Висока школа струковних
студија за образовање
васпитача у Кикинди

У Кикинди,
Број: 421-6

Правилник о безбедности информационо-комуникационог система Високе школе струковних студија за образовање васпитача у Кикинди

2023.

САДРЖАЈ

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16 и 94/17), 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), Савет Високе школе струковних студија за образовање васпитача у Кикинди на седници одржаној_____ дононео је:

Правилник о безбедности информационо-комуникационог система Високе школе струковних студија за образовање васпитача у Кикинди

I ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Правилником о безбедности информационо-комуникационог система Високе школе струковних студија за образовање васпитача у Кикинди (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 Високе школе струковних студија за образовање васпитача у Кикинди (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Правилника о безбедности информационо-комуникационог система 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.

Значење појединих термина

Члан 3

Поједини термини у смислу закона којим се уређује ова област имају следеће значење:

1. **Информационо-комуникациони систем (ИКТ систем)** је технолошко-организациона целина која обухвата:
   a) електронске комуникационе мреже у смислу закона који уређује електронске комуникације
   b) 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
   c) податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из подтачке (а) и (б) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања
   d) организациону структуру путем које се управља ИКТ системом;
   e) 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 односно обезбеђивање доступности информација само овлашћеним корисницима информатичких ресурса, као и немогућност приступа информацијама лицима која немају таква овлашћења ;
5. **Интегритет** значи очуваност изворног садржаја и комплетности податка односно немогућност неовлашћене измене информација;
6. **Расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан односно доступност информација корисницима информатичких ресурса у обиму корисничког овлашћења;
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. **Јединствени систем за пријем обавештења о инцидентима** је информациони систем у који се уносе подаци о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности;
13. **Мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
14. **Тајни податак** је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
15. **ИКТ систем за рад са тајним подацима** је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
16. **Служба безбедности** је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије;
17. **Компромитујуће електромагнетно зрачење (КЕМЗ)** представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
18. **Криптобезбедност** је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
19. **Криптозаштита** је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
20. **Криптографски производ** је софтвер или уређај путем кога се врши криптозаштита;
21. **Криптоматеријали** су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
22. **Безбедносна зона** је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
23. **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;
24. **Услуга информационог друштва** је услуга у смислу закона којим се уређује електронска трговина;
25. **Пружалац услуге информационог друштва** је правно лице које је пружалац услуге у смислу закона којим се уређује електронска трговина.
26. **MAC адреса (Media Access Control Adress)** је јединствени број, којим се врши идентификација уређаја на мрежи
27. **VPN (Virtual Private Network)** је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију
28. **Download** је трансфер података са централног рачунара или web презентације на локални рачунар
29. **UPS (Uninterruptible power supply)** је уређај за непрекидно напајање електричном енергијом
30. **Opensource** је софтвер отвореног кода

31. **Firewall** је „заштитни зид“ односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности
32. **USB или флеш меморија** је спољашњи медијум за складиштење података
33. **CD-ROM (Compact disk – read only memory)** се користи као медијум за снимање података
34. **DVD** је оптички диск високог капацитета који се користи као медијум за складиштење података
35. **Backup** је резервна копија података
36. **Freeware** је бесплатан софтвер
37. **Администраторско овлашћење** је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;
38. **Кориснички налог** јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно, овлашћења корисника и нивое компетенција);
39. **Администраторски налог** јесте јединствен налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога, и додељује се искључиво администратору.

Обавеза примене одредби Акта о безбедности

Члан 4.

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

Овај акт је обавезујући за све организационе целине Школе и за све кориснике информатичкх ресурса, као и за сва трећа лица која користе информатичке ресурсе Школе.

Запослени у Високој школи струковних студија за образовање васпитача у Кикинди 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.

Директор Школе одговоран је за спровођење мера безбедности регулисане овим Актом и интерним процедурама.

Руководилац послова ИКТ одговоран је 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 5.

Запослени у Високој школи струковних студија за образовање васпитача у Кикинди 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.

Сви запослени су у обавези на примену тајности података које је регулисано законом или интерним актима Школе.

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

Предмет заштите

Члан 6.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, 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.

II МЕРЕ ЗАШТИТЕ

Члан 7.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Школе, 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.

Предмет заштите су:

1. хардверске и софтверске компоненте информатичких ресурса;
2. подаци који се обрађују или чувају на информатичким ресурсима;
3. кориснички налози и други подаци о корисницима информатичких ресурса у Школи.

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру ВШССОВ у Кикинди

Члан 8.

Висока школа струковних студија за образовање васпитача у Кикинди овим Актом утврђује начин доделе овлашћења за приступ ИКТ систему и начин одобравања приступа запосленима од стране директора Школе, односно непосредно надређеног лица или руководиоца за ИКТ.

Висока школа струковних студија за образовање васпитача у Кикинди у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

Директор Школе је дужан да донесе појединачни акт или да у складу са актом о организацији и систематизацији радних места одреди одговорна лица за обезбеђивање и праћење безбедности информационог система Високе школе струковних студија за образовање васпитача у Кикинди.

Интерни акти и друга документа која уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу су:

- Правилник о унутрашњој организацији и систематизацији радних места
- Уговори о раду
- Изјаве о поверљивости
- Уговори о чувању поверљивости са правним лицима
- Правилник о приступу посебно осетљивим подацима и информацијама у ИКТ систему уколико постоје

Посебним актом утврђује се одговорност запослених и одговорног лица и прописује дисциплинска одговорност у случају непоштовања одредби које уређују информациону безбедност.

Информатички ресурси Школе

Члан 9.

Информатички ресурси Школе су сви ресурси који садрже пословне информације Школе у електронском облику, или служе за приступ корисника ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и слично.

Корисник информатичких ресурса

Члан 10.

Корисник информатичких ресурса јесте постављено лице, запослено лице на одређено или неодређено време, лице ангажовано по основу уговора, консултант или друго радно ангажовано лице коме је одобрен приступ неком информатичком ресурсу Школе.

Корисник информатичких ресурса одговоран је за правилну употребу, тачност и сигурност података приликом коришћења информатичких ресурса Школе, односно, лично је одговоран за остваривање својстава података у ИКТ систему Школе.

Корисник информатичких ресурса нема имовинска права над информатичким ресурсима Школе.

Дужности корисника информатичких ресурса

Члан 11.

Корисник не сме спроводити активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система Школе.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне сврхе, а Школа задржава право да информатичке ресурсе повуче у било ком тренутку и у потпуности задржи све податке, без обавезе да их накнадно преда кориснику.

Корисник непреносиве радне станице је дужан да пословне податке смешта на одређене мрежне дискове на серверу Школе.

Изузетно од става 3. овог члана, због потребе посла, подаци се могу привремено сместити на локални диск непреносиве радне станице, ако се са тим сагласи директор Школе.

Корисник преносиве радне станице има право да привремено смешта пословне податке на локални диск преносиве радне станице, као и обавезу да уради копију докумената са локалног диска на мрежни диск сервера Школе.

Запослено, односно ангажовано лице у Школи са администраторским овлашћењима (у даљем тексту: администратор), као и лица која су задужена за израду резервних копија, дужни су да дневно израђују резервне копије података са мрежних дискова Школе.

Корисник информатичких ресурса дужан је да поштује следећа правила безбедног и примереног коришћења информатичких ресурса и то да:

1) користи информатичке ресурсе искључиво у пословне сврхе;
2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Школе и да могу бити предмет надгледања и прегледања;
3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4) безбедно чува своје лозинке, односно, да их не одаје другим лицима;

5) пре сваког удаљавања од радне станице одјави се са ситема („log out“);
6) користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење директора Школе, а на основу образложеног предлога корисника;
7) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране стручних органа школе;
8) обезбеди сигурност података у складу са важећим прописима;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права/нивоа компетенције;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) не сме да на радној станици складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (backup) података, у складу са прописаним процедурама;
13) користи Internet и Internet e-mail сервис у Школи у складу са прописаним процедурама;
14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, upgrade firmware, покретање антивирусног програма и сл.) обављају у утврђено време;
15) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
16) прихвати да технике сигурности (антивирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;
17) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер;
18) се уздржи од активности којима се изазива неоправдано оптерећење информатичких ресурса Школе, као и повећано ангажовање особља на одржавању тих ресурса;
19) не сме неовлашћено да објављује или преноси личне податке до којих је дошао коришћењем информатичких ресурса Школе, као што су лозинке, бројеви платних картица, приватни телефонски бројеви и слично и да тиме повреди приватност појединаца;
20) се уздржи од неуобичајено и неоправдано великог коришћења информатичких ресурса Школе, а посебно у приватне сврхе.

Основна правила сигурности информација

Члан 12.

При дефинисању организационо-техничких мера заштите података неопходно је поштовати следећа основна правила:

- разграничење дужности,
- правило „неопходно да зна“ (need-to-know),
- процена ризика,
- перманентна контрола и
- перманентно усавршање постојећих решења.

Разраничење дужности

Циљ разграничења дужности је да се спрече нежељене појаве и инциденти. Ово се може постићи расподелом задатака и доделом корисничких налога од којих је сваки за специфичан пословни процес.

Приступни параметри за сваки део информационог система чувају се у листи за чију се безбедност брине Руководилац послова за ИКТ.

Правило „Неопходно да зна“(need-to-know)

Корисници могу да имају приступ само информацијама или функционалностима које су неопходне за правилно извршење њихових пословних задатака. Приступ информационим ресурсима мора бити експлицитно одобрен са јасном разликом између потребе да се подацима само приступи (енг. „read only“) и потребе да се подаци мењају (енг.„write“).

Процена ризика

Одговарајуће мере сигурности информација заснивају се напословним захтевима, као и на проценама ризика, економској ефикасности и законским ограничењима. С обзиром на то да ниједан информациони систем никада не може да буде потпуно сигуран, треба проценити прихватљив ниво ризика након примене мера безбедности.

Перманентна контрола

Морају се вршити периодичне ревизије (минимум једном годишње) и провере како би се пратила општа усаглашеност са захтевима заштите информација, као и да би се открише сигурносне слабости или недостаци за које постоји сумња да могу утицати на ниво заштите информација.

Перманентно усавршање постојећих решења

Неопходно је вршити ревизију организационо-техничких решења у складу са променама у окружењу, након великих промена на информационом систему или у оквиру бизнис процеса, са циљем брзог и ефикасног реаговања и одржавања жељеног нивоа безбедности.

Безбедносни профил корисника информатичких ресурса

Члан 13.

У зависности од описа задатака, послова радног места на које је распоређен и нивоа компетенције, корисник информатичких ресурса, на предлог директора Школе, стиче одређена права приступа ИКТ систему Школе.

Администраторска овлашћења могу добити само лица која су задужена за одржавање информатичких ресурса у Школи, уз претходну сагласност директора Школе.

Креирање лозинке

Члан 14.

Лозинка мора да садржи минимум шест карактера, комбинованих од малих и великих слова , цифара и специјалних знакова.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке.

Ако корисник информатичких ресурса посумња да је друго лице открило његову лозинку, дужан је да се писмено обрати администратору који ће му лозинку променити, или је може сам променити ако му је дато то право.

Иста лозинка се не сме понављати у периоду од годину дана.

Употреба корисничког налога

Члан 15.

Кориснички налог може употребљавати само корисник информатичких ресурса коме је налог издат.

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору у случају подешавања радне станице.

Корисник информатичких ресурса је непосредно одговоран за активности које су реализоване на основу његовог корисничког налога.

Кориснички налози са администраторским овлашћењима користе се само за потребе неопходних интервенција којима се обезбеђује несметан рад информатичких ресурса (у даљем тексту: информатичке интервенције).

Употреба администраторског налога

Члан 16.

Администраторски налози свих пословних апликација, сервера база података и системских апликација за управљање мрежном опремом и уређајима за складиштење података чувају се у затвореним, непровидним ковертама са отиском службеног печата, у сефу Школе , коме има приступ само директор Школе или лице које он овласти.

Право коришћења администраторског налога имају само администратори за потребе информатичких интервенција.

Поступци у случајевима сигурносних инцидената

Члан 17.

Корисник информатичких ресурса дужан је да, без одлагања, пријави директору Школе у ком се инцидент десио свако уочавање или сумњу о наступању инцидената којим се угрожава сигурност ИКТ система.

Информацију о инциденту руководилац става 1. овог члана дужан је да одмах проследи администратору.

По пријави инцидента мора се поступати адекватно и ефикасно, а по хитном поступку у случајевима:

1) нарушавања поверљивости информација,
2) откривања вируса или грешака у функционисању апликација,
3) вишеструких покушаја неауторизованог приступа,
4) системских падова и престанка рада сервиса и пада целог сервера.

Руководилац сектора је дужан да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести директора Школе, у складу са законом којим се уређује информациона безбедност.

Заштита од малициозног софтвера

Члан 18.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена:

1) лиценцираног софтвера, односно, забрана коришћења неауторизованог софтвера
2) правила за заштиту од ризика приликом преузимања фајлова из екстерних извора (података, апликација и сл.).

Приликом преузимања фајлова из става 1. тачка 2) овог члана преносиви медији пре коришћења морају бити проверени на присуство вируса.

Ако се утврди да преносиви медиј садржи вирусе, врше се чишћења медија од вируса, уз сагласност доносиоца медија.

Ризик од евентуалног губитка података, приликом чишћења медија антивирусним софтвером, сноси доносилац медија.

Инсталација и одржавање софтвера

Члан 19.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужени су администратори, који су дужни да поступају у складу са прописаним процедурама и упутствима.

Директор Школе обезбеђује запосленом, односно, ангажованом лицу, коришћење радне станице (десктоп или лаптоп) са преинсталираним и правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачки програми (драјвери), пословно и развојно окружење, софтвер за антивирусну заштиту, разне помоћне апликације), који је типски за све радне станице и који преставља минимум потребан за обављање стандардних послова радних места у Школи.

Администратор врши оцену конзистентности траженог софтвера са постојећим инсталираним софтвером на предметној радној станици и, уколико оцени да тражени софтвер неће угрозити или ометати рад, инсталираће захтевани софтвер, и то искључиво лиценцирану или бесплатну верзију.

Основна подешавања из става 2. овог члана су:

1) додељивање имена и TCP/IP адресе радној станици и њено придруживање домену;
2) подешавање mail клијента;
3) подешавање web претраживача;
4) инсталација лиценцираног антивирус софтвера, одобреног од стране директора Школе;
5) инсталација званичног апликативног софтвера који одређени делови Школе користе у свом раду.

У случају да је кориснику информатичких ресурса потребно да се изврши инсталација одређеног специфичног софтвера на радној станици, електронским путем, подноси образложени захтев директору Школе.

Корисник информатичког ресурса дужан је да сваки проблем у функционисању оперативног система, mail клијента, web претраживача, пословног софтвера (MS Office или Open Office) и апликативног софтвера, пријави руководиоцу стручног већа, који ову информацију прослеђује електронским путем администратору система или администраторима система директно.

Проблем у функционисању антивирусног софтвера мора се пријавити без одлагања.

Администратор је дужан да проблеме из става 6. и 7. овог члана отклони у најкраћем могућем року на локацији корисника, даљинском конекцијом ка радној станици или одношењем радне станице у сервис за поправку.

Сигурност електронске поште

Члан 20.

У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

1) електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;

2) забрањено је коришћење електронске поште у приватне сврхе, као и коришћење приватних налога електронске поште у пословне сврхе.

Поступање са преносивим медијима

Члан 21.

Преносиви медији који садрже податке морају да буду прописно обележени , потписани и чувани на безбедном месту, код овлашћеног лица.

У случају да је потребно брисање података који се налазе на преносивим медијима, неопходно је обезбедити њихово неповратно брисање.

Уколико се донесе одлука о стављању одређених преносивих медија ван употребе, они тада, приликом стављања ван употребе, морају бити физички уништени.

Физичка сигурност информатичких ресурса

Члан 22.

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови:

1) сервиси, сторици (storage) и комуникационо чвориште у просторијама Школе морају бити смештени у посебној просторији (сервер соби), која испуњава стандарде противпожарне заштите и поседује редудантно напајање електричном струјом и адекватну климатизацију, као и видео надзор, са забраном приступа незапосленим лицима;
2) приступ сервер соби, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење директора Школе;
3) радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;
4) просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
5) штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;
6) медији са поверљивим подацима (USB и екстерни hard diskovi) морају бити заштићени од неауторизованог приступа и прегледа.

Приступ ИКТ систему Школе

Члан 23.

Приступ свим компонентама ИКТ система мора бити аутентификован.

Администратор, на основу прецизног писаног захтева , додељује кориснику информатичког ресурса корисничко име, лозинку и привилегије, као и налог за електронску пошту.

Кориснику информатичких ресурса додељују се само привилегије које су неопходне за реализацију његових радних обавеза.

У случају престанка радног односа, или радног ангажовања у Школи, кориснику информатичког ресурса укида се право приступа ИКТ систему.

У случају одсуства са посла у периоду дужем од месец дана (у законом предвиђеним случајевима), кориснику информатичког ресурса се привремено укида право приступа ИКТ систему, до повратка на посао.

О престанку радног односа или радног ангажовања, одсуству са посла дужем од месец дана, као и о промени радног места корисника информатичких ресурса, секретар је дужан да обавести директора Школе ради укидања, односно, измена приступних привилегија тог корисника.

Корисник информатичких ресурса, након престанка радног ангажовања у Школи, не сме да открива поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система.

Корисник информатичких ресурса не може имати удаљени (remote) приступ ИКТ систему. Удаљени приступ може имати искључиво администратор, или лице које овласти директор Школе.

Трећем лицу се могу одобрити права приступа ИКТ систему уз претходно склапање одговарајућег уговора, којим се прецизно дефинишу услови и обим права приступа, укључујући и све релевантне безбедносне захтеве.

Изузетно од става 8. овог члана, у случају неопходних и хитних послова, могу се одобрити права приступа трећем лицу по усменом налогу директора Школе, односно, овлашћеног лица, о чему ће се накнадно, по завршетку хитног посла, сачинити записник о оствареном приступу.

Ако се установи повреда уговорне обавезе или прекорачење овлашћења по основу уговора, одобрени приступ се одмах укида.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 24.

Висока школа струковних студија за образовање васпитача у Кикинди 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.

Ауторизованим корисницима није дозвољено да користе мрежу Високе школе струковних студија за образовање васпитача у Кикинди за активности које нису у домену пословних

активности, радних и других задатака у вези са послом и предметом рада појединачно запосленог.

Термин мобилни уређај укључује: преносиве рачунаре, мобилне телефоне, есктерне меморијске медијуме (диск, УСБ кључ, и слично).

Радни однос за обављање послова ван просторија послодавца обухвата:

- Рад на даљину
- Рад од куће

Приликом удаљеног приступа ИКТ добрима неопходна је примена додатних мера заштите, укључујући аутентикацију на два нивоа, односно проверу приликом приступања ИКТ систему и проверу приликом приступања ИКТ подсистему. Приступање ИКТ систему и ИКТ подсистему могуће је ако корисник зна одговарајуће лозинке.

Приликом коришћења мобилних уређаја мора се обезбедити заштита пословних података и смањити ризике коришћења мобилних уређаја у незаштићеним окружењима (јавним местима, мрежама са непознатом или недовољном заштитом и слично).

За коришћење информатичких сервиса који су стандардно доступни преко интернета, а преко приватног мобилног уређаја запосленог, као на пример електронска пошта, нису потребне посебе сагласности.

Службени мобилни уређаји су у надлежности Високе школе струковних студија за образовање васпитача у Кикинди и издају се запосленима ради коришћења приликом обављања службених обавеза.

Приликом коришћења бежичних мрежа морају се примењивати мере заштите бежичних мрежа предложене од стране Руководиоца послова за ИКТ.

Приликом коришћења службеног рачунара за приступ са удаљене локације мрежи ВШССОВ у Кикинди, ауторизовани корисник не сме истовремено бити повезан и на неку другу мрежу која може угрозити безбедност комуникације

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 ВШССОВ у Кикинди

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.

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

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

Висока школа струковних студија за образовање васпитача у Кикинди 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.

Сваки нови запослени може добити приступ информационим и техничким ресурсима тек пошто прође одговарајућу обуку за рад, упозна се са прихватљивом употребом информатичких ресурса.

Директор Високе школе струковних студија за образовање васпитача у Кикинди је дужан да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази у примени код Високе школе струковних студија за образовање васпитача у Кикинди.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код ВШССОВ у Кикинди

Члан 25.

Запослени 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. 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:

- Процедуром о правима приступа информационом систему
- Уговором о раду
- Уговором о ангажовању лица ван радног односа
- Споразумом о поверљивости

Приликом престанка радног односа запосленог, преласка запосленог на друге послове или престанка сарадње са пословним партнером, потребно је да директор Школе информише запосленог, односно пословног партнера, о свим захтевима везаним за заштиту информација и подсети га на законске обавезе из области заштите информација.

Измена одговорности или промена послова морају се третирати као престанак тренутних одговорности, а нове одговорности разматрати као да се ради о запошљавању и закључењу новог уговора или споразума.

За поступања приликом престанка запослења или ангажовања задужен је Руководилац послова ИКТ, који предузима следеће активности:

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату;
- прегледа све налоге и приступе систему који су били доступни запосленом;
- преузима од запосленог електронске и друге мобилне уређаје;
- проверава враћене мобилне уређаје и уређаје за преношење података;
- даје налог за укидање налога електронске поште, сертификате и свих других права приступа систему ВШССОВ у Кикинди на дан престанка радног односа или другог основа ангажовања бившег запосленог;
- прегледа све налоге за приступ одлазећег запосленог и прикупља приступне шифре и кодове са циљем укидања/промене истих на дан одласка;
- преузима кључеве, картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Школе.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 26.

Шеф рачуноводства води евиденцију о ИКТ добрима. Руководилац послова ИКТ мора бити упознат од стране шефа рачуноводства о ИКТ добрима, који може имати паралелно и своју евиденцију. ВШССОВ у Кикинди мора да:

- на ИКТ добра примењује мере заштите прописне Законом о информационој безбедности и актима ВШССОВ у Кикинди
- да мере заштите ИКТ добара примењује у складу са степеном осетљивости и критичности тих добара, узимајући у обзир могуће последице нарушавања поверљивости, интегритета и расположивости добара

Сви запослени, извођачи радова и пословни партнери морају бити на одговарајући начин упознати са правилима и одговорностима за коришћење информација и опреме за процесирање информација и у обавези су да их се придржавају.

Пописивање имовине

Члан 27.

Висока школа струковних студија за образовање васпитача у Кикинди 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. Висока школа струковних студија за образовање васпитача у Кикинди прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води служба рачуноводства и руководилац послова информационих система и технологија надлежног за послове ИКТ система.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај

Члан 28.

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

Висока школа струковних студија за образовање васпитача у Кикинди може у оквиру интерног акта о руковању имовином ближе да уређује правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација.

Запослени и екстерни корисници су обавезни да врате сву имовину Високој школи струковних студија за образовање васпитача у Кикинди коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

Током отказног рока запослених, Висока школа струковних студија за образовање васпитача у Кикинди контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности

Члан 29.

Мере заштите података који су, у складу са законом који уређује област тајности података, означени као тајни, одређују се у складу са прописима који регулишу ову област.

Избор и ниво примене мера заштите података се заснива на процени ризика, потреби за превенцијом ризика и отклањању последица ризика који се остварио, укључујући све врсте ванредних околности.

Висока школа струковних студија за образовање васпитача у Кикинди својим активностима генерише податке који су доступни јавности на увид. Откривање таквих података не изазива никакву штету. Подаци који су заштићени су лични подаци студената и лица укључених у процес рада Школе.

Заштита носача података

Члан 30.

Висока школа струковних студија за образовање васпитача у Кикинди обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, воде: директор, руководиоци организационих јединица, координатори наставе, наставници и библиотекар.

У циљу спречавања неовлашћеног приступа, модификовања, уклањања или уништења података постоје одговарајуће оперативне процедуре за заштиту, рад, транспорт и складиштење докумената и носилаца података (медијума за смештај података као дискови, екстерне меморије, "CD", "DVD" медијуми, документације о ИКТ добрима и системима и слично), као и процедуре за безбедно брисање података са носилаца података.

За размену информација ограниченог приступа морају се стандардизовати и користити одговарајуће техничке мере заштите и доследно их примењивати.

Обавезно је минимизовати коришћења преносних медијума. Пре коришћења преносни носачи информација морају се подвргнути провери средствима за заштиту од злонамерног софтвера. За коришћење преносних медијума потребна је дозвола директора Школе.

Обавезно је поуздано уништење података са носача података који се не користе. У случају немогућности поузданог уништења података мора се обавити физичко уништење носача.

Приликом рада са носиоцима података корисници се придржавају следеће процедуре:

- Корисник је дужан да процени поузданост носиоца података – поуздани носиоц је онај који је обезбедила Школа. Сви носиоци података из других извора морају да се проследе на проверу Руководиоцу послаова за ИКТ. После овакве провере може се приступити раду са носиоцем података.
- Корисник у току рада мора да има надзор над носиоцем података у сваком тренутку. Не сме се остављати носиоц података доступан другим лицима, како би се спречила могућност да дође до читања или уписа података од стране неовлашћеног лица.
- По завршетку рада корисник одјављује носиоц података са система и лично води рачуна о безбедности носиоца података или га предаје на чување Руководиоцу послаова за ИКТ.

Заштита носиоца података:

- Корисник је дужан да чува носиоце података на безбедном месту које је под његовим надзором или поверити чување Руководиоцу послаова за ИКТ.
- Проверу поседовања носиоца података дужан је да обавља на дневном нивоу.
- У случају нестанка носиоца података у најкраћем року обавештава Руководиоца послаова за ИКТ.

Транспорт ноциоца података:

- У случају да се носиоц података износи из просторија Школе корисник има обавезу да обезбеди сигурност истог.
- Корисник мора да зна које податке транспортује на носиоцу података, како би у случају нестанка носиоца података могло да се процени да ли постоји и колики је ризик по безбедност информационог система.
- У случају нестанка носиоца података приликом транспорта корисник је дужан да у најкраћем року обавести о нестанку Руководиоца послаова за ИКТ.

Складиштење носиоца података:

- Корисник је у обавези да носиоц података чува на безбедном, закључаном месту које је обезбеђено од могућности приступа неовлашћених лица.
- Безбедност места за складиштење корисник проверава свакодневно.
- О складиштењу носиоца података који нису додељени кориснику брине се Руководилац послаова за ИКТ.

Брисање носиоца података:

- Корисник је у обавези да приликом брисања података обезбеди да се податак избрише и из привремене меморије рачунара.
- Носиоц података који није предвиђен за брисање се уништава физички када више није потребан.
- Носиоц података који више није потребан кориснику, а који се не брише или уништава предаје се Руководиоцу послаова за ИКТ.

Ограничење приступа подацима и средствима за обраду података

Члан 31.

Корисницима се додељују минимална права приступа и привилегије за приступ ИКТ добрима, потребна за обављање пословних задатака, укључујући у то и приступ рачунарској мрежи и мрежним ресурсима.

Ограничење приступа подразумева:

- физичку контролу приступа (браве)
- административно ограничење приступа (раздвајање надлежности)
- техничка контрола приступа (корисници система са дефинисаним врстама приступа у оквиру мрежних уређаја, логови догађаја у систему, софтвер за заштиту од злонамерног софтвера, бекап података и слично).

Ограничење приступа врши се у складу са улогом корисника ИКТ система. Све методе контроле приступа морају се разматрати заједно. Приступ се ограничава уређајима које

корисник користи за приступ информационим и техничким ресурсима. Контрола минимално подразумева аутентикацију корисника и контролу приступа информационим услугама.

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

Члан 32.

Власник информација је Школа и она управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

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

Додељивање привилегованих (администраторских) права на приступ врши се на основу Уговора о раду.

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.

Школа једном годишње 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.

Корисници приликом напуштања радног места, морају предузети мере за заштиту радног места од неовлашћеног приступа. У току рада корисници морају да поштују правила „чистог стола“и „чистог екрана“ што значи да се напуштањем радног места, то место мора очистити од докумената, а рачунар закључати тако да је обавезна наредна операција пријава на систем (уношење корисничког налога и шифре).

Корисничко име и лозинке се морају користити као стандардно средство за верификацију идентитета корисника пре давања приступа информационом систему или услузи, у складу са овлашћењима корисника.

Рад корисника у оквиру оперативног система обавља се под корисничким налозима са ограниченим правима. Приступ оперативном систему омогућен је корисницима тек након што прођу процедуре идентификације и аутентификације.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 33.

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

Сви корисници су дужни да:

- корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
- избегавају чување корисничког имена и шифре у писаном облику;
- •промене шифру када примете да постоји било какав наговештај могућег компромитовања.

Шифре морају да:

- садрже најмање 6 алфанумеричких карактера;
- садрже најмање једно велико и једно мало слово
- садрже најмање једну цифру.

Шифре не заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и не смеју садржати више од 3 узастопна идентична бројчана или словна знака. Корисници су дужни да привремене шифре промене приликом првог пријављивања.

Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Члан 33.

Школа у свом пословању нема података које треба да заштити криптографски. Област у којој се користи криптографска заштита је дигитални потпис ради потврде аутентичности документа. Дигитални потпис се користи у складу са правилима издаваоца дигиталног сертификата.

Управљање кључевима

Члан 34.

Висока школа струковних студија за образовање васпитача у Кикинди примењује следеће методе за управљање кључевима које обухватају њихов цео животни циклус:

- генерисање кључева;

- издавање и добијање сертификата за јавне кључеве;
- складиштење кључева (кључеви се чувају на посебним уређајима или паметним картицама, на месту које је физички обезбеђено);
- дистрибуцију кључева (додела кључева намењеним ентитетима и активација самог кључа);
- замену или ажурирање кључева;
- поступак у случају компромитовања кључева;
- деактивацију кључева;
- обнављање изгубљених или оштећених кључева;
- прављење резервних копија или архивирање кључева;
- уништавање кључева;
- евидентирање и проверу активности у вези са управљањем кључевима.
- кључеви се могу користити само у периоду који одреди директор Школе.

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

Члан 35.

Неопходно је спречити неовлашћен физички приступ објектима, просторима, просторијама у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему.

Зона раздвајања и успостављање система физичке безбедности

Члан 36.

Опрема за обраду информација се штити закључавањем просторија у којима се налази. У складу са проценом ризика дефинисане су следеће зоне раздвајања:

- зоне раздвајања у згради или на локацији која садржи опрему за обраду информација треба да буду физички исправне (тј. не треба да постоје процепи у зони или области у којој би се лако могао десити упад); спољни кров, зидови и подови на тој локацији треба да буду од чврстог материјала, а сва спољна врата треба да буду потпуно заштићена од неовлашћеног приступа помоћу контролних механизама, нпр. решеткама, алармима, бравама итд.; врата и прозори треба да буду закључани у свим случајевима када су без надзора, а када су у питању прозори, треба размотрити спољну заштиту, посебно у приземљу;
- треба поставити пријавнице/дежуране са особљем или друга средства за контролу физичког приступа до локације или зграде; приступ локацијама или зградама треба да буде ограничен само на овлашћено особље;
- онда када је то применљиво, треба да буду изграђене физичке препреке како би се спречио неовлашћени физички приступ и загађење из околине;

- сва пожарна врата у безбедносној зони раздвајања треба да имају алармни уређај, да буду под надзором и да се испитују на спој са зидовима како би се успоставио потребан ниво отпорности у складу са одговарајућим регионалним, националним и међународним стандардима; треба да функционишу у складу са локалним противпожарним правилима у погледу осигурања од отказа;
- да би се надгледала сва спољна врата и доступни прозори, треба поставити погодне противпровалне алармне системе у складу са националним, регионалним или међународним стандардима; области без особља треба да буду под алармом у сваком тренутку; надзор треба такође обезбедити и за друге области, нпр. за просторију са рачунарима или за просторије за комуникације;
- опрема за обраду информација којом управља организација треба да буде физички одвојена од оне којом управљају трећа лица.

Контрола физичког уласка

Члан 37.

Безбедносне области морају бити заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ, складу са смерницама.

Смернице за контролу физичког уласка:

- евиднетирати датуме и време уласка и изласка посетилаца, а све посетиоце треба надгледати, осим ако њихов приступ није претходно одобрен; приступ треба одобравати само за специфичне, ауторизоване сврхе и издавати упутства о захтевима за безбедност области и о процедурама за ванредне ситуације;
- приступ областима у којима се обрађују или чувају поверљиве информације треба да буде ограничен само на овлашћене особе, применом одговарајућих контрола приступа, нпр. имплементацијом двофакторских механанизама за проверу веродостојности, као што су картице за приступ и тајни лични идентификациони број (PIN);
- треба безбедно одржавати и надгледати евиденцију или електронску проверу свих приступа;
- од свих запослених, уговарача и треће стране, као и од свих посетилаца треба захтевати да носе видљиву идентификацију и да известе особље уколико наиђу на посетиоце без пратиоца или примете особу која не носи видљиву идентификацију;
- запосленима код пружаоца услуга обезбеђења треба одобрити ограничен приступ безбедосним областима или опреми за обраду осетљивих података и омогућити када за то постоји потреба; овакав приступ треба да буде одобрен и надгледан у сваком тренутку;

- 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

Члан 38.

Висока школа струковних студија за образовање васпитача у Кикинди 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

Члан 39.

Према постојећој организационој структури Школа нема дефинисане безбедносне зоне. У случају њиховог настанка безбедносне зоне подлежу следећим мерама заштите:

- особље мора бити обавештено о активностима унутар безбедносне зоне;
- забрањује се рад без надзора у безбедносним зонама;
- безбедносне зоне које се не користе морају бити физички закључане и чија провера се врши периодично;
- не дозвољава се уношење фотографских, видео, аудио или других уређаја за записивање, осим уз претходно одобрење одговорног лица.
- евиденцију о уласку у безбедносну зону води Руководилац послаова за ИКТ

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

Члан 40.

Неопходно је заштитити средства која чине ИКТ систем од губитка, оштећења, крађе или другог облика угрожавања безбедности. У циљу заштите средстава, неопходно је водити рачуна о постављању средстава на безбедна места, елиминисати непотребан приступ у простор у коме се налазе, вршити редовне провере заштићености средстава од крађа, пожара, и других претњи и пратити услове околине (температура, влажност и др.) који би могли негативно да утичу на рад средстава.

Средства треба да буду заштићена у случају поремећаја у дистрибуцији електричне енергије, телекомуникационих капацитета, воде, вентилације обезбеђивањем алтернативних решења која омогућују наставак рада ИКТ система.

Измештање имовине ИКТ подсистема може да се врши само уз претходно одобрење овлашћеног лица, уз примену безбедносних механизама, узимајући у обзир различите ризике приликом рада изван просторија организације.

Области приступа где неовлашћена лица могу ући у службене просторије, треба контролисати, како би се избегао неовлашћени приступ опреми ИКТ система.

Информациони и технички ресурси се морају физички заштитити да би се спречио губитак, оштећење, крађа или други негативни утицаји, који могу представљати претњу.

Техничка средства се морају одржавати у складу са експлоатационом документацијом и упутством произвођача како би се осигурала непрекидна расположивост и интегритет података.

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.

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.

Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана.

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.

Носачи података као што су дискови и flash меморија морају бити одложени и закључани.

Шифре за приступ не смеју бити написане и остављене на приступачном месту.

Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.

Материјал који је намењен за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

Након оштећења уређаја који садрже критичне или поверљиве податке, неопходно је спровести процену ризика да дође до одлива поверљивих података приликом предаје уређаја ради одржавања екстерним организацијама. У случају доношења одлуке о немогућности предаје уређаја, уређај се уништава уз састављање одговарајућих докумената, након чега се врши његова замена у складу са утврђеним стандардима.

Помоћне функције за подршку

Члан 41.

Опрема се штити од прекида напајања, тако што се:

- помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
- капацитет помоћне опреме редовно процењује;
- редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова;
- обезбеђује вишеструко напајање са различитих траса.

Безбедносни елементи приликом постављања каблова

Члан 42.

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:

- водови напајања и телекомуникациони водови који улазе у просторије за обраду информација су подземни, онда када је то могуће, или имају адекватну алтернативну заштиту;
- каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње;
- за осетљиве или критичне системе се постављају оклопљени водови, користе се закључане просторије или кутије и примењује се електромагнетско оклапање ради заштите каблова;
- неовлашћено прикључење уређаја на каблове се врши техничким претраживањем и физичком провером;
- приступ до разводних табли и у просторије са кабловима се контролише.

Одржавање опреме

Члан 43.

Опрема се одржава како би се осигурали њена непрекидна расположивост и неповредивост, и то на следећи начин:

- опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;
- поправке и сервисирање опреме обавља само особље овлашћено за одржавање;
- о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;
- осетљиве информације треба избрисати из опреме;

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

Измештање и премештање имовине

Члан 44.

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

- треба да се одреде запослени и спољни корисници који имају овлашћење да одобре 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 и ова документација треба да буде враћена са опремом, информацијама или софтвером.

Безбедност измештене опреме и имовине

Члан 45.

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

Безбедно расходовање или поновно коришћење опреме

Члан 46.

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

Члан 47.

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

Члан 48.

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.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 49.

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.

Школа користи радне процедуре које садрже инструкције за детаљно извршење следећих послова:

а) инсталација и конфигурација система

- Системски софтвер сервера инсталира и конфигурише фирма коју Школа ангажује. Инсталације се обављају уз проверу Руководиоца послова ИКТ.
- База података се инсталира на серверу фирме коју Школа ангажује. За инсталацију је задужен Руководилац послова ИКТ.
- Веб апликација се инсталира копирањем валидних фајлова

б) обраду и поступање са информацијама (аутоматски и мануелно)

- Обрада и поступање са информацијама се обавља коришћењем апликације Школе. Апликација својим подешавањем корисницима дозвољава рад само над оним делом података који су додељени том кориснику. Путем апликације корисник не може да види податке ван својих ингеренција.

в) израда резервних копија;

- Резервне копије документације Школе, односно њен садржај се прави на дневном нивоу. Као додатна мера праве се резервне копије се на сториџ дисковима намењен прављењу резервних копија или се нарезује на двд дискове. За прављење резервне копије документације и информације базе података задужени су сви запослени, а контролу спровођења врше руководиоци организационих јединица.

- Апликације Школе (базе података) копирају се периодично по потреби после уношења измена на програму. Копира се садржај фолдера на серверу за коју је задужена партнерска фирма за израду апликација. За апликације које нису на серверу обавезно је прављење бекап података после сваке промена. Бекап се ради на ектерном хард диску или сторицу. За контролу копирање апликације задужен је Руководилац послова за ИКТ.
- Веб презентација Школе се налази на веб адреси https://www.vaspitacka.edu.rs. За бекап веб презентације задужена је партнерска фирма за израду веб презентације. За контролу копирање веб презентације задужен је Руководилац послова за ИКТ.
- Електронска пошта за сваког корисника се налази на његовом службеном рачунару. За резервну копију своје електронске поште задужен је сваки корисник лично. Резервна копија електронске поште прави се најмање једном месечно.
- Радна документа са корисничких рачунара: у свом раду корисници израђују радне фајлове који су њихова лична олакшица у раду и као такви нису од вишег интереса за Школу. Радне фајлове корисници треба да групишу у фолдере у оквиру путање C:\Users\ime.usera \Documents или на десктопу. Копију својих радних фајлова корисници праве лично, минимално једном месечно. Фајлове копирају корисници на УСБ меморију добијену од Школе или на сторицима.

г) 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;

- У случају грешке на информационом систему корисник бележи датум и време настајања грешке, место на апликацији на којем је настао проблем, копира поруку коју је јавио систем у електронској форми или прави писану забелешку поруке, обавештава Руководиоца послова за ИКТ о случају грешке.

д) утврђивање листе контаката за подршку и есклацију (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;

- У случају неочекиваних оперативних или техничких потешкоћа подршка се тражи од Руководиоца послова за ИКТ.
- Екстерну подршка за случај проблема спроводи Руководилац послова за ИКТ

ђ) процедуре за поновно покретање система и опоравак, које се користе у случају отказа система;

- У случају отказивања системског софтвера тражи се екстерна подршка од партнера Школе.

- У случају отказивања апликације и базе података, ради се резервна копија базе података и резервна копија апликације. Ове копије служе за даљу анализу насталог проблема.
- Преко постојеће базе података на серверу се ради ресторирање последње верзије базе из бекапа.
- После ових поступака рестартује се сервер и врши провера информационог система. Корисници при првом приступању апликацији проверавају последње податке које су унели и извештавају о успеху или неуспеху.

За усвајање, измене и допуне радних процедура овлашћен је Руководилац послова за ИКТ. Коришћење ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе система.

Управљање расположивим капацитетима

Члан 50.

Коришћење ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капаци- тетима, како би се осигурале неопходнеперформансе система. Периодично се спроводе слеће активности:

а) брисање застарелих података;

б) повлачење из употребе апликација, система, база података или окружења; в) оптимизација серије процеса и распореда;

г) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нисукритичне за пословање.

Раздвајање окружења за развој, испитивање и рад

Члан 51.

Окружења за развој, испитивање и рад су међусобно раздвојена. Како би се смањио ризик од неовлашћеног приступа или промена у радном окружењу:

- преношење софтвера из развојног статуса у оперативни статус обавља Руководилац послова ИКТ;
- развојни и оперативни софтвери треба да се извршавају на различитим системима или рачунарским процесорима, као и у различитим доменима или директоријумима;
- промене у оперативним системима и апликацијама треба испитивати у окружењу за испитивање или режиму одржавања пре него што се примене на оперативне системе;
- испитивање не треба да се ради на оперативним системима, осим у изузетним околностима;
- компајлери, едитори и други развојни алати или системски помоћни програми не треба да буду доступни из оперативних система, ако се то не захтева;

- да би се смањио ризик од грешке, корисници треба да примењују различите корисничке профиле за оперативне и системе за испитивање, а менији треба да приказују одговарајуће идентификационе поруке;
- осетљиве податке не треба копирати у системско развојно окружење, осим ако нису обезбеђене еквивалентне контроле за систем за испитивање.

За обезбеђивање исправног и безбедног функционисања средстава за обраду података и примену радних процедура задужен је Руководилац послова ИКТ.

Заштита података и средства за обраду података од злонамерног софтвера

Члан 52.

Злонамерни софтвер представља значајну претњу за ІКТ систем, јер може да доведе до оштећења или губитка података. Одговарајући антивирусни системи се морају применити на свим нивоима (радне станице / лаптопови, сервери, електронска пошта, приступ интернету) да би се омогућила ефикасна заштита.

1. Антивирус системи морају да се инсталирају само од стране овлашћеног особља и на начин који неће омогућити корисницима да их уклоне или да им промене конфигурацију.
2. Антивирус систем мора да омогући корисницима да у потпуности скенирају своје радне станице / лаптопове или преносиве медијуме, односно да се то врши аутоматски.
3. Антивирус систем мора да буде тако конфигурисан да може да скенира податке када се они уносе у компјутер. Овај поступак ће обухватити скенирање сваког фајла, идентификовање злонамерног кода, уклањање или стављање истих у карантин, ако уклањање није могуће. Ако антивирус систем не може да уклони малвер или да га стави у карантин, онда заражени објекат/фајл мора да се пошаље испоручиоцу антивируса на додатну анализу.
4. Фајлови који долазе са Интернета, поруке путем електронске поште и прилози, као и сви преносиви медијуми за складиштење података (као што су USB меморије, екстерни хард дискови, CD-ови / DVD-јеви, итд.) морају се аутоматски скенирати пре него што се прикључе у ИКТ систем.
5. Антивирус систем мора редовно аутоматски да се ажурира и такав поступак треба да буде транспарентан крајњем кориснику.
6. Строго је забрањено поседовање, дистрибуција и развој злонамерног софтвера.
7. Управљање и обнављање средстава за заштиту од злонамерног софтвера врши се централизовано, од стране Руководиоца послова ИКТ.
8. Анализирати случајеве продирања и имплементације злонамерног софтвера у оквиру мера за управљање инцидентима информационе безбедности.
9. У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Руководиоцу послова ИКТ.

10. У циљу заштите од упада у ИКТ систем, Руководилац послова ИКТ је дужан да одржава систем за спречавање упада.
11. Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета Руководилац послова ИКТ може укинути приступ.

Поступак контроле и предузимање мера против злонамерног софтвера

Члан 53.

Висока школа струковних студија за образовање васпитача у Кикинди 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;
3. имплементација контрола које спречавају или откривају коришћење познатих или сумњивих компромитованих веб-сајтова;
4. 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;
5. смањење рањивости које може да експлоатише непријатељски софтвер, нпр. кроз управљање техничким рањивостима;
6. спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе; присуство било каквих неодобрених датотека или неауторизованих допуна треба формално истражити;
7. 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 које се спроводе:

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 ВШССОВ у Кикинди;
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;
8. 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.
9. Препоручује се доношење и процедуре о антивирусној заштити и процедуре о подизању свести запослених о информационој безбедности.
10. У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави непосредном руководиоцу и Руководиоцу за ИКТ.
11. У циљу заштите одупада у ИКТ систем Руководилац за ИКТ је дужан да одржава систем за спречавање упада.
12. Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета Руководилац за ИКТ може укинути приступ.

Заштита од губитка података

Члан 54.

Висока школа струковних студија за образовање васпитача врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.

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.

Заштитне 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 заштитних копија користе се издвојени сервери, екстерни хард дискови, сторици и CD/DVD медији.

Руководилац за ИКТ извршава следеће задатке:

- процењује осетљиве и критичне податке за које је потребно правити резервне копије;
- креира план прављења резервних копија;
- даје налог за израду заштитне копије, конфигурационих фајлова, апликације, и базе података;
- верификује успешно прављење резервних копија;
- води евиденцију урађених резервних копија;
- одлаже копије на безбедно место;
- тестира исправност резервних копија и процедуре за прављење заштитних копија;
- рестаурира податке са резервних копија.

Израда резервних копија, поступак приликом израде и учесталост израде резервних копија наведена је у члану 49 под тачком в).

Израда резервних копија треба да:

- одражавају пословне потребе организације и критичност тих информација по континуитет пословања организације;
- треба их складиштити на локацији на довољној удаљености, како би се избегло свако оштећење на главној локацији;
- резервним копијама информација треба дати одговарајући ниво физичке заштите и заштите од утицаја околине који је доследан мерилима која се примењују на главној локацији;
- медијуме са резервним копијама треба редовно проверавати, ради сигурности њихове употребе у ванредним ситуацијама и када је то неопходно;
- у ситуацијама у којима је важна поверљивост, резервне копије треба заштитити помоћу шифровања.

За заштиту од губитка података одговоран је непосредни руководилац организационе јединице уколико није поступио у складу са овим правилником и налогу Руководиоца послова за ИКТ.

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

Члан 55.

Обезбедити евидентирање свих активности корисника, администратора, оператера, порука о процесима, грешкама, промени конфигурације система и слично. Уколико другим нормативним актом није другачије прописано, минималан рок обавезног чувања наведене евиденције је једна година.

Средства за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене. Записи се редовно преиспитују у циљу заштите.

За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужен је Руководилац послова за ИКТ.

Обезбеђивање интегритета софтвера и оперативних система

Члан 56.

У циљу одржавања исправности софтвера врше се мере отклањања слабих тачака софтвера. Отклањање слабих тачака софтвера се постиже редовним инсталирањем нових верзија софтвера. Ажурирање оперативних ситема и другог опште-системског и апликативног софтвера врши Руководилац послова за ИКТ.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 57.

У циљу правовременог и ефикасног реаговања на објављене и уочене слабе тачке софтвера се предузимају мере за контролу заштићености средстава за обраду, чување и предају информација.

Контрола заштићености се врши на следећи начин:

- периодичном анализом заштићености помоћу скенерања безбедносним алатима/софтверима
- мониторингом заштићености
- анализом конфигурационих фајлова средстава за обраду, чување и пренос информација

Подаци о слабим тачкама софтверских решења редовно се обнављају са сајтова произвођача конкретних решења. Уочене слабе тачке средстава за обраду, чување и пренос информација отклањају се помоћу нових верзија софтвера („update“) или применом препоручених конфигурација које нуде произвођачи софтвера.

Ограничења у погледу инсталације софтвера

Члан 58.

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедносним ризицима.

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

Члан 59.

Приликом спровођења контроле ИКТ система, Школа обезбеђује да предузете активности имају што мањи утицај на функционисање система, тако што планира адекватно време

спровођења ревизије и редослед активности који не ометају пословне процесе унутар ИКТ система.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 60.

У циљу заштите података у комуникационим мрежама, уређајима и водовима врши се њихова контрола и заштита од неовлашћеног приступа, дефинише одговорност за управљање мрежном опремом, одговорност за рад мреже, посебне контроле за заштиту поверљивости и интегритета података који пролазе путем јавних или бежичних мрежа.

За спровођење редовних провера постојања адекватне безбедности мрежних сервиса ангажују се фирме које се баве одржавањем мрежа рачунара.

Комуникационим мрежама адекватно управљати и контролисати их, како би се оне заштитиле од претњи, да би се одржала сигурност система и апликација које користе мрежу, укључујући и заштиту информације које су у протоку.

Приликом закључивања уговора о мрежним услугама, за све мрежне услуге треба идентификовати ризике и узети у обзир елементе заштите информација да се ризици минимизују.

У мрежама су међусобно раздвојене групе информационих услуга, корисника и системи, а мрежни администратор је одговоран за управљање мрежом.

Руководилац послова за ИКТ је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Безбедност података који се преносе унутар ВШССОВ у Кикинди, као и између ВШССОВ у Кикинди и лица ван ВШССОВ у Кикинди

Члан 61.

Заштита података који се преносе комуникационим средствима унутар Школе, између Школе и лица ван Школе, обезбеђује се утврђивањем одговарајућих правила, процедура и применом адекватних контрола.

Споразуми о преносу информација

Безбедан пренос пословних информација између Школе и трећег лица обезбеђује се поштовањем споразума о преносу информација.

Споразуми о преносу информација треба да укључе следеће:

1. одговорности руководства за контролу и извештавање о преносу, отпреми и пријему;
2. процедуре за обезбеђење следљивости и непорецивости;

3. минималне техничке стандарде за паковање и пренос;
4. стандарде за идентификовање курира;
5. обавезе и одговорности у случају инцидената нарушавања безбедности информација, као што је губитак података;
6. коришћење договореног система означавања осетљивих или критичних информација, уз осигуравање да је значење ознака одмах разумљиво и да су те информације заштићене на одговарајући начин;
7. посебне контроле које су потребне да би се заштитили осетљиви детаљи, попут криптографије; одржавање ланца надзора за информације у току преноса;
8. одржавање ланца надзора за информације у току преноса.

Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са успостављеним процедурама и адекватним контролама над спровођењем истих. Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

Правила коришћења Интернета

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

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом.

Размена електронских порука

Заштита информација укључених у размену електронских порука се регулише Процедуром о безбедности у размени електронских порука.

Процедура о безбедности у размени електронских порука треба да обухвати:

- заштиту порука од неовлашћеног приступа, модификовања или одбијања услуга које су у складу са класификационом шемом коју је усвојила ВШССОВ у Кикинди;
- осигурање исправног адресирања и транспорта поруке;
- поштовање законских одредби, на пример захтеве за електронске потписе;
- добијање одобрења пре коришћења јавних спољних услуга, као што су размена хитних порука, приступ и коришћење друштвене мреже или заједничко коришћење датотека;
- строже нивое утврђивања веродостојности, контролисањем приступа из мрежа са јавним приступом

Споразуми о поверљивости или неоткривању

Споразуми о поверљивости или неоткривању имају за циљ заштиту информација Високе школе струковних студија за образовање васпитача у Кикинди 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:

1. дефиницију информација које треба заштитити;
2. очекивано трајање споразума, укључујући случајеве у којима је потребно да се поверљивост сачува неограничено;
3. поступања које се захтевају по истеку споразума, попут повраћаја или уништавања информација;
4. дозвољено коришћење поверљивих информација и пословних тајни, као и права потписника да користи информације;
5. право на проверу и праћење активности које укључују поверљиве информације;
6. процес за обавештавање и извештавање о неовлашћеном откривању или приступу поверљивим информацијама;
7. радње које треба предузети у случају кршења овог споразума.

Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 62.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, Висока школа струковних студија за образовање васпитача у Кикинди је у обавези да обезбеди информациону безбедност у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења.

Руководилац послова за ИКТ је задужен за технички надзор над реализацијом од стране извођача, односно испоручиоца.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система Руководилац послова за ИКТ води евиденцију.

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

Информациона и техничка решења обухватају оперативне системе, инфраструктуру, пословне апликације, ИТ услуге других лица, готове софтверске пакете и хардвер.

За увођење новог система за обраду информација мора се претходно обезбедити:

- сагласност Руководиоца послова за ИКТ, којом се потврђује да имплементација новог система не нарушава постојећи систем заштите информација и

- сагласност Руководиоца послова за ИКТ којом се потврђује да имплементација новог система не нарушава функционисање и неопходне перформансе ИКТ система.

Школа је обавезна да контролише промене везане за информациона добра ИКТ система. Информациона добра као што су хардвер, комуникациона инфраструктура, системски софтвер и апликативни софтвер морају бити предмет строге контроле управљања променама.

Примена мера заштита информација је обавезна током целог животног века информационих и техничких решења у:

- фази пројектовања,
- фази обезбеђења буџета,
- фази поступка набавке,
- фази поступка уговарања,
- фази експолатације,
- фази поступка измене или унапређења постојећег система и
- фази поступка престанка са коришћењем система.

Руководиоца послова за ИКТ проверава примену мера заштите у свим наведеним фазама.

Анализа и спецификација захтева за информациону безбедност

Члан 63.

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

Захтеви за информациону безбедност укључују:

- Проверу идентитета корисника;
- Доступност, поверљивост, непорецивост и интегритет података и имовине;
- Надгледање пословних процеса;
- Омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке кориснике.

Спецификација захтева обухвата аутоматску контролу која ће бити уведена у информациони систем, као и потребу да постоји и ручна контрола, која мора бити примењена при вредновању развијених или купљених пакета софтвера, намењених за пословне апликације.

Системски захтеви за информациону безбедност и процеси за увођење безбедности се интегришу у фази дизајнирања информационих система.

Формално тестирање и процес имплементације ће се примењивати за све купљене производе.

У уговору са извођачем, односно испоручиоцем купљених производа, посебно се дефинишу захтеви за информациону безбедност.

У случају да безбедносна функционалност предложеног производа не задовољава одређен захтев, ризик и повезане контроле ће бити преиспитане пре куповине производа.

Обезбеђивање апликативних услуга у јавним мрежама

Члан 64.

Информације обухваћене апликативним услугама које пролазе кроз јавне мреже треба заштити од малверзација, неовлашћеног откривања података и модификовања. Неопхнодно је потврдити идентитет корисника и извршити поделу овлашћења и одговорности за постављање садржаја, електронског потписивања или обављања трансакција.

Заштита трансакција апликативних услуга

Члан 65.

Информације укључене у трансакције апликативних услуга се штите да би се спречио непотпун пренос, погрешно усмеравање, неовлашћено мењање порука, неовлашћено разоткривање, неовлашћено копирање порука или поновно емитовање.

Трансакције морају да подрже следеће услове:

- Обе стране које учествују у транскакцији морају да примене електронски потпис;
- Приватност свих страна које учествују у трансакцији;
- На комуникационим каналима примењено шифровање;
- Безбедност протокола који се користе у трансакцијама.

Заштита података који се користе за потребе тестирања ИКТ система односно делова система

Члан 66.

За потребе тестирања ИКТ система односно делова система Школа користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

Апликације и софтвер оперативног система имплементирати тек после успешно спроведеног тестирања, којим треба обухвати проверу применљивости, сигурности, утицаја на друге системе и погодности за коришћење.

Током тестирања избегавати коришћење продукционих база података које садрже осетљиве информације. Ако се за сврху испитивања користе информације о личности или неке друге осетљиве информације, неопходно је применити мере заштите информација као на стварним, продукционим системима у складу са прописима и овлашћењима.

Уколико је за тестирање неопходно користити оперативне податке, примењују се следеће смернице:

- за свако копирање оперативних података у тестно окружење се издаје посебно овлашћење;
- приликом тестирања апликативних система примењују се процедуре за контролу приступа које се примењују и на оперативним системима;
- оперативне информације се одмах по завршетку испитивања бришу из тестног окружења.

Приступ изворном програмском коду и припадајућим информацијама строго контролисати, како би се спречило увођење недокументованих и неауторизованих функција, као и да би се избегле ненамерне промене.

Заштита средстава ВШССОВ у Кикинди која су доступна пружаоцима услуга

Члан 67.

Размену информација и софтвера са пословним партнерима заснивати на званичној политици размене, регулисане одговарајућим уговорима, односно споразумима.

Коришћење екстерних организација за управљање информационим и техничким ресурсима представља сигурносни ризик, те је неопходно унапред извршити процену ризика, припремити одговарајуће мере заштите.

Ангажовани од стране Пословног партнера не могу имати права администрирања која су потребна за промену параметара аутентификације, ауторизације и права приступа. Током пружања услуга, ангажовани од стране Пословног партнера, морају имати минимална права потребна за обављање послова, а која нису у супротности са претходним ограничењима.

Морају се применити следеће мере:

- употреба персонализованих корисничких налога (име и презиме);
- непходно је увек прво приступити приступној тачки на којој се бележе све активности у дневницима (логовима).

Мере заштите које се примењују приликом приступа лица која су ангажована идентичне су мерама заштите које се примењују на запослене у Школи. У свим фазама рада са информационим и техничким ресурсима, треба обезбедити могућност контроле и увида у активности ангажованих екстерних организација.

Политика безбедности размене информација у пословним односима са пружаоцима услуга и између независних пружалаца услуга

Члан 68.

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација Висока школа струковних студија за

образовање васпитача у Кикинди морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

Пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са ВШССОВ у Кикинди.

Висока школа струковних студија за образовање васпитача у Кикинди успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга:

- идентификовање и документовање врсте пружаоца услуга којима ће Висока школа струковних студија за образовање васпитача у Кикиндидозволити да приступ информацијама;
- стандардизовани процес за управљање односима између пружаоца услуга;
- дефинисање врста информација које ће различитим типовима пружаоца услуга бити дозвољено ради приступања, праћења и контроле приступа;
- минимални захтеви за безбедност информација за сваку врсту информација и врсту приступа;
- процеси и процедуре за праћење придржавања утврђених захтева за безбедност за сваку врсту добављача и врсту приступа;
- контроле за осигурање интегритета информација или обраде информација коју обезбеђује било која страна;
- поступање са инцидентима и непредвиђеним ситуацијама које су у вези са приступом пружаоца услуга, укључујући одговорности и организације и пружаоца услуга;
- управљање неопходним променама информација, опреме за обраду информација и свега осталог што треба да се премешта и осигурање да се безбедност информација одржава током прелазног периода.

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

Члан 69.

Пре отпочињања преговора, потенцијални пружалац услуга у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, која садржи обавезу за пружаоца услуга да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране Висока школа струковних студија за образовање васпитача у Кикинди, а за потребе извршења предмета преговора.

Потребно је да изјава о поверљивости, односно уговор о пружању услуга, садржи одредбу о поверљивости са јасно утврђеном обавезом и одговорношћу пружаоца услуге уз претњу раскида уговора и накнаде штете у корист Високе школе струковних студија за образовање васпитача у Кикиндиу случају повреде ове одредбе.

Пример: *"Сви подаци и информације садржани у овом Уговору о пружању услуга се сматрају поверљивим пословним подацима и не смеју бити саопштени или на други начин учињени доступним трећим лицима. Нарочито се сматрају поверљивим сви пословни подаци и информације које једна страна учини доступним другој уговорној страни ради извршења обавеза из овог уговора, уколико ти подаци нису јавно доступни нити су били претходно познати другој страни.*
Свака уговорна страна се обавезује да податке и информације које јој буду учињене доступним у складу са овим уговором и обавезом извршења уговорених послова и обавеза, буду стављене на располагање и увид запосленима, уколико је то неопходно ради извршења обавеза из овог уговора.
Уговорне стране се нарочито обавезују да поступају обазриво са подацима о личности до којих могу доћи у поступку извршења услуга за ВШССОВ у Кикинди, као и да те податке чувају и поступају у свему у складу са прописима који уређују заштиту података о личности.
У случају повреде ове обавезе уговорна страна чији су подаци коришћени има право раскида уговора и право да захтева накнаду штете услед неовлашћеног коришћења података и информација друге стране."

Пружаоци услуга дужни су да захтеве Високе школа струковних студија за образовање васпитача у Кикинди у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе.

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга

Члан 70.

У циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, неопходно је успоставити механизме надзора над пружањем услуга. Руководилац послова ИКТ задужен је за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности.

Управљање променама уговорених услуга од стране пружаоца услуга

Члан 71.

Уговором са пружаоцем услуга треба обезбедити могућност континуираног управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контролу безбедности информација.

Промене које се узимају у обзир су промене у споразумима са пружаоцима услуга, повећање обима текућих услуга које се нуде, као и промене које уводи Висока школа струковних студија за образовање васпитача у Кикиндиради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

Превенција и реаговање на безбедносне инциденте

Члан 72.

Подразумева адекватну размену информација о безбедносним слабостима ИКТпретњама система, инцидентима и ВШССОВ у Кикинди утврђује:

- одговорно лице задужено за превенцију и реаговање је Руководилац послова ИКТ
- план поступања у случају опасности од настанка безбедносних инцидената или настанка безбедносних инцидената,
- обавезе вођења евиденције о предузетим активностима,
- обавезе извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.

Сви запослени и пружаоци услуга су обавезни да одговорном лицу, задуженом за превенцију и реаговање из става 1. овог члана, без одлагања пријављују безбедносне слабости, претње и инциденте у ИКТ систему. Руководилац послова ИКТ обавештава директора Школе о безбедносним слабостима, претњама и инцидентима у ИКТ систему.

ВШССОВ у Кикинди одређује секретара Школе, као лице одговорно за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности.

Одговорно лице примењује поступак идентификације, прикупљања и чувања информација које могу да послуже као доказ ради покретања дисциплинског, прекршајног или кривичног поступка. У овом поступку помаже и Руководиоца послова ИКТ.

У циљу правовременог утврђивања прекршаја у области информационе безбедности врши се контрола догађаја у оперативним и апликативних системима, уређајима и окружењу, уз обавезно вођење дневника догађаја.

Обавезна је регистрација за:

- активности корисника које се тичу приступа оперативним и апликативним системима, информационим ресурсима и мрежним сервисима,
- активности корисника које се тичу рада са преносним носачима информација на њиховим радним местима и
- активности на измени подешавања средстава за обраду, чување и пренос информација, средстава за заштиту информација и права приступа корисника.

Морају се предвидети механизми за заштиту дневника (лога) догађаја од препуњавања, неовлашћеног прегледања и уношења измена.

Дневници (логови) догађаја се редовно анализирају од стране Руководиоца послова за ИКТ. Након оштећења уређаја који садрже критичне или поверљиве податке, неопходно је спровести процену ризика да дође до одлива поверљивих података приликом предаје уређаја ради одржавања екстерним организацијама. У случају доношења одлуке о немогућности предаје уређаја, уређај се уништава уз састављање одговарајућих докумената, након чега се врши његова замена у складу са утврђеним стандардима. Све запослене, извођаче радова и

екстерне кориснике треба упознати са процедурама за извештавање о догађајима и слабостима које могу имати последице по пословање.

Извештавање о догађајима у вези са безбедношћу информација

Члан 73.

Сви запослени морају бити упознати са обавезом и процедуром извештавања о догађајима у вези са информационом безбедношћу.

Руководилац послова ИКТ припрема план и неколико метода комуникације које би могле да се примене у зависности од инцидента. Могуће методе комуникације су: електорнска пошта, веб сајтови (интерни, екстерни, портали), телефонска комуникација, говорна порука, писмено извештавање, директан контакт.

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

Извештавање о утврђеним слабостима система заштите

Члан 74.

Сви запослени су у обавези да о уоченим и утврђеним слабостима ИКТ система известе Руководиоца послова ИКТ, у што краћем року, како би се инциденти нарушавања информационе безбедности спречили и спречио настанак штете.

Одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности, поступа у складу са одговарајућом процедуром.

Догађаји у вези са информационом безбедношћу се оцењују и у складу са анализом се доноси одлука да ли је потребно да се класификују као инциденти нарушавања информационе безбедности.

Одговор на инциденте нарушавања информационе безбедноости

Члан 75.

Висока школа струковних студија за образовање васпитача у Кикинди је у обавези да усвоји План за превенцију од безбедносних ризика.

План за превенцију од безбедносних ризика садржи одговоре на питања ко треба да буде контактиран, када и како и које акције треба предузети моментално у случају одређеног напада?

- Класификациона шема – детаљи о подацима који се налазе у систему, њихов ниво осетљивости и поверљивости.

- Листа услуга – попис свих услуга које Висока школа струковних студија за образовање васпитача у Кикинди пружа, рангиране по важности.
- План за backup и restore података – дефинише за које податке се ради backup, носаче података на које ће се снимати, где се носачи чувају и колико често се backup изводи. Дефинише и поступак за restore података.
- План за замену опреме: Садржи списак потребне опреме, рангиране по важности.
- Односи са јавношћу: Утврђена је одговорна особа (директор) задужена за одосе са јавношћу, као и упутство које информације је дозвољено јавно објавити у случају напада.

Прикупљено знање из анализе и решавања инцидената који су нарушили информациону безбедност, Висока школа струковних студија за образовање васпитача у Кикинди користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

Прикупљање доказа

Члан 76.

Висока школа струковних студија за образовање васпитача у Кикинди спроводи процедуру за идентификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају покретања дисциплинског, прекршајног или кривичног поступка.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 77.

Висока школа струковних студија за образовање васпитача у Кикинди дефинише мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

Планирање континуитета мера безбедности информација

Континуитет пословања се осигурава кроз План за обезбеђење континуитета пословања и План опоравка од нежељених догађаја ИКТ система.

При изради Плана за обезбеђење континуитета пословања за хардверске компоненте ИКТ система треба обухватити следеће:

- документацију за логички и физички дијаграм и копије пројеката;
- заштитне копије конфигурационих фајлова и оперативног система активних уређаја;
- постојање резервне опреме;
- унапред направљене конфигурације за различите сценарије;
- израду резервних копија.

При изради Плана опоравка од нежељених догађаја ИКТ система:

- проценити најкритичније апликације, податке, конфигурационе фајлове и системски софтвер за који треба направити резервне копије;
- одредити место чувања копије;
- одредити нову локацији рада ИКТ система у случају немогућности рада на основној локацији/избор рачунара који ће привремено заменити сервер док се сервер не стави у функцију.;
- навести податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја;
- одредити изворе непрекидног напајања електричном енергијом.

Такође, при изради Плана опоравка од нежељених догађаја ИКТ система потребно је предвидети:

- постојање документације за сервисе, апликације и базе података;
- процедуре инсталације и конфигурисања сервиса, апликација и база података;
- место чувања инсталација сервиса, апликација и база података и резервне копије података;
- податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја;
- развијене и одобрене документоване планове, одговоре и процедуре за опоравак, детаљно наводећи како ће организација управљати догађајима који узрокују поремећаје и како ће одржавати своју безбедност информација.

Имплементација континуитета безбедности информација

Да би се осигурао потребан ниво континуитета безбедности информација током ванредних ситуација, Руководилац послова ИКТ примењује процедуре и контроле описане у Плану за обезбеђење континуитета пословања.

Руководилац послова ИКТ врши проверу усвојених процедура контроле континуитета безбедности информација, како би оне биле адекватне и ефективне током ванредних ситуација.

Провера се врши вежбањем и испитивањем знања и рутине приликом руковања процесима, процедурама и контролама, као и преиспитивањем ефективности мера безбедности информација у случају промене информационих система, процеса, процедуре и контроле безбедности информација.

ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза

Члан 78.

Обавеза Високе школе струковних студија за образовање васпитача у Кикинди је да једном годишње изврши проверу ИКТ система и изврши евентуалне измене Правилника о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Школе.

Одговорности и препоруке

Члан 79.

За примену мера заштите ИКТ система дефинисаних Законом о информационој безбедности одговоран је Директор Школе.

За израду, измене, допуне и тумачење одредби овог Правилника одговоран је Савет Школе.

За управљање информационом безбедношћу у складу са Законом о информационој безбедности на нивоу ИКТ система задужен је Руководилац послова информационих система и технологија.

За примену овог Акта одговорни су сви запослени у оквиру своје организационе јединице и домена рада.

Члан 80.

Овај акт ступа на снагу осмог дана од дана објављивања на огласној табли и сајту Школе.

Председник Савета

ВШССОВ у Кикинди

Др Србислава Павлов, проф.

Датум доношења: 19. 10. 2023. године

Датум објављивања: 23. 10. 2023. године