РЕПУБЛИКА СРБИЈА
Топличка академија
струковних студија
Бр. 890/2
Датум 11. 10. 2022. год.
ПРОКУПЉЕ

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ТОПЛИЧКА АКАДЕМИЈА СТРУКОВНИХ СТУДИЈА

ТОПЛИЧКА АКАДЕМИЈА СТРУКОВНИХ СТУДИЈА • ПРОКУПЉЕ •

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16 , 94/17 и 77/2019), чл. 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), и члана 53. Статута Топличке академије струковних студија број 20/2022-2 од 03.06.2022.године, Привремени Савет Топличке академије струковних студија доноси, на седници одржаној дана 11.10.2022.године, доноси Акт о безбедности информационо-комуникационог система Топличке академије струковних студија.

1. ОСНОВНЕ ОДРЕДБЕ

Предмет Акта
Члан 1.

Актом о безбедности информационо-комуникационог система Топличке академије струковних студија (у даљем тексту: Акт о безбедности), у складу са Законом о информационој безбедности („Службени гласник РС”, број 6/16 и 94/17, 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 Топличке академије струковних студија (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности
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;

5.свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Акта о безбедности
Члан 3.

Мере заштите ИКТ система које су ближе уређене Актом о безбедности служе превенцији од настанка инцидената и минимизирању штете од инцидената и њихова примена је обавезна за све запослене.

Запослени у Топличкој академији струковних студија 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.

Руководилац послова информационих система и технологија и Администратори информационих система и технологија одговорни су, свако у свом Одсеку и опису

радних обавеза, за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност запослених

Члан 4.

Запослени у Топличкој академији струковних студија су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

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

Предмет заштите

Члан 5.

Предмет заштите ИКТ система обухвата и односи се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмске кодове, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

2.МЕРЕ ЗАШТИТЕ

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Топличка академија струковних студија, односно заштиту података садржаних у ИКТ систему, од неовлашћеног приступа, обраде, модификовања, коришћења или уништења података који су садржани у ИКТ систему.

Члан 6.

Топличка академија струковних студија у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

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

1.Правилник о унутрашњој организацији и систематизацији радних места,

2.Уговори о раду,

3.Изјаве о поверљивости,

4.Уговори о чувању поверљивости са правним лицима,

5.Правилник о приступу посебно осетљивим подацима и информацијама у ИКТ систему.

Сви запослени морају бити упознати са процедуром заштите безбедности ИКТ система.

Топличка академија струковних студија утврђује начин доделе овлашћења за приступ ИКТ систему, степен обуке и квалификацију запослених, начин одобравања

приступа запосленима од стране руководиоца, односно непосредно надређеног лица. Посебним актом се може утврдити и одговорност сваког запосленог и одговорног лица, и прописује дисциплинска одговорност запосленог, у случају непоштовања одредби које уређују информациону безбедност.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 7.

Топличка академија струковних студија дозвољава рад на даљину и употребу мобилних уређаја од стране запослених, 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.

Рад на даљину

Радни однос за обављање послова ван просторија послодавца обухвата:

1.Рад на даљину,

2.Рад од куће,

3.Виртуелно радно окружење.

Такође, рад на даљину у смислу овог Акта односи се на ситуацију када је запослени и други радно ангажовани обавезан да изврши одређене послове на мрежи послодавца, а налази се ван просторија послодавца.

Предметно ангажовање и омогућавање обављања задатих и неопходних послова се уређује путем Процедуре за VPN приступ информационом систему (у даљем тексту: VPN процедура).

VPN процедура дефинише правила и услове за повезивање на мрежу Топличке академије струковних студија са удаљене локације. Правилном применом утврђеног поступка и начина приступа, Топличка академија струковних студија своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи.

VPN процедура се примењује на све запослене у Топличкој академији струковних студија и сараднике који користе рачунаре или мобилне уређаје за повезивање на мрежу Топличке академије струковних студија, и уређује приступ са удаљених локација у сврху обављања посла у име и за рачун Топличке академије струковних студија, укључујући коришћење електронске поште и мрежних ресурса, као и начин приступа мрежи Топличке академије струковних студија са удаљених локација.

Ауторизованим корисницима није дозвољено да користе мрежу Топличке академије струковних студија за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада запосленог.

Захтеви који морају бити испуњени и дефинисани у VPN процедури:

1.Приступ са удаљених локација мора бити заштићен коришћењем криптографских алгоритама,

2.Ауторизовани корисници морају чувати креденцијале својих налога и не смеју омогућити приступ било ком трећем лицу,

3.Приликом коришћења службеног рачунара за приступ мрежи Топличке академије струковних студија са удаљене локације, ауторизовани корисник не сме истовремено бити повезан и на неку другу мрежу која може угрозити безбедност комуникације,

4.Приступ са удаљене локације мора бити одобрен од стране одговорног лица за надзор

спровођења VPN процедуре,

5.Сви уређаји који су повезани на интерну мрежу преко удаљених локација морају имати инсталирану заштиту у виду антивирусног софтвера. Трећа лица су у обавези да примењују захтеве из закључених уговора са Топличком академијом струковних студија,

6.Сви пословни подаци који се креирају приликом рада на даљину складиште се у информационом систему. Ради безбедности, пословни подаци се не складиште на мобилним уређајима,

7.Рад на даљину запослених или других радно ангажованих (ангажованих за рад у просторијама послодавца) одобрава Руководилац послова информационих система и технологија.

Коришћење мобилних уређаја

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

Топличка академија струковних студија спроводи обуку запослених који користе мобилне уређаје, у циљу подизања свести о додатним ризицима до којих долази услед оваквог начина рада.

Процедуром о коришћењу мобилних уређаја потребно је установити следећа правила:

1.Сви уређаји морају бити заштићени јаком шифром,

2.Мора бити инсталирана антивирусна заштита,

3.Крађа или губитак мобилног уређаја се мора без одлагања пријавити надлежној организационој јединици за информационе технологије и одговорном лицу, који затим спроводе активности у смислу очувања безбедности. Уколико се уређај пронађе, потребно је предати исти одговорним лицима,

4.Корисницима није дозвољено да врше измене на хардверу или инсталираном софтверу који је власништво Топличке академије струковних студија без претходне писане дозволе Руководиоца послова информационих система и технологија.

Процедура се примењује на све стално запослене, запослене на одређено време или лица ангажована по другим основима, који имају приступ или користе мобилне уређаје у власништву Топличке академије струковних студија.

Право на коришћење мобилних уређаја ван седишта Топличке академије струковних студија се стиче на основу писаног захтева корисника мобилног уређаја упућеног одговорном лицу.

Рад на даљину може се остварити и коришћењем уређаја који нису мобилни (на пример, десктоп рачунари). Ови уређаји, при томе, морају имати примењене најмање исте безбедносне мере као и сродни уређаји који се налазе у оквиру мреже, док се за заштиту комуникације морају применити исте мере као и за заштиту комуникације мобилних уређаја. Подешавање ових уређаја врше Администратори информационих система и технологија. Корисници ових уређаја морају обезбедити довољно безбедан простор за њихов рад (засебна соба, положај дисплеја мора бити такав да онемогући посматрање од стране неовлашћених особа и слично).

Администратор информационих система и технологија одговоран је за вођење евиденције о свим уређајима намењеним за рад на даљину. Евиденција о уређајима треба да садржи податке који су неопходни да би се уређај и/или корисник недвосмислено идентификовали, као што су произвођач, модел, серијски број, инвентарски број, име и презиме корисника који је задужио уређај и његов јединствени матични број.

Корисник мобилног уређаја у обавези је да сваки безбедносни инцидент пријави Руководиоцу послова информационих система и технологија без одлагања, а у року од 24 сата да достави писану изјаву о околностима безбедносног инцидента. Под појмом безбедносни инцидент се сматра крађа, губитак мобилног уређаја или било који други догађај који доводи до нарушавања тајности и интегритета података који се налазе на мобилном уређају. Руководилац послова информационих система и технологија је у обавези да, по пријави безбедносног инцидента, неодложно блокира несталом мобилном уређају приступ информационом систему и кориснику промени креденцијале за приступ систему.

Оспособљеност и одговорност корисника ИКТ система

Члан 8.

Топличка академија струковних студија 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, уговором о ангажовању за рад ван радног односа или неким другим интерним актом.

Провера кандидата и услови запошљавања

Топличка академија струковних студија спроводи радње у циљу провере испуњености услова сваког појединачног кандидата за запослење, у складу са одговарајућим прописима и етичким правилима, сразмерно пословним захтевима, класификацији информација којима ће имати приступ и сагледаним ризицима.

Сви запослени и радно ангажовани појединци по другом основу којима је 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.

Обавезе у току запослења

Руководство Топличке академије струковних студија је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

Топличка академија струковних студија у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

1.Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету,

2.Штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама,

3.Спроводи програме заштите на конзистентан и уједначен начин у свим организационим јединицама,

4.Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

Запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура 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.

Упознавање са безбедношћу информација, стицање знања и обука

Сви запослени/корисници ИКТ система Топличке академије струковних студија 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.

Дисциплински поступак

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике која је на снази и у примени код Топличке академије струковних студија.

Дисциплински поступак се покреће на предлог Руководиоца послова информационих система и технологија.

Заштита од ризика који настају приликом промене статуса корисника ИКТ система

Члан 9.

Запослени и лица ангажована по другом основу, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања. Дужности и обавезе које остају важеће и после престанка ангажовања и треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа, односно уговора о ангажовању лица ван радног односа.

Ова мера је ближе одређена:

1.Процедуром о правима приступа информационом систему

2.Уговором о раду

3.Уговором о ангажовању лица ван радног односа

4.Споразумом о поверљивости

За поступања приликом престанка запослења или ангажовања задужена је Служба правних, кадровских и административних послова, Руководилац Одсека или Руководилац послова информационих система и технологија, који предузимају следеће активности:

1.проверавају испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату,

2.прегледају све налоге и приступе систему који су били доступни запосленом,

3.преузимају од запосленог електронске и друге мобилне уређаје,

4.утврђују начин контакта са бившим запосленим након одласка,

5.проверавају враћене мобилне уређаје и уређаје за преношење података,

6.дају налог за укидање налога електронске поште и свих других права приступа систему Топличке академије струковних студија на дан престанка радног односа или другог основа ангажовања бившег запосленог,

7.прегледају све налоге за приступ одлазећег запосленог и прикупљају приступне шифре и кодове са циљем укидања / промене истих на дан одласка,

8преузимају картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Топличке академије струковних студија.

Идентификација информационих добара и њихова заштита

Члан 10.

Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију и податке о корисничким налозима.

Пописивање имовине

Топличка академија струковних студија врши идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација. Топлича академија струковних студија прави попис информационих добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Евиденцију о информационим добрима и средствима, и имовини за обраду информационих добара води Администратор информационих система и технологија на нивоу Одсека у саставу Топличке академије струковних студија.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај

Појединци којима је дата одговорност за контролисање животног циклуса имовине дужни су да правилно управљају имовином током целог животног циклуса.

Запослени и екстерни корисници у обавези су да након престанка њиховог радног ангажовања врате имовину Топличкој академији струковних студија којом су располагали за време трајања уговора или споразума о ангажовању на одређеним пословима и задацима, у истом или прихватљивом стању у коме су је и преузели.

Током отказног рока запослених, Топличка академија струковних студија контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

Класификација података по значају

Члан 11.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности података, у складу са њиховим значајем за Топличку академију струковних студија.

Топличка академија струковних студија означава типове и локације података као поверљиве, интерне или јавне. Имовина се означава уз помоћ идентификационих налепница које носе одговарајућу класификациону ознаку.

Топличка академија струковних студија класификациону шему поверљивости информација базира на четири нивоа, а у складу са Актом о процени ризика у заштити лица, имовине и пословања:

1.откривање не изазива никакву штету,

2.откривање изазива мању непријатност или мању штету,

3.откривање има значајан краткорочни утицај на пословање или тактичке циљеве,

4.откривање има озбиљан утицај на дугорочне стратешке циљеве или угрожава опстанак.

Топличка академија струковних студија врши класификацију ради:

1.Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење,

2.Подизања свести о вредности информације или документа,

3.Заштите података у покрету ради боље и интелигентније интеграције са DLP, WEB gateway и осталим производима за заштиту параметара и крајњих уређаја,

4.Заштите садржаја,

5.Интеграције са системима за архивирање.

Класификација документа мора да буде усклађена са правилима контроле приступа.

Посебном процедуром се могу дефинисати радње за поступање, обраду, складиштење и пренос података.

Процедура о поступању са имовином мора да подразумева:

1.ограничења приступа која подржавају захтеве за заштиту сваког нивоа класификације,

2.одржавање званичног записа о овлашћеним примаоцима имовине,

3.заштиту привремених или трајних копија података на нивоу који је у складу са заштитом оригиналне информације,

4.складиштење информационе имовине у складу са спецификацијама произвођача,

5.јасно обележавање свих копија медија на које овлашћени прималац треба да обрати пажњу.

Ограничење приступа подацима и средствима за обраду података

Члан 12.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности података и Шемом класификовања података према члану 11. овог акта. Топличка академија струковних студија ће формирати Контролну листу приступа која садржи попис свих информационих објеката и субјекте који им могу приступити.

Корисницима је дозвољен приступ само мрежи и мрежним услугама за чије коришћење су овлашћени.

Топличка академија струковних студија ће посебним документом уредити приступ мрежи и мрежним уређајима.

Садржај процедуре о приступу мрежи и мрежним уређајима:

1.листа мрежа и мрежних услуга којима је приступ дозвољен;

2.начини ауторизације ради утврђивања коме је одобрен приступ, којој мрежи и којим услугама;

3.начин управљања заштитом приступа мрежним прикључцима и услугама;

4.средства која се користе за приступ мрежама и мрежним услугама;

5.захтеви у погледу верификације корисника за приступ различитим мрежним услугама;

6.начини надгледања коришћења мрежних услуга.

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему

Члан 13.

Топличка академија струковних студија управља приступом ИКТ систему и услугама кроз употребу корисничких 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.коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење;

3.корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;

4.периодично идентификовање и уклањање или онемогућавање вишеструких корисничких идентификатора;

5.вишеструки идентификатори неког корисника се не издају другим корисницима.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за приступ и јединствена шифра за приступ, који се не смеју делити са другим корисницима.

Додељивање привилегованих (администраторских) права на приступ врши Руководилац послова информационих система и технологија.

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 редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

Шифре за приступ општим корисничким идентификаторима администратора се мењају променом корисника.

Топличка академија струковних студија по потреби врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај

запослења).

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

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 14.

Аутентификација корисника којима је одобрен приступ систему врши се путем јединственог корисничког имена и шифре.

Сви корисници су дужни да:

1.корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;

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).

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.

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

Члан 15.

Топличка академија струковних студија 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 спречавање оштећења и ометања информација.

Зона раздвајања и успостављање система физичке безбедности

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

У складу са Актом о процени ризика у заштити лица, имовине и пословања дефинисане су следеће зоне раздвајања:

1.зоне раздвајања у згради или на локацији која садржи опрему за обраду информација су физички исправне, а сва спољна врата су потпуно заштићена од неовлашћеног приступа помоћу контролних механизама,

2.постављене су пријавнице са особљем или друга средства за контролу физичког

приступа до локације или зграде и приступ локацијама или зградама је ограничен само на овлашћено особље,

3.пожарна врата у безбедносној зони раздвајања су под надзором и испитана су на споју са зидовима како би се успоставио потребан ниво отпорности у складу са одговарајућим регионалним, националним и међународним стандардима и функционишу у складу са локалним противпожарним правилима у погледу осигурања од отказа,

4.постављена је опрема за праћење контролу приступа просторијама са рачунарима или просторијама за комуникације, а постављање система техничке заштите и алармних система извршено је у складу са националним, регионалним или међународним стандардима,

5.опрема за обраду информација којом управља Академија струковних студија физички је одвојена од оне којом управљају трећа лица.

Контрола физичког уласка

Безбедносне области требају бити заштићене одговарајућим контролама уласка како би се осигурао приступ само овлашћеним појединцима.

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 областима у којима се обрађују или чувају поверљиве информације треба да буде ограничен само на овлашћене особе;

3.треба безбедно одржавати и надгледати евиденцију или електронску проверу свих приступа;

4.лицима која су запослена код пружаоца услуга обезбеђења треба одобрити ограничен приступ безбедносним областима или опреми за обраду осетљивих података, и омогућити им приступ када за то постоји неизоставна потреба, а овакав приступ треба да буде одобрен и надгледан у сваком тренутку;

5.права приступа безбедносним областима треба редовно преиспитивати и ажурирати, а уколико постоји потреба и укинути.

Заштита канцеларија, просторија, средстава, као и заштита од претњи екстерних фактора из окружења.

Топличка академија струковних студија обезбеђује и примењује одговарајућу контролу приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава. Такође, безбедним конфигурисањем се онемогућава приступ кључној опреми а у циљу спречавања видљивости поверљивих информација, активностима споља. Физичка заштита се мора планирати и за случајеве природних катастрофа, непријатељских напада или несрећа.

Рад у безбедносним зонама

Безбедносне зоне подлежу следећим мерама заштите:

1.особље мора бити обавештено 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 чија провера се врши периодично,

4.не дозвољава се уношење фотографских, видео, аудио или других уређаја за записивање, осим уз претходно одобрење одговорног лица.

Евиденцију о уласку у безбедносну зону врши Администратор послова информационих система и технологија.

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

Члан 16.

Постављање и заштита опреме

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа, 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 особама;

3.Врши се редовна контрола система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, електронске комуникације и сл.;

4.Просторије са опремом треба редовно чистити од прашине;

5.Забрањује се конзумирање хране и пића или пушење и коришћење запаљивих средстава у близини опреме за обраду информација;

6.Редовно се прате температура и влажност ваздуха;

7.Опрема мора бити заштићена од атмосферских падавина.

Администратор информационих система и технологија редовно прати услове околине, као што су температура и влажност, који би могли негативно да утичу на рад опреме за обраду информација.

Помоћне функције за подршку

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.

Безбедносни елементи приликом постављања каблова

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од прислушкивања, ометања или оштећења на следећи начин:

1.водови 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.активна мрежна опрема се мора налазити у закључаним орманима,

4.неовлашћено прикључење уређаја на каблове се врши техничким претраживањем и физичком провером,

5.приступ до разводних табли и у просторије са кабловима се контролише.

Одржавање опреме

Опрема се одржава како би се осигурали 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 обавља само особље овлашћено за одржавање,

3.о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи,

4.осетљиве информације треба избрисати из опреме,

5.пре враћања опреме у рад након одржавања, потребно је исту прегледати како би проверили да није неовлашћено коришћена или оштећена.

Измештање и премештање имовине

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

1.треба да се одреде запослени и спољни корисници који имају овлашћење да одобре измештање имовине;

2.треба да се поставе временска ограничења за измештање опреме и да се проверава усклађеност приликом повратка;

3.треба документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања и ова документација треба да буде враћена са опремом, информацијама или софтвером.

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

Безбедно расходовање или поновно коришћење опреме

Сви 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.

Безбедност опреме корисника без надзора

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

Остављање осетљивих и поверљивих докумената и материјала

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 по следећој процедури:

1.Све осетљиве и поверљиве информације у штампаном или електронском облику запослени морају одложити на сигурно место на крају радног дана или када нису присутни на свом радном месту,

2.Рачунари морају бити закључани корисничким налозима у одсуству запосленог, и угашени на крају радног дана,

3.Ормари 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.Лаптопови морају бити везани уз помоћ одговарајуће опреме која их штити од крађе или закључани у фиоци. Таблети и остали преносни уређаји морају бити закључани у фиоци,

5.Носачи података као што су дискови и flash 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.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 17.

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 информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевима измештања делова ИКТ система.

Усвајање и примена радних процедура

Топличка академија струковних студија успоставља радне процедуре које садрже инструкције за детаљно извршење следећих послова:

1.инсталација и конфигурација система,

2.обраду и поступање са информацијама (аутоматски и мануелно),

3.израда резервних копија,

4.обрада захтева за временски распоред активности,

5.израда инструкција за поступање у случају грешке или у другим ванредним ситуацијама која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција,

6.утврђивање листе контаката за подршку (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа,

7.израда инструкција за управљање поверљивим подацима,

8.процедуре за поновно покретање система и опоравак, које се користе у случају отказа система,

9.управљање системским записима (логовима),

10.процедуре за надгледање.

За усвајање, измене и допуне радних процедура овлашћен је Руководилац послова информационих система и технологија.

Управљање расположивим капацитетима

Коришћење ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе система. Периодично се спроводе слеће активности:

1.брисање застарелих података,

2.повлачење из употребе апликација, система, база података или окружења,

3.оптимизација серије процеса и распореда,

4.одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису критичне за пословање.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 18.

Злонамерни софтвер обухвата све програме који су направљени у намери да онемогуће или отежају рад или оштете неки умрежен или не умрежен рачунар. Заштита од злонамерног софтвера се заснива на софтверу за откривање злонамерног софтвера и отклањање штете, на познавању информационе безбедности, као и на одговарајућим контролама приступа систему и управљању захтеваним и потребним променама.

Поступак контроле и предузимање мера против злонамерног софтвера

Топличка академија струковних студија одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Садржај процедуре о заштити од злонамерног софтвера:

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 од или преко спољних мрежа, или на било ком другом медијуму,

указујући на то које заштитне мере треба предузети,

4.спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе, а присуство било каквих неодобрених датотека или неауторизованих допуна треба формално истражити,

5.инсталирање и редовно ажурирање софтвера за откривање злонамерног софтвера и опоравак ради претраживања рачунара и медијума као контролу из предострожности, или на рутинској основи.

Листа провера коју је потребно спроводити:

1.проверу, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер,

2.проверу, пре коришћења, садржаја прилога електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер; ову проверу треба спроводити на разним местима, нпр. на серверима за електронску пошту, на стоним рачунарима или приликом уласка у мрежу оператора ИКТ система,

3.проверу постојања злонамерних софтвера на веб-страницама,

4.дефинисање процедура за менаџмент и одговорности за поступање са заштитом од злонамерног софтвера у системима, обука за њихово коришћење, извештавање и опоравак од напада злонамерним софтвером,

5.припрему одговарајућих планова за континуитет пословања приликом опоравка од напада злонамерним софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак,

6.имплементацију процедура за редовно прикупљање информација, као што је претплата на адресне спискове за доставу или провера веб-страница на којима се дају информације о новим злонамерним софтверима,

7.имплементацију процедура за верификовање информација о злонамерним софтверима и обезбеђење да су упозоравајући извештаји тачни и информативни; руководиоци треба да осигурају да се за разликовање лажних од стварних злонамерних софтвера користе квалификовани извори, нпр. проверени часописи, поуздане странице на Интернет мрежи или испоручиоци програма против злонамерних софтвера; сви корисници треба да буду свесни проблема појаве духовитих или злонамерних обмана и онога што треба да раде после њиховог пријема.

О процедурама и мерама о антивирусној заштити и процедури о подизању свести запослених о информационој безбедности Руководилац послова информационих система и технологија упознаје све запослене/кориснике информационог система.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Администратору информационих система и технологија у Одсеку.

У циљу заштите од упада у ИКТ систем, Администратор информационих система и технологија у Одсеку је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета Администратор информационих система и технологија у Одсеку може укинути приступ.

Заштита од губитка података

Члан 19.

Топличка академија струковних студија 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.

Резервне копије информација и података

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих и log фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Администратор информационих система и технологија у Одсеку извршава следеће задатке:

1.процењује осетљиве и критичне податке за које је потребно правити резервне копије;

2.креира план прављења резервних копија;

3.прави заштитне копије серверског оперативног система и података, комуникационог оперативног система и конфигурационих фајлова, апликација, сервиса и база података;

4.верификује успешно прављење резервних копија;

5.води евиденцију урађених резервних копија;

6.одлаже копије на безбедно место;

7.тестира исправност резервних копија и процедуре за прављење заштитних копија;

8.рестаурира податке са резервних копија.

План израде резервних копија информација обухвата следеће:

1.тачне и потпуне записе о резервним копијама и документоване процедуре обнављања,

2.обим и учесталост израде резервних копија,

3.резервне копије треба да одражавају пословне потребе организације и критичност тих информација по континуитет пословања организације,

4.треба их ускладиштити на локацији на довољној удаљености, како би се избегло свако оштећење на главној локацији,

5.резервним копијама информација треба дати одговарајући ниво физичке заштите и заштите од утицаја околине који је доследан мерилима која се примењују на главној локацији,

6.медијуме са резервним копијама треба редовно проверавати, ради сигурности њихове употребе у ванредним ситуацијама и када је то неопходно.

За примену мера заштите од губитка података одговоран је Администратор информационих система и технологија у Одсеку.

Обезбеђивање интегритета софтвера и оперативних система

Члан 20.

Топличка академија струковних студија 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 оспособљени администратори, по добијању одговарајућег овлашћења од руководиоца,

2.оперативни системи треба да садрже само одобрене извршне кодове, а не и развојне кодове или компилаторе,

3.апликације и оперативни системски софтвер треба имплементирати тек после обимног и успешно спроведеног испитивања, које обухвата испитивање применљивости, безбедности, утицаја на друге системе и погодности за коришћење, а треба их спроводити на засебним системима, односно тестним окружењима,

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 треба сачувати претходне верзије апликативног софтвера.

Инсталацију и подешавање софтвера може да врши само Администратор информационих система и технологија, односно запослени - корисник који има овлашћење за то.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 21.

Актом о процени ризика у заштити лица, имовине и пословања Топличке академије струковних студија извршена је анализа ИКТ система и утврђен степен изложености ИКТ система потенцијалним безбедносним слабостима.

Ограничења у погледу инсталације софтвера

Забрањено је свако инсталирање софтвера на свим уређајима које може довести до изложености ИКТ система безбедносним ризицима.

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

Члан 22.

Заштита података који се преносе комуникационим средствима унутар Академије струковних студија Јужна Србија, између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

Правила коришћења електронске поште:

1Употреба 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 нежењена пошта биће уклоњена ради даљег несметаног наставка коришћења платформе за пријем и слање електронске поште.

Правила коришћења Интернета

1.Приступ садржајима на Интернету је дозвољен искључиво за пословне намене. На мрежи је омогућено надгледање, односно користи се поступак периодичне ревизије и контролисања логовања, како на пријему тако и на слању.

Правила коришћења информационих ресурса

1.Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намену коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

Размена електронских порука

Заштита информација укључених у размену електронских порука се регулише Процедуром о безбедности у размени електронских порука која треба да обухвати:

1.заштиту порука од неовлашћеног приступа, модификовања или одбијања услуга које су у складу са класификационом шемом коју је усвојио Оператор ИКТ система,

2.осигурање исправног адресирања и транспорта поруке,

3.поштовање законских одредби, на пример захтеве за електронске потписе,

4.добијање одобрења пре коришћења јавних спољних услуга, као што су размена хитних порука, приступ и коришћење друштвене мреже или заједничко коришћење датотека,

5.строже нивое утврђивања веродостојности, контролисањем приступа из мрежа са јавним приступом.

3. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Академије струковних студија Јужна Србија

Члан 23.

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

Ступање на снагу Акта о безбедности

Члан 24.

Овај Акт о безбедности ступа на снагу осмог дана од дана објављивања на огласној табли Академије.

Председник Привременог Савета Академије

Милош Ђокић, дипл.правник.

ПОТВРДА О СТУПАЊУ НА СНАГУ
АКТА О БЕЗБЕДНОСТИ
ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА
ТОПЛИЧКА АКАДЕМИЈА СТРУКОВНИХ СТУДИЈА

Акт о безбедности информационо-комуникационог система објављен је на огасној табли Академије 11.10.2022.године и ступа на снагу дана 19.10.2022.године.

Председник Привременог Савета
Топличке академије струковних студија
Милош Ђокић, дипл.правник