Основна школа „Павле Поповић“
Трг палих бораца број 3
11 427 Вранић

Правилник о безбедности информационо - комуникационог система ОШ „Павле Поповић"

Вранић, децембар 2022. године

Република Србија
Град Београд, општина Барајево
ОШ „Павле Поповић“ Вранић
Трг палих бораца 3

Телефон: 011/8332-022
Е-пошта:
direktor.ospavlepopovic@gmail.com
ospavlepopovicvranic@gmail.com
www.ospavlepopovic.edu.rs
ПИБ бр.100141791 МБ -07001185
Текући рачун број 840-1285660-62

Деловодни број: 1956-2-22
Дана: 29. 12. 2022. године

На основу члана 119. став 1. тачка 1. Закона о основама система образовања и васпитања („Службени гласник РС” бр. 88/2017, 27/2018 - други закони и 10/2019), а у вези примене Закона о информационој безбедности („Сл. гласник РС”, број 6/2016 и 94/2017), члана 2. Уредбе о 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 („Сл. Гласник РС“, бр. 94/2016), Школски одбор ОШ „Павле Поповић“ на четвртој редовној седници која је одржана 29. 12. 2022 године доноси:

О Д Л У К У

1. Доноси се Правилник о безбедности информационо - комуникационог система ОШ „Павле Поповић" (деловодни број 1956-1-22 од 29. 12. 2022. године)

Образложење

Школски одбор је у писаној форми и електронској форми добио на увид Правилник о безбедности информационо - комуникационог система ОШ „Павле Поповић". Одлука о доношењу Правилника о безбедности информационо - комуникационог система ОШ „Павле Поповић" је саставни део Правилника.
Правилник о безбедности информационо - комуникационог система ОШ „Павле Поповић" је представио Дејан Тмушић, секретар установе.

Имајући у виду све изнето Школски одбор је одлучио као у изреци одлуке.

Поука о правном леку: Одлука органа управљања је коначна.

Председник Школског одбора

Сузана Јевтић

На основу члана 119. став 1. тачка 1. Закона о основама система образовања и васпитања („Службени гласник РС” бр. 88/2017, 27/2018 - други закони и 10/2019), а у вези примене Закона о информационој безбедности („Сл. гласник РС”, број 6/2016 и 94/2017), члана 2. Уредбе о 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 („Сл. Гласник РС“, бр. 94/2016), п Школски одбор ОШ „ Павле Поповић“ на четвртој редовној седници која је одржана 29.12. 2022 године донос:

ПРАВИЛНИК
о безбедности информационо - комуникационог система

Уводне одредбе
Члан 1.

Овим правилником, у складу са Законом о информационој безбедности и Уредбом 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 („Сл. Гласник РС“, бр. 94/2016), утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система у Основној школи „Павле Поповић“ (у даљем тексту: Школа).

Члан 2.

Мере прописане овим правилником се односе на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе школе.

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

1) информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата:

- електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
- 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;
- податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКТ системом;

2) 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;

3) тајност је својство које значи да податак није доступан неовлашћеним лицима;

4) интегритет значи очуваност изворног садржаја и комплетности податка;

5) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) 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;

7) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

8) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

9) 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;

10) инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

11) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

12) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

13) ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

14) компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

15) криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

16) криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

17) криптографски производ је софтвер или уређај путем кога се врши криптозаштита;

18) криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

19) безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

20) информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

24) Download је трансфер података са централног рачунара или web презентације на локални рачунар;

25) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;

26) Freeware је бесплатан софтвер;

27) Opensource софтвер отвореног кода;

28) 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;

29) USB или флеш меморија је спољашњи медијум за складиштење података;

30) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;

31) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

Мере заштите

Члан 4.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Члан 5.

Сваки запослени-корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности.

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност;
- послови управљање 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, измене 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.

У случају инцидента запослени обавештава техничара одржавања информационих система и технологија.

Члан 7.

У случају промене послова, односно надлежности корисника-запосленог, Запослени на радном месту техничара одржавања информационих система и технологија ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу налога директора школе.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида, директор школе је обавезан да именује другог запосленог као корисника корисничког налога и да о томе обавести писменим путем запосленог на радном месту техничара одржавања информационих система и технологија и новог корисника налога.

Директор школе је дужан да о промени налога спроведе поступак давања овлашћења односно промени овлашћења надлежној институцији, најкасније у року од седам дана од дана доношења решења о промени привилегија, односно у року од седам дана од дана престанка радног односа запосленог који је био корисник привилегија.

Корисник ИКТ ресурса, након престанка радног ангажовања у школи, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

Електронски дневник (есДневник)

Члан 8.

Запослени који имају приступ есДневнику имају обавезу чувања података у њему, о било ком лицу, у било ком облику (укључујући и коришћење туторијала у виду снимака екрана на којима се виде или помоћу којих је могуће открити било који податак о лицу), осим ако за то постоји изричита писана сагласност лица на које се податак односи, односно родитеља или законског заступника малолетног лица

Двофакторску аутентификацију су обавезни да користе директор, координатори есДневника, стручни сарадници, организатор практичне наставе, одељењске старешине и друга лица по решењу директора.

Препорука је да и сви наставници имају двофакторску аутентификацију.

Наставници који не користе двофакторску аутентификацију, имају обавезу да користе јаку лозинку.

Јака лозинка треба да садржи бар једно мало слово, бар једно велико слово, бар једну цифру, бар један знак који није ни слово ни цифра и треба да буде веће дужине, препоручено најмање 10 карактера. Није дозвољено коришћење лозинки наведених у упутствима и туторијалима (тестне лозинке попут "тест123 или админ), како би се спречила свака могућност неовлашћеног приступа есДневнику и подацима који су у њему садржани. Такође, не препоручује се да лозинке садрже податке о особи (лична имена и презимена. као ни датуме рођења), податке о школи (назив школе, адресу школе, као ни било који други општепознат податак о школи), као ни друге податке који се лако могу асоцирати са лицем које штити свој приступ есДневнику.

У случају радног ангажовања лица на радно место наставника, стручног сарадника, организатора практичне наставе и директора установе, координатор есДневника додељује приступ есДневнику, у складу са послом који запослени обавља.

У случају престанка радног ангажовања лица из става 6. овог члана, а координатор есДневника, одузима право приступа наставника есДневнику са даном престанка радног ангажовања лица.

Заштита података и средства за обраду података од злонамерног софтвера

Члан 9.

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, имејлом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефиниција, а најмање једном месечно.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером.

Ризик од евентуалног губитка података приликом чишћења медија од вируса сноси доносилац медија.

У циљу заштите, односно упада у ИКТ систем школе са интернета, запослени на радном месту одржавања рачунара је дужан да одржава систем за спречавање упада.

Корисници ИКТ система који користе интернет морају 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 запослени на радном месту одржавања рачунара.

Приликом коришћења интернета треба избегавати сумњиве WEB странице, с обзиром да то може проузроковати проблеме - неприметно инсталирање шпијунских програма и слично.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави запослени на радном месту одржавања рачунара.

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" WEB страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

Недозвољена употреба интернета обухвата:

- 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 друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимање (download) података велике “тежине” које проузрокује “загушење” на мрежи;
- преузимање (download) материјала заштићених ауторским правима;

- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

Заштита од губитка података
Обезбеђивање интегритета софтвера и оперативних система

Члан 10.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву школе, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само запослени на радном месту одржавања рачунара.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера.

Пре сваке инсталације нове верзије софтвера, односно подешавања, неопходно је направити копију постојећег, како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 11.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, router, firewall), која се налази у учионицама, се мора налазити у закључаном rack орману.

Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система

Члан 12.

Размена података са Министарством просвете, Трезором, Пореском управом Централним регистром социјалног и здравственог осигурања Управом за јавне набавке, Агенција за борбу против корупције и сличним институцијама са којом се врши размена података се врши у складу са Уговором (протоколом).

Запослени који имају администраторске или корисничке налоге.

Члан 13.

Запослени у школи који имају кориснички или административни налог су:

1. За рад на Порталу Централног регистра социјалног осигурања секретар школе а у његовом одсуству шеф рачуноводства и директор установе;

2. За рад у програму «Доситеј» лице које је одређено Решењем директора и директор,
3. За рад на порталу Пореске управе и Трезора шеф рачуноводства а у његовом одсуству административни радник, уз писмену примопредају токена ,
4. За рад на порталу министарства финснсија„Искра“ Секретар установе, шеф рачуноводства и административно финансијски радник;
5. За рад на електронском дневнику одељењски старешина, стручни сарадник, организатор практичне наставе, директор и координатор ес Дневника;
6. За рад на издавању јавних исправа административни радник а у његовом одсуству помоћник директора школе;
7. За рад на електронском упису ученика, лице које именује директор,
8. За рад на Порталу јавних набавки секретар школе, у његовом одсуству шеф рачуноводста,
9. За рад на веб сајту школе директор или задужен наставник у оквиру 40 часовне радне недеље,
10. За рад на финансијској документацији шеф рачуноводства,
11. За рад на ПП документацији, педагог односно психолог школе,
12. За рад на одржавању мреже лице по уговору, односно запослени на одржавању рачунара,
13. За рад на датотеци рачунара у зборници сви запослени у настави.

Прелазне и завршне одредбе
Члан 14.

У случају да школа изменом систематизације радних места изгуби радно место запосленог техничара одржавања информационих система и технологија или запослено лице на том радном месту престане са радом послове, обавезу и одговорност запосленог на одржавању рачунара прописане овим Правилником преузима лице са којим школа закључи уговор о обављању тих послова.

Члан 15.

Измене и допуне овог Правилника врше се по постуку доношења Правилника.

Члан 16.

Правилник ступа на снагу осмог дана од дана објављивања на огласној табли Установе.

Председница Школског одбора

_____

Сузана Јевтић

Правилник је заведен под деловодним бројем 1956-1-22 од 29. 12. 2022. године, а објављен је на огласној табли Установе, дана 29. 12. 2022. године. Правилник ступа на снагу 06. 01. 2023. године.

Секретар установе

_____

Дејан Тмушић