На основу члана 8. Закона о информационој безбедности („Службени гласник РС“, број 6/16), чланова 1-8 Уреде 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, Владе РС („Службени гласник РС“, број 94/16 од 24.11.2016. године) Савет Високе школе струковних студија за образовање васпитача и тренера на седници одржаној дана 12. 12. 2017. године донео је

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

ВИСОКЕ ШКОЛЕ СТРУКОВНИХ СТУДИЈА ЗА ОБРАЗОВАЊЕ ВАСПИТАЧА И ТРЕНЕРА

Члан 1.

Предмет

Овим Актом ближе се дефинишу мере заштите информационо-комуникационих система (у даљем тексту ИКТ систем) у Високој школи струковних студија за образовање васпитача и тренера (у даљем тексту Школа), а нарочито принципи и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника ИКТ система у Школи.

Члан 2.

Циљеви

Циљеви доношења овог Акта су:

1) допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
2) минимизација безбедносних инцидената;
3) обезбеђивање конзистентне контроле свих компонената ИКТ система.

Члан 3.

Обавезност

Овај Акт је обавезујући за све унутрашње организационе јединице Школе и за све кориснике информатичких ресурса Школе (студенте и посетиоце Школе).

Непоштовање овог Акта повлачи дициплинску одговорност корисника информатичких ресурса.

За праћење примене овог Акта надлежан је Стручни сарадник за информационе технологије и рачунарску технику.

Члан 4.

Појмови

Поједини изрази употребљени у овом Акту имају следеће значење:

1) *интегритет* је немогућност неовлашћене измене информација;
2) *расположивост* је доступност информација корисницима информатичких ресурса у обиму корисничког овлашћења;
3) *тајност* је обезбеђивање доступности информација само овлашћеним корисницима информатичких ресурса, као и немогућности приступа информацијама лицима која немају таква овлашћења.

4) *администраторско овлашћење* је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;
5) *кориснички налог* јесте корисничко име и лозинка на основу којих информатички ресурс спроводи проверу индетитета корисника и проверу права приступа, односно овлашћења корисника;
6) *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.

Мере заштите

Члан 5.

Мерама заштите се обезбеђухе 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.

Информатички ресурси Школе

Члан 6.

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.

Предмет заштите

Члан 7.

Предмет зашите обухвата:

1) хардверске и софтверске компоненте информатичких ресурса;
2) податке који се обрађују или чувају на информатичким ресурсима;
3) корисничке налога и друге податке о корисницима информатичких ресурса у Школи

Корисник информатичких ресурса

Члан 8.

Корисник информатички ресурса јесте постављено лице, запосленолице на неодређено или одређено време, лице ангажовано на основу уговора, или друго радно ангажовано лице, као студент који је уписан и похађа студије у Школи, а коме је одобрен приступ неком информатичком ресурсу Школе.

Корисник информатичких ресурса одговоран је за правилну употребу, тачности и сигурност података приликом коришћења 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 9.

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

Корисник добија информатичке ресурсе на коришћење искључиво у пословне и едукационе 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 док је сервер ван функције или га нема у том облику, корисник може смештати привремено податке унутар радних станица у ИКТ систему.

Запослено лице на радном месту Стручни сарадник за информационе системе и рачунарску технику са администраторским овлашћењима (у даљем тексту: администратор), као и друга лица које поседују иста овлашћења, дужна су да се старају о резервним копијама података. У случају кад се подаци налазе на мрежним дисковима на серверу Школе администратор је дужан да прави дневне резервне копије.

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

1) да користи информатичке ресурсе искључиво у пословне односно едукационе сврхе;
2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру ИКТ система власништво Школе и да могу биди 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) тамо где је могуће, пре сваког удаљавања од радне станице одјави са система („log out”);
6) користи USB, DVD-R/W, CD-R/W и остале типове екстерних меморија на радној станици само уз одобрење администратора;
7) захтев за инсталацију софтвера или хардвера подноси искључиво администратору, који одобрава да ли је инсталација неопходна, безбедна и не угрожава поузданост ИКТ система или не;
8) обезбеди сигурност података у складуса важећим прописима;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
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 по потреби заштитне копије (backup) података у складу са проописаним процедурама;
13) користи Internet и e-mail сервисе у Школи у складу са прописаним процедурама;
14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, поправке и препправке итд.) 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 (антивируси, програми, системи за детекцију упада, средства за шифрирање, средства за проверу индетитета, 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) да се удржи 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 итд. и да тиме повреди приватност појединаца;
20) да се уздржи од неуобичајено и неоправдано великог коришћења информатичких ресурса Школе, а посебно у приватне сврхе.

Безбедносни профил корисника информатичких ресурса

Члан 10.

У зависности од описа задатака и послова радног места на које је распоређен, корисникинформатичких ресурса, на предлог непосредног руководиоца, 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 помоћника директора.

Креирање лозинке

Члан 11.

Лозинка на радним станицама у ИКТ систему по потреби да задржи минимум осам карактера састављених од слова и цифара.

Лозинке 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, или је исту изгубио, заборавио итд. дужан је одмах да се обрати администратору који ће лозинку променити.

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

Употреба корисничког налога

Члан 12.

Кориснички налог може употребљаватисамо корисник информатичких ресурса коме је исти издат.

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору који се стара о истом.

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

Кориснички налози са администраторским овлашћењима користе се за потребе непоходних интервенција којима се обезвеђује несметан рад информатичких ресурса.

Поступци у случајевима сигурностних интервенција

Члан 13.

Корисник информатичких ресурса дужан је да, без одлагања, пријави администратору ИКТ ситема свако уочавање или сумњу о наступању инцидента којим се угрожава сигурност ИКТ система.

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

1) нарушавања поверљивости информација,
2) откривања рачунарских вируса и другог малициозног софтвера или грешака у функционисању апликација неопходних за рад
3) вишеструких покушаја неауторизованог приступа,
4) системских падова и престанка рада система

Стручни сарадник за информационе системе и одржавање рачунарске технике, који је истовремено и администратор ИКТ ситема дужан је да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести надлежни орган, у складу са законом којим се уређује информациона безбедност.

Заштита од малициозног софтвера

Члан 14.

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

1) лиценцираног софтвера, односно забрана коришћења и инсталирања софтвера који потичу са непознатих интернет адреса, или које су пренете са неког меморијског медија.
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 или малициозног софтера.
- Ако се утврди да преносиви медиј садржи вирусе или други малициозни софтвер, врши се чишћење медија од вируса, уз сагласност доносиоца медија.
- Ризик од евентуалног губитка података приликом чишћења медија антивирусним софтвером, сноси доносилац медија.

Сигурност електронске поште

Члан 15.

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 пословне електронске поште у приватне сврхе.

Поступање са преносивим медијима

Члан 16.

Преносиви медији који садрже поверљиве податке морају да буду прописно обележени и пописани.

У сличању брисања поверљивих података којима је неопходно брисање на преносивим медијима, потребно је обезбедити њихово неповратно брисање.

Физичка сигурност информатичких ресурса

Члан 17.

У циљу физичке сигурностиинформатичких реусрса морају се обезбедити следећи услови:

1) сервери и слична опрема, као и комуникационо чвориште уколико Школа поседује исто морају бити смештени у посебној просторији Школе, која испуњава стандарде противпожарне заштите и редудантног напајања струјом, као и адекватну климатизацију, и у којој је приступ забрањен незапосленим лицима;
2) приступ просторији из става 1) може да се омогући осим администратору и другим запосленим у Школи уз претходно одобрење помоћника директора и самог администратора;
3) радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења виталних компонената;
4) просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
5) штампачи, фотокопир машине и факс машине морају бити лоциране тако да главни корисник истих (запослено лице задужено за исте машине) може да има увек надзор на њима, односно ради спречавања неовлашћеног копирања и преноса осетљивих информација;
6) медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

Приступ ИКТ систему Школе

Члан 18.

Приступ свим компонентама ИКТ система мора бити ауторизован односно аутентификован.

Администратор, на основупрецизног писаног захтева запосленог у Школи, а у консултацији за непосредним руководиоцима додељује или прави измене кориснику информатичких 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 информатичких ресурса укида се право приступа ИКТ система (бришу се сви налози које корисник поседује).

У случају одсуства са посла дуже од месец дана, корисник информатичких ресурса је обавезан да исто одсуство пријави администратору ИКТ система, након чега ће администратор суспендовати по потреби налог корисника до повратка на посао или до његовог личног захтева.

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.

Трећем лицу се могу одобрити права приступа ИКТ систему уз претходно склапање уговора, уз поштовање овог акта, којим се прецизно дефинишу услови и обим приступа.

Изузетно од става 7. овог члана, у случају неопходних и хитних послова, могу се одобрити права приступа трећем лицу, по налогу овлашћеног лица, а све на одговорност администратора који мора пажљиво да испрати и надзире иста права и зачини евентуални записник након истог.

Ако се установи повреда овог акта или прекорачење овлашћења, или било каква намерна и контрапродуктивна активност усмерена рушењу безбедности ИКТ система, одобрени приступ се одмах укида и врши се забрана приступа кориснику информатичких ресурса.

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.

Стручни сарадник за инфромационе послове и рачунарску техникуобезбеђује запослено, односно ангажованом лицу, коришћење радне станице (десктоп или лаптоп рачунар) са преинсталираним и конфигурисаним софтвером (оперативни систем, сви неопходни управљачки програми односно драјвери, друге апликације потребне за пословно окружење, софтвер за антивирусну заштиту као и друге разне помоћне апликације), који је типски за све радне станице и представља минимум потребан за обављање основних послова.

Администратор врши оцену конзистетности траженог софтвера са постојећим инсталираним софтвером на предметној радној станици и уколико оцени да тражени софтвер неће угрозити или ометати рад, инсталираће захтевани софтвер, 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 интернет прегледача и мејл клијената
3) инсталација антивирусног софтвера (лиценцираног или бесплатног)
4) инсталација званичног апликативног софтвера који одређене јединице Школе користе у свом раду

У случају да је кориснику потребно да се изврши инсталација одређеног специфичног софтвера на радној станици, он мора да поднесе захтев администратору који ће исти прегледати и оценити да ли је софтвер могуће инсталирати без угрожавања интегритета ИКТ система.

Корисник информатичког ресурса дужан је да сваки проблему функционисању оперативног система, интернет претраживача, мејл клијента, пословног софтвера и апликативног софтвера, пријави администратору (телефонским или електронским путем) како би он поступио решњавању проблема.

Проблем у функционисању антивирусног софтвера се мора пријавити одмах без одлагања.

Администратор је дужан да проблеме из става 6. и 7. отклони у најкраћем могућем року на локацији корисника, даљинском конекцијом ка радној станици или доношењем радне станице (уколико је проблем нерешив на лицу места) у свој кабинет.

Завршна одредба

Члан 20.

Овај Акт ступа на снагу наредног дана од дана објављивања на огласној табли и интернет страници Школе. За акт је одговоран у техничком смислу стручни сарадник за информационе системе и рачунарску технику.

Број: 1741-02/17

У Суботици, 12.12.2017.године

Председник Савета

др Бранислав Филиповић