

Дел. бр. 1235
Датум: 13. новембар 2019.

На основу члана 119. став 1. тачка 1) Закона о основама система образовања и васпитања (у даљем тексту „Закон“) - („Службени гласник РС“ бр. 88/2017 и 27/2018- др. закони и 10/2019), члана 94. став 1. тачка 1) Статута МШ „Ватрослав Лисински“, дел. бр. 766 од 28. 08. 2019. године, члана 8. Закона о информационој безбедности („Службени гласник РС“, број 6/16, 94/2017, 77/2019), чланова 1-8. 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 од 24. 11. 2016. године), у поступку спровођења Плана интегритета, Школски одбор МШ „Ватрослав Лисински“, у Београду, дана 13. 11. 2019. године, једногласно доноси

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

I Опште одредбе

Члан 1.

Овим актом ближе се дефинишу мере заштите информационо-комуникационих система у МШ „Ватрослав Лисински“, (у даљем тексту Школа), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса у Школи.

II Циљеви

Члан 2.

Циљеви доношења овог акта су :

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

У случају обраде података о личности приликом вршења надлежности и испуњења обавеза из овог закона поступа се у складу са прописима који уређују заштиту података о личности.

III Обавезност

Члан 3.

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

Непоштовање овог акта повлачи дисциплинску одговорност корисника информатичких ресурса.

За праћење примене овог акта надлежни су директор Школе и администратори мреже Школе.

IV Појмови

Члан 4.

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 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 и нивое компетенција);
- 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, и додељује се искључиво администратору.

V Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају обављање делатности Школе, као и 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.

VI 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.

VII Предмет заштите

Члан 7.

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.

VIII Корисник информатичких ресурса

Члан 8.

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.

IX Дужности корисника информатичких ресурса

Члан 9.

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.

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 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 директора 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 неубичајено и неоправдано великог коришћења информатичких ресурса Школе, а посебно у приватне сврхе.

X Безбедносни профил корисника информатичких ресурса

Члан 10.

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.

XI Креирање лозинке

Члан 11.

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.

XII Употреба корисничког налога

Члан 12.

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).

XIII Употреба администраторског налога

Члан 13.

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.

XIV Поступци у случајевима сигурносних инцидената

Члан 14.

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 руководиоца 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.

Корисник 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.

XV Заштита од малициозног софтвера

Члан 15.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена правила за заштиту од ризика приликом преузимања фајлова из екстерних извора (података, апликација и сл).

Приликом преузимања фајлова из става 1. тачка 1) 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.

XVI 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 отворати 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.

XVII Поступање са преносивим медијима

Члан 17.

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.

XVIII Физичка сигурност информатичких ресурса

Члан 18.

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

- 1) просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
- 2) штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;
- 3) медији са поверљивим подацима (USB и екстерни hard diskovi) морају бити заштићени од неауторизованог приступа и прегледа.

XIX Приступ ИКТ систему Школе

Члан 19.

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.

XX Инсталација и одржавање софтвера

Члан 20.

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

Управа Школе обезбеђује запосленом, односно, ангажованом лицу, коришћење радне станице (десктоп или лаптоп) са преинсталираним и правилно и потпуно конфигурираним 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 представља 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 управе 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, 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.

XXI Завршна одредба

Члан 21.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли и интернет мрежи Школе.

Председник Школског одбора
Душица Радуловић

Правилник је заведен под деловодним бројем 1235, од 13. 11. 2019. године, објављен на огласној табли Школе дана 14. 11. 2019. године, а ступа на снагу дана 22. 11. 2019. године.

Секретар школе
Биљана Столић