РЕПУБЛИКА СРБИЈА

ОШ“ДЕСАНКА МАКСИМОВИЋ“КАТУН

Бр:02-

Дана:

КАТУН

На основу члана 119.став1.тачка 1.Закона о основама система образовања и васпитања(„Службени гласникРС“ Бр.88/2017,27/2018-други закони И 10/2019,6/2020 и 129/2021) а у вези Закона о информационој безбедности("Сл.гласник РС“, број6/2016,94/2017 и 77/2019), и члана 2.Уредбе о ближем садржају акта о безбедности информацоних система од посебног значаја, начину провере и садржаја извештаја о провери безбедности информационо-комуникационих система од посебног значаја („СЛ.гласник РС“, бр.94/2016)Школски одбор ОШ“Десанка Максимовић“, донео је дана 28.01.2022.године

**ПРАВИЛНИК**

**О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА**

**Уводне одредбе**

**Члан1.**

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.гласникРС“, ббр.94/2016), утврђује се мере заштите , принципи, начин и процедуре постизања и државања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система у ОШ“Десанка Максимовић“( у даљем тексту:школа)

**Члан2.**

 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 тремини у смислу овог правилника имају следеће значење :

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

.елетронске комуникационе мреже у смислу закона који уређује елетронске комуникације;

.уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја , врши аутоматска обрада подтака коришћењем рачунарског програма;

.податке који се воде , чувају, обрађују, претражују или преносе помоћу срдстава из подтач.(1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

.организациона структуру путем које се управља ИКТ сиситемом;

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 интегритете, расположивост,аутентичност и непорецивост тих података , да би тај сиистем функционисао како 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 комплетност података;

5) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда кака 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 одређенарадња или 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 остани у прописаним и прихватљивим оквирима;

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

11)мере заштите ИКТ система су техничке и организациооне 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 елетромагнетно значење (КЕМЗ) представља ненамерне елетромагнетне емисије приликом преноса , обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

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

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

17) криптографски производ је софтер 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 поадци;

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

21) Downald је трасфер података са центарлног рачунара или web презентације на локални рачунар;

22)UPS(UNINTERRRUPTIBLE POWER SUPPLY) је уређај за непрекидно напајање елетричном енергијом;

23) Opensource софтер отвореног кода

24)Firewall je „заштитни зид“ односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

25) USB или флеш меморија је спољашни медијум за складиштеа података;

26)CD-ROM(compact disk-read onlu memory) се користи као медијум за снимање података;

27) DVD је оптички диск високог квалитета који се кориси као медијум за складиштење података;

**Члан 4**

Послове одржавања ИКТ система може вршити лице запослено на радном месту техничара одржавања ИКТ система , лице ангажовано по уговору или запослени у школи по налогу директора;

**Члан 5**

Мере 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 пружћања услуга другим лицима.

**Члан 6**

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

**Члан 7**

 Под пословима из области безбодности утврђују се

.послови заштите информационих добара, односно средстава 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 , оштећење или злоупотребе средстава, односно информационих добара ИКТ система школе, као и приступ , измене или коришћење средстава без овлашћења и евиденцијено томе;

Бекап података неопходних за обављање делатности

.спречавање изношења тајних података изван ИКТ система школе

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

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

**ЕЛЕТРОНСКИ ДНЕВНИК**

**Члан 8**

Запослени који имају приступ есДневнику имају обавезу чувања података у њему, о било ком лицу , и било ком облику( укључујући и коришћење туторијала ( упуства ) у виду снимака екрана на којима се вииде 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, одељенске старешине и друга лица по решењу директора.

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 упуствима и туторијалима(тестне лозинке попут „тест 123 или админ), Како би се спречила свака могућност неовлашћеног приступа есДневнику и подацима који су у њему садржани.Такође, не препоручује се да лозинка 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), каоо ни друге податке који се лако могу асоцирати са лицем свој приступ есДневнику.

 У случају радног ангажовања лица на радно место наставника, стручног сарадника 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 , координатор есДневника, одузима право приступа наставника есДневнику са даном престанка радног ангажовања лица.

**ЗАШТИТА ПОДАТАКА И СРЕДСТВА ЗА ОБРАДУ ПОДАТАКА ОД ЗЛОНАМЕРНОГ СОФТЕРА**

**Члан 9**

 Заштита од злонамерног софтера 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 софтера 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 софтера током скенирања преносних медија.

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

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 или лице ангажовано на пословима одржавања рачунара , је дужан да одржава ситем 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 или лице ангажованои на пословима одржавања рачунара.

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

 У случају да корисник примети необично понашање рачунара, запажање треба без олагања да пријави лицу запосленом или ангажованом 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 доступних“пиратских“ или других софтерских 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 софтера);

.недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено:;

.преузимање(downland) података велике тежине које проузрокује“загушивање“ На мрежи;

. преузимање (downland) материјала заштићених ауторским правима;

. коришћење линкова који нису у вези са послом ( гледање филмова , аудио и видеостреаминг и сл)

. недозвољен приступ, промена, брисање или прерада садржаја преко интернета.

**ЗАШТИТА ОД ГУБИТКА ПОДАТАКА**

**ОБЕЗБЕЂИВАЊЕ ИНТЕГРИТЕТА СОФТЕРА И ОПЕРАТИВНИХ СИСТЕМА**

**Члан 10**

 Инсталацију и подешавање софтера може да врши запослени на радном месту одржавања рачунара, запослени по овлашћењу директора и треће лице , у складу са Уговором о набавци, односно одржавању софтера.

 Пре сваке инсталације нове верзије софтера, односно подешавања , неопходно је направити копију постојећег, какао би се обезбедила могућност повратка на претходно стање у случају неочикаване ситуације.

**ЗАШТИТА ПОДАТАКА У КОМУНИКАЦИОНИМ МРЕЖАМА УКЉУЧУЈУЋИ УРЕЂАЈЕ И ВОДОВЕ**

**Члан 11**

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицима, тако да се онемогући неовалшћен 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 здраственог осигурања, Канцеларијом за јавне набавке, Агенцијом за борбу против корупције и сличним институцијама са којом се врши размена података у складу са Уговором ( протоколом)

**ЗАПОСЛЕНИ КОЈИ ИМАЈУ АДМИНИСТРАТОРСКЕ И КОРИСНИЧКЕ НАЛОГЕ**

**Члан 13**

**Запослени у школи који имају кориснички или административни налог су;**

1. За рад на порталу Центарлног регистра социјалног осигурања секретар школе
2. За рад у програму Доситеј лице које је одређено Решењем директора
3. За рад на Порталу Пореске управе и Трезор шеф рачуноводства
4. За рад на елетронском дневнику одељенски старешина, стручни сарадник, директор и координатор есДненика,
5. За рад на издавању јавних исправа секретар школе,
6. За рад на елетронском упису ученика , секретар школе и лице које именује директор школе
7. За рад на Порталу јавних набавки секретар школе,
8. За рад на веб сајту школе наставник задужен у оквиру 40 часовне радне недеље
9. За рад на финансијској документацији шеф рачуноводства,
10. За рад на ПП документацији , психолог школе
11. За рад на одржавању мреже лице по уговору, односно запослени на одржавању рачунара,
12. За рад на датотеци рачунара у зборници сви запослени у настави.

**ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ**

**Члан 13**

 Правилник као и измене и допуне овог Правилника доноси Школски одбор на предлог директора школе

**Члан 14**

 Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли Школе

 **ПРЕДСЕДНИК ШКОЛСКОГ ОДБОРА**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **Марија Илић Костић**

**Правилник је објављен на огласној табли Школе дана \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ а ступио је на снагу дана\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022.године**