентима, као и информације везане за функционисање ИС Факултета морају бити одговарајуће заштићене. У том циљу запослени су дужни да предузму све техничке мере које су потребне да би се информације заштитиле од губитка, уништења, недопуштеног приступа, промене, објављивања и сваке друге злоупотребе.

Није дозвољено поверљиве информације о запосленима и студентима, као и поверљиве податке везано за функционисање ИС Факултета копирати на приватне носаче података и износити са Факултета, као ни слати их путем интернета мејлом или копирати на удаљене приватне ресурсе.

Сваку активност везану за кршење безбедности система: интернет напад, откривена лозинка, нестанак медија са поверљивим подацима и сл. запослени - корисник је дужан да пријави запосленима у Служби за одржавање рачунарске мреже Факултета, а о инцидентима већих размера потребно је обавестити и декана Факултета.

Члан 15.

Предмет заштите ИС Факултета обухвата:

- хардверске и софтверске компоненте ИС,
- интегритет података који се обрађују или чувају на компонентама ИС,
- корисничке налоге и друге податке о корисницима информатичких ресурса ИС.

Члан 16.

Мере заштите ИС Факултета се односе на:

1) успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру ИС Факултета,
2) постизање безбедности рада на даљину,
3) обезбеђивање потребних средстава у складу са финансијским могућностима Факултета како би се омогућила контрола приступа рачунарској мрежи и надгледање саобраћаја као и безбедност ИС од напада преко интернета,
4) обезбеђивање да лица која користе ИС односно управљају ИС Факултета буду оспособљена за посао који раде и разумеју своју одговорност,
5) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених на Факултету,
6) идентификовање информационих добара и одређивање одговорности за њихову заштиту,
7) класификовање података тако да ниво њихове заштите одговара значају података,
8) заштиту носача података,
9) ограничење приступа подацима и средствима за обраду података,
10) одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИС и услугама које ИС пружа,
11) утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију,
12) физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИС и обрађују подаци у ИС Факултета,
13) заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИС,
14) обезбеђивање исправног и безбедног функционисања средстава за обраду података,
15) заштиту података и средства за обраду података од злонамерног софтвера,
16) заштиту од губитка података,
17) обезбеђење чувања ажурне резервне копије података и барем једне копије на удаљеној локацији, у складу са финансијским могућностима Факултета,
18) чување података о догађајима који могу бити од значаја за безбедност ИС Факултета,
19) обезбеђивање да активности на ревизији ИС имају што мањи утицај на функционисање система,
20) безбедност података који се преносе унутар оператора ИС система, као и између оператора ИС система и лица ван оператора ИС система,
21) заштиту средстава оператора ИС система која су доступна пружаоцима услуга,
22) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИС, инцидентима и претњама,
23) мере које обезбеђују континуитет обављања посла у ванредним околностима.

Члан 17.

Медији који садрже поверљиве информације (flash 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 кориштење трећој страни, обавезно је уништавање података са дискова посебним програмима који неповратно бришу садржаје.

Члан 18.

Мере прописане овим актом се односе на све организационе јединице информационог система Факултета, на све запослене - кориснике информатичких ресурса.

Одредбе овог Правилника примењују се и на трећа лица којима Факултет на основу уговора повери израду, управљање и чување информационих добара, као и послове администрације ИС.

Члан 19.

Мерама заштите ИС Факултета обезбеђује се превенција од настанка инцидената, односно превенција и

минимализација штете од инцидената који угрожавају вршење делатности и обављање надлежности.

Члан 20.

Овај Правилник ступа на снагу у року од 8 дана од објављивања на интернет страни Факултета.

Д Е К А Н К А

Проф. Др Мирјана Кијевчанин