На основу члана 52. став 1. алинеје 16. и на основу утврђеног Предлога Наставно-научног већа број 1395/1-01 од 27.11.2019. године, Савет Факултета на седници одржаној дана 14.01.2020. години доноси

О Д Л У К У
о
усвајању Акта о безбедности информационог-комуникационог система Природно-математичког факултета Универзитета у Нишу

1. Усваја се Акт о безбедности информационог-комуникационог система Природно-математичког факултета Универзитета у Нишу.
2. Акт о безбедности информационог-комуникационог система Природно-математичког факултета Универзитета у Нишу је саставни део ове Одлуке.
3. Доставити: декану, продекану за научно-истраживачки рад, Рачунарском центру и архиви Секретаријата.

ПРЕДСЕДНИК САВЕТА

Проф. др Бранимир Тодоровић

На основу члана 8, став 1, Закона о информационој безбедности („Службени гласник РС”, број 6/2016 и 94/2017), чланова 2 и 3 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 („Службени гласник РС”, број 94/16), Савет Природно-математичког факултета на основу утврђеног Предлога Наставно-научног већа Факултета број 1395/1-01 од 27.11.2019. године је на седници одржаној дана 14.01.2020. године усвојио

Акт о безбедности информационо-комуникационог система Природно-математичког факултета

I. ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Актом о безбедности информационо-комуникационог система (у даљем тексту: Акт о безбедности) Природно-математичког факултета (у даљем тексту: Факултет), у складу са Законом о информационој безбедности („Службени гласник РС”, број 6/2016 и 94/2017, у даљем тексту: Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система Факултета (у даљем тексту: ИКТ систем).

Члан 2.

Циљеви доношења Акта о безбедности су:

1) одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2) спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
3) подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4) прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;

Члан 3.

Корисници ИКТ система Факултета (у даљем тексту: корисници) јесу запослени и студенти. Изузетно, корисници могу бити и трећа лица ангажована уговором за обављање послова у вези ИКТ система.

Корисници морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

Декан је одговоран за праћење примене мера безбедности.

Члан 4.

Корисници су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних радних активности.

Непоштовање одредби Акта о безбедности, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

Дисциплински поступак се покреће по пријави шефа Рачунарског центра који представља службу овлашћену за праћење прикупљања, анализе и обраде података.

II. МЕРЕ ЗАШТИТЕ

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Факултета, односно заштита података садржаних у ИКТ систему, од неовлашћеног приступа, модификације, коришћења и деструкције на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Факултет је у обавези да набави и одржава потребну софтверску и хардверску опрему помоћу које ће се омогућити примена мера заштите предвиђених Актом о безбедности.

Члан 6.

Интерни акти који уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу:

- Правилник о организацији и систематизацији радних места.
- Уговори о раду.
- Изјаве о поверљивости.
- Уговори о чувању поверљивости са правним лицима.
- Правилник о уносу података у базу информационог система и постављању обавештења на интернет презентацију Природно-математичког факултета.
- Правилник о управљању информацијама и безбедности информационог система ПМФ-а.

Удаљени приступ

Члан 7.

Факултет дозвољава удаљени приступ и употребу мобилних уређаја од стране запослених лица, уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја.

Члан 8.

Удаљени приступ се омогућава помоћу заштићене VPN конекције преко које се корисници повезују на ИКТ систем Факултета. Овај начин приступа се примењује и када се користе мобилне уређаји за повезивање на мрежу Факултета.

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

Удаљени приступ одобрава декан Факултета на основу предлога шефа Рачунарског центра.

Члан 9.

Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Корисник мобилног уређаја преко којег је омогућен приступ мрежи Факултета у обавези је да крађу или губитак мобилног уређаја пријави Рачунарском центру без одлагања, а у року од 72 сата да достави писану изјаву о околностима губитка или крађе мобилног уређаја. Рачунарски центар је у обавези да, по пријави крађе или губитка мобилног уређаја, неодложно блокира несталом мобилном уређају приступ информационом систему и кориснику промени креденцијале за приступ. У случају да се пронађе мобилни уређај чији је нестанак пријављен, Рачунарски центар ће извршити преглед уређаја и утврдити да ли он може бити поново коришћен за удаљени приступ.

Оспособљеност корисника

Члан 10.

Факултет се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају. Њихове одговорности су утврђене уговором о раду или ангажовању на привременим и повременим пословима.

Запослени и друга лица којима је на основу посебог уговора додељен приступ поверљивим информацијама, морају потписати споразум о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Члан 11.

Запослени у Рачунарском центру континуирано се обучавају у циљу унапређења техничког и технолошког знања. Ова лица су ауторизована за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Запослени у стручним службама Факултета су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују

безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Заштита од ризика који настају при промени статуса корисника

Члан 12.

Запослени, као и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања, под претњом кривичне и материјалне одговорности. Обавезе које остају важеће и после престанка запослења треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа.

Ова мера је ближе одређена Уговором о раду запосленог.

Члан 13.

Служба за опште и правне послове, односно Служба за наставу и студентска питања, у обавези су да Рачунарски центар обавесте о престанку статуса запосленог, односно студента, у року од три дана. Након тога, Рачунарски центар предузима следеће активности:

- прегледа све налоге и приступе систему који су били доступни кориснику,
- проверава враћене мобилне уређаје и уређаје за преношење података,
- укида налог електронске поште и свих других права приступа ИКТ систему Факултета кориснику коме је престао статус. Ова активност извршиће се у року од три дана по пријему одговарајућег обавештења.

Идентификација информационих добара и њихова заштита

Члан 14.

Факултет врши идентификацију информационих добара и документује њихов значај. У информациона добра Факултета спадају хардверске и софтверске компоненте ИКТ система, подаци који се чувају и обрађују као и подаци о корисничким налозима.

Евиденцију о информационим добрима воде Рачунарски центар и Служба за материјално и финансијско пословање.

Члан 15.

Факултет може да означи типове и локације података као поверљиве, интерне или јавне. Сврха ове класификације је:

- Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и буду свесни одговорности за неовлашћено коришћење или преношење;
- Подизања свести о вредности информације или документа;
- Заштите садржаја;

- Интеграције са системима за архивирање.

Класификација документа мора да буде усклађена са правилима контроле приступа.

Члан 16.

Факултет обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података и имају посебан значај за функционисање ИКТ система.

Евиденцију носача података на којима су снимљени подаци од значаја за Факултет води Рачунарски центар.

Члан 17.

Када престане потреба да неки медијум садржи податке који су од посебног значаја, безбедно уклањање података врши се применом форматирања медијума.

Медијуми код којих није могуће извршити форматирање морају се физички уништити.

Члан 18.

Када је потребно транспортовати носаче података који садрже информације од посебног значаја за Факултет, за случај да је неопходно задржати њихов садржај, потребно је извршити њихову додатну физичку заштититу.

Одабрани начин транспорта мора да буде у складу са потребом заштите интегритета података.

Члан 19.

Подацима и средствима за обраду података може се ограничити приступ у складу са степеном поверљивости.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју корисник има. Свака злоупотреба додељеног корисничког налога повлачи дисциплинску или кривичну одговорност корисника.

Члан 20.

Факултет управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

Управљање корисничким идентификаторима врши се поштујући следеће принципе:

- Кориснички идентификатори запослених су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности.
- За приступ студентском порталу студентима се додељују јединствени кориснички идентификатори.

- Студенти користе заједнички идентификатор који омогућава ограничени приступ ресурсима ИКТ система за потребе наставе;
- Кориснику коме је престао статус запосленог или студента укида се кориснички идентификатор.

Додељивање привилегованих (администраторских) права на приступ врши се на основу одлуке шефа Рачунарског центра.

Привилегована права на приступ додељују се посебно за сваки системски објекат уз дефинисан рок трајања тих права.

Привилегована права на приступ која 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 периодично преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење администраторских корисничких идентификатора.

Лозинке за администраторске корисничке налоге мењају се са променом администратора.

Факултет једном годишње врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и престанак статуса).

Члан 21.

Аутентификација корисника коме је одобрен приступ систему врши се путем његовог јединственог корисничког имена и лозинке.

Сви корисници су дужни да:

- Корисничко име и лозинку држе у тајности и не откривају их другим лицима, укључујући и надређене особе.
- Избегавају чување корисничког имена и лозинке у писаном облику.
- Промене лозинку увек када постоји било какав наговештај могућег компромитовања.

Лозинке морају да:

- садрже најмање 8 алфанумеричких знакова при чему у себи не смеју да садрже више од 3 узастопна идентична бројчана или словна знака,
- садрже комбинацију најмање три знака из следећих категорија: мало слово, велико слово, цифра и специјални знак.

Лозинке не смеју бити засноване на личним подацима особе, као што су име, телефонски број или датум рођења.

Корисници су дужни да привремене лозинке промене приликом првог пријављивања.

Физичко обезбеђење ИКТ система

Члан 22.

Факултет је дужан да предузме мере ради спречавања неовлашћеног физичког приступа просторијама у којима се налазе средства и документи ИКТ система, као и спречавање оштећења информатичке имовине.

Опрема за обраду информација се штити закључавањем просторија у којима се налази. Просторије које садрже опрему за обраду информација, а налазе се у приземљу, додатно се обезбеђују решеткама на прозорима.

У рачунарске учионице дозвољен је приступ наставницима, сарадницима и студентима у терминима наставе.

У серверску салу могу да уђу само овлашћена лица из Рачунарског центра.

Члан 23.

Запослени у Рачунарском центру редовно прате услове околине у серверској сали.

Опрема у серверској сали се штити од прекида напајања уградњом уређаја за непрекидно напајање који се редовно одржавају и проверавају у складу са спецификацијама произвођача.

Одржавање опреме и заштита интегритета информационих добара

Члан 24.

Рачунарска опрема се одржава како би се осигурале њена непрекидна расположивост и неповредивост. Уколико рачунарска опрема садржи осетљиве информације, а износи се ради сервисирања, онда се те информације уклањају пре сервисирања.

Опрема, информације или софтвер се измештају само уз одобрење Рачунарског центра, а током измештања се примењују следећа правила:

- Треба да се одреде запослени и спољни сарадници који имају овлашћење да врше измештање имовине.
- Треба да се поставе временска ограничења за измештање опреме и да се проверава усклађеност приликом повратка.
- Треба документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања.

Приликом расходовања или поновног коришћења опреме која садржи медијуме за чување података, треба уклонити осетљиве податке и лиценцирани софтвер.

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

Члан 25.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

Корисници ИКТ система Факултета су уобавези да закључају радну станицу када је остављају без надзора.

Члан 26.

Запослени у Рачунарском центру, у циљу обезбеђивања исправног и безбедног функционисања ИКТ система, обавезни су да поступају према радним процедурама за извршење следећих послова:

- Израда резервних копија база података.
- Процедуре за поновно покретање система и опоравак које се користе у случају отказа система.
- Надгледање активности на мрежи.
- Одржавање ажурног списка контаката за подршку (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа.

Резервне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

За чување резервних копија користе се екстерни хард дискови и снимање на удаљеној локацији.

Рачунарски центар извршава следеће задатке:

- Процењује осетљиве и критичне податке за које је потребно правити резервне копије.
- Креира план прављења резервних копија.
- Верификује успешно прављење резервних копија.
- Води евиденцију урађених резервних копија.
- Одлаже копије на безбедно место.
- Периодично тестира исправност резервних копија и процедуре за прављење заштитних копија.
- Рестаурира податке са резервних копија.

За усвајање, измене и допуне радних процедура као и за заштиту од губитка података одговоран је Рачунарски центар.

Члан 27.

На опреми која је део ИКТ система Факултета мора се инсталирати и одржавати софтверска заштита од злонамерног софтвера и софтверски алати за спречавање упада

у ИКТ систем. Заштита од злонамерног софтвера спроводи се у циљу заштите од вируса и друге врсте злонамерног софтвера који у рачунарску мрежу могу доспети путем интернета, елктронске поште, заражених преносних медијума, инсталацијом нелиценцираног софтвера и слично.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања радних станица или преносних медијума.

Преносиви медијуми, пре коришћења, морају бити проверени на присуство вируса. Ако се утврди да преносиви медијум садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером. Уколико чишћење није могуће, заражени медијум се не сме користити.

Ризик од евентуалног губитка података приликом чишћења медијума од вируса сноси доносилац медијума.

Корисницима ИКТ система је забрањено да самостално прикључују на систем уређаје који нису прошли проверу особља Рачунарског центра.

Недозвољена употреба интернета обухвата:

- Коришћење и дистрибуцију нелиценцираног софтвера.
- Намерно ширење злонамерног софтвера.
- Преузимање огромне количине података којим се проузрокује загушење на мрежи.
- Неовлашћено преузимање материјала заштићених ауторским правима.
- Коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и слично).

Корисницима ИКТ система, у случају доказане злоупотребе интернета, Рачунарски центар може укинути приступ.

Члан 28.

Рачунарски центар чува и редовно преипитује аутоматски генерисане записе о догађајима и бележи активности корисника, грешке и догађаје у вези са безбедношћу информација.

Систем за контролу и дојаву о грешкама и неовлашћеним активностима мора бити подешен тако да одмах обавештава администраторе ИКТ система о свим нерегуларним активностима корисника и о покушајима упада и упадима у систем.

Члан 29.

Факултет спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система.

Инсталацију и подешавање софтвера, на основу писменог захтева корисника, могу да врши само запослени у Рачунарском центру, односно корисник који има овлашћење за то добијено од стране Рачунарског центра.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера.

Приликом инсталације софтвера, лица која врше инсталацију морају да воде рачуна о могућности повратка на претходно стање.

Члан 30.

Факултет врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

Запослени у Рачунарском центру благовремено прикупљају информације о техничким рањивостима информационих система који се користе, вреднују изложеност тим рањивостима и предузимају одговарајуће мере, узимањем у обзир припадајућих ризика.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, запослени у Рачунарском центру су дужни да одмах изврше подешавања, односно инсталирају софтвер који ће отклонити уочене рањивости. Прво се узимају у разматрање системи са високим ризиком.

Забрањено је инсталирање софтвера који могу довести до изложености ИКТ система безбедносним слабостима.

Члан 31.

Приликом спровођења ревизије ИКТ система, Факултет обезбеђује да ревизија има што мањи утицај на фукционисање система.

Ревизија ИКТ система врши се по потреби а при том се корисници о томе благовремено обавештавају. У правилу, ревизија се врши ван радног времена, осим када је у питању хитност потребе за њом.

Члан 32.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно спречи могуће оштећење.

Активна мрежна опрема се мора налазити у закључаном орману.

Запослени у Рачунарском центру су у обавези да контролишу мрежну опрему и благовремено предузимају мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коју могу да користе студенти Факултета и друга лица мора бити одвојена од интерне мреже коју користе запослени и кроз коју се врши размена службених података.

Члан 33.

Коришћење рачунарске мреже Факултета, система електронске поште и интернета врши се у складу са Правилником о општим правилима приступа и коришћења услуга AMPEC (Академска мрежа Републике Србије).

Електронска пошта се може користити искључиво за пословне потребе. Није дозвољено корисничке налоге додељене за приступ ИКТ систему користити за регистровање на друштвеним мрежама и другим порталима (изузев портала којима се приступа због потреба посла).

Електронском поштом не смеју се слати подаци чија компромитација може да угрози безбедност ИКТ система Факултета.

Сарадња са трећим лицима

Члан 34.

Споразуми о поверљивости или неоткривању штите информације Факултета и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

Да би се идентификовали захтеви за споразуме о поверљивости или неоткривању, треба узети у обзир следеће елементе:

- Дефиницију информација које треба заштитити.
- Очекивано трајање споразума, укључујући случајеве у којима је потребно да се поверљивост сачува неограничено.
- Поступања које се захтевају по истеку споразума, попут повраћаја или уништавања информација.
- Право на проверу и праћење активности које укључују поверљиве информације.
- Радње које треба предузети у случају кршења овог споразума.

Члан 35.

Рачунарски центар је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система, запослени у Рачунарском центру воде документацију.

Документација из претходног става мора да садржи описе свих процедура а посебно процедура које се односе на безбедност ИКТ система.

Члан 36.

У захтеве за нове информационе системе или за побољшање постојећих информационих система морају бити укључени захтеви који се односе на безбедност информација и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Захтеви за безбедност информација укључују:

- Проверу идентитета корисника.
- Доступност, поверљивост, непорецивост и интегритет података и имовине.
- Надгледање пословних процеса.
- Омогућавање приступа за кориснике са различитим нивоима привилегије.

У уговору са набављачем за купљене производе дефинишу се захтеви безбедности, тестирања и имплементације.

Поступање у случају безбедносних инцидената

Члан 37.

У сврху опоравка ИКТ система од последица инцидената који угрожавају безбедност ИКТ система, запослени у Рачунарском центру су у обавези да:

- направе и воде ажурно документацију за сервисе, апликације и базе података;
- чувају резервне копије конфигурационих фајлова сервера, апликација и база података;
- чувају резервне копије података на најмање три локације (од којих бар једна мора бити на удаљеној локацији);
- воде податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, корисник је дужан да одмах обавести Рачунарски центар.

У случају погрешног функционисања или других аномалијских понашања система врши се исто извештавање као и у случају догађаја у вези са безбедношћу информација.

Корисник који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и путем електронске поште или телефона обавестити Рачунарски центар.

Рачунарски центар врши проверу пријављеног инцидента и извршава активности на успостављању нормалног функционисања ИКТ система.

Рачунарски центар води евиденцију о свим инцидентима, као и пријавама инцидената, на основу којих се против одговорног лица могу водити дисциплински, прекршајни или кривични поступци.

III. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 38.

Обавеза Факултета је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Факултета.

Члан 39.

Ступањем на снагу Акта о безбедности, престају да важе чланови 7-14 и 16-19 Правилника о управљању информацијама и безбедности инфорационог система ПМФ-а.

Члан 40.

Овај Акт о безбедности ступа на снагу даном доношења а примењиваће се осмог дана од дана објављивања на огласној табли и сајту Факултета.

Председник Савета

Проф. др Бранимир Тодоровић

Додатак А

Речник коришћених термина

Значење појединих термина коришћених у Закону о информационој безбедности и/или Акту о информационој безбедности Природно-математичког факултета је следеће:

***Информационо-комуникациони систем* (*ИКТ систем*)** је технолошко-организациона целина која обухвата:

(1) Електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
(2) 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;
(3) Податке који се похрањују, обрађују, претражују или преносе помоћу средстава из тачака (1) и (2), а у сврху њиховог рада, употребе, заштите или одржавања;
(4) Организациону структуру путем које се управља ИКТ системом.

Оператор ИКТ система је правно лице, орган јавне власти или организациона јединица органа јавне власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности.

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.

Тајност је својство које значи да податак није доступан неовлашћеним лицима.

Интегритет значи очуваност изворног садржаја и комплетности податка.

Расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан.

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;

Непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи.

Ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система.

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.

Инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност.

Мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система.

Тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности.

ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима.

Орган јавне власти је државни орган, орган аутономне покрајине, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, правно лице које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе, као и правно лице које се претежно, односно у целини финансира из буџета.

Служба безбедности је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије.

Самостални оператори ИКТ система су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове и службе безбедности.

Компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података.

Криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите.

Криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима.

Криптографски производ је софтвер или уређај путем кога се врши криптозаштита.

Криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви.

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

Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и слично.

Уређај за непрекидно напајање – UPS (*Uninterruptable power supply*) је уређај који током одређеног времена омогућава напајање рачунарског система електричном енергијом иако је дошло до прекида напајања у електричној мрежи.

VPN (*Virtual private network*) – Приватна комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију.

Мобилни уређаји – Подразумевају све преносне електронске уређаје намењене за комуникацију на даљину. У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони, PDA и сви други мобилни уређаји који садржи податке и имају могућност повезивања на мрежу.

PDA (*Personal Digital Assistant*) – Лични дигитални асистент је *palmtop* рачунар (рачунар малих димензија који се може дружати у руци, тј. на длану) који омогућава особи која га користи да организује своје пословне активности али и за приступ рачунарској мрежи и интернету уопште.

Аутоматски генерисани записи о догађајима – У рачунарству уопште под *log* фајлом (датотеком) подразумева се датотека која садржи записе о догађајима који се јављају у оперативном систему или другој врсти софтвера као и поруке које се размењују између различитих корисника комуникационог софтвера.

Активна мрежна опрема – Представља део рачунарске опреме који се активно односи према сигналима који се преносе у оквиру рачунарске мреже тако што их појачава, модуфикује, процењује и сл. У ову опрему спадају уређаји типа *switch* (прекидач – уређај који повезује посебне делове исте мреже), *repeater* (појачава мрежне сигнале), *hub* (слично као *repeater* али повеузје више делова мреже), *bridge* (уређај који повезује више локалних мрежа у јединствену мрежу), *router* (усмеривач – рачунар који је као део комуникационе подмреже код мрежа ширег подручја задужен за усмеравање пакета кроз подмрежу) и друго.

Медијум/носач података – Уређај за масовно меморисање података који може бити *интерни* (када је уграђен у саму радну станицу – најчешће се ради о хард дисковима), *екстерни* када се прикључује на радну станицу али се може преносити (екстерни хард диск, флеш меорија, CD/DVD и сл.) или удаљени (хард диск на удаљеном сереверу а који је доступан преко мреже).

Класификовање података је поступак утврђивања и појединачног додељивања нивоа тајности података, у складу са њиховим значајем за оператора ИКТ система.

Администратор је лице које има привелогована права у ИКТ систему. На основу уговора о раду и Систематизације то су запослени у Рачунарском центру.