

На основу чл. 50. алинеја 15. Статута Факултета, Савет ПМФ-а на седници одржаној дана 29.12.2017. године, доноси

**О Д Л У К У**  
о усвајању Правилника о управљању информацијама и безбедности  
информационог система ПМФ-а

I

**УСВАЈА СЕ** Правилник о управљању информацијама и безбедности информационог система ПМФ-а.

II

Правилник о управљању информацијама и безбедности информационог система ПМФ-а, саставни је део ове одлуке.

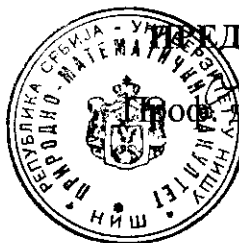
III

Одлуку доставити: декану, продекану за координацију међународних пројеката, секретару, Служби за опште и правне послове и архиви Секретаријата Факултета.

**САВЕТ ПРИРОДНО-МАТЕМАТИЧКОГ ФАКУЛТЕТА У НИШУ**

Број: 1285 | 1 - 01

Датум: 29. 12. 2017.



**ПРЕДСЕДНИК САВЕТА**

Проф. др Мирослав Ћирић

На основу одредбе Закона о информационој безбедности („Службени гласник РС“, број 6/16) и одредби Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС“, број 94/16), Савет Природно-математичког факултета на седници одржаној дана 29.12.2017 године доноси

РЕПУБЛИКА СРБИЈА  
УНИВЕРЗИТЕТ У НИШУ  
ПРИРОДНО-МАТЕМАТИЧКИ  
ФАКУЛТЕТ

## ПРАВИЛНИК

Број: 1285/2-01 О УПРАВЉАЊУ ИНФОРМАЦИЈАМА И  
Датум: 29.12.2017 БЕЗБЕДНОСТИ ИНФОРМАЦИОНОГ СИСТЕМА ПМФ-а  
Н И Ш

### І Опште одредбе

#### Члан 1.

Високошколска установа 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.

Високошколска установа води: матичну књигу студената, евиденцију о издатим дипломама и додацима диплома, евиденцију о запосленима, евиденцију о признатим страним високошколским исправама ради наставка школовања и записник о полагању испита.

Ближе услове у погледу вођења, прикупљања, уноса, ажурирања, доступности података о којима се води евиденција, као и друга питања од значаја за вођење евиденција, прописује министар.

#### Члан 3.

У оквиру јединственог информационог система просвете, који успоставља и води 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 Природно-математичког факултета (у даљем тексту: Факултет).

#### **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 високошколске институције,
- опрема која се у те сврхе користи,
- рачунарска мрежа,
- људски ресурси који тај ИС користе.

### **II Безбедност ИС**

#### **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 и без евиденције о томе,
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу,
- обавештавање надлежних органа о инцидентима у ИС, у складу са прописима.

#### **Члан 8.**

Сваки запослени је дужан да потпише изјаву о заштити поверљивих података.

#### **Члан 9.**

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 10.**

У случају престанка радног односа корисника - запосленог, кориснички налог се укида. Корисник ИС ресурса, коме је престало радни однос по било ком основу, не сме да открива податке који су од значаја за информациону безбедност ИС.

### **III Администраторски и кориснички налог**

#### **Члан 11.**

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 и отварање нових и измена постојећих налога. 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 и то тек након уноса података о запосленом у базу ИС-а. На основу послова и радних задатака запосленог, 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 Службе за опште и правне послове, односно надлежног руководиоца у организационим јединицама Факултета.

### **IV Одговорности корисника за заштиту сопствених средстава за аутентификацију**

#### **Члан 12.**

Кориснички налог се састоји од корисничког имена и лозинке.

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

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. 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.

### **III Коришћење ИС-а**

#### **Члан 13.**

Стручна лица која су задужена за безбедност и функционисање ИС су дужна да сваког новозапосленог корисника ИС ресурса упозна са одговорностима и правилима коришћења ИС ресурса Факултета, да га обучи за коришћење ресурса ИС и додели му одговарајућа права у складу са описом радних задатака.

#### **Члан 14.**

Корисници ИС су сви запослени и сви студенти који се са корисничким налогом и шифром пријављују на рачунарску мрежу Факултета ради обављања послова или извођења наставе и тиме користе ресурсе ИС.

## **Члан 15.**

### **IV Обавезе запослених у Служби за опште и правне послове**

- унос и ажурирање електронске базе података са свим подацима везаним за запослене: општи подаци, промене статуса, избор у звање, промене функција и сл. и о томе обавештавају РЦ ради одређивања одговарајућих права запослених за коришћење ИС,
- контрола података.

### **V Обавезе запослених у Служби за наставу и студентска питања**

- унос и ажурирање електронске базе података са свим подацима везаним за наставу и студенте: општи подаци, ангажовања наставника, испитни рокови, пријемни испити, упис на студије, дипломирање и сл.,
- контрола података,
- РЦ-у достављају информације о променама статуса студената, ради одређивања одговарајућих права студената за коришћење ИС.

### **VI Обавезе запослених у Рачунарском центру**

- обезбеђује континуирано функционисање целокупног информационог система,
- израда резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима и чување једне копије на удаљеној локацији, која ће бити изнајмљена у ту сврху,
- тестира исправност резервних копија и процедуре за прављење заштитних копија.

### **VII Обавезе запослених везано за безбедност ИС Факултета**

## **Члан 16.**

Запослени – корисник се обавезује да своје приватне рачунаре или носаче података донесу на антивирусну проверу у Службу РЦ пре прикључивања у факултетску мрежу.

Није дозвољено поверљиве информације о запосленима и студентима, као и поверљиве податке везано за функционисање ИС Факултета копирати на приватне носаче података и износити из институције, као ни слати их путем интернета маилом или копирати на удаљене приватне ресурсе – cloud storage...

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 РЦ, а о инцидентима већих размера потребно је обавестити и декана Факултета.

### **VIII Предмет и мере заштите информационог система**

## **Члан 17.**

Предмет заштите ИС Факултета обухвата:

- хардверске и софтверске компоненте ИС,
- интегритет података који се обрађују или чувају на компонентама ИС,
- кориснички налози и други подаци о корисницима информатичких ресурса ИС.

### Члан 18.

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 и употребе мобилних уређаја,

3) обезбеђивање потребних средстава 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 средстава 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,

18) чување података о догађајима који могу бити од значаја за безбедност ИС Факултета,

19) обезбеђивање интегритета софтвера и оперативних система,

20) обезбеђивање да активности на ревизији ИС имају што мањи утицај на функционисање система,

21) безбедност података који се преносе унутар оператора ИС система, као и између оператора ИС система и лица ван оператора ИС система,

22) заштиту средстава оператора ИС система која су доступна пружаоцима услуга - , потписивање изјаве о заштити информација,

23) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИС, инцидентима и претњама,

24) мере које обезбеђују континуитет обављања посла у ванредним околностима.

## **IX Обавезе запослених везано за уништавање медија са подацима и расходоване опреме**

### **Члан 19.**

Медији који садрже поверљиве информације (flash меморије, екстерни дискови,...), 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 рачуарска опрема даје на кориштење трећој страни, обавезно је уништавање података са дискова посебним програмима који неповратно бришу садржаје.

## **X Завршне одредбе**

### **Члан 20.**

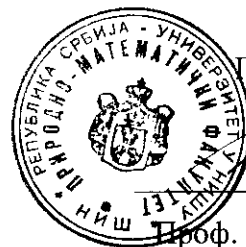
Мере прописане овим актом се односе на све организационе јединице ИС система Факултета, на све запослене-кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе ПМФа.

### **Члан 21.**

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

### **Члан 22.**

Правилник ступа на снагу даном доношења, а примењује се осмог дана од дана објављивања на огласној табли Факултета и на сајту Факултета.



ПРЕДСЕДНИК САВЕТА

Проф. Др Мирослав Ђирић