На основу члана 57. став 1. тачка 1. Закона о основама система образовања и васпитања („Сл. гласник РС” бр.72/2009, 52/2011 и 55/2013, 35/2015 – аутентично тумачењe , 68/2015 и 62/16 – УС), а у вези примене Закона о информационоj безбедности („Сл. гласник РС”, бр. 6/2016), члана 2. Уредбе о ближем садржаjу Правилника о безбедности информационо-комуникационих система од посебног значаjа, начину провере информационо-комуникационих система од посебног значаjа и садржаjу извештаjа о провери информационо-комуникационог система од посебног значаjа („Сл. Гласник РС“, бр. 94/2016) и на основу члана122. и 255. Статута ОШ „Краљ Петар II Карађорђевић“, Школски одбор донео jе дана 15.09. 2017. године:

**ПРАВИЛНИК**

**о безбедности информационо - комуникационог система**

**ОШ „Краљ Петар II Карађорђевић“**

**Уводне одредбе**

**Члан 1.**

Овим правилником, у складу са Законом о информационоj безбедности и Уредбом о ближем садржаjу Правилника о безбедности информационо-комуникационих система од посебног значаjа, начин провере информационо-комуникационих система од посебног значаjа и садржаj извештаjа о провери информационо-комуникационог система од посебног значаjа („Сл. Гласник РС“, бр. 94/2016), утврђуjу 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 ОШ „Краљ Петар II Карађорђевић“.

**Члан 2.**

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

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог.

За праћење примене овог правилника обавезуjе се наставник информатике

**Члан 3.**

Поjедини термини у смислу овог правилника имаjу следеће значење:

1) *информационо-комуникациони систем*(ИКТ систем) jе технолошко-организациона целина коjа обухвата:

(1) електронске комуникационе мреже у смислу закона коjи уређуjе електронске комуникациjе;

(2) уређаjе или групе међусобно повезаних уређаjа, таквих да се у оквиру уређаjа, односно у оквиру барем jедног из групе уређаjа, врши аутоматска обрада података коришћењем рачунарског програма;

(3) податке коjи се похрањуjу, обрађуjу, претражуjу или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

(4) организациону структуру путем коjе се управља ИКТ системом;

2) *информациона безбедност*представља скуп мера коjе омогућаваjу да подаци коjима се рукуjе путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би таj систем функционисао како jе предвиђено, када jе предвиђено и под контролом овлашћених лица;

3) *таjност*jе своjство коjе значи да податак ниjе доступан неовлашћеним лицима;

4) *интегритет*значи очуваност изворног садржаjа и комплетности податка;

5) *расположивост*jе своjство коjе значи да jе податак доступан и употребљив на захтев овлашћених лица онда када им jе потребан;

6) *аутентичност*jе своjство коjе значи да jе могуће проверити и потврдити да jе податак створиo или послаo онаj за кога jе декларисано да jе ту радњу извршио;

7) *непорецивост*представља способност доказивања да се догодила одређена радња или да jе наступио одређени догађаj, тако да га накнадно ниjе могуће порећи;

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

9) *управљање ризиком*jе систематичан скуп мера коjи укључуjе планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

10) *инцидент*jе унутрашња или спољна околност или догађаj коjим се угрожава или нарушава информациона безбедност;

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

12) *таjни податак*jе податак коjи jе, у складу са прописима о таjности података, одређен и означен одређеним степеном таjности;

13) *ИКТ систем за рад са таjним подацима*jе ИКТ систем коjи jе у складу са законом одређен за рад са таjним подацима;

14) *компромитуjуће електромагнетно зрачење (КЕМЗ)*представља ненамерне електромагнетне емисиjе приликом преноса, обраде или чувања података, чиjим приjемом и анализом се може открити садржаj тих података;

15) *криптобезбедност*jе компонента информационе безбедности коjа обухвата криптозаштиту, управљање криптоматериjалима и развоj метода криптозаштите;

16) *криптозаштита*jе примена метода, мера и поступака ради трансформисања података у облик коjи их за одређено време или траjно чини недоступним неовлашћеним лицима;

17) *криптографски производ*jе софтвер или уређаj путем кога се врши криптозаштита;

18) *криптоматериjали*су криптографски производи, подаци, техничка документациjа криптографских производа, као и одговараjући криптографски кључеви;

19) *безбедносна зона*jе простор или просториjа у коjоj се, у складу са прописима о таjности података, обрађуjу и чуваjу таjни подаци;

20) *информациона добра*обухватаjу податке у датотекама и базама података, програмски кфд, конфигурациjу хардверских компонената, техничку и корисничку документациjу, унутрашње опште правилнике, процедуре и слично;

21) VPN (Virtual Private Network)-jе „приватна“ комуникациона мрежа коjа омогућава корисницима на раздвоjеним локациjама да преко jавне мреже jедноставно одржаваjу заштићену комуникациjу;

22) MAC адреса (Media Access Control Address) jе jединствен броj, коjим се врши идентификациjа уређаjа на мрежи;

23) Backup jе резервна копиjа података;

24) Download je трансфер података са централног рачунара или web презентациjе на локални рачунар;

25) UPS (Uninterruptible power supply*)* jе уређаj за непрекидно напаjање електричном енергиjом;

26) Freeware jе бесплатан софтвер;

27) Opensource софтвер отвореног кода;

28) Firewall jе „заштитни зид“ односносистем преко кога се врши надзор и контролише проток информациjа између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

29) USB или флеш мемориjа jе спољшњи медиjум за складиштење података;

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

31) DVD jе оптички диск високог капацитета коjи се користи као медиjум за складиштење података;

**1. Мере заштите**

**Члан 4.**

Мерама заштите ИКТ система се обезбеђуjе превенциjа од настанка инцидената, односно превенциjа и минимизациjа штете од инцидената коjи угрожаваjу вршење надлежности и обављање делатности, а посебно у oквиру пружања услуга другим лицима.

**Члан 5.**

Сваки запослени-корисник ресурса ИКТ система jе одговоран за безбедност ресурса ИКТ система коjе користи ради обављања послова из своjе 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 школе надлежан/на jе запослени на радном месту одржаваоца рачунара са којим је Општина Врачар закључила уговор за све школе на територији општине Врачар

**Члан 6.**

**Под пословима из области безбедности утврђуjу се:**

·  послови заштите информационих добара, односно средстава иимовине за надзор над пословним процесима од значаjа 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 евиденциjе о томе

·  праћење активности, ревизиjе и надзора у оквиру управљања информационом безбедношћу

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

У случаjу инцидента запослени на радном месту одржаваоца рачунара, обавештава директора школе, коjи у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

Сви запослени коjи су корисници ИКТ система школе дужни су под претњом дисциплинске одговорности одмах обавестити запосленог на радном месту одржаваоца рачунара, у случаjу инцидента из става 1 овог члана.

**2.Бeзбeднoст рaдa нa дaљину и упoтрeба мoбилних урeђaja**

**Члан 7.**

Рад на даљину и употреба мобилних уређаjа у ИКТ систему ниjе омогућен.

Нерегистровани корисници, путем мобилних уређаjа могу да приступе само оним деловима мреже коjи су конфигурисани тако да омогућаваjу приступ Интернету али не и деловима мреже кроз коjу се обавља службена комуникациjа.

Запослени-корисници ресурса ИКТ система школе, могу путем мобилних уређаjа, коjи су у власништву школе, и коjи су подешени од стране, да приступаjу само оним деловима ИКТ система коjи им омогућаваjу обављање радних задатака у оквиру њихове надлежности (електронска пошта,  а на основу писане сагласности директора школе.

Мобилни уређаjи мораjу бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и листе MAC адреса уређаjа путем коjих jе дозвољен приступ, уз активан одговараjући софтвер за заштиту од вируса и другог злонамерног софтвера.

Приступ ресурсима ИКТ система школе са удаљених локациjа, од стране запослених-корисника, у циљу обављања радних задатака, омогућен jе путем заштићене VPN/интернет конекциjе.

Запосленом-кориснику, забрањена jе самостална инсталациjа софтвера и подешавање мобилног уређаjа, као и давање уређаjа другим неовлашћеним лицима (на услугу, сервисирање и сл.)

Запослени на радном месту одржаваоца рачунара, свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаjа (са непознатих MAC адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а наjкасниjе сутрадан обавештава директора школе, а та MAC адреса се уноси у «block“ листу софтвера коjи се користи за контролу приступа.

Приступ ресурсима ИКТ система, са приватног уређаjа, ниjе дозвољен, осим ако jе уређаj у власништву школе, оштећен и ниjе обезбеђена замена.

Евиденциjу приватних уређаjа са коjих ће бити омогућен приступ води Запослени на радном месту одржаваоца рачунара, а по одобрењу директора школе.

Приватни уређаjи са коjих ће се приступати ресурсима ИКТ система мораjу бити подешени од стране запосленог на радном месту одржаваоца рачунара, могу се користити само за обављање послова у надлежности корисника-запосленог и то само у периоду када ниjе могуће користити уређаj у власништву школе.

Запослени на радном месту одржаваоца рачунара jе дужан да пре предаjе уређаjа овлашћеном сервису, уколико квар ниjе такве врсте да то онемогућава,уради *backup* података коjи се налазе у мобилном уређаjу, а потом их обрише из уређаjа, и по повратку из сервиса поново врати податке у мобилни уређаj.

**3. Обезбеђивање да лица коjа користе ИКТ систем односно управљаjу ИКТ системом буду оспособљена за посао коjи раде и разумеjу своjу одговорност**

**Члан 8.**

ИКТ системом управљаjу запослени у складу са важећом систематизациjом радних места.

Запослени на радном месту одржаваоца рачунара, jе дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса школе, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденциjу о изjавама новозапослених – корисника да су упознати са правилима коришћења ИКТ ресурса.

У вези примене одредбе из става 1 овог члана запослени на радном месту одржаваоца рачунара jе дужан да прибави и чува код себе изjаве свих запослених да су упознати са правилима коришћења ресурса ИКТ система, тj са овимПравилником.

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

**4. Заштита од ризика коjи настаjу при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система**

**Члан 9.**

У случаjу промене послова, односно надлежности корисника-запосленог, Запослени на радном месту одржаваоца рачунара ће извршити промену привилегиjа коjе jе корисник-запослени имао у складу са описом радних задатака, а на основу налога директора школе.

У случаjу престанка радног ангажовања корисника-запосленог, кориснички налог се укида, директор школе jе обавезан да именуjе другог запосленог као корисника корисничког налога и да о томе обавести писменим путем запосленог на радном месту одржаваоца рачунара и новог корисника налога.

Директор школе jе дужан да о промени налога спроведе поступак давања овлашћења односно промени овлашћења надлежноj институциjи, наjкасниjе у року од седам дана од дана доношења решења о промени привилегиjа, односно у року од седам дана од дана престанка радног односа запосленог коjи jе био корисник привилегиjа.

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

**5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту**

**Члан 10.**

Информациона добра школе су сви ресурси коjи садрже пословне информациjе о раду школе, запослених, родитеља и ученика, односно, путем коjих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључуjући све електронске записе, рачунарску опрему, мобилне уређаjе, базе података, пословне апликациjе, конфигурациjу хардверских компонената, техничку и корисничку документациjу, унутрашње правилнике коjи се односе на ИКТ систем и сл.)

Евиденциjу о информационим добрима води запослени на радном месту одржаваоца рачунара, у папирноj или електронскоj форми.

**Предмет заштите су:**

·  хардверске и софтверске компоненте ИКТ система

·  подаци коjи се обрађуjу или чуваjу на компонентама ИКТ система

·  кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система

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

**Члан 11.**

Подаци коjи се налазе у ИКТ систему представљаjу таjну, ако су тако дефинисани одредбама посебним прописима.

Подаци коjи се означе као таjни, мораjу бити заштићени у складу са одредбама Уредбе о посебним мерама заштите таjних података у информационо-телекомуникационим системима („Сл. Гласник РС“, бр. 53/2011).

Детаљан опис информациjа, носачима информациjа и доступности података налази се у Информатору о раду школе.

**7. Заштита носача података**

**Члан 12.**

Директор школе, ће успоставити организациjу приступа и рада са подацима, посебно онима коjи буду означени степеном службености или таjности у складу са Законом о таjности података, тако да:

·  подаци и документи (посебно они са ознаком таjности) могу да се сниме (архивираjу, запишу) на серверу на коме се снимаjу подаци, у фолдеру над коjим ће право приступа имати само запослени-корисници коjима jе то право обезбеђено одлуком начелника.

·  подаци и документи (посебно они са ознаком таjности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника.

Евиденциjу носача на коjима су снимљени подаци, води запослени на радном месту одржаваоца рачунара и ти медиjи мораjу бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случаjу транспорта медиjа са подацима,директор школе ће одредити одговорну особу и начин транспорта.

У случаjу истека рокова чувања података коjи се налазе на медиjима, подаци мораjу бити неповратно обрисани, а ако то ниjе могуће, такви медиjи мораjу бити физички оштећени, односно уништени.

**8. Ограничење приступа подацима и средствима за обраду података**

**Члан 13.**

Приступ ресурсима ИКТ система одређен jе врстом налога, односно додељеном улогом коjу запослени-корисник има.

Запослени коjи има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталациjе, одржавања, подешавања и управљања ресурсима ИКТ система.

Запослени - корисник може да користи само своj кориснички налог коjи jе добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налогa, сем администратору за подешавање корисничког профила и радне станице.

Запослени-корисник коjи на било коjи начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичноj и дисциплинскоj одговорности.

Запослени-корисник дужан jе да поштуjе и следећа правила безбедног и примереног коришћења ресурса ИКТ система, и то да:

1) користи информатичке ресурсе искључиво у пословне сврхе;

2) прихвати да су сви подаци коjи се складиште, преносе или процесираjу 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 своjе лозинке, односно да их не одаjе другим лицима;

5) мења лозинке сагласно утврђеним правилима;

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

7) захтев за инсталациjу софтвера или хардвера подноси у писаноj форми, одобрен од стране непосредног руководиоца;

8) обезбеди сигурност података у складу са важећим прописима;

19) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;

10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опциjе, нити да неовлашћено инсталира други антивирусни програм;

11) на радноj станици не сме да складишти садржаj коjи не служи у пословне сврхе;

12) израђуjе заштитне копиjе (backup) података у складу са прописаним процедурама;

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

14) прихвати да се одређене врсте информатичких интервенциjа (израда заштитних копиjа, ажурирање програма, покретање антивирусног програма и сл.) обављаjу у утврђено време;

15) прихвати да сви приступи информатичким ресурсима и информациjама треба да буду засновани на принципу минималне неопходности;

16) прихвати да технике сигурности (анти вирус програми, firewall, системи за детекциjу упада, средства за шифрирање, средства за проверу интегритета и др.) спречаваjу потенциjалне претње ИКТ систему.

17) не сме да инсталира, модификуjе, искључуjе из рада или брише заштитни, системски или апликативни софтвер.

**9. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама коjе ИКТ систем пружа**

**Члан 14.**

Право приступа имаjу само запослени коjи имаjу администраторске или корисничке налоге.

Администраторски налог jе jединствени налог коjим jе омогућен приступ и администрациjа свих ресурса ИКТ система, као и отварање нових и измена постоjећих налога.

Администраторски налог за управљање доменом може да користи само запослени на пословима запосленог на радном месту одржаваоца рачунара.

Адинистраторски налог за управљање базом података могу да користе само запослени на радном месту коjи су овим Правилником одређени за вођење базе података, односно Планом рада школе и коjе jе писменим путем овластио директор школе.

Кориснички налог се састоjи од корисничког имена и лозинке, коjи се могу укуцавати или читати са медиjа на коме постоjи електронски сертификат, на основу кога/jих се врши аутентификациjа – провера идентитета и ауторизациjа – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налог додељуjе директор школе писменим овлашћењем уз сагласност запосленог, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Директор школе води евиденциjу о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге.

**10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикациjу**

**Члан 15.**

Кориснички налог се састоjи од корисничког имена и лозинке.

Корисничко име се креира по матрици име.презиме, латиничним писмом без употребе слова ђ,ж,љ, њ, ћ, ч, џ, ш.

(Препорука: Уместо ових слова користити слова из табеле. )

Отвори табелу

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

Лозинка не сме да садржи име, презиме, датум рођења, броj телефона и друге препознатљиве податке.

Ако запослени-корисник посумња да jе друго лице открило његову лозинку дужан jе да исту одмах измени и о томе обавести запосленог на радном месту одржаваоца рачунара.

Запослени-корисник дужан jе да мења лозинку наjмање jедном у 6 месеци и не сме понављати у временском периоду од годину дана, уколико иста ниjе траjног карактера прописана актом даваоца апликациjе.

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

Приjављивање у ИКТ систем школе се врши убацивањем медиjа са електронским сертификатом у читач картица.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинскоj одговорности.

**11. Предвиђање одговараjуће употребе криптозаштите ради заштите таjности, 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 аутентификациjу и ауторизациjу приступа поjединим апликациjама.

Запослени на радном месту одржаваоца рачунара jе задужен за инсталациjу потребног софтвера и хардвера за коришћење сертификата.

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

**12. Физичка заштита обjеката, простора, просториjа односно зона у коjима се налазе средства и документи ИКТ система и обрађуjу подаци у ИКТ систему**

**Члан 17.**

·  Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организуjе са као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, коjи jе обезбеђен механичком бравом.

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

·  Директор школе одређуjе просториjе у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организуjе са као административна зона.

·  Евиденциjу о уласку у ову зону води служба, односно радник физичког обезбеђења.

**13. Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава коjа чине ИКТ систем**

**Члан 18.**

·  Улаз у просториjу у коjоj се налази ИКТ опрема, дозвољен jе само администратору ИКТ система, односно запосленима на пословима ИКТ.

·  Осим администратора система, приступ административноj зони могу имати и трећа лица у циљу инсталациjе и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу директора школе и уз присуство запосленог на радном месту одржавања рачунара.

·  Приступ административноj зони може имати и запослена на пословима одржавања хигиjене уз присуство запосленог корисника ИКТ опреме.

·  Просториjа мора бити видљиво обележена и у њоj се мора налазити противпожарна опрема, коjа се може користити само у случаjу пожара у просториjи у коjоj се налази ИКТ опрема и медиjи са подацима.

·  Прозори и врата на овоj просториjи мораjу увек бити затворени.

·  Сервери и активна мрежна опрема (switch, modem, router, firewall), мораjу стално бити прикључени на уређаjе за непрекидно напаjање – UPS.

·  У случаjу нестанка електричне енергиjе, у периоду дужем од капацитета UPS-а, овлашћено лице jе дужно да искључи опрему у складу са процедурама произвођача опреме.

·  ИКТ опрема из просториjе се у случаjу опасности (пожар, временске непогоде и сл.) може изнети и без одобрења директора школе.

·  У случаjу изношења опреме ради селидбе, или сервисирања, неопходно jе одобрење директора школе коjи ће уjедно одредити услове, начин и место изношења опреме.

·  Ако се опрема износи ради сервисирања, поред одобрења директора школе, потребно jе да запослени на радном месту одржаваоца рачунара сачини записник у коме се наводи назив и тип опреме, сериjски броj, назив сервисера, име и презиме овлашћеног лица сервисера.

·  Уговором, односно наруџбеницом са сервисером мора бити дефинисана обавеза заштите података коjи се налазе на медиjима коjи су део ИКТ ресурса школе.

**14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података**

**Члан 19.**

Запослени на пословима ИКТ континуирано надзиру и провераваjу функционисање средстава за обраду података и управљаjу ризицима коjи могу утицати на безбедност ИКТ система и, у складу са тим, планираjу, односно предлажу директору школе одговараjуће мере.

Пре увођења у рад новог софтвера неопходно jе направити копиjу-архиву постоjећих података, у циљу припреме за процедуру враћања на претходну стабилну верзиjу

Инсталирање новог софтвера као и ажурирање постоjећег, односно инсталациjа нове верзиjе, може се вршити на начин коjи не омета оперативни рад запослених-корисника.

У случаjу да се на новоj верзиjи софтвера коjи jе уведен у оперативни рад примете битни недостаци коjи могу утицати на рад, потребно jе применити процедуру за враћање на претходну стабилну верзиjу софтвера.

За развоj и тестирање софтвера пре увођења у рад у ИКТ систем мораjу се користити сервери и подаци коjи су намењени тестирању и развоjу.

При тестирању софтвера jе потребно обезбедити неометано функционисање ИКТ система. Забрањено jе коришћење сервера коjи се користе у оперативном раду за тестирање софтвера, на начин коjи може да заустави нормално функционисање ИКТ система.

**15. 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 коjи у рачунарску мрежу могу доспети интернет конекциjом, имеjлом, зараженим преносним медиjима (USB мемориjа, CD итд.), инсталациjом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару jе инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефинициjа, а наjмање jедном месечно.

Сваког претпоследњег радног дана у недељи, тj. у четвртак jе потребно оставити укључене и закључане рачунаре ради скенирања на вирусе.

Забрањено jе заустављање и искључивање антивирусног софтвера током скенирања преносних медиjа.

Преносиви медиjи, пре коришћења, мораjу бити проверени на присуство вируса. Ако се утврди да преносиви медиj садржи вирусе, уколико jе то могуће, врши се чишћење медиjа антивирусним софтвером.

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

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

Директор школе одређуjе коjи запослени имаjу право приступа интернету ради прикупљања података и осталих информациjа везаних за обављање послова у њиховоj надлежности.

Корисницима коjи су прикључени на ИКТ систем jе забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему директор школе може укинути приступ интернету у случаjу доказане злоупотребе истог.

Корисници ИКТ система коjи користе интернет мораjу да се придржаваjу мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чиjи се запослени-корисник прикључуjе на Интернет мора бити одговараjуће подешен и заштићен, при чему подешавање врши запослени на радном месту одржавања рачунара.

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

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

Строго jе забрањено гледање филмова и играње игрица на рачунарима и "крстарење" WЕB страницама коjе садрже недоличан садржаj, као и самовољно преузимање истих са интернета.

**Недозвољена употреба интернета обухвата:**

·  инсталирање, дистрибуциjу, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа коjи нису лиценцирани на одговараjући начин;

·  нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникациjе;

·  намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет троjански коњи, интернет црви и друге врсте малициозних софтвера);

·  недозвољено коришћење друштвених мрежа и других интернет садржаjа коjе jе ограничено;

·  преузимање (download) података велике “тежине” коjе проузрокуjе “загушење” на мрежи;

·  преузимање (download) материjала заштићених ауторским правима;

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

·  недозвољени приступ садржаjу, промена садржаjа, брисање или прерада садржаjа преко интернета.

Корисницима коjи неадекватним коришћењем интернета узрокуjу загушење, прекид у раду или нарушаваjу безбедност мреже може се одузети право приступа

**16. Заштита од губитка података**

**Члан 21.**

·  Базе података обавезно се архивираjу на преносиве медиjе (CDROM, DVD, USB, „strimer“ трака, екстерни хард диск), наjмање jедном дневно, недељно, месечно и годишње, за потребе обнове базе података.

·  Остали фаjлови-документи се архивираjу наjмање jедном недељно, месечно и годишње.

·  Подаци о запосленима-корисницима, архивираjу се наjмање jедном месечно.

·  Дневно копирање-архивирање врши се сваког радног дана.

·  Недељно копирање-архивирање врши се последњег радног дана у недељи, до 20 часова, у онолико недељних примерака колико има последњих радних дана у месецу.

·  Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно, до 20 часова.

·  Годишње копирање-архивирање врши се последњег радног дана у години.

·  Сваки примерак годишње копиjе-архиве чува се у року коjи jе дефинисан Упутством о канцелариjском пословању органа државне управе („Сл. Гласник РС“, бр 10/93, 14/93-испр. и 67/2016).

·  Сваки примерак преносног информатичког медиjа са копиjама-архивама, мора бити означен броjем, врстом (дневна, недељна, месечна, годишња), датумом израде копиjе-архиве, као и именом запосленог-корисника коjи jе извршио копирање-архивирање.

·  Дневне, недељне и месечне копиjе-архиве се чуваjу у просториjи коjа jе физички и у складу са мерама заштите од пожара обезбеђена.

·  Годишње копиjе-архиве се израђуjу у два примерка, од коjих се jедан чува у просториjи у коjоj се чуваjу дневне, недељне и месечне копиjе-архиве а други примерак у просториjи запосленог на радном месту одржавања рачунара.

·  Исправност копиjа-архива проверава се наjмање на шест месеци и то тако што се изврши повраћаj база података коjе се налазе на медиjу, при чему враћени подаци након повраћаjа треба да буду исправни и спремни за употребу.

**17. Чување података о догађаjима коjи могу бити од значаjа за безбедност ИКТ система**

**Члан 22.**

О активностима администратора и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др).

Сваког последњег радног дана у недељи датотеке у коjима се налази дневник активности се архивираjу по процедури за израду копиjа-архива осталих података у ИКТ систему, у складу са чл. 20 овог правилника.

Систем за контролу и доjаву о грешкама, неовлашћеним активностима и др, мора бити подешен тако да одмах обавештава администратора, запосленог на радном месту одржавања рачунара и директора школе, о свим нерегуларним активностима запослених-корисника, покушаjима упада и упадима у систем.

**18. Обезбеђивање интегритета софтвера и оперативних система**

**Члан 23.**

У ИКТ систему може да се инсталира само софтвер за коjи постоjи важећа лиценца у власништву школе, односно Freeware и Opensource верзиjе.

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

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

Пре сваке инсталациjе нове верзиjе софтвера, односно подешавања, неопходно jе направити копиjу постоjећег, како би се обезбедила могућност повратка на претходно стање у случаjу неочекиваних ситуациjа.

**19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система**

**Члан 24.**

Запослени на радном месту одржавања рачунара наjмање jедном месечно а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др ) у циљу идентификациjе потенциjалних слабости ИКТ система.

Уколико се идентификуjу слабости коjе могу да угрозе безбедност ИКТ система, запослени на радном месту одржавања рачунара jе дужан да одмах изврши подешавања, односно инсталира софтвер коjи ће отклонити уочене слабости.

**20. Обезбеђивање да активности на ревизиjи ИКТ система имаjу што мањи утицаj на функционисање система**

**Члан 25.**

Ревизиjа ИКТ система се мора вршити тако да има што мањи утицаj на пословне процесе корисника-запослених. Уколико то ниjе могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чиjи би пословни процес био ометан, уз претходну сагласност директора школе.

**21. Заштита података у комуникационим мрежама укључуjући уређаjе и водове**

**Члан 26.**

Комуникациони каблови и каблови за напаjање мораjу бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолациjа од могућег оштећења.

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

Запослени на радном месту одржавања рачунара jе дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коjу могу да користе посетиоци обjеката у надлежности школе, мора бити одвоjена од интерне мреже коjу користе корисници запослени у школи и кроз коjу се врши размена службених података.

Та мрежа треба да буде означена (ССИД) по моделу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(нпр. imegrada/opstine/gradskeopstine\_guest)

**22. Безбедност података коjи се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система**

**Члан 27.**

Размена података са Министарством просвете, Трезором, Пореском управом Централним регистром социjалног и здравственог осигурања Управом за jавне набавке, Агенциjа за борбу против корупциjе и сличним институциjама са коjом се врши размена података се врши у складу са Уговором (протоколом).

**23. Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система**

**Члан 28.**

Начин инсталирања нових, замена и одржавање постоjећих ресурса ИКТ система од стране трећих лица коjа нису запослена у школи, биће дефинисан уговором коjи ће бити склопљен са тим лицима.

Запослени на радном месту одржавања рачунара jе задужен за технички надзор над реализациjом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постоjећих делова ИКТ система запослени на радном месту одржавања рачунара води документациjу.

Документациjа из претходног става мора да садржи описе свих процедура а посебно процедура коjе се односе на безбедност ИКТ система.

**24. Заштита података коjи се користе за потребе тестирања ИКТ система односно делова система**

**Члан 29.**

Приликом тестирања система, подаци коjи су означени ознаком таjности, односно службености као поверљиви подаци, или су лични подаци директор школе, односно запослени на радном месту одржавања рачунара или лице коjем jе директор школе дао налог, одговара за податке у складу са прописима коjима jе дефинисана употреба и заштита такве врсте података).

**25. Заштита средстава оператора ИКТ система коjа су доступна пружаоцима услуга**

**Члан 30.**

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима коjи се налазе у базама података коjе су део софтвера коjи су они израдили, односно за коjе постоjи уговором дефинисан приступ.

Запослени на радном месту одржавања рачунара jе одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог Правилника коjима су такве активности дефинисане.

**26. Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима коjи су уговорени са пружаоцем услуга**

**Члан 31.**

Школа нема склопљен уговор са трећим лицима за пружање услуга информационе безбедности.

Запослени на радном месту одржавања рачунара jе одговоран за надзор над поштовањем уговорених обавеза од стране трећих лица-пружаоца услуга, посебно у области поштовања одредби коjима jе дефинисана безбедност ресурса ИКТ система уколико школа закључи уговор са трећим лицима за пружање услуга информационе безбедности.

У случаjу непоштовања уговорених обавеза лице из става 2 овог члана jе дужан да одмах обавести директора школе, како би он могао да предузме мере у циљу отклањања неправилности.

**27. Превенциjа и реаговање на безбедносне инциденте, што подразумева адекватну размену информациjа о безбедносним слабостима ИКТ система, инцидентима и претњама**

**Члан 32.**

У случаjу било каквог инцидента коjи може да угрози безбедност ресурса ИКТ система, запослени-корисник jе дужан да одмах обавести запосленог на радном месту одржавања рачунара.

По приjему приjаве запослени на радном месту одржавања рачунара jе дужан да одмах обавести Директора школе и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту коjи jе дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значаjу инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаjа, „Сл. Гласник РС“, бр, 94/2016), запослени на радном месту одржавања рачунара jе дужан да поред директора школе обавести и надлежни орган дефинисан овом уредбом.

Запослени на радном месту одржавања рачунара води евиденциjу о свим инцидентима, као и приjавама инцидената, у складу са уредбом, на основу коjе, против одговорног лица, могу да се воде дисциплински, прекршаjни или кривични поступци.

**28. Мере коjе обезбеђуjу континуитет обављања посла у ванредним околностима**

**Члан 33.**

У случаjу ванредних околности, коjе могу да доведу до измештања ИКТ система из зграде школе, запослени на радном месту одржавања рачунара jе дужан да у наjкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредноj ситуациjи на резервну локациjу, у складу са планом реаговања у ванредним и кризним ситуациjама.

Спецификациjу делова ИКТ система коjи су неопходни за функционисање у ванредним ситуациjама израђуjе запослени на радном месту одржавања рачунара и то у три примерка, од коjих се jедан налази код њега, други код запосленог надлежног за послове одбране и ванредне ситуациjе а трећи примерак код директора школе.

Делове ИКТ система коjи нису неопходни за функционисање у ванредним ситуациjама, складиште се на резервну локациjу, коjу одреди директор школе. Складиштење делова ИКТ система коjи нису неопходни, се врши тако да опрема буде безбедна и обележена, у складу са евиденциjом коjа се о њоj води.

**I ИЗМЕНА ПРАВИЛНИКА О БЕЗБЕДНОСТИ**

**Члан 34.**

У случаjу настанка промена коjе могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаjа на глобалном и националном нивоу коjи могу нарушити информациону безбедност, секретар школе и Запослени на радном месту одржавања рачунара су дужни да обавести директора школе, како би он могао 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.

**I Провера ИКТ система**

**Члан 35.**

Проверу ИКТ система ће вршити запослени на радном месту одржавања рачунара или лице коjе буде изабрано у складу са одредбама Закона о jавним набавкама. Провера ће се вршити последњег месеца у години.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимаjући у обзир и правилнике на коjа 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 примењуjу предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама интервjуа, симулациjе, посматрања, увида у предвиђене евиденциjе и другу документациjу;

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

О извршеноj провери сачињава се извештаj, коjи се доставља директору школе.

**II Садржаj извештаjа о провери ИКТ система**

**Члан 36.**

Извештаj о провери ИКТ система садржи:

1) назив оператора ИКТ система коjи се проверава;

2) време провере;

3) подаци о лицима коjа су вршила проверу;

4) извештаj о спроведеним радњама провере;

5)закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;

6) закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;

7) закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система;

8) оцена укупног нивоа информационе безбедности;

9) предлог евентуалних корективних мера;

10) потпис одговорног лица коjе jе спровело проверу ИКТ система.

**III Запослени коjи имаjу администраторске или корисничке налоге**

**Члан 37.**

Запослени у школи коjи имаjу кориснички, или административни налог су:

1.  За рад на Порталу Централног регистра социjалног осигурања секретар школе

2.  За рад у програму «Доситеj» финансијско администативни радник.

3.  За рад на порталу Пореске управе и Трезора шеф рачуноводства и финансијско администативни радник

4.  За рад на електронском дневнику одељењски старешина и наставници

5.  За рад на бази података за стручне предмете запослени наставник коjи jе у оквиру 40 часовне раднеj недеље Планом рада школе задужен за примену рачунара у настави,

6.  За рад на издавању jавних исправа административни радник,

7.  За рад на упису ученика секретар школе,

8.  За рад на Порталу jавних набавки службеник за јавне набавке,

9.  За рад на веб саjту школе задужен наставник у оквиру 40 часовне радне недеље или по уговору,

10.  За рад на финансиjскоj документациjи благаjник школе и шеф рачуноводства,

11.  За рад на документациjи Школског одбора секретар школе,

12.  За рад на ПП документациjи педагог школе,

13.  За рад на одржавању мреже лице по уговору, односно запослени на одржавању рачунара,

14.  За рад на датотеци меjла школе директор школе ,

15.  За рад на датотеци рачунара у зборници сви запослени у настави.

**IV Прелазне и завршне одредбе**

**Члан 38.**

Директор школе jе у обавези да обавести запослене о донесеном Правилнику на огласноj табли школе, да достави запосленом на радном месту одржавања рачунара Уредбу о ближем садржаjу Правилника о безбедности информационо-комуникационих система од посебног значаjа, начину провере информационо-комуникационих система од посебног значаjа и садржаjу извештаjа о провери информационо-комуникационог система од посебног значаjа („Сл. Гласник РС“, бр. 94/2016) и стара се да запослени на одржавању.

**Члан 39.**

Измене и допуне овог Правилника врше се на начин и по поступку прописаним овим Правилником и Законом.

Оваj правилник ступа на снагу даном обjављивања на огласноj табли школе.

Обjављено на огласноj табли школе

дана 18.09. 2017. године.

Председник Школског одбора

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Вера Живановић

На основу члана 57. став 1. тачка 1. Закона о основама система образовања и васпитања („Сл. гласник РС” бр.72/2009, 52/2011 и 55/2013, 35/2015 – аутентично тумачењe и 68/2015), а у вези примене Закона о информационоj безбедности („Сл. гласник РС”, бр. 6/2016), члана 2. Уредбе о ближем садржаjу Правилника о безбедности информационо-комуникационих система од посебног значаjа, начину провере информационо-комуникационих система од посебног значаjа и садржаjу извештаjа о провери информационо-комуникационог система од посебног значаjа („Сл. Гласник РС“, бр. 94/2016) и на основу члана122. и 255. .Статута ОШ „Краљ Петар II Карађорђевић“, Школски одбор донео jе дана 15.09. 2017.године следећу :

О д л у к у

Доноси се Правилник  о безбедности информационо - комуникационог система

ОШ „Краљ Петар II Карађорђевић“

Председник Школског одбора

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Вера Живановић