ВИСОКА ТЕХНИЧКА МАШИНСКА ШКОЛА СТРУКОВНИХ СТУДИЈА
ТРСТЕНИК

ПРАВИЛНИК
О БЕЗБЕНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

Трстеник, АПРИЛ 2019.

Висока техничка
машинска школа
струковних студија
Број: 107/2019-01
Датум: 12. 04. 2019.
Т р с т е н и к

На основу члана 8. Закона о информационој безбедности Републике Србије („Сл. гласник РС“ бр. 6/2016 и 94/2017) и члана 97. и 171. став 4. Статута Високе техничке машинске школе струковних студија Трстеник, вршилац дужности директора Високе техничке машинске школе струковних студија Трстеник, доноси

ПРАВИЛНИК
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ВИСОКЕ ТЕХНИЧКЕ МАШИНСКЕ ШКОЛЕ СТРУКОВНИХ СТУДИЈА ТРСТЕНИК

Предмет Акта

Члан 1.

Правилником о безбедности информационо-комуникационог система (У даљем тексту: Правилник), ближе се дефинишу мере заштите информационо-комуникационог система на Високој техничкој машинској школи струковних студија Трстеник (У даљем тексту: Школа), а нарочито принципи и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса на Школи.

Члан 2.

Циљеви доношења Правилника су:

1) допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
2) минимизација безбедносних инцидената;
3) допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистентне контроле свих компонената информационо-комуникационог система (У даљем тексту: ИКТ систем).

Обавезност Акта

Члан 3.

Овај Правилник је обавезујући за све унутрашње јединице Школе и за све кориснике информатичких ресурса, као и за трећа лица која користе информатичке ресурсе Школе.

Непоштовање овог Правилника, повлачи дисциплинску одговорност корисника информатичких ресурса у складу са општим актима Школе.

За праћење примене овог Правилника надлежна је Катедра за информатику (У даљем тексту: Катедра за ИТ).

Појмови

Члан 4.

Поједини изрази употребљени у овом Правилнику 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 немогућност 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 аутентификацију (проверу идентитета корисника) и ауторизацију (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 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 сме бити компромитован.

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 заштите обухвата:

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

Корисник информатичких ресурса

Члан 8.

Корисник информатичких ресурса јесте постављено лице, запослено лице на неодређено или одређено 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.

Дужност корисника информатичких ресурса

Члан 9.

Корисник не сме да спроводи 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 радне станице је дужан да пословне податке смешта на локалне дискове непреносиве радне станице или мрежне дискове.

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

Корисник информатичких ресурса дужан је да поштује и 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 сагласно утврђеним правилима;
5) мења лозинке сагласно утврђеним правилима;
6) пре сваког удаљавања од радне станице, одјави се са система („излогује“), односно закључа радну станицу (CTRL+ALT+DEL+LOCK или WINDOWS L);
7) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8) обезбеди сигурност података у складу са 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 заштитне копије података (*backup*) у складу са прописаним процедурама;
13) користи *Internet* и *Internet e-mail* сервис на 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 технике сигурности (антивирус програм, *firewall*, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) које спречавају потенцијалне претње ИКТ систему;
17) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

Безбедносни профил корисника информатичких ресурса

Члан 10.

У зависности од описа задатака и послова радног места на које је распоређен, корисник информатичких 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 на Школи.

Креирање лозинке

Члан 11.

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

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

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 13.

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

Поступци у случајевима сигурносних инцидената

Члан 14.

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

Информацију о инциденту, руководилац из става 1. овог члана дужан је да одмах проследи администратору, као и Катедри за информатику.

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) вишеструког покушаја неауторизованог приступа;
4) системских радова и престанка рада сервиса.

Катедра за ИТ је дужна 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 15.

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.

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

Сигурност електронске поште

Члан 16.

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;
3) не смеју се користити приватни налози електронске поште у пословне сврхе;
4) програми који користе сервисе електронске поште морају се искључити када се рачунар не користи.

Поступање са преносивим медијима

Члан 17.

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

Преносиви медији из става 1. овог члана, пре стављања ван употребе, морају бити физички уништени.

Физичка сигурност информатичких ресурса

Члан 18.

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови:
1) сервери, сторици (*storage*) и комуникационо чвориште у седишту Школе морају бити смештени у посебној просторији (сервер сала) која испуњава стандарде противпожарне заштите и поседује редундантно напајање електричном струјом и адекватну климатизацију;

2) приступ сервер сали, поред лица која су задужена за одржавање ИКТ система, могу имати друга лица, уз претходно одобрење шефа Катедре за ИТ;
3) радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичких 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 морају бити заштићени од неауторизованог приступа и прегледа.

Приступ ИКТ Школе

Члан 19.

Приступ свим компонентама ИКТ система мора бити аутентификован.

Администратор, на основу прецизног писаног захтева непосредног руководиоца, додељује кориснику информационог 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, на Школи, кориснику информатичких ресурса укида се право приступа ИКТ систему.

О престанку радног односа или радног ангажовања, као и о промени радног места корисника информатичких ресурса, непосредни руководилац је дужан да обавести администратора ради укидања, односно измена приступних привилегија тог корисника.

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

Трећем лицу могу се 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 7. овог члана, у случају неопходних и хитних послова могу се одобрити права приступа ИКТ систему трећем лицу по усменом налогу директора Школе, односно овлашћеног лица, о чему ће накнадно, по завршетку посла, сачинити записник о оствареном приступу.

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

Инсталација и одржавање софтвера

Члан 20.

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

Катедра за ИТ обезбеђује запосленом, односно радно ангажованом лицу, коришћење радне станице (десктоп или лап-топ) са преинсталираним и правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачки програми-драјвери, пословно и развојно окружење, софтвер за вирусну заштиту, разне помоћне апликације), који је типски за све радне станице и који представља минимум потребан за обављање стандардних послова.

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

Основна подешавања из става 2. овог члана су:

1) додељивање имена и TCP/IP адреса радној станици и њено придруживање домену или радној групи;
2) подешавање *mail*-клијента;
3) подешавање *Web*-претраживача (TCP/IP-адреса прокси сервера);
4) инсталација антивирусног софтвера;
5) инсталација званичног апликативног софтвера који одређене унутрашње јединице Школе користе у свом раду;

У случају да је кориснику потребно да се изврши инсталација одређеног специфичног софтвера на радној станици, непосредни руководилац подноси захтев електронским путем Катедри за ИТ.

Проблем у функционисању антивирусног антиспајвер 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.

Завршне одредбе

Члан 21.

Правилник ступа на снагу осмог дана од дана објављивања истицањем на интернет страници Школе.

в.д. директора
др Миломир Мијатовић, проф.