На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16, 94/17 и 77/19), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Сл. гласник РС", бр. 94/16) (у даљем тексту: Уредба) , члана 119. став 1. тачка 1. Закона о основама система образовања и васпитања ("Службени гласник РС" бр. 88/2017, 27/2018- други закон, 10/2019,27/2018- други закон и 6/2020) и члана 24. Статута Културног центра општине Лучани, Гуча (број 399 од 30. 4. 2018. год), Управни одбор Културног центра на тридесет другој седници одржаној дана 23. 12. 2024. године донео је:

ПРАВИЛНИК
О БЕЗБЕДНОСТИ
ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

Уводне одредбе

Члан 1.

Правилником о безбедности информационо-комуникационог система (у даљем тексту: Правилник), у складу са Законом о информационој безбедности (у даљем тексту: Закон) и Уредбом, 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 информационо-комуникационог система (у даљем тексту: ИКТ систем) Културног центра општине Лучани, Гуча (у даљем тексту: Установа).

Члан 2.

Мере прописане овим правилником се односе на ИКТ систем Установе, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Установе.

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

За праћење примене овог Правилника обавезује се запослени који је именован одлуком директора Установе (у даљем тексту: **оператор ИКТ система**).

Члан 3.

Поједини термини у смислу Правилника имају следеће значење:

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

- електронске комуникационе мреже у смислу закона који уређује електронске комуникације,
- 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,
- податке који се похрањују, обрађују, претражују или преносе помоћу средстава из алинеје 1. и 2. ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања,
- 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) безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци,

16) информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашња општа правила, процедуре и слично,

17) Backup је резервна копија података,

18) Download је трансфер података са централног рачунара или web презентације на локални рачунар,

19) USB или флеш меморија је спољашњи медијум за складиштење података,

20) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података,

21) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података.

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. Организацина структура са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Установе

Члан 5.

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

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Установе, задужен је оператор ИКТ система.

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност,
- послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности,
- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Установе, 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 оператор ИКТ система, обавештава директора Установе, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

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

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву Установе, и који су подешени од стране оператора ИКТ система, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности.

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

Оператор ИКТ система, свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC адреса).

Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен, осим ако је уређај у власништву Установе, оштећен и није обезбеђена замена, када се приступ врши под контролом оператора ИКТ система.

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

Члан 8.

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

Оператор ИКТ система је дужан 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. Образац Изјаве је саставни део овог Правилника.

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

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

Члан 9.

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

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

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра Установе 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.

Евиденцију о информационим добрима води оператор ИКТ система, у папирној или електронској форми.

Предмет заштите су:

- хардверске и софтверске компоненте ИКТ система,
- подаци који се обрађују или чувају на компонентама ИКТ система,
- кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система.

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

Члан 11.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани посебним прописима.

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

7. Заштита носача података

Члан 12.

Оператор ИКТ система ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података.

Евиденцију носача на којима су снимљени подаци, води оператор ИКТ системаи ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, директор Установе одређује одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на медијима, подаци морају бити неповратно обрисани, а ако то није могуће, такви медији морају бити физички оштећени, односно уништени.

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

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

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

Запослени-корисник може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, сем администратору за подешавање корисничког профила и радне станице.

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

Запослени-корисник дужан је да поштује и следећа правила оператора 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 сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности,

15) 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,

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

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

Члан 14.

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

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

Администраторски налог може да користи само запослени на пословима оператора ИКТ система.

Администраторски налог за управљање доменом и за управљање базом података може да користи само запослени на пословима оператора ИКТ система.

Кориснички налог се састоји од корисничког имена и лозинке на основу кога/јих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налог додељује администратор, на основу захтева запосленог-корисника и одобрења директора Установе, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева директора Установе.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

Ако запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 16.

Приступ ресурсима ИКТ система Установе не захтева посебну криптозаштиту.

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

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

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

Члан 17.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује са као административна зона.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу директора Установе и уз присуство администратора система.

Приступ административној зони може имати и запослени на пословима одржавања хигијене.

13. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 18.

О исправности и безбедном функционисању средстава за обраду података брине се и стара оператор ИКТ система.

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

Члан 19.

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 (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

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

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

У циљу заштите, односно упада у ИКТ систем Установе са интернета, оператер ИКТ система је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет.

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 оператер ИКТ система.

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

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.

15. Заштита од губитка података

Члан 20.

Базе података обавезно се архивирају на преносиве медије (CDROM, DVD, USB, „strimer“ трака, екстерни хард диск), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

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

Члан 21.

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

17. Обезбеђивање интегритета софтвера и оперативних система

Члан 22.

Инсталацију и подешавање софтвера може да врши само оператер ИКТ система, односно запослени-корисник који има овлашћење за то.

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.

18. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 23.

Оператор ИКТ система, најмање једном месечно а по потреби и чешће 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, оператор ИКТ система је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

Оператор ИКТ система треба да подешавањем корисничких полиса, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

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

Члан 24.

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.

20. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 25.

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.

Бежична мрежа коју могу да користе посетиоци Установе, мора бити одвојена од интерне мреже коју користе корисници запослени и кроз коју се врши размена службених података.

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

Члан 26.

Размена података са Министарством просвете и Школском управом врши се у складу Законом о основама система образовања и васпитања.

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

Члан 27.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Установи, биће дефинисан уговором који ће бити склопљен са тим лицима.

Оператор ИКТ система је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система оператор ИКТ система, води документацију.

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

23. Заштита података који се користе за потребе тестирања ИКТ система односно делова система

Члан 28.

За потребе тестирања ИКТ система односно делова система оператор ИКТ система,може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

24. 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.

Оператор ИКТ система, је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог Правилника којима су такве активности дефинисане.

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

Члан 30.

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

По пријему пријаве оператор ИКТ система је дужан да одмах обавести директора Установе 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 инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, („Сл. гласник РС“, бр, 94/2016), оператор ИКТ система, је дужан да обавести и надлежни орган дефинисан овом уредбом.

Оператор ИКТ система води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

26. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 31.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Установе, оператор ИКТ система је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Измена Правилника

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, оператор ИКТ система је дужан да обавести директора Установе, како би се покренуо поступак измене овог правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Провера ИКТ система

Члан 33.

Проверу ИКТ система врши оператор ИКТ система.
О извршеној провери сачињава се извештај, који се доставља директору Установе.

Прелазна и завршна одредба

Члан 34.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли/сајту Установе.

ПРЕДСЕДНИК
УПРАВНОГ ОДБОРА

Наташа Миленковић