На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. гласник РС“, бр. 94/2016) директор Високе школе примењених стуковних студија у Врању донео је:

ПРАВИЛНИК О БЕЗБЕДНОСТИ
ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

1. Опште одредбе

Члан 1.

Овим Правилником се, у складу са Законом о информационој безбедности и Уредбом о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја, утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система, (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система Високе школе примењених струковних студија у Врању (у даљем тексту: Школа).

Члан 2.

Информациона добра Школе су сви ресурси који садрже пословне информације Школе, односно сви ресурси путем којих се врши израда, обрада, чување, пренос, брисање и уништвање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, веб презентацију и сл. О информационим добрима води се евиденција послова на посебном обрасцу од стране Инжењера информатике.

Члан 3.

Под пословима из области безбедности ИКТ система сматрају се:

- послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност,
- послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности
- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Школе, као и приступ, измена или коришћење средстава без овлашћења и без евиденције о томе.

- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу.

- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

2. Коришћење ИКТ система

Члан 4.

ИКТ системом управља надлежни субјект ИКТ система. Надлежни субјект ИКТ система је дужан да сваког новозапосленог - корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Школе.

Члан 5.

У случају промене радног места, односно надлежности корисника - запосленог надлежни субјект ИКТ система ће извршити промену права у коришћењу ИКТ система које је корисник -запослени имао у складу са описом радних задатака.

Члан 6.

У случају престанка радног ангажовања корисника - запосленог, кориснички налог се укида.

Корисник ИКТ ресурса, коме је престало радно ангажовање по било ком основу код Школе, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

Администраторски и кориснички налог

Члан 7.

Право приступа ИКТ систему имају само запослени, односни корисници који имају администраторске и корисничке налоге

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

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

Кориснички налог додељује администратор, на основу захтева запосленог задуженог за управљање људским ресурсима и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима. На основу послова и радних задатака

запосленог, администратор одређује права приступа у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог на пословима управљања људским ресурсима, односно надлежног руководиоца у организационим јединицима Школе.

Одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 8.

Кориснички налог се састоји од корисничког имена и лозинке.

Лозинка мора да садржи минимум седам карактера комбинованих од малих и великих слова и цифара.

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

Ако запослени - корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

3. Предмет, мере и субјекти заштите ИКТ Система

Члан 9.

Предмет заштите ИКТ система су:

- хардверске и софтверске компоненте ИКТ система
- подаци који се обрађују или чувају на компонентама ИКТ система
- кориснички налози и други подаци о корисницима информатичких ресурса ИКТ Система

Члан 10.

Мере прописане овим актом се односе на све организационе јединице ИКТ система Школе, на све запослене - кориснике информатичких ресурса.

Члан 11.

Мерама заштите ИКТ система Школе обезбеђује се превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности.

Ради заштите тајности, аутентичности и интегритета података, Школа може да размотри коришћење одговарајућих мера криптозаштите.

Члан 12.

За обављање послова из области безбедности ИКТ система Школе надлежан је Инжењер информатике.

Обавезе запослених

Члан 13.

Запослени у Школи је дужан да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система:

1) да користи информатичке ресурсе искључиво у пословне сврхе;

2) да 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) да поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;

4) да безбедно чува своје лозинке у односу на друга лица;

5) да мења лозинке сагласно утврђеним правилима;

6) да се, пре сваког удаљавања од радне станице, одјави са система, односно закључа радну станицу;

7) да користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење надлежног субјекта ИКТ система;

8) да захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;

9) да обезбеди сигурност података у складу са важећим прописима;

10) да приступа информатичким ресурсима само на основу изричито додељених корисничких права од стране надлежног субјекта;

11) да не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;

12) да не сме да на радној станици складишти садржај који не служи у пословне сврхе;

13) да израђује заштитне копије (бекапа) података у складу са прописаним процедурама;

14) да користи Интернет и Интернет е-маил сервис Оператора у складу са прописаним процедурама;

15) да прихвати да се одређене врсте информатичких интервенција обављају у утврђено време;

16) да прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;

17) да прихвати инсталацију техника и програма у циљу сигурности ИКТ система.

18) да не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

Ограничење приступа подацима и средствима за обраду података

Члан 14.

Приступ ресурсима ИКТ система одређен је врстом налога који запослени има.

Запослени који има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Запослени може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, сем администратору за подешавање корисничког профила и радног окружења. Запослени који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.

4. Појединачне мере заштите

Члан 15.

Простор у коме се налазе рачунари за вођење база података и централни рачунар (сервер), мрежна или комуникациона опрема ИКТ система, организује се као административна зона.

Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом.

Члан 16.

Приступ ресурсима ИКТ система са приватног уређаја није дозвољен, осим ако је уређај у власништву Оператера оштећен и није обезбеђена замена.

Сагласност на коришћење приватног уређаја у случају из става 1. овог члана даје непосредног руководиоца.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води надлежни субјект ИКТ система.

Формирање ранг листе кандидата

Члан 17.

База података кандидата који се рангирају је заштићена шифром.

Контролу уноса и промене података врши субјект ИКТ система уз надзор комисије за рангарање.

Сваки приступ бази података као и свака измена података се евидентира у специјалном лог фајлу и лог табели на локалном серверу.

Заштита носача података

Члан 18.

Подаци који се налазе у ИКТ систему представљају тајну у складу са одредбама Закона о слободном приступу информацијама од јавног значаја, Закона о заштити података о личности, Закона о тајности података, као и Уредбе о начину и поступку означавања тајности података, односно докумената.

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима.

Члан 19.

Надлежни субјект у ИКТ систему ће успоставити организацију приступа подацима, посебно онима који буду означени тајним у складу са Законом о тајности података, тако да документи са ознаком тајности могу да се сниме, односно архивирају или запишу на фајл серверу у фолдеру над којим ће право приступа имати само запослени - корисници који на то буду имали право.

У случају транспорта носача са подацима са ознаком тајности, непосредног руководиоца ће одредити одговорну особу и начин транспорта.

Приликом брисања података за ознаком тајности са носача на којима су се налазили, подаци морају бити неповратно обрисани, а ако то није могуће, такви носачи морају бити физички оштећени, односно уништени.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 20.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери који су намењени тестирању и развоју. Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера. Пре увођења у рад новог софтвера неопходно је направити копију - архиву постојећих података. Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове

верзије врши се по завршетку радног времена, како не би био заустављен оперативни рад запослених - корисника.

Заштита података и средства за обраду података од злонамерног софтвера

Члан 21.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, е-маилом, зараженим преносним медијима (USB меморија, CD и тд.), инсталацијом нелиценцираног софтвера и сл. За успешну заштиту од вируса на сваком рачунару се инсталира антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефиниција. Антивирусни програм у континуитету контролише рачунаре у реалном времену.

Заштита при коришћењу интернета

Члан 22.

У циљу заштите, односно упада у ИКТ систем Школе са интернета, надлежни субјект ИКТ система је дужан да одржава систем за спречавање упада путем Firewall-a или рутера.

Руководиоци организационих јединица Школе одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Функционери и запослени којима је одобрено коришћење интернета и електронске поште дужни су да приликом коришћења истог поступају по међународним конвенцијама и правилима понашања.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључење на интернет, односно прикључење преко сопственог модема.

Надлежни субјект ИКТ система може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система којима је одобрено коришћење интернета дужни су да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени - корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши надлежни субјект ИКТ система.

Приликом коришћења интернета корисник ИКТ система коме је одобрено коришћење интернета дужан је избегавати сумњиве WEB странице, у циљу спречавања инсталирања програма који могу нанети штету ИКТ систему. У случају да корисник примети необично понашање рачунара, ту појаву је дужан да без одлагања пријави надлежном субјекту ИКТ система.

Члан 23.

Кориснику ИКТ система коме је дозвољено коришћење интернета забрањено је гледање филмова и играње игрица на рачунарима и претраживање WEB страница које садрже порнографски и остали недоличан садржај, као и самовољно преузимање истих са интернета.

Члан 24.

Недозвољена употреба интернета обухвата и:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друга врста недозвољених софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено одлуком надлежног органа Школе;
- преузимање података у количини која проузрокује велико оптерећење на мрежи;
- преузимање материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом;
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

Заштита од губитка података

Члан 25.

Базе података и остали фајлови се обавезно архивирају на бекуп диску, најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

Члан 26.

Дневно копирање - архивирање врши се аутоматски за сваки радни дан у седмици, у 16:00 часова сваког радног дана у седишту Школе.

Недељно копирање - архивирање врши се последњег радног дана у недељи.

Месечно копирање - архивирање врши се последњег радног дана у месецу, за сваки месец посебно.

Годишње копирање - архивирање врши се последњег радног дана у години.

Члан 27.

За потребе обнове базе података у случају пожара, поплава итд. бекапована база података се мора чувати ван институције.

Чување података о догађајима који могу бити од значајаза безбедност ИКТ система

Члан 28.

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

Систем за контролу

Члан 29.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и другим могућим проблемима у ИКТ систему, мора бити подешен тако да одмах обавештава надлежног субјекта ИКТ система о свим нерегуларним активностима запослених - корисника, покушајима упада и упадима у систем.

Контрола приступа заштићеним фајловима

Члан 30.

ИКТ систем има могућност регистровања неуспелих пријава ка поверљивим информацијама. Такве пријаве се евидентирају у специјалном лог фајлу као и у лог табели на локалном серверу.

После неколико неуспелих покушаја систем ће аутоматски блокирати налог корисника којим се приступа подацима, забележити локалну адресу рачунара као и корисничко име, датум и време приступа.

Члан 31.

Субјект ИКТ система је дужан да неуспеле пријаве и блокаде налога провери и уколико није било злонамерног упада, активира налог корисника система.

Заштита од злоупотребе безбедносних слабости ИКТ система

Члан 32.

Надлежни субјект ИКТ система најмање једном месечно, а по потреби и чешће врши анализу дневника активности (лога) у циљу идентификације потенцијалних слабости ИКТ система.

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

Ревизија ИКТ система

Члан 33.

Ревизија ИКТ система се мора вршити тако да не омета пословне процесе корисниказапослених. Надлежни субјект ИКТ система одредиће време обављања ревизије, у зависности од врсте послова и радних задатака запослених – корисника у Школи.

Заштита опреме ИКТ система

Члан 34.

Комуникациони каблови и каблови за напање морају бити постављени у зид или каналнице, тако да се онемогући неовлашћен приступ, односно да се изврши изолација.

Надлежни субјект ИКТ система је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коју могу да користе посетиоци објеката, мора бити одвојена од интерне мреже коју користе корисници запослени и кроз коју се врши размена службених података. Та мрежа треба да буде означена (SSID).

Превентивне мере и реаговање на безбедносне инциденте

Члан 34.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени - корисник је дужан да одмах обавести надлежниог субјекта ИКТ система.

По пријему пријаве става 1. овог члана надлежни субјект ИКТ система је дужан да одмах обавести непосредног руководиоца и предузме мере у циљу заштите ресурса ИКТ система.

5. Провера ИКТ система

Члан 35.

Проверу ИКТ система врши надлежни субјект ИКТ система.

6. Повреда радне обавезе

Члан 36.

Непоштовање одредби овог Правилника представља повреду радних обавеза.

Члан 37.

Свако коришћење ИКТ ресурса Школе од стране запосленог - корисника, ван додељених овлашћења представља неовлашћено коришћење имовине.

Члан 38.

Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже може се одузети право приступа.

7. Едукација запослених

Члан 39.

Запослени у ИТ сектору се морају едуковати о новим технолошким достигнућима, савременим претњама на пољу информационих система.

Члан 40.

Субјект ИКТ система је дужан да организује курсеве за обуку и осавремењавање знања запослених Школе из домена информационих технологија како би се подигла свест о новим претњама које могу да угрозе ИКТ систем.

7. Измена правилника

Члан 41.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност надлежни субјект ИКТ система је дужан да обавести непосредног руководиоца, како би он могао да приступи измени овог Правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивања овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

8. Прелазнем и завршне одредбе

Члан 42.

Овај Правилник ступа на снагу даном доношења.

Директор

_____

др Љиљана Ђорђевић, проф.с.с