

Основна школа „Слободан Секулић“ Ужице
Дел. број 102-620/1
Датум 22.10.2019.године

На основу члана 119 Закона о основама система образовања и васпитања („Сл.гласник РС“ број 88/2017,27/2018 и 10/2019) а у вези са чланом 8. Закона о информационој безбедности ("Службени гласник РС", број 6/16) и чланом 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 ("Сл. гласник РС", бр. 94/2016) и члана 46 Статута основне школе „Слободан Секулић“ Ужице Школски одбор Основне школе „Слободан Секулић“ Ужице из Ужица, на седници одржаној дана 22.10. 2019. године, донео је

ПРАВИЛНИК о безбедности информационо - комуникационог система Установе

I Уводне одредбе

Члан 1.

Овим Правилником, 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 „Слободан Секулић“ Ужице из Ужица (у даљем тексту: ИКТ систем).

Члан 2.

Мере прописане овим Правилником се односе на све организационе јединице Основне школе „Слободан Секулић“ Ужице (у даљем тексту: Школа), на све запослене - кориснике информатичких ресурса.

Непоштовање одредби овог Правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса Школе.

Члан 3.

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 код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

- 21) **VPN** (Virtual Private Network) - је "приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
- 22) **MAC адреса** (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
- 23) **Backup** је резервна копија података;
- 24) **Download** је трансфер података са централног рачунара или веб 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 спољшњи 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.

II 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.

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Школе

Члан 5.

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

2. Поверавање активности у вези са ИКТ системом трећим лицима

Члан 6.

Директор Школе може задужити запосленог или ангажовати лице ван установе у циљу предузимања активности на заштити ИКТ система (лице за безбедност рачунара).

Под активностима из става 1. овог члана се подразумева обрада, чување односно могућност приступа подацима којима располаже Школа, а односе се на пословање, као и активности развоја, односно одржавања софтверских и хардверских компоненти од којих непосредно зависи исправно поступање приликом вршења послова из надлежности Школе.

Члан 7.

Под пословима из области заштите и безбедности утврђују се:

- послови заштите информационих добара, односно средстава и 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, 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, лице за безбедност рачунара обавештава директора, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедносног инцидента.

3. Безбедност рада на даљину и употреба мобилних уређаја

Члан 8.

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

4. 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.

Лице за безбедност рачунара је дужно да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Установе, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденцију о изјавама новозапослених - корисника да су упознати са правилима коришћења ИКТ ресурса.

Свако коришћење ИКТ ресурса Установе, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

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

Члан 10.

У случају промене послова, односно надлежности корисника-запосленог, лице за безбедност рачунара ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева директора Установе.

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

По престанку радног односа или радног ангажовања, као и промени радног места, лице за безбедност рачунара, укида односно мења приступну привилегију тог запосленог-корисника.

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

6. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра Школе су сви ресурси који садрже пословне информације Установе, 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.

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.

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

Члан 12.

Установа има развијену информационо-комуникациону инфраструктуру.

Информациони систем Министарства просвете који се примењују у Школи (Доситеј) садржи базу података о Школи, личне податке запослених и друге податке везане за

њихово радно ангажовање , броју одељења и ученика и учбеницима који се користе за одређену школску годину .

Електронски дневници садрже базу личних података о ученицима и њихови оствареним резултатима током школске године

Рачуноводствено-књиговодствени систем састоји се од неколико програма који су организовани као системи на базама података и служе за вођење рачуноводства и књиговодства, обрачун плата и благајне, евиденција боравка ученика у продуженом боравку као и магацинске картице које се односе на пријем, ускладиштење и издавање намирница које служе за припремање хране за ученике и запослене.

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) и Правилником о правилима понашања у Школи.

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).

8. Заштита носача података

Члан 13.

Лице за безбедност рачунара ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да :

- подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено одлуком директора;
- подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, УСБ, ЦД, ДВД) само од стране овлашћених запослених - корисника и то шеф Службе финансија за податке из области рачуноводства и финансија и референт са студентска питања из области података о студентима.

9. Ограничење приступа подацима и средствима за обраду података

Члан 14.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има и утврђује се одлуком директора Установе.

Лице за безбедност рачунара, 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 лица за безбедност рачунара и не сме да омогући другом лицу коришћење његовог корисничког налога, сем лицу за безбедност рачунара 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 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 Установе 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) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
- 11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
- 12) израђује заштитне копије (Backup) података у складу са прописаним процедурама;
- 13) користи интернет и електронску пошту у Установи у складу са прописаним процедурама;

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

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

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

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

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

Члан 15.

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 се врши аутентификација - провера идентитета и ауторизација - провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налог додељује лице за безбедност рачунара, на основу захтева секретара 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.

Лице за безбедност рачунара води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева секретара, односно надлежног руководиоца.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 16.

Кориснички налог се састоји од корисничког имена и лозинке.

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

Уместо слова из става 2. овог члана користити се слова из табеле:

Ћирилична слова	Латинична слова
Ђ	dj
Ж	z
Љ	lj
Њ	nj
ћ, ч	c
Ш	s
Ц	dz

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

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

Ако 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 6 месеци.

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

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 17.

Приступ ресурсима ИКТ система Установе не захтева посебну криптозаштиту.

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

Члан 18.

Ако постоји сервер и друге мрежне и комуникационе опреме ИКТ система, налазе се у оквиру пословног простора Установе. Ограничење приступа просторији у којој се налази

ИКТ опрема се успоставља са ограничењем физичким приступом који је обезбеђен механичком бравом од које кључ имају само запослени којима је радна просторија у делу пословног простора где се налази опрема ИКТ система.

Евиденцију о уласку у простор где се налази сервер и мрежна опрема ИКТ система се не води.

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

Члан 19.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само запосленима на пословима ИКТ и техничком особљу које одржава хигијену у просторијама. Осталим лицама је дозвољен улазак уз присуство запослених на пословима ИКТ система.

Осим лица за безбедност рачунара, приступ могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу директора, и уз присуство запослених на пословима ИКТ система.

Приступ административној зони може имати и запослени на пословима одржавања хигијене уз присуство запослених на пословима ИКТ система

Прозори и врата на овој просторији морају увек бити затворени.

Сервери и активна мрежна опрема (switch, modem, router, firewall), 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 Директора.

У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење директора који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења директора, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив лица овлашћеног за сервисирање рачунара.

Уговором са лицем овлашћеним за сервисирање рачунара, ако није истовремено и лице за безбедност рачунара мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Установе

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 20.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим, планирају, односно предлажу директору Установе одговарајуће мере.

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 приметите 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.

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

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

Члан 21.

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.

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

Сваког претпоследњег радног дана у недељи је потребно оставити укључене и закључане рачунаре ради скенирања на вирусе.

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.

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 лице за безбедност 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 директору.

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.

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

16. Заштита од губитка података

Члан 22.

Базе података обавезно се архивирају на преносиве медије (CD-ROM, DVD, USB, "стример" трака, екстерни хард диск) на крају школске године, за потребе обнове базе података.

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).

Сваки примерак преносног информатичког медија са копијама-архивама, мора бити означен бројем, врстом, датумом израде копије-архиве, као и именом запосленог-корисника који је извршио копирање-архивирање.

Годишње копије-архиве се чувају у сефу који се налази у просторији у којој ради секретар Установе.

17. Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Члан 23.

О активностима лица за безбедност рачунара и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др).

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Установе.

Инсталацију и подешавање софтвера може да врши само лице за безбедност рачунара које има овлашћење за то, као и овлашћени представници оператора ИКТ система из члан 28. овог Правилника.

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.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

Лице за безбедност рачунара једном годишње врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.

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

20. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Члан 26.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност директора Установе.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 27.

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) се мора налазити у закључаном rack орману.

Лице за безбедност рачунара је дужно да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Ако постоји бежична мрежа коју могу да користе ученици, она је одвојена од интерне мреже коју користе корисници-запослени у Установи и кроз коју се врши размена службених података.

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

Члан 28.

Размена података са INFO SYS d.o.o. Ужице и Technomedia d.o.o. Крагујевац се врши у складу са Уговором који се закључује на годишњем нивоу након спроведеног поступка јавне набавке у преговарачком поступку без објављивања.

23. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 29.

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

Лице за безбедност рачунара је одговорно за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

24. Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга

Члан 30.

Установа закључује годишњи уговор са лицем за безбедност рачунара у који су укључене и услуга информационе безбедности, с тим у складу са лиценцом коју поседује због економичности ово лице може да обавља и послове серверирања рачунара Установе.

Секретар је одговоран за надзор над поштовањем уговорених обавеза од стране лица за безбедност рачунара, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система. У случају непоштовања уговорених обавеза секретар је дужан да одмах обавести директора, како би он могао да предузме мере у циљу отклањања неправилности.

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

Члан 31.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести директора и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значају инцидента и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, "Сл. гласник РС", бр, 94/2016), директор је дужан да обавести и надлежни орган дефинисан овом уредбом.

У Установи се води евиденција о свим инцидентима, као и пријавама инцидента, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

III Измена Правилника о безбедности

Члан 32.

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, на предлог директора врши се измена 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.

IV Провера ИКТ система

Члан 33.

Проверу ИКТ система ће вршити лице за безбедност рачунара. Провера ће се вршити последњег радног дана на крају школске године.

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.

О извршеној провери сачињава се извештај, који се доставља директору.

V Садржај извештаја о провери ИКТ система

Члан 34.

Извештај о провери ИКТ система садржи:

- 1) назив оператора ИКТ система који се проверава;
- 2) време провере;
- 3) подаци о лицима која су вршила проверу;
- 4) извештај 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 које је спровело проверу ИКТ система.

VI Прелазне и завршне одредбе

Члан 35.

Овај правилник ступа на снагу и примењује се осмог дана од дана објављивања на огласној табли Установе.

Председник Школског одбора

Душко Мијаиловић с.р.

Правилник је објављен на огласној табли установе 22.10.2019.год а ступио је на снагу дана 30.10.2019.године

секретар Школе

Снежана Матић с.р.