На основу члана 8. Закона о информационој безбедности (,,Службени гласник РС“, бр. 6/16, 94/17, 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 (,,Службени гласник РС“, бр. 94/16) и члана 48. Одлуке о организацији Општинске управе општине Владичин Хан (,,Службени гласник града Врања“ бр. 9/19), начелник Oпштинске управе општине Владичин Хан, дана 03. јуна 2022. године, доноси

**ПРАВИЛНИК**

**о безбедности информационо–комуникационог система Општинске управе општине Владичин Хан**

**I УВОДНЕ ОДРЕДБЕ**

**Члан 1.**

Овим правилником се, у складу са Законом о информационој безбедности и Уредбом о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја утврђују 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 Општинске управе општине Владичин Хан (у даљем тексту: ИКТ систем).

**Члан 2.**

Мере прописане овим правилником односе се на све организационе јединице Општинске управе на све запослене–кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Општинске управе општине Владичин Хан.

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса Општинске управе општине Владичин Хан.

За праћење примене овог правилника обавезује се запослени на пословима у области информационо-комуникационих технологија.

**Члан 3.**

Поједини термини у смислу овог 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 подтачке (1) и (2) ове тачке а у сврху њиховог рада, употребе, заштите или одржавања;

- организациону структуру путем које се управља ИКТ системом;

1. ***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;
2. ***Тајност***je својство које значи да податак није доступан неовлашћеним лицима;
3. ***Интегритет***значи очуваност изворног садржаја и комплетности података;
4. ***Расположивост***је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
5. ***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;
6. ***Непорецивост*** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
7. ***Ризик*** значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
8. ***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;
9. ***Инцидент*** је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
10. ***Мере заштите***ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
11. ***Тајни податак***је податак који је у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
12. ***ИКТ систем за рад са тајним подацима***је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
13. ***Компромитујуће електромагнетно зрачење***(КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чување података, чијим пријемом и анализом се може открити садржај тих података;
14. ***Криптобезбедност*** је компонента информационе безбедности које обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
15. ***Криптозаштита***је примена метода, мера и поступака ради трансформисања података у облику који их за одређено време или трајно чини недоступним неовлашћеним лицима;
16. ***Криптографски производ*** је софвтер или уређај путем кога се врши криптозаштита;
17. ***Криптоматеријали***су криптографски производи, подаци, техничка докуметација криптографских производа, као и одговарајући криптографски кључеви;
18. ***Безбедоносна зона***је простор или просторија у којој се у складу са прописима о тајности података обрађују и чувају тајни подаци;
19. ***Информациона добра*** обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и сично;
20. ***VPN (Virtual Private Network)***je приватна комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
21. ***MAC адреса (Media Access Control Address)***је јединствен број, којим се врши идентификација уређаја на мрежи;
22. ***Backup***је резервна копија података*;*
23. ***Download***је трансфер података са централног рачунара или web презентације на локални рачунар;
24. ***UPS (Uninterruptible power supply)***је уређај за непрекидно напајање електричном енергијом;
25. ***Freeware***је бесплатан софвтер;
26. ***Opensource***софтвер отвореног кода;
27. ***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;
28. ***USB*** или флеш меморија је спољашњи медијум за складиштење података;
29. ***CD-ROM***(Compact disk read only memory) се користи као медијум за снимање података;
30. ***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 Општинске управе општине Владичин Хан***

**Члан 5.**

Сваки запослени-корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система који 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 Општинске управе општине Владичин Хан, надлежан је запослени на пословима у области информационо-комуникационих технологија.

**Члан 6.**

Под пословима из области безбедности утврђују се:

* послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја 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 општине, 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 инцидената запослени на пословима у области информационо-комуникационих технологија, обавештава начелника Општинске управе, 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.**

Запослени-корисници ресурса ИКТ система, 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.

1. ***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 запослени у складу са важећом систематизацијом радних места.

Запослени на пословима у области информационо-комуникационих технологија дужан је да сваког новозапосленог-корисника ресурса ИКТ система упозна са одговорностима и правилима коришћења ИКТ ресурса Општинске управе општине Владичин Хан, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденцију о изјавама новозапослених-корисника да су упознати са правилима коришћења ресурса ИКТ система.

Свако коришћење ресурса ИКТ система Општинске управе општине Владичин Хан од стране запосленог-корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

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

**Члан 9.**

У случају промене послова, односно надлежности корисника-запосленог, запослени на пословима у области информационо-комуникационих технологија ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

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

О престанку радног односа или радног ангажовања као и промени радног места, начелник Општинске управе у сарадњи са непосредним руководиоцем дужан је да обавести запосленог на пословима у области информационо-комуникационих технологија, ради укидања односно измену приступних привилегија тог запосленог корисника.

Корисник ИКТ ресурса, након престанка радног ангажовања у управи, 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 Општинске управе општине Владичин Хан су сви ресурси који садрже пословне информације Општинске управе општине Владичин Хан, односно путем којих се врши израда, обрада, чувања, 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 запослени на пословима у области информационо-комуникационих технологија, у папирној или електронској форми, а уз помоћ запосленог у Општинској управи задуженог за материјално књиговодство.

Предмет заштите су:

* хардверске и софтверске компоненте ИКТ система;
* подаци који се обрађују или чувају на компонентима 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 о информационој безбедности***

**Члан 11.**

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама Закона о слободном приступу информацијама од јавног значаја, Закона о заштити података о личности, Закона о тајности података, као и Уредбе о начину и поступку означавања тајности података, односно докумената.

Подаци који се означе као тајни морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникаионим системима.

Детаљан опис информација, носача информација и доступности података налази се у Информатору о раду Општинске управе општине Владичин Хан.

1. ***Заштита носача података***

**Члан 12.**

Запослени на пословима у области информационо-комуникационих технологија 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 начелника;
* подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге начине (екстерни хард диск, USB, CD, DVD) само од стране овлашћених, запослених на пословима у области информационо-комуникационих технологија.

Евиденцију носача на којима су снимљени подаци, води запослени на пословима у области информационо-комуникационих технологија и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, начелник управе ће одредити 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.

1. ***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 право 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 безбедног и примереног коришћења ресурса ИКТ система, и то да:

* користи информатичке ресурсе искључиво у пословне сврхе;
* прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Општинске управе општине Владичин Хан и да могу бити предмет надгледања и прегледања;
* поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
* безбедно чува своје лозинке, односно да их не одаје другим лицима;
* мења лозинке сагласно утврђеним правилима;
* пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу;
* захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
* обезбеди сигурност података у складу са важећим прописима;
* приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
* не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
* на радној станици не сме да складишти садржај који не служи у пословне сврхе;
* израђује заштите копије (backup) података у складу са прописаним процедурама;
* користи интернет и електронску пошту у Општинској управи општине Владичин Хан у складу са прописаним процедурама;
* прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
* прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
* прихвати да технике сигурности (антивирусни програми, firewall, системи за детекцију упада средства за шифрирање, средства за проверу интегритета и друго) спречавају потенцијалне претње ИКТ систему;
* не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

1. ***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 могу да користе само запослени на пословима у области информационо-комуникационих технологија.

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/јих се врше 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 задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем и то тек након уноса података о запосленом, односно радно ангажованом лицу у софтвер за управљање људским ресурсима 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 запосленог на пословима управљања људским ресурсима, односно надлежног руководиоца.

1. ***Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију***

**Члан 15.**

Кориснички налог се састоји од корисничког имена и лозинке.

Лозинка мора да садржи минимум 8 карактера комбинованих од 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 лозику најмање једном у 6 месеци.

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

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

**Члан 16.**

Приступ ресурсима ИКТ система Општинске управе општине Владичин Хан 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 17.**

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује се као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору који је обезбеђен механичком бравом.

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

Контролу о уласку у ову зону врши запослени на пословима у области информационо-комуникационих технологија.

***13. Заштита од губитка, оштећеења, крађе или другог облика угрожавања безбедносних средстава која чине ИКТ систем***

**Члан 18.**

Приступ простору у коме се налази ИКТ опрема, дозвољен је само запосленом на пословима у области информационо-комуникационих технологија.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу начелника управе, уз присуство запосленог на пословима у области информационо-комуникационих технологија.

Приступ административној зони може имати запослени/а на пословима одржавања хигијене уз присуство запосленог на пословима у области информационо-комуникационих технологија.

Простор мора бити видљиво обележен и у њему се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима.

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-UPS.

У случају нестанка електричне енергије, у периоду дужим од капацитета UPS-a, овлашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.

ИКТ опрема из простора се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења начелника управе.

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

Ако се опрема износи ради сервисирања, поред одобрења начелника управе, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су ИКТ ресурс Општинске управе општине Владичин Хан.

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

**Члан 19.**

Запослени на пословима у области информационо-комуникационих технологија 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 начелнику управе 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 на оперитивни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

***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 који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносом медија (USB меморија, CD, итд), инсталацијом нелиценцираног софтвера и сл.

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

Сваког петка 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 медији садрже 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 Општинске управеопштине Владичин Хан саинтернета, запослени/а на пословима информационо-комуникационих технологија дужан је да одржава систем за спречавање упада.

Руководиоци организационих јединица одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација у вези са обављањем послова у њиховој надлежности.

Корисницима који су прукључени на ИКТ систем, забрањено је самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему запослени у области информационо-комуникационих технологија може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени - корисник прикључује на интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши запослени уобласти информационо-комуникационих технологија.

Приликом коришћења интернета треба избегавати WEB странице с обзиром да то може проузроковати проблем–неприметно инсталирање шпијунских програма и слично.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави запосленом уобласти информационо-комуникационих технологија.

Строго је забрањено гледање филмова и других видео садржаја, 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 видео стреаминг 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 21.**

Базе података обавезно се архивирају на HD једном дневно или једном недељно, а на преносиве медије (CD ROM, DVD, USB, “strimer” трака, екстерни хард диск) најмање једном недељно, месечно и годишње, за потребе обнове базе података.

Остали фајлови–документи на серверима се архивирају најмање једном недељно, месечно и годишње.

Подаци о запосленима, корисницима, архивирају се најмање једном месечно.

Дневно копирање–архивирање врши се за сваки дан у седмици, после 14 часова сваког радног дана.

Недељно копирање–архивирање врши се последњег радног дана у недељи после 14 часова, у унолико недељних примерака колико има последњих радних дана у месецу.

Месечно копирање–архивирање врши се последњег радног дана у месецу за сваки месец посебно, после 14 часова.

Годишње копирање–архивирање врши се последњег радног дана у години.

Сваки примерак годишње копије–архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе.

Сваки примерак преносног информатичког медија са копијама – архивама, мора бити означен бројем, врстом (дневна, недељна, месечна, годишња), датумом израде копије –архиве, као и именом запосленог – корисника који је извршио копирање – архивирање.

Дневне, недељне, месечне и годишње копије архиве се чувају у просторији која је физички и у складу са мерама заштите од пожара обезбеђена.

Исправност копија – архива проверава се најмање на 6 месеци и то тако што се изврши повраћај база података које се налазе на медију, при чему враћени подаци након повраћаја треба да буду исправни и спремни за употребу.

***17. Чување података о догађајима који могу бити од значаја 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 којима се налази дневник ативности се архивирају по процедури за израду копија – архива осталих података у ИКТ систему, у складу са чланом 20. овог Правилника.

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

**Члан 23.**

У ИКТ систему може да се инсталира само софтвер за који постоји само важећа лиценца у влаништву општине Владичин Хан, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само запослени уобласти информационо-комуникационих технологија, 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.

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

**Члан 24.**

Запослени уобласти информационо-комуникационих технологија 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 индентификују слабости које могу да угрозе безбедност ИКТ система, запослени уобласти информационо-комуникационих технологија је дужан 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 25.**

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 начелника управе.

***21. Заштита података у комуникационим мрежама укључујући уређаје и водове***

**Члан 26.**

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћени приступ, односно да се изврши изолација од могућег оштећења.

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

Запослени уобласти информационо-комуникационих технологија су дужни да стално врше контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалне неправилности.

Бежична мрежа коју могу да користе посетиоци објекта у надлежности управе, уколико постоје технички услови, мора бити одвојена од интерне мреже коју користе корисници запослени у управи и кроз коју се врши размена службених података.

Та мрежа треба да буде означена (ССИД) по моделу ОВ – Vladicinhan-broj.

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

**Члан 27.**

Размена података са другим државним органима врши се према закону и подзаконским актима којима се предвиђа ова врста размене података.

Протокол размене поменутих података уређен је од старне надлежних органа којима се подаци достављају.

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

**Члан 28.**

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

Запослени уобласти информационо-комуникационих технологија 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 ситема запослени уобласти информационо-комуникационих технологија води документацију.

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

***24. Заштита података који се користе за потребе тестирања ИКТ система, односно делова ситема***

**Члан 29.**

Приликом тестирања система у раду са подацима који су означени ознаком тајности, односно службености као поверљиви подаци, или су лични подаци, запослени уобласти информационо-комуникационих технологија одговара за податке у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

***25. Заштита средстава оператора ИКТ система која су досупна пружаоцима услуга***

**Члан 30.**

Трећа лица – пружаоци услуга, израде и одржавање 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.

Запослени уобласти информационо-комуникационих технологија је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог Правилника којима су такве активности дефинисане.

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

**Члан 31.**

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

***27. Превенција и реаговање на безбедоносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама***

**Члан 32.**

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ ситема, запослени–корисник је дужан да одмах обавести запосленог уобласти информационо-комуникационих технологија.

По пријему пријаве запсолени уобласти информационо-комуникационих технологија је дужан/а да одмах обавести начелника општинске управе и предуземе мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, запослени уобласти информационо-комуникационих технологија је дужан да поред начелника обавести и надлежни орган дефинисан овом Уредбом.

Запослени уобласти информационо-комуникационих технологија 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.

***28. Мере које обезбеђују континуитет обављања посла у ванредним околностима***

**Члан 33.**

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде управе, запослени уобласти информационо-комуникационих технологија је дужан да у најкраћем року пренесе делове ИКТ система (или обезбеди функционисање редудантних компоненти на резервној локацији уколико постоје) неопходне за функционисање у ванредној ситуацији на резервну локацију у складу са планом реаговања у ванредним и кризним ситуацијама уз потпуну сарадњу Општинске управе.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђују запослени уобласти информационо-комуникационих технологија у сарадњи са начелником општинске управе и то у три примерака, од којих се један налази код њега/е, други код запосленог надлежног за послове одбране и ванредне ситуације, а трећи примерак код начелника управе.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама складиште се на резервну локацију, коју одреди начелник управе.

Складиштање делова ИКТ система који нису неопходни, се врши тако да опрема буде безбедна и обележена у складу са евиденцијом која се о њој води.

**III ИЗМЕНА ПРАВИЛНИКА О БЕЗБЕДНОСТИ**

**Члан 34.**

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 наруши информациону безбедност, запослени уобласти информационо-комуникационих технологија је дужан да обавести начелника управе, како би он могао да приступи измени овог Правилника, у циљу унапређења 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 35.**

Проверу ИКТ система врши запослени у области информационо-комуникационих технологија.

О извршеној провери сачињава се извештај, који се доставља начелнику управе.

**V САДРЖАЈ ИЗВЕШТАЈА О ПРОВЕРИ ИКТ СИСТЕМА**

**Члан 36.**

Извештај о провери ИКТ система садржи:

* назив оператора ИКТ система који се проверава;
* време провере;
* подаци о лицима који су вршили провере;
* извештај о спроведеним радњама провере;
* закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;
* закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
* закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система;
* оцена укупног нивоа информационе безбедности;
* предлог евентуалних корективних мера;
* потпис одговорног лица које је спровело проверу ИКТ система.

**VI ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ**

**Члан 37.**

Овај правилник ступа на снагу наредног дана од дана објављивања на огласној табли Општинске управе општине Владичин Хан и биће објављен на званичној интернет страници Општинске управе општине Владичин Хан.

Ступањем на снагу овог Правилника престаје да важи Правилник о безбедности информационо-комуникационог система општине Владичин Хан, број 090-1/2017-02 од 08.02.2017. године.

**ОПШТИНСКА УПРАВА ОПШТИНЕ ВЛАДИЧИН ХАН**

**Број: 090-1/2022-IV**

**НАЧЕЛНИК ОПШТИНСКЕ УПРАВЕ**

**Милош Стојановић**