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, 10/2019, 6/2020 и 129/2021), члана 8. 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 ("Службени гласник РС", бр. 94/2016) и члана 60. Став 1. тачка 1) Статута Основне школе „Надежда Петровић“ у Сићеву, Школски одбор Основне школе „Надежда Петровић“ у Сићеву, на седници одржаној дана 30.06.2023.године доноси

ПРАВИЛНИК

о безбедности информационо - комуникационог система Основне школе “Надежда Петровић” у Сићеву

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, начин провере информационо-комуникационих система од посебног значаја и садржај извештаја о провери информационо-комуникационог система од посебног значаја, 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 Основне школе “Надежда Петровић” у Сићеву (у даљем тексту: ИКТ систем).

Члан 2.

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

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса школе.

За праћење примене овог правилника обавезује се овлашћено лице школе или лице кога оно одреди.

Члан 3.

Установа је дужна да обезбеди да се:

а) чувају копије података на потпуно заштићеном серверу ван установе, односно на екстерној меморији која се налази ван установе,

б) лог фајлови – посебни хронолошки записи о ИТ активностима, чувају ван установе, 2

в) аутоматски региструју неуспеле пријаве ка поверљивим и осетљивим подацима,

г) омогући систему да препознаје са ког рачунара је извршена неуспела пријава,

д) омогући аутоматска забрана у случају понављања неуспелих пријава,

ђ) истраже неуспеле пријаве, ако се покажу сумњивим – у зависности од броја покушаја пријављивања и нивоа поверљивости података који се траже.

Члан 4.

Поједини термини у смислу овог правилника имају следеће значење:

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

(1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;

(2) 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;

(3) 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;

(4) 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;

21) ВПН (Виртуал Привате Нетворк)-је "приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;

22) МАЦ адреса (Медиа Аццесс Цонтрол Аддресс) је јединствен број, којим се врши идентификација уређаја на мрежи;

23) Бацкуп је резервна копија података;

24) Довнлоад је трансфер података са централног рачунара или веб презентације на локални рачунар;

25) УПС (Унинтерруптибле повер супплу*)* је уређај за непрекидно напајање електричном енергијом;

26) Фреевare је бесплатан софтвер;

27) Опенсоурце софтвер отвореног кода;

28) Фиревалл је "заштитни зид" односносистем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

29) УСБ или флеш меморија је спољшњи медијум за складиштење података;

30) ЦД-РОМ (Цомпацт диск - реад онлу мемору) се користи као медијум за снимање података;

31) ДВД је оптички диск високог капацитета који се користи као медијум за складиштење података.

Мере заштите

Члан 5.

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.

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Основне школе “Надежда Петровић” Сићево

Члан 6.

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

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Основне школе “Надежда Петровић” Сићево, надлежан је овлашћено лице школе.

Члан 7.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава иимовине 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 Града/Општине/Градске општине, 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.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 8.

Рад на даљину и употреба мобилних уређаја у ИКТ систему није омогућен.

Нерегистровани корисници, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ Интернету али не и деловима мреже кроз коју се обавља службена комуникација.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем ВПН мреже ИКТ система и листе МАЦ адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Приступ ресурсима ИКТ система са удаљених локација, од стране запослених-корисника, у циљу обављања радних задатака, омогућен је путем заштићене ВПН/интернет конекције.

Запосленом-кориснику, забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.)

Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен, осим ако је уређај у власништву Града/Општине/Градске општине, оштећен и није обезбеђена замена.

3. Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност

Члан 9.

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места.

Свако коришћење ИКТ ресурса од стране запосленог-корисника, ван додељених овлашћење, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

4. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Члан 10.

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

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

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра школе су сви ресурси који садрже пословне информације, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем и сл.)

Евиденцију о информационим добрима води запослени кога одреди директор школе, у папирној или електронској форми.

Предмет заштите 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.

6. Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности

Члан 12.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебним прописима *(Закон о слободном приступу информацијама од јавног значаја ("Сл. гласник РС", бр.120/04, 54/07, 104/09 И 36/10), Закон о заштити података*

о личности ("Сл. гласник РС", бр.97/08,104/09-ДР. Закон 68/12,-ОДЛУКА УС И 107/2012), Закон о тајности података ("Сл. гласник РС", 104/2009), као и Уредба о начину и поступку означавања тајности података, односно докумената ("Сл. гласник РС", бр. 8/2011).

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима ("Сл. гласник РС", бр. 53/2011).

7. Ограничење приступа подацима и средствима за обраду података

Члан 13.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник 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 - корисник 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 радне станице.

Запослени-корисник који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.

Запослени-корисник дужан је да поштује и следећа правила *(у складу са архитектуром ИКТ система (домен-без домена), прилагодити правила систему)* безбедног и примереног коришћења ресурса ИКТ система, 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 ОШ “Надежда Петровић” Сићево 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) мења лозинке сагласно утврђеним правилима;

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

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

11) израђује заштитне копије (бацкуп) података у складу са прописаним процедурама;

12) користи интернет и електронску пошту у школи у складу са прописаним процедурама;

13) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;

14) прихвати да технике сигурности (анти вирус програми, фиревалл, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;

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

8. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Члан 14.

Право приступа имају само запослени/корисници који имају администраторске или корисничке налоге.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу кога/јих 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 у сарадњи са непосредним руководиоцем и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима, а 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.

9. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

Лозинка мора да садржи минимум осам 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 запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Запослени-корисник дужан је да мења лозинку најмање једном у шест месеци.

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

Кориснички налог може да се се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр. лична карта са чипом и уписаним сертификатом).

Пријављивање у ИКТ систем школе се врши убацивањем медија са електронским сертификатом у читач картица.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

10. Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Члан 16.

Приступ ресурсима ИКТ система школе не захтева посебну криптозаштиту.

Запослени-корисници користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама.

Запослени на пословима ИКТ су задужени за инсталацију потребног софтвера и хардвера за коришћење сертификата.

Запослени-корисници су дужни да чувају своје квалификоване електронске сертификате како не би дошли у посед других лица.

11. Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему

Члан 17.

Простор мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор).

12. Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем

Члан 18.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система/запосленима на пословима ИКТ.

Прозори и врата на овој просторији морају увек бити затворени.

Сервери и активна мрежна опрема (cwитцх, модем, роутер, фирewалл), морају стално бити прикључени на уређаје за непрекидно напајање - УПС.

У случају нестанка електричне енергије, у периоду дужем од капацитета УПС-а, овлашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења начелника.

13. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију.

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запослених-корисника.

У случају да се на новој верзији софтвера који је уведен у оперативни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери и подаци који су намењени тестирању и развоју.

14. Заштита података и средства за обраду података од злонамерног софтвера

Члан 20.

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 (УСБ меморија, ЦД итд.), инсталацијом нелиценцираног софтвера и сл.

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.

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

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" WEБ 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 (downлоад) података велике "тежине" које проузрокује "загушење" на мрежи;

- преузимање (downлоад) 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.

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

15. Заштита од губитка података

Члан 21.

Базе података обавезно се архивирају на преносиве медије (ЦДРОМ, ДВД, УСБ, "стример" трака, екстерни хард диск), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

Остали фајлови-документи се архивирају најмање једном недељно, месечно и годишње.

Подаци о запосленима-корисницима, архивирају се најмање једном месечно.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе ("Сл. Гласник РС", бр 10/93, 14/93-испр. и 67/2016).

16. Обезбеђивање интегритета софтвера и оперативних система

Члан 22.

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.

17. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 23.

Овлашћено лице школе најмање једном месечно а по потреби и чешће врши анализу дневника активности (ацтивитулог, хистору, сецуритулог, трансацтионлог и др) у циљу идентификације потенцијалних слабости ИКТ система.

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

18. Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама

Члан 24.

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

Овлашћено лице школе или лице кога оно овласти води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Измена Правилника о безбедности

Члан 25.

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, овлашћено лице школе би могло да приступи измени овог правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Провера ИКТ система

Члан 26.

Проверу ИКТ система врши овлашћено лице школе.

Проверу ИКТ система ће вршити лице које буде изабрано у складу са одредбама Закона о јавним набавкама.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на која се врши упућивање, са прописаним условима, односно проверава да ли су правилником адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;

2) проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама

интервјуа, симулације, посматрања, увида у предвиђене евиденције и другу документацију;

3) врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

ПРЕДСЕДНИК ШКОЛСКОГ ОДБОРА,

_____

.

Правилник је заведен под деловодним бројем_____ од _____2023. године, објављен је на огласној табли Школе дана_____2023.године, а ступио је снагу дана_____2023.године.

Секретар,

_____

Марија

Милутиновић