**РЕПУБЛИКА СРБИЈА**
**АКАДЕМИЈА ТЕХНИЧКО-УМЕТНИЧКИХ СТРУКОВНИХ СТУДИЈА БЕОГРАД**
**Београд, ул. Старине Новака бр. 24**
Број: 4330/1
Датум: 12.12.2023. године

На основу члана 65. Статута Академије техничко-уметничких струковних студија Београд (бр. 603/1 од 27.02.2023. године - пречишћен текст - у даљем тексту: Статут Академије), а у вези члана 8. став 1. Закона о информационој безбедности ("Сл. гласник РС", бр. 6/2016, 94/2017 и 77/2019 - у даљем тексту: Закон о информационој безбедности) и чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери информационо-комуникационог система од посебног значаја ("Сл. гласник РС", бр. 94/2016 - у даљем тексту: Уредба), Савет Академије техничко-уметничких струковних студија Београд (у даљем тексту: Савет Академије), на 29. седници одржаној дана 12.12.2023. године, доноси

# ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

## I. ОПШТЕ ОДРЕДБЕ

Члан 1.

Овим Правилником се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система од посебног значаја (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система Академије техничко-уметничких струковних студија Београд (у даљем тексту: Академија).

Члан 2.

Поједини термини који ће бити употребљени у овом Правилнику 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 алинеје 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) *оператор ИКТ система* је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3) *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;

4) *тајност* је својство које значи да податак није доступан неовлашћеним лицима;

5) *интегритет* значи очуваност изворног садржаја и комплетности податка;

6) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

7) *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;

8) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

9) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

10) *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;

11) *инцидент* је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система;

12) *мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

13) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

14) *орган власти* је државни орган, орган аутономне покрајине, орган јединице локалне самоуправе, организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења;

15) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

16) к*риптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

17) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

18) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку 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.

Члан 3.

Под пословима из области безбедности ИКТ система 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 ИКТ система Академије, као и приступа, измена или коришћења средстава без овлашћења и без евиденције о томе;
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу;
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

## II. МЕРЕ ЗАШТИТЕ ИКТ СИСТЕМА

Члан 4.

Академија одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се односе на:

1. успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система;
2. постизање безбедности рада на даљину и употребе мобилних уређаја;
3. обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност;
4. заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;
5. идентификовање информационих добара и одређивање одговорности за њихову заштиту;
6. класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком;

7. заштиту носача података;
8. ограничење приступа подацима и средствима за обраду података;
9. одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;
10. утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију;
11. предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности и интегритета података;
12. физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;
13. заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;
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. чување података о догађајима који могу бити од значаја за безбедност ИКТ система;
18. обезбеђивање интегритета софтвера и оперативних система;
19. заштиту од злоупотребе техничких безбедносних слабости ИКТ система;
20. обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система;
21. заштиту података у комуникационим мрежама укључујући уређаје и водове;
22. безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;
23. испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;
24. заштиту података који се користе за потребе тестирања ИКТ система односно делова система;
25. заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга;
26. одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;
27. превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама;
28. мере које обезбеђују континуитет обављања посла у ванредним околностима.

## 1. Успостављање организационе структуре са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

Члан 5.

Организациона структура са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу утврђена је:

- Правилником о организацији и систематизацији послова на Академији;
- Правилником о начину евидентирања, класификовања, архивирања и чувања архивске грађе и документарног материјала;
- Правилником о раду Академије;
- Уговором о раду.

Академија утврђује начин доделе овлашћења за приступ ИКТ систему, степен обуке и квалификацију запослених и других радно ангажованих лица која користе ИКТ систем (корисници), односно запослених и и других радно ангажованих лица која управљају

ИКТ системом (администратори), као и начин одобравања приступа ИКТ систему од стране руководиоца Одсека, односно непосредно надређеног лица.

Свако запослено и одговорно лице, у случају непоштовања одредби Закона и Уредбе који уређују информациону безбедност, сматраће се лично одговорним и сносиће последице у складу са законским, подзаконским актима и општим актима Академије.

## 2. Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 6.

Дозвољава се рад на даљину (уз посебну одлуку овлашћеног лица) и употреба мобилних уређаја од стране запослених, уколико је осигурана безбедност рада у случају обављања послова ван просторија Академије, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја.

Академија настоји да обезбеди VPN (виртуелни приватни тунел) од крајњег корисника до ИКТ система, у циљу обезбеђења безбедног рада на даљину.

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

Члан 7.

Право приступа ИКТ систему имају само запослена и друга радно ангажована лица која користе ИКТ систем (у даљем тексту: корисници) који имају корисничке налоге, односно запослена и друга радно ангажована лица која управљају ИКТ системом (у даљем тексту: администратори), који имају администраторске налоге.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, само са једним корисничким налогом, као и отварање нових и измена постојећих налога. Може га користити само запослени који је распоређен на послове и радне задатке администратора.

Кориснички налог је налог који садржи корисничко име и лозинку, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу којих се врши аутентификација, провера идентитета и ауторизација, провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог - корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и може да укида корисничке налоге на основу захтева руководиоца одсека који се налази у саставу Академије.

Члан 8.

Академија се стара да корисници, односно администратори имају адекватан степен образовања и способности, у складу са Правилником о организацији и систематизацији послова на Академији, као и свест о значају послова које обављају.

Њихове одговорности су одређене Уговором о раду, Уговором о радном ангажовању ван радног односа и општим актима Академије.

Сви корисници и администратори на Академији дужни су да примењују мере заштите безбедности прописане овим актом.

Корисници ИКТ система, односно администратори који управљају ИКТ системом дужни су да се континуирано обучавају у циљу унапређења техничког и

технолошког знања, на начин који одговара њиховом пословном ангажовању и радном месту. Ова лица су дужна да предузимају хитне и неодложне мере у случају постојања непосредне опасности за податке и документацију, у што краћем року.

У случају да било ко од запослених или других радно ангажованих лица наруши безбедност ИКТ система, сматраће се лично одговорним и сносиће последице у складу са законским, подзаконским актима и општим актима Академије.

## 4. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Члан 9.

Сва запослена и друга радно ангажована лица дужна су да у случају промене послова, као и након престанка радног односа, односно радног ангажовања чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система.

Запослени у Служби за информационе технологије и информатичку подршку, односно лице овлашћено на основу одлуке донете од стране руководиоца Одсека (у даљем тексту: надлежни субјект ИКТ система), приликом престанка запослења или радног ангажовања, предузима следеће активности:

- прегледа све налоге и приступе систему који су били доступни одлазећем запосленом, односно радно ангажованом лицу;
- преузима од одлазећег запосленог, односно радно ангажованог лица електронске и друге мобилне уређаје;
- преузима картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми академије;
- проверава враћене мобилне уређаје и уређаје за пренос података;
- даје налог за укидање или онеспособљавање налога електронске поште и свих других права приступа систему Академије, на дан престанка радног односа или другог основа ангажовања;
- прегледа све налоге за приступ одлазећег запосленог, односно радно ангажованог лица, прикупљају приступне шифре и кодове са циљем укидања, односно промене истих на дан одласка;
- утврђује начин контакта са бившим запосленим, односно радно ангажованим лицем.

## 5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра Академије су сви ресурси који садрже пословне информације Академије, односно сви ресурси путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, базе података, пословне апликације, веб презентацију и сл.

Академија врши идентификацију имовине којом се обрађују информациона добра и документује њен значај.

Информациона добра пролазе кроз више фаза почевши од креирања, обраде, складиштења, преноса, брисања и уништавања података и информација.

Академија прави попис информационих добара који мора бити тачан, ажуран и конзистентан.

Евиденција о информационим добрима и средствима и имовини за обраду информационих добара води се од стране лица овлашћеног за ове послове, у складу са Правилником о организацији и систематизацији послова на Академији, односно одлуком руководиоца Одсека који се налази у саставу Академије.

Сви запослени и друга радно ангажована лица на Академији у обавези су да након престанка радног ангажовања врате имовину Академије којом су располагали за време трајања уговора у истом или прихватљивом стању у односу на стање у ком су је преузели.

Током отказног рока, Академија се стара да сва запослена и друга радно ангажована лица не врше неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

## 6. Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком

### Члан 11.

Класификовање података врши се узимајући у обзир осетљивост, важност података, штету која може да настане услед неовлашћеног откривања, измене или брисања података и прописе који уређују питања заштите података (о тајним подацима, пословној тајни, подацима о личности и сл.).

Подаци се деле на тајне и остале податке.

Тајни подаци су они подаци који су доступни само овлашћеним лицима.

Заштита података који су, у складу са законом који уређује област тајности података, означени као тајни, врши се у складу са прописима који регулишу ову област.

Имовина се означава уз помоћ идентификационих бројева.

## 7. Заштита носача података

### Члан 12.

Надлежни субјекти ИКТ система дужни су да успоставе организацију приступа подацима, посебно онима који су означени као тајни у складу са одредбама Закона о тајности података, Закона о слободном приступу информацијама од јавног значаја и Закона о заштити података о личности, тако да документи са ознаком тајности могу да се сниме, односно архивирају или запишу на фајл серверу у фолдеру над којим ће право приступа имати само запослени који су за то овлашћени.

У случају транспорта носача података са ознаком тајности, руководилац одсека ће одредити одговорну особу и начин транспорта.

Приликом брисања података са ознаком тајности, бришу се сви подаци са носача података који се на њему налазе.

## 8. Ограничење приступа подацима и средствима за обраду података

**Члан 13.**

Председник Академије ће овластити руководиоце Одсека у саставу Академије да одлуком одреде лице/лица које/која ће имати приступ мрежи и мрежним уређајима.

Процедура о приступу мрежи и мрежним уређајима састоји се од следећих елемената:

- листе мрежа и мрежних услуга којима је приступ дозвољен;
- начина ауторизације којима се утврђује којим лицима је одобрен приступ којој мрежи и којим услугама;
- начином управљања заштитом приступа мрежним прикључцима и услугама;
- средствима која се користе за приступ мрежама и мрежним услугама;
- захтевима у погледу верификације корисника за приступ различитим мрежним услугама.

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

**Члан 14.**

Академија управља приступом ИКТ систему и услугама кроз употребу корисничког идентификатора.

Управљање корисничким идентификаторима врши се уз поштовање следећих принципа:

1) кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
2) корисницима којима је престао радни однос или период ангажовања моментално им се онемогућавају или уклањају кориснички идентификатори.

Сваком кориснику се додељује право приступа ИКТ систему, у складу са радним задацима које обавља.

Кориснику се додељују јединствени подаци и јединствена шифра за приступ, који се не смеју делити са другим корисницима.

Додељивање привилегованих (администраторских) права на приступ врше надлежни субјекти ИКТ система.

Привилегована права на приступ које треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности. Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора.

Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење корисничких идентификатора администратора.

Шифре за приступ корисничким идентификаторима администратора се мењају променом корисника.

Академија, по потреби, врши преиспитивање права корисника на приступ, а обавезна је да врши преиспитивање након сваке промене радног статуса корисника (унапређење, разрешење и крај запослења).

Свим запосленима, другим радно ангажованим лицима и екстерним корисницима информација и опреме за обраду информација, по престанку запослења или истеку уговора, укида се право на приступ.

## 10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

### Члан 15.

Аутентификација корисника којима је одобрен приступ систему врши се путем јединственог корисничког идентификатора.

Сви корисници су дужни да:

1) корисничко име и шифру држе у тајности, не откривају их другим лицима (укључујући и надређене);
2) избегавају чување корисничког имена и шифре у писаном облику;
3) промене шифру када примете да постоји било какав наговештај могућег компромитовања;

Шифре морају да:

1) садрже најмање 8 (осам) алфанумеричких карактера;
2) садрже најмање једно велико и једно мало слово;
3) садрже најмање 1 (један) број (0-9);
4) садрже најмање 1 (један) специјални знак.

Шифре се не смеју заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и не смеју садржати више од 3 (три) узастопна идентична бројчана или словна знака.

Корисници су дужни да привремене шифре промене приликом првог пријављивања.

Неовлашћено уступање корисничког налога другом лицу подлеже дисциплинској одговорности.

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

### Члан 16.

Криптозаштита на Академији се обезбеђује коришћењем алгоритама који су уграђени у ИКТ систем.

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

### Члан 17.

Академија је дужна да предузме мере ради спречавања неовлашћеног физичког приступа објекту, простору, просторијама или зони у којима се налазе средства и документи ИКТ система, као и мере за спречавање оштећења и ометања информација.

Опрема за обраду информација се штити закључавањем просторија у којима се налази.

Безбедносне зоне морају бити заштићене одговарајућом контролом уласка како би се осигурао приступ само овлашћеним лицима.

Мере и активности које треба предузети:

1) евидентирати датуме и време уласка и изласка посетилаца, а све посетиоце треба надгледати, осим ако њихов приступ није претходно одобрен;
2) приступ зонама у којима се обрађују или чувају поверљиве информације треба да буде ограничен само на овлашћена лица;
3) у случају да Академија има сарадњу са пружаоцем услуге обезбеђења ИКТ система, лицима која су запослена код истог, треба одобрити ограничен приступ безбедносним зонама или опреми за обраду осетљивих података и омогућити им приступ (када за то постоји неизоставна потреба), а овакав приступ треба бити одобрен;
4) права приступа безбедносним зонама треба редовно преиспитивати и ажурирати, а у случају постојања потребе и укинути.

**Члан 18.**

Академија обезбеђује и примењује одговарајућу контролу приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава.

Безбедним конфигурисањем се онемогућава приступ кључној опреми, а све у циљу спречавања видљивости поверљивих информација споља.

Физичка заштита се мора планирати и у случају природних катастрофа, непријатељских напада или несреће.

**Члан 19.**

Безбедносне зоне подлежу следећим мерама заштите:

1) надлежни субјекти ИКТ система морају бити обавештени о активностима унутар безбедносне зоне;
2) забрањује се рад без надзора у безбедносним зонама;
3) безбедносне зоне које се не користе морају бити физички закључане и њихова провера се мора вршити периодично;
4) не дозвољава се уношење фотографских, видео, аудио или других уређаја за записивање, осим уз претходно одобрење овлашћеног лица.

Евиденцију о уласку у безбедносну зону врши лице овлашћено за ове послове, у складу са Правилником о организацији и систематизацији послова на Академији, односно одлуком руководиоца Одсека који се налази у саставу Академије.

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

**Члан 20.**

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења као и могућност неовлашћеног приступа и то на следећи начин:

1) опрема се поставља на месту које се може обезбедити од неовлашћеног приступа;
2) опрема за обраду информација која служи за приступ и коришћење осетљивих података се поставља на местима која нису видљива неовлашћеним лицима;
3) врши се редовна контрола система за обезбеђење, аларма, противпожарне заштите, инсталација за воду, струју, електронске комуникације и слично;

4) просторије са опремом треба редовно чистити од прашине;
5) забрањује се конзумирање хране и пића, пушење и коришћење запаљивих средстава у близини опреме за обраду информација;
6) редовно се прате услови под којима опрема ради;
7) опрема мора бити заштићена од атмосферских падавина.

Надлежни субјекти ИКТ система дужни су да редовно прате услове околине, који би могли негативно да утичу на рад опреме за обраду информација.

**Члан 21.**

Опрема се штити од прекида напајања, тако што се:
1) помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
2) капацитет помоћне опреме редовно процењује;
3) редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова;
4) обезбеђује вишеструко напајање са различитих траса (уколико га је могуће обезбедити).

Каблови за напајање и телекомуникациони каблови који преносе податке или представљају подршку информационим услугама штите се од прислушкивања, ометања или оштећења на следећи начин:
1) водови и напајања и телекомуникациони водови који улазе у просторије за обраду информација су подземни (онда када је то могуће) или имају адекватну алтернативну заштиту;
2) каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње;
3) неовлашћено прикључење уређаја на каблове се проверава физичким односно техничким претраживањем;
4) приступ до разводних табли и у просторије са кабловима се контролише.

Опрема се одржава како би се осигурала њена непрекидна расположивост и неповредивост и то на следећи начин:
1) опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;
2) поправке и сервисирање опреме обављају само запослени овлашћени за одржавање и пружалац услуге обезбеђења ИКТ система (у случају постојања такве врсте сарадње);
3) о свим сумњивим или стварним неисправностима, као и о целокупном превентивном или корективном одржавању чувају се записи;
4) осетљиве информације треба избрисати из опреме, уколико је то могуће,
5) пре враћања опреме у рад након одржавања, потребно је исту прегледати како би се утврдило да није неовлашћено коришћена или оштећена.

Опрема, информације или софтвер се измештају само уз одобрење овлашћеног лица, а током измештања се примењују следећа правила:
1) потребно је да се одреде лица која имају овлашћење да одобре измештање имовине;
2) треба да се поставе временска ограничења за измештање опреме;
3) треба документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања и ову документацију вратити са опремом, информацијама или софтвером.

На измештену опрему треба применити безбедносне механизме заштите, узимајући у обзир различите ризике приликом рада изван просторија.

Све делови опреме који садрже медијуме за чување података потребно је верификовати да би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњени.

Корисници треба да обезбеде да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.

Сва осетљива и поверљива документа и материјали морају бити уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када корисник/администратор није присутан на свом радном месту или када се документа и материјали не користе по следећој процедури:

1) све осетљиве и поверљиве информације у штампаном или електронском облику, корисници/администратори морају одложити на сигурно на крају радног дана или када нису присутни на свом радном месту;
2) рачунари морају бити закључани корисничким налозима у одсуству корисника/администратора и/или угашени на крају радног дана;
3) ормани и фиоке у којима се чувају поверљиви подаци морају бити закључани када се не користе, а кључеви не смеју бити остављени на приступачном месту без надзора;
4) преносни уређаји морају бити осигурани уз помоћ одговарајуће опреме која их штити од крађе или закључани;
5) носачи података као што су дискови и флеш меморија морају бити одложени и закључани;
6) шифре за приступ не смеју бити написане и остављене на приступачном месту;
7) штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања;
8) материјал који је намењен за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

## 14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

### Члан 22.

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података дефинишу се процедуре за руковање средствима које се односе на отпочињање и завршетак приступа ИКТ систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа серверским просторијама, просторијама са комуникационом опремом и системима за складиштење података, као и у случајевима измештања делова ИКТ система.

Академија успоставља радне процедуре које садрже инструкције за детаљно извршење следећих послова:

1) инсталација и конфигурација система;
2) обраду и поступање са информацијама;
3) израду резервних копија;
4) обраду захтева за временски распоред активности;
5) израду инструкција за поступање у случају настанка грешке или у другим ванредним ситуацијама које могу да настану у току извршавања послова;

6) утврђивање листе контаката за подршку (укључујући екстерне контакте за подршку) у случају неочекиваних потешкоћа;
7) израду инструкција за управљање поверљивим подацима;
8) процедуре за поновно покретање система и опоравак, које се користе у случају пада система;
9) управљање системским записима (логовима);
10) процедуре за надгледање.

За усвајање, измене и допуне радних процедура овлашћени су надлежни субјекти ИКТ система.

**Члан 23.**

Коришћење ресурса се континуирано надгледа, подешава и пројектује, у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе система, па се стога периодично спроводе следеће активности:
1) брисање застарелих података;
2) повлачење из употребе апликација, система или база података;
3) оптимизација серије процеса и распореда;
4) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако они нису критични за пословање.

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

**Члан 24.**

Заштита од злонамерних софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом и мејлом, зараженим преносним медијима (као што су: usb меморија, CD..) и сл.

За успешну заштиту од вируса на сваком рачунару се инсталира антивирусни програм. Антивирусни програм у континуитету контролише рачунаре у реалном времену.

Академија одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Процедура заштите од злонамерног софтвера је следећа:
1) формална забрана коришћења неауторизованих софтвера;
2) имплементација контрола које спречавају или откривају коришћење неовлашћеног софтвера или сумњивих компромитованих веб - сајтова;
3) успостављање формалне политике ради заштите од ризика повезаних са добијањем датотека и софтвера преко спољних мрежа или било ког другог медијума, указујући на то које заштитне мере треба предузети;
4) спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе;
5) присуство било каквих неодобрених датотека или неауторизованих допуна потребно је формално истражити;
6) инсталирање и редовно ажурирање антивирусних програма.

Листа провера које је потребно спроводити:
1) проверу, пре коришћења, свих датотека на свим врстама медија као и датотека примљених путем мрежа;
2) проверу, пре коришћења, садржаја прилога електронске поште и преузетих садржаја;

3) проверу постојања злонамерних софтвера на веб - страницама;
4) припрему одговарајућих планова за наставак пословања приликом опоравка од напада злонамерним софтвером;
5) имплементацију процедура за редовно прикупљање информација као што је претплата на адресне спискове за доставу;

Надлежни субјект ИКТ система дужан је да упозна све кориснике информационог система са процедурама и мерама о антивирусној заштити и процедуром о подизању свести запослених о информационој безбедности.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави надлежном субјекту ИКТ система.

Корисницима који су прикључени на ИКТ систем, у случају доказане злоупотребе интернета, надлежни субјект ИКТ система може укинути приступ.

## 16. Заштита од губитка података

### Члан 25.

Базе података и фајлови се обавезно архивирају на бекап диску, најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података и то:
Дневно копирање – архивирање се врши аутоматски за сваки дан у недељи.
Недељно копирање – архивирање се врши последњег радног дана у недељи.
Месечно копирање – архивирање се врши последњег радног дана у месецу за сваки месец посебно.
Квартално копирање - архивирање се врши последњег радног дана сваког трећег месеца у години;
Годишње копирање – архивирање се врши последњег радног дана у години.

За потребе обнове базе података у случају настанка више силе, бекапована база података се мора чувати на додатном носачу података.

### Члан 26.

**Ради вршења свих послова финансијске природе,** пријављивање у ИКТ систем Академије врши се уз помоћ корисничког идентификатора.

Аутоматском обрадом података, односно у електронском облику воде се и обрађују подаци за финансијско пословање Академије/Одсека (пословне књиге, рачуноводствене исправе, финансијски извештаји, обрачун и евиденције плата и накнада), подаци за базу података о студентима, изборима у звања, као и електронска пошта. Заштита података у електронском облику обезбеђује се:

- обезбеђењем рачунарске мреже уређајем за непрекидно напајање електричном енергијом,
- заштитом од вируса,
- израдом заштитних копија,
- заштитом приступа подацима.

Заштитне копије раде се месечно, квартално и годишње на екстерним хард дисковима, који се чувају у металној каси.

Заштиту података у финансијском пословању Академије, у електронском облику, обезбеђују руководилац финансијско-рачуноводствених послова Академије и надлежни субјект ИКТ система. За финансијско пословање користи се софтвер који обезбеђује очување података о свим прокњиженим трансакцијама, омогућава функционисање система интерних рачуноводствених контрола и онемогућава брисање прокњижених пословних промена. Пословне књиге, рачуноводствене исправе, финансијски извештаји

штампају се у папирном облику и чувају се у Академији/Одсеку, у складу са Листом категорија архивске грађе и документарног материјала.

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

**Члан 27.**

О активностима администратора и корисника води се дневник активности (лог).

## 18. Обезбеђивање интегритета софтвера и оперативних система

**Члан 28.**

Академија спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за контролу промена и инсталацију софтвера.

Смернице за контролу промена и инсталацију софтвера:

1) ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљена лица;
2) оперативни системи треба да садрже искључиво одобрене апликације;
3) апликације и оперативни системски софтвер треба имплементирати тек после обимног и успешно спроведеног испитивања примењивости, безбедности и утицаја на друге системе;
4) треба осигурати да су све одговарајуће библиотеке изворних програма ажуриране;
5) пре имплементације било каквих промена, треба успоставити стратегију повратка на претходно стање;
6) приликом свих ажурирања на библиотекама оперативних програма, треба одржавати записе за проверу;
7) као меру предострожности за неочекиване ситуације потребно је чувати претходне верзије апликативног софтвера.

Инсталацију и подешавање софтвера може да врши надлежни субјект ИКТ система.

**Члан 29.**

Надлежни субјект ИКТ система дужан је да периодично врши анализу дневника активности (лога), у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, надлежни субјект ИКТ система је дужан да одмах изврши подешавања, односно инсталира софтвер који ће открити уочене слабости.

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

**Члан 30.**

Ревизија ИКТ система се мора вршити тако да не омета пословне процесе запослених, уколико је то могуће.

Надлежни субјект ИКТ система одредиће време обављања ревизије, у зависности од врсте послова и радних задатака запослених у Академији.

## 20. Заштита података у комуникационим мрежама (укључујући уређаје и водове)

### Члан 31.

Комуникациони каблови и каблови за напајање морају бити постављени у зид или каналице, тако да се онемогући неовлашћен приступ, односно да се изврши изолација. Надлежни субјект ИКТ система је дужан да стално врши контролни преглед мрежне опреме и благовремено предузме мере у циљу отклањања евентуалних неправилности. Бежична мрежа коју могу да користе посетиоци установе, мора бити одвојена од интерне мреже коју користе запослени и кроз коју се врши размена службених података. Обе мреже морају бити означене различитим називима (SSID), док само мрежа коју користе запослени мора бити обезбеђена лозинком за приступ.

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

### Члан 32.

Заштита података који се преносе комуникационим средствима унутар Академије, између Академије и лица ван Академије, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

1. Правила коришћења електронске поште:
   - Употреба електронске поште мора бити у складу са успостављеним процедурама и адекватним контролама над спровођењем истих. Електронска пошта која у свом називу садржи и назив домена Академије или Одсека сматра се службеном и може се користити **искључиво** за пословне потребе, те размена порука личног садржаја путем ове адресе није дозвољена. Сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података. Забрањено је регистровање и остављање службене електронске поште на сајтовима који шаљу велике количине непожељне поште, која може изазвати застоје у свакодневној комуникацији (спам поруке или друго слање нежељених масовних порука без икаквог критеријума). Оваква нежељена пошта биће уклоњена ради даљег несметаног наставка коришћења платформе за пријем и слање електронске поште.
2. Правила коришћења интернета
   - Приступ садржајима на интернету је дозвољен искључиво за пословне намене.
   - На мрежи је могуће надгледање, односно вршење поступка периодичне ревизије и контролисања логовања, како на пријему тако и на слању.

     За коришћење интернета у супротности са алинејом. 1. и 2. ове тачке, корисник ће се сматрати лично одговорним.
3. Правила коришћења информационих ресурса
   - Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намену коришћења посебно одобрава надлежни субјект ИКТ система, на образложени захтев корисника.

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

**Члан 33.**

Појединци којима је дата одговорност за контролисање животног циклуса имовине, дужни су да правилно управљају имовином током целог животног циклуса.
У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, Академија је у обавези да обезбеди безбедност информација у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система, јер такво разматрање доводи до ефективнијих и рационалнијих решења.

## 23. Заштита података који се користе за потребе тестирања ИКТ система, односно делова система

**Члан 34.**

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања**.**

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери који су намењени тестирању и развоју. Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера. Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података. Инсталирање новог софтвера, као и ажурирање постојећег, односно инсталирање нове верзије врши се на начин којим се не омета/обуставља оперативни рад запослених.

## 24. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

**Члан 35.**

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

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

**Члан 36.**

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга, у складу са условима који су уговорени са пружаоцем услуга, Академија успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

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

### Члан 37.

Орган државне управе надлежан за безбедност ИКТ система је министарство надлежно за послове информационе безбедности (у даљем тексту: надлежни орган).

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени, односно радно ангажовано лице је дужан да одмах обавести надлежног субјекта ИКТ система на Одсеку.

По пријему пријаве из става 1. овог члана, надлежни субјект ИКТ система је дужан да изврши процену стања и предузме мере у циљу заштите ресурса ИКТ система.

У случају да надлежни субјект ИКТ система утврди да је настао било какав инцидент у ИКТ систему који може да има значајан утицај на нарушавање информационе безбедности, дужан је да о томе одмах обавести руководиоца Одсека и предузме мере у циљу заштите ресурса ИКТ система.

Руководилац Одсека је дужан да, у случају настанка било каквог инцидента у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности о томе, у писаној форми, обавести председника Академије – који је дужан да о томе обавести надлежне државне органе.

Обавештавање о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности, Академија врши преко веб странице Надлежног органа или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима којег одржава министарство надлежно за послове информационе безбедности.

Након пријаве инцидента, уколико је инцидент и даље у току, Академија доставља обавештења о битним догађајима у вези са инцидентом и активностима које предузима до престанка инцидента органу коме је, пријавила инцидент.

Академија доставља завршни извештај о инциденту органу кога је обавештавала о инциденту у року од 15 дана од дана престанка инцидента, а који обавезно садржи врсту и опис инцидента, време и трајање инцидента, последице које је инцидент изазвао, предузете активности ради отклањања последица инцидента и, по потреби, друге релевантне информације.

### Члан 38.

Академија је дужна да пријави следеће инциденте који могу да имају значајан утицај на нарушавање информационе безбедности:

1) инциденте који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;

2) инциденте који утичу на велики број корисника услуга, или трају дужи временски период;

3) инциденте који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;

4) инциденте који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;

5) инциденте који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе;

Академија је дужна да, поред обавештавања о инцидентима, достави Националном ЦЕРТ-у статистичке податке о свим инцидентима у ИКТ систему у претходној години најкасније до 28. фебруара текуће године.

### 27. Мере које обезбеђују континуитет обављања посла у ванредним околностима

**Члан 39.**

Академија врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

## III. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

**Члан 40.**

Обавеза Академије је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалну измену овог Правилника, у циљу провере адекватности прописаних мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Академије.

**Члан 41.**

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли и званичној интернет страници Академије.

ПРЕДСЕДНИЦА САВЕТА АКАДЕМИЈЕ

др Адела Медовић Баралић, проф.струк.студ.

**Потврда о објављивању**

Правилник о безбедности информационо-комуникационог система Академије техничко-уметничких струковних студија Београд (број: 4330/1 од 12.12.2023. године објављен је дана 14.12.2023. године на огласној табли и на интернет страници Академије техничко-уметничких струковних студија Београд, што својим потписом потврђује:

Одговорно лице