ПРАВИЛНИК
О УПРАВЉАЊУ ИНФОРМАЦИЈАМА

2018. године

САДРЖАЈ

На основу Закона о информационој безбедности („Службени гласник РС”, број 6/2016 и 94/2017), на седници Школског одбора Основне школе „Душан Радовић“ одржаној 30.08.2018.године, донео је

ПРАВИЛНИК
о управљању информацијама

Предмет управљања информацијама

Члан 1.

Правилником о управљању информацијама (у даљем тексту:Правилник) ближе се уређује процедура управљања информацијама, приступ, коришћење, контрола, обнова, уништавање података и опреме у Основној школи „Душан Радовић“ Ниш(у даљем тексту:Школа).

Правилником се одређују надлежности, начин прикупљања и објављивања информација, одговорност за садржај информација, ажурирање и санкције за необјективно информисање.

Правилником се уређују учесници, одговорности, начин управљања информацијама у складу са законом којим се уређује информациона безбедност, а нарочито се уређује начин приступа и коришћења информација (критеријуми, правила и начин одређивања приступу података, организован систем за вођење свих података који су значајни за складиштење, чување, идентификовање и коришћење), одговорност за податке који се због заштите података о личности не објављују као и неки интерни акти. Право приступа систему имају само запослени, односно корисници који имају администраторске и корисничке налоге. Администраторски налог је јединствен налог којим је омогућен приступ и администрација свих ресурса ИКТ система. Администраторски налог може да користи само запослени који је распоређен на послове и радне задатке администратора ИКТ система. Кориснички налог је налог који садржи корисничко име и лозинку, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу којих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране корисника ИКТ система.

Подаци се објављују на сајту Школе. Информације на веб страници школе прикупљају се и објављују у складу са стратегијом комуницирања са јавношћу и дефинисаним циљним групама. Циљне групе којима се омогућавају ажурне, објективне и тачне информације су: ученици, родитељи, пословни сарадници, институције, предузећа, медији, запослени.

Правилником се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

Неопходно је коришћење лиценцираног оперативног система (који се редовно абдејтује) и лиценцираних програма или опен сорс програма.

Одговорно лице је директор Школе.

Људи који раде на рачунарима деле се на кориснике и пружаоце информационих услуга.

Корисници су особе које користе рачунаре у свом раду, производе документе или уносе податке, али не одговарају на инсталацију и конфигурацију софтвера, нити на исправан и непрекидан рад рачунара и мрежа.

Сваки корисник информационог система мора знати која је његова улога у побољшању целокупне сигурности система.

Дужности корисника су:

- Да се придржавају правила за прихватљиву употребу, што значи да не смеју користити рачунаре за активности које нису у складу са важећим законима, етичким стандардима и локалним сигурносним политикама.
- Да изаберу квалитетне лозинке и повремене промене
- Да пријаве безбедносни инцидент како би решили проблеме што пре

Корисници који производе податке и документе су одговорни за њихово складиштење. То значи да, на пример, провајдер услуга мора успоставити аутоматско резервно копирање важних информација, или у супротном морају се направити резервне копије.

Документи у електронској форми се сматрају службеним документима на исти начин као и документи на папиру, тако да их треба осигурати и ограничити приступ само овлашћеним лицима.

Школа користи апликације за обраду података, као што су рачуноводствени програми, правни програми, административно информационе системе, онлајн Excel табеле. Приступ одређеном рачунару и апликацији ограничен је на овлашћену особу која се именује за главног корисника.

Главни корисник је одговоран за веродостојност података, проверу исправности података, за проверу исправности и сигурности апликације, за одобравање приступа подацима, као и за спречавање промене података од неовлашћених лица.

Главни корисник контактира произвођача апликације и организује достављање нових верзија, захтева инсталирање сигурносних механизама.

Подручје установе је подељено на део који је отворен за јавност, подручје у којем је приступ само запосленима и ученицима, а просторије у којима је приступ ограничен на групе запослених, у зависности од врсте посла који обављају.

Институција је дужна да састави списак лица која имају приступ заштићеним подручјима (рачунарима и просторијама), а домар мора имати листу особа које могу добити кључеве од одређених просторија.

Рад на више рачунара од стране више запослених и могућност да свако уђе у установу, изискује обавезно уношење корисничке лозинке. Због велике френквенције ученика и спољних сарадника у свим просторијама и рачунарима као и могућности да може да се деси да идентификују шифру, а онда неопрезно и неовлашћено је искористе, неопходно је мењати шифру рачунара бар два пута годишње.

Ажурирање података врши се од стране овлашћених особа, а по налогу и/или одобрењу директора. Информације које спадају у групу вести ажурирају се дневно, а остале информације по потреби, динамиком која је у складу са насталим променама у активностима школе.

Контролу управљања информацијама врши директор, односно овлашћена лица од стране директора и запослени који имају стручна знања из области информатике и рачунарства и остала овлашћена лица, корисници одређених апликација (правне, економске струке, информационе технологије и др).

Запослени у Школи у обављању својих послова поступају одговорно, објективно, стручно, поштују принципе поверљивости података.

Медији који садрже поверљиве информације не бацају се, већ се уништавају методом која обезбеђује трајно и поуздано уништавање садржаја (спаљивањем, поделом, притиском).

Ако је застарела и потрошена рачунарска опрема обезбеђена за употребу треће стране, обавезно је одбацити податке диска специјалним програмом који неповратно брише садржај диска.

Значење појединих термина

Члан 2.

Тајност је својство које значи да податак није доступан неовлашћеним лицима;

Интегритет значи очуваност изворног садржаја и комплетности података;

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

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;

Непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи.

Основне одредбе

Члан 3.

Упознавање запослених са актом

Директор је обавезан да све запослене упозна са овим Правилником.

Члан 4.

Рестриктиван приступ интернету

Директор је обавезан да успостави рестриктиван приступ интернету и приватним поштанским налозима на рачунарима, на којима се чувају, преносе или обрађују поверљиве и остељиве информације. Сигурнсот и заштита података је основни циљ управљања информацијама. У сваком случају, информациони системи требају бити заштићени како би се осигурала поверљивост, интегритет и доступност података.

Сваки корисник је обавезан да доприноси заштити целокупног система путем избора лозинке и повремених промена. Сви запослени и ученици који користе рачунаре у свом раду обавезни су да поштују правила коришћења лозинке.

Правила за коришћење лозинки:

1. Минимална дужина лозинке

Крађу лозинку је лакше пробити. Због тога минимална дужина лозинке треба да буде шест карактера, али се препоручује да се користе дуже лозинке.

2. Не користити речи из речника

Хакери имају збирке речника, што олакшава пребацивање таквих лозинки (такозвани речник напада).

3. Додајте мала и велика слова бројевима

На пример: х0бо3ниЦа. На први поглед је бесмислено и тешко запамтити, али је сигурније.

4. Немојте користити имена блиских особа, кућних љубимаца, датума итд.

Такве лозинке лако откривају социјалним инжењерингом.

5. Трајање лозинке

Промена лозинке смањује вероватноћу његовог откривања. Неки корисници користе алтернативу две стандардне лозинке. Иако су две лозинке боље од оне, ови трикови су и даље основна намена промене лозинки.

6. Тајна лозинке

Корисници су одговорни за своју лозинку. Хакери покушавају лажно се представити као администратори. Прави администратори имају могућност да решавају проблеме без познавања корисничких лозинки.

7. Чување ваше лозинке

Корисник је одговоран за тајност своје лозинке и мора наћи начин да је сакрије.

Запослени који не поштују ова правила угрожавају безбедност информационог система. Директор школе је обавезан да едукује и образује запослене у креирању сигурних лозинки.

Е-маил је део свакодневне комуникације, пословне и приватне. Комуницирање путем е-поште директор захтева да се размотре сви аспекти електронске комуникације у вези са могућим последицама.

Коришћење е-поште:

1. Протоколна несигурност

Поруке се крећу као обичан текст, отворене као разгледница, и лако пресрећу и читају, или чак мењају садржај.

Лако је фалсификовати адресу пошиљаоца, тако да нисте сигурни ко вам је послао поруку.

2. Незгоде

Увек је могуће притиснути погрешан тастер или кликнути мишем на суседној икони. Ово може довести до непоправљиве штете, не можете зауставити поруку која је већ нестала. Ако уместо Reply притиснете Reply All, порука ће прећи на више примаоца уместо једног примаоца, а поверљиве информације ће доћи до нежељених прималаца.

Уобичајена грешка је када се покрене погрешна адреса из адресара.

3. Неспоразуми

Људи желе да напишу е-пошту на лежернији и опуштенији начин. То може довести до неспоразума уколико друга страна не схвати поруку на исти начин. Због тога напишите службену кореспонденцију у званичном тону.

4. Радна етика

Велики број порука које морате прочитати сваког дана може вам одузети знатан дио вашег времена. Зато ограничите број приватних и забавних порука.

Коришћење електронске поште сматра се активношћу која предузима ризик, а запослени су обавезни да се придржавају одређених правила:

- Запослени отварају налог за обављање посла.
- Приватне поруке су дозвољене у умереном износу ако се не омета рад.
- Пишући поруке, будите свесни да не представљате само себе, већ институцију за коју радите.
- Све поруке ће се прегледати помоћу аутоматске апликације за откривање вируса. Ако порука садржи вирус, неће бити испоручена, а пошиљалац и прималац ће бити обавештени о томе.
- У случају безбедносног инцидента, директор може да види комплетан садржај диска, а тиме и е-маил поруку.
- Поруке које су део пословног процеса треба архивирати и држати у прописаном времену, као и документе на папиру.

Члан 5.

Процедура за коришћење приватних преносивих меморија (усб, цд и др.)

Уколико се подаци чувају и користе дељењем докумената онлајн смањује се потреба за коришћењем приватних преносивих меморија (УСБ, ЦД и др.) које представљају велику потенцијалну опасност за преношење вируса и могућност да се са одређеног рачунара неовлашћено преузму подаци. Забрањује се њихово коришћење осим за овлашћену особу за рачунар, или дозволити приступ само на одређеном рачунару на коме имају приступ сви запослени, а не поседује поверљиве податке. И на њима спровести обавезну процедуру скенирања анти вирус програма.

Члан 6.

Копија података

Директор одређује лице и/или лица која ће копије података чувати ван Школе, као мера заштите података у случају пожара, поплава итд..

Члан 7.

Лог фајлови

Управљање лог фајловима је кључан сегмент заштите и одржавања операција информационог система. Логови могу бити од помоћи при откривању безбедносних инцидената, оперативних проблема итд..

Управљање логивима одређено је као кључан део обезбеђења и одржавања операција информационог система.

Оперативни системски записи означавају хронолошке записе о догађајима и активностима на ресурсима информационог система (записи оперативних система, апликативног система, база података, мрежних уређаја и др.).

Директор прописује обавезу чувања лог фајлова.

Члан 8.

Сви запослени који су имали увид у поверљиве податке у складу са Законом, дужни су да чувају као поверљиве и одбију давање информације која би значила повреду поверљивости података.

Члан 9.

Неуспеле пријаве

Директор налаже да се истраже неуспеле пријаве, ако се покажу сумњивим наначин да се омогући да систем препозна са ког рачунара је извршена неуспела пријава.

Члан 10.

Пријава кршења безбедносних процедура

Сви запослени и ученици су дужни да пријаве било какве инциденте у вези кршења безбедносних процедура попут успореног рада сервиса, немогућности приступа, губитка или неовлашћене измене података, појаве вируса итд.

Лице задужено за пријем пријаве је запослени кога одреди директор

Свака поднета пријава се евидентира и води записник о насталом догађају.

Сврха пријаве, односно истраге је да се утврди узрок проблема и извуче закључак о томе како спречити понављање инцидента или барем бити боље припремљен за сличне ситуације.

Члан 11.

Едукација запослених

Директор школе ће омогућити континуирано стручно усавршавање запослених у ИТ сектору о новим међународним стандардима на пољу безбедности информација.

Члан 12.

Заштита поверљивих информација

За објективност, тачност и ажурност информација, одговорна лица дефинисана су чланом 1. овог Правилника,

Свако необјективно и нетачно информисање, као и изостанак ажурирања подлежу мерама санкционисања.

Са запосленима који су откривени да откривају поверљиве информације, уговор о раду ће бити поништен. Због тога установа у уговор треба унети ставке по којима је повреда поверљивости података довољан разлог за раскид уговора.

Завршне одредбе

Члан 13.

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

Председник Школског одбора
Основне школе“Душан Радовић“ Ниш

_____
Славољуб Динић

Правилник је евидентиран деловодним бројем 610-212/1-2018-05 од 30.08.2018.године, објављен је на огласној табли Школе дана 30.08.2018.године, ступа на снагу дана 07.09.2018.године.

Секретар Основне школе“Душан Радовић“
Ниш

_____
Владислава Петровић