УНИВЕРЗИТЕТ У БЕОГРАДУ - ГЕОГРАФСКИ ФАКУЛТЕТ
Број: 349
Датум: 15.03.2023. године

На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16, 94/17, 77/19), Уредбе о ближем садржају акта о безбедности информационокомуникационих система од посебног значаја („Службени гласник РС“, број 94/16), члана 35. Статута Географског факултета, доносим

П РАВ И Л Н И К
О УПРАВЉАЊУ ИНФОРМАЦИЈАМА И БЕЗБЕДНОСТИ ИНФОРМАЦИОНОГ СИСТЕМА

Члан 1.

Овим Правилником утврђују се 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.

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

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

Члан 3.

Мерама заштите ИС Факултета обезбеђује се превенција од настанка инцидената, односно превенција и минимализација штете од инцидената који угрожавају обављање делатности Факултета.

Члан 4.

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

Члан 5.

Информациони систем Факултета представља уређен скуп који чине:

-методи, 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 користи за складиштење података,
- људски ресурси који тај ИС користе.

Члан 6.

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

Члан 7.

Корисници ИС су запослени и студенти који се са корисничким налогом и шифром пријављују на рачунарску мрежу Факултета.

У случају промене радног места запосленог, овлашћени администратор извршиће промену права у коришћењу ИС, које је запослени имао у складу са описом радних задатака.

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

Члан 8.

У случају престанка радног односа 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.

Члан 9.

Право приступа ИС-у Факултета имају само запослени, односно корисници који имају администраторске и корисничке налоге.

Администраторски налогом је омогућен приступ и администрација свих ресурса ИС-а, отварање нових и измена постојећих налога и могу да га користе само запослени распоређени на послове и радне задатке администратора.

Кориснички налог је налог који садржи корисничко име и лозинку. Кориснички налог додељује администратор, на основу захтева надлежног руководиоца. На основу послова и радних задатака запосленог - корисника, администратор одређује право и обим приступа ИС-у Факултета.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења право приступа и укида корисничке налоге, на основу захтева руководиоца организационе јединице Факултета.

Члан 10.

Кориснички налог се састоји од корисничког имена и лозинке.

Лозинка мора да задовољи минималне захтеве комплексности, дефинисане у оквиру доменске политике Факултета.

Ако запослени-корисник посумња да је друго лице открило његову лозинку, дужан је да исту одмах измени.

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.

Запослени-корисник дужан је да мења лозинку најмање једном у 6 (шест) месеци.

Члан 11.

Запослени на Факултету, администратор информационих система и технологија, у обавези је да сваког новозапосленог упозна са одговорностима и правилима коришћења ИС и да га обучи за коришћење ресурса ИС.

Члан 12.

Обавезе запослених у организационим јединицама Факултета јесу да уносе и ажурирају одговарајућу електронску базу података за коју имају право приступа.

Обавеза администратора информационих система и технологија јесте да обезбеди континуирано функционисање целокупног информационог система.

Члан 13.

Информације о запосленима и студентима, као и информације везане за функционисање ИС Факултета морају бити заштићене. Запослени су дужни да предузму све техничке мере 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 везане за функционисање ИС Факултета копирати на приватне носаче података и износити са Факултета, нити их слати 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 слично, запослени је дужан да пријави администратору информационих система и технологија или непосредном руководиоцу. О инцидентима већих размера администратор обавештава декана Факултета.

Члан 14.

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 15.

Мере заштите ИС Факултета се односе на:

- успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру ИС Факултета,
- постизање безбедности рада на даљину и употребе мобилних уређаја,
- обезбеђивање потребних средстава како би се омогућила контрола приступа рачунарској мрежи и надгледање саобраћаја као и безбедност ИС од напада преко интернета,

- обезбеђивање да лица која користе ИС односно управљају ИС Факултета буду оспособљена за посао који раде и разумеју своју одговорност,
- заштиту од ризика који настају при промени посла или престанка радног ангажовања лица запослених на Факултету,
- идентификовање информационих добара и одређивање одговорности за њихову заштиту,
- класификовање података тако да ниво њихове заштите одговара значају података,
- заштиту носача података,
- ограничење приступа подацима и средствима за обраду података,
- одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИС и услугама које ИС пружа,
- физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИС и обрађују подаци у ИС Факултета,
- заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИС,
- обезбеђивање исправног и безбедног функционисања средстава за обраду података,
- заштиту података и средства за обраду података од злонамерног софтвера,
- заштиту од губитка података,
- обезбеђење чувања ажурне резервне копије података, и барем једне копије на удаљеној локацији,
- чување података о догађајима који могу бити од значаја за безбедност ИС Факултета,
- обезбеђивање интегритета софтвера и оперативних система,
- обезбеђивање да активности на ревизији ИС имају што мањи утицај на функционисање система,
- безбедност података који се преносе унутар оператора ИС, као и између оператора ИС и лица ван оператора ИС,
- заштиту средстава оператора ИС која су доступна пружаоцима услуга,
- превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИС, инцидентима и претњама,
- мере које обезбеђују континуитет обављања посла у ванредним околностима.

Члан 16.

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 ИС, подлеже дисциплинској одговорности.

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

1) користи информатичке ресурсе искључиво у пословне сврхе;

2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Факултета и да, у случају потребе, могу бити предмет надзора;

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) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8) обезбеди сигурност података у складу са важећим прописима;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (backup) података у складу са прописаним процедурама;
13) користи интернет и електронску пошту у Факултета у складу са прописаним процедурама;
14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и слично) обављају у утврђено време;
15) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
16) не користи ИС и информатичке ресурсе Факултета за нарушавање права интелектуалне својине других лица;
16) прихвати да технике сигурности (анти вирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.)
спречавају потенцијалне претње ИС систему;
17) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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 коришћење трећој страни, обавезно је уништавање података са дискова посебним програмима који неповратно бришу садржаје.

Члан 18.

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

ДЕКАН

_____

проф. др Велимир Шећеров