На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16) и 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", број 94/16) и члана 15. став 1, 2. и 5. Закона о државној управи („Службени гласник РС", број 79/05, 101/07, 95/10 и 99/14), директор Републичког геодетског завода доноси

ПРАВИЛНИК
о безбедности информационо-комуникационих система у Републичком геодетском заводу

I Уводне одредбе

Члан 1.

Овим правилником, ближе се дефинишу и утврђују мере заштите, информационо - комуникационих система, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења, дужности и одговорности корисника информатичких ресурса у Републичком геодетском заводу (у даљем тексту: Завод).

Члан 2.

Циљеви доношења овог правилника су:

1) допринос подизању нивоа опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;

2) минимизација безбедоносних ризика;

3) допринос развоју одговарајућих безбедоносних апликација и обезбеђивања перменентне контроле свих компонената информационо-комуникационих система (удаљем тексту: ИКТ систем).

Члан 3.

Мере прописане овим правилником обавезујуће су за све унутрашње организационе јединице Завода, за све запослене - кориснике информатичких ресурса, као и за трећа лица која користе информатичке ресурсе Завода.

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

За праћење примене овог правилника надлежан је Сектор за информатику и комуникације (у даљем тексту: Сектор за ИКТ).

Члан 4.

Поједини изрази употребљени у овом правилнику имају следеће значење:

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

(а) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;

(б) 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;

(в) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтач. (а) и (б) ове тачке, а у сврху њихове употребе, заштите или одржавања;

(г) организациону структуру путем које се управља ИКТ системом;

2) *информациона безбедност* је 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 кôд, 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 web презентације на локални рачунар;

25) УПС (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" односносистем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

29) УСБ 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;

32) Сториџ системи омогућавају складиштење, великих количина података, на ефикасан и сигуран начин, са тренутном доступношћу, без обзира на тип сервера и оперативног система.

II Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Завода, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

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

Члан 6.

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 Завода, надлежан је Сектор за ИКТ, односно сви запослени са администраторским овлашћењима који су задужени за одржавање информатичких ресурса у Заводу.

Члан 7.

Послови из области безбедности су:

1) послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност;
2) послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности;
3) послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Завода, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе;
4) праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу;
5) обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента, корисник информатичких ресурса дужан је да, у циљу решавања насталог безбедоносног инцидента, инцидент, без одлагања, пријави непосредном руководиоцу, који ову информацију прослеђује електронским путем Сектору за ИК.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 8.

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 Завода и који су подешени од стране запослених из Сектора за ИКТ, односно Одељења за информатичку подршку (у даљем тексту: Одељење за ИП), на основу писане сагласности помоћника директора Сектора за ИКТ, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и листе MAC адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Приступ ресурсима ИКТ система Завода са удаљених локација, од стране запослених-корисника, у циљу обављања радних задатака, омогућен је путем заштићене ВПН/интернет конекције.

Запосленом-кориснику, забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима.

Запослени из Сектора за ИК, односно Одељења за ИП свакодневно контролишу приступ ресурсима ИКТ система и проверавају да ли је остварен приступ са непознатих уређаја (са непознатих МАЦ адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава начелник Одељења за ИП, односно помоћник директора Сектора за ИКТ, а та MAC адреса се уноси у "блоцк" листу софтвера који се користи за контролу приступа.

Приступ ресурсима ИКТ система, са приватног уређаја, није дозвољен, осим ако је уређај у власништву Завода, оштећен и није обезбеђена замена.

Трећем лицу могу се одобрити права приступа ИКТ систему уз претходно закључење одговарајућег уговора, којим се прецизно дефинишу услови и обим права приступа, укључујући и све релевантне безбедоносне захтеве.

Изузетно од става 8. овог члана, у случају неопходних и хитних послова могу се одобрити права приступа ИКТ систему трећем лицу по усменом налогу директора Завода, односно овлашћеног лица, о чему ће се накнадно, по завршетку посла, сачинити записник о оствареном приступу.

Ако се установи повреда уговорне обавезе или прекорачење овлашћења по основу уговора, одобрени приступ се одмах укида.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води запослени из Сектора за ИК, односно Одељења за ИП, а по одобрењу директора, на основу предлога помоћника директора Сектора за ИК.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени-сертификовани од стране запослених из Сектора за ИК, односно Одељења за ИП и могу се користити само за обављање послова у надлежности запосленог-корисника.

Запослени из Сектора за ИК, односно Одељења за ИП су дужни да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава,ураде бацкуп података који се налазе у мобилном уређају, а потом их обришу из уређаја и по повратку из сервиса поново врате податке у мобилни уређај.

3. 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.

Руководиоци ужих организационих јединица су дужни да сваког новозапосленог-корисника ИКТ ресурса упознају са одговорностима и правилима коришћења ИКТ ресурса Завода, са правилима коришћења ресурса ИКТ система, као и да воде евиденцију о изјавама новозапослених–корисника да су упознати са правилима коришћења ИКТ ресурса.

Свако коришћење ИКТ ресурса Завода од стране запосленог-корисника, ван додељених овлашћења, подлеже дисциплинској одговорности.

4. 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 запосленог-корисника, запослени са администраторским овлашћењима из Службе и Сектора за ИК, ће извршити промену привилегија које је запослени-корисник имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

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

По престанку радног односа или радног ангажовања, као и промени радног места запосленог-корисника, непосредни руководилац је дужан да електронским путем Сектор за ИК ради укидања, односно измене приступних привилегија тог запосленог-корисника.

Корисник ИКТ ресурса, након престанка радног ангажовања у Заводу, не сме да открива податке који су од значаја за информациону безбедност ИКТ система., под претњом кривичне и материјалне одговорности.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра Завода су сви ресурси који садрже пословне информације Завода у електронском облику или служе за приступ корисника ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и слично, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему.

Евиденцију о информационим добрима води Сектор за ИК и Одељење за финансије и контролу, у папирној или електронској форми.

Предмет заштите су:

1) хардверске и софтверске компоненте ИКТ система;
2) подаци који се обрађују или чувају на компонентама ИКТ система;
3) 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 12.

Подаци који се налазе у ИКТ систему представљају тајну и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. гласник РС“, бр. 53/2011).

Детаљан опис информација, носачима информација и доступности података који су означени одређеним степеном тајности, одређени су Одлуком о одређивању тајних података у Републичком геодетском заводу број 021-68/2016 од 26.04.2016. године и Каталогом докумената, података и информација који треба да буду означени степеном тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у Републичком геодетском заводу број 021-68/2016-2 од 23.11.2016. године.

7. Заштита носача података

Члан 13.

Директор или помоћник директора Сектора за ИК успостави ће организацију приступа и рада са подацима, посебно онима који буду означени степеном тајности у складу са Законом о тајности података („Службени гласник РС“, бр.104/09), тако да:

1) 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 којима је издат сертификат за приступ тајним подацима;
2) подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, УСБ, ЦД, ДВД, сториџ систем), само од стране запослених којима је издат сертификат за приступ тајним подацима, а по налогу директора или помоћника директора Сектора за ИК.

Евиденцију носача на којима су снимљени подаци, воде запослени којима је издат сертификат за приступ тајним подацима, а по налогу директора или помоћника директора Сектора за ИК 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, помоћник директора Сектора за ИК 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.

8. 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.

Запослени-корисник који има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским, 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, осим администратору за подешавање корисничког профила и радне станице.

Запослени-корисник који на било који начин злоупотреби корисничка права, односно ресурсе ИКТ система, подлеже кривичној, материјалној 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 Завода 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 електронским путем Сектору за ИК, односно начелнику Службе, ако је у Служби за катастар непокретности запослен администратор са администраторским овлашћењима;
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 (бацкуп) података у складу са прописанимпроцедурама;
13) користи интернет и електронску пошту у Заводу у складу са прописаним правилима наведеним у Упутству о коришћењу Интернет и Интернет е-маил сервиса у Заводу бр. 021-11/04 од 05.04.2004. године;
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.

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

Члан 15.

Администраторски налози свих пословних апликација, сервера база података и системских апликација за управљање мрежном опремом и уређајима за складиштење података чувају се у затвореним, непровидним ковертама са отиском службеног печата, у каси код руководиоца уже унутрашње организационе јединице.

Право коришћења администраторског налога имају само запослени са администраторским овлашћењима за потребе информатичких интервенција.

Након сваког отварања коверте и коришћења администраторског налога од стране запослених са администраторским овлашћењима, руководилац уже унутрашње организационе јединице је дужан да промени лозинку администраторског налога.

Право приступа имају само запослени који имају администраторска овлашћења.

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

Администраторска овлашћења могу добити само лица која су задужена за одржавање информатичких ресурса у Заводу, уз претходну сагласност помоћника директора Сектора за ИК.

Администраторски налог могу да користе само запослени са администраторским овлашћењима.

Администраторски налог за управљање доменом могу да користе само запослени из Сектора за ИК, односно Одељења за ИП.

Адиниструторски налог за управљање базом података могу да користе само запослени са администраторским овлашћењима одобреним од стране Помоћника директора Сектора за ИК.

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.

Запослени са администраторским овлашћењима, на основу прецизног писаног захтева непосредног руководиоца, додељује кориснику информационог ресурса корисничко име, лозинку, привилегије и налог за електронску пошту.

Запослени са администраторским овлашћењима воде евиденцију о корисничким налозима, проверавају њихово коришћење, мењају права приступа и укидају корисничке налоге на основу захтева непосредног руководиоца.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 16.

Кориснички налог се састоји од корисничког имена и лозинке.

Лозинка мора да садржи минимум седам карактера.

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 три месеца.

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

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

Пријављивање у ИКТ систем Завода се врши убацивањем медија са електронским сертификатом у читач картица.

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 Завода не захтева посебну криптозаштиту.

За приступ ресурсима ИКТ система који се односе на послове одбране, односно, за које је надлежно министарство прописало коришћење криптозаштите, посебним правилником ће бити дефинисана употреба одговарајућих мера криптозаштите узимајући у обзир осетљивост информација које треба да се штите, пословне процесе који се спроводе, ниво захтеване заштите, имплементацију примењених криптографских техника и управљање криптографским кључевима.

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

Запослени на пословима ИКТ задужени су за инсталацију потребног софтвера и хардвера за коришћење сертификата.

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

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.

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

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

Евиденцију о уласку у ову зону воде запослени у Сектору за ИК, односно у Одељењу за ИП.

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 администратору ИКТ система, односно запосленима на пословима одржавања ИКТ система.

Осим администратора система и запослених на пословима одржавања ИКТ система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу начелника Одељења за ИП, помоћника директора Сектора за ИК и уз присуство дежурног из Сектора за ИК.

Приступ административној зони може имати и лице које обавља послове одржавања хигијене уз присуство дежурног из Сектора за ИК.

Просторија мора бити видљиво обележена и у њој 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 - 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 слично) може изнети и без одобрења руководиоца организационе јединице, начелника Одељења за ИП, помоћника директора Сектора за ИК.

У случају изношења опреме ради селидбе или сервисирања, неопходно је одобрење помоћника директора Сектора за ИК.

Ако се опрема износи ради сервисирања, потребно је сачинити и 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 део ИКТ ресурса Завода.

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 помоћнику директора Сектора за ИК 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 примете 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 средстава 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 слично.

За успешну заштиту од вируса на свакој радној станици је инсталиран антивирусни програм, који се аутоматски ажурира.

Сваке среде у току радног времена је потребно оставити укључене све радне станице ради антивирус скенирања.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања радних станица или 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 Завода са интернета, Сектор за ИК је дужан да одржава систем за спречавање упада.

Руководиоци организационих јединица одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет, при чему запослени са администраторским овлашћењима из Службе и Сектора за ИК могу 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 свака радна станица на којој се запосленом омогућује приступ Интернету мора бити одговарајуће подешена и заштићена, при чему подешавања врше запослени са администраторским овлашћењима из Службе и Сектора за ИК.

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

Корисник информатичких ресурса дужан је да, без одлагања, пријави непосредном руководиоцу свако уочавање или сумњу о наступању инцидента којим се угрожава сигурност ИКТ система.

Информацију о инциденту руководилац је дужан да одмах проследи запосленима са администраторским овлашћењима у Служби и Сектору за ИК.

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:

1) инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
2) нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
3) намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси и друге врсте малициозних софтвера);
4) недозвољено коришћење друштвених мрежа;
5) преузимање (download) података велике “величине” које проузрокује загушење на мрежи;
6) преузимање (download) материјала заштићених ауторским правима;
7) коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и слично);
8) 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.

Израда резервних копија база података се обавезно врши на преносиве медије (CD ROM, DVD, USB, „strimer“ трака, екстерни хард диск, сториџ систем), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

Израда резервних копија идентификованих фолдера, фајлова-докумената се врши најмање једном недељно, месечно и годишње.

Израда резервних копија података о запосленима-корисницима, се врши најмање једном месечно.

Израда дневних резервних копија података се врши сваки радни дан у недељи.

Израда недељних резервних копија података се врши последњег радног дана у недељи, у онолико недељних примерака колико има последњих радних дана у месецу.

Израда месечних резервних копија података се врши последњег радног дана у месецу, за сваки месец посебно.

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 („Сл. Гласник РС", бр 10/93, 14/93-исправка и 67/2016).

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 обезбеђена физички и у складу са мерама заштите од пожара.

Годишње копије-архиве се израђују у два примерка, од којих се један чува у просторији у којој се чувају дневне, недељне и месечне копије-архиве а други примерак се предаје Одељењу архива.

Исправност копија-архива проверава се најмање на шест 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 23.

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

Сваког последњег радног дана у недељи датотеке у којима се налази дневник активности се архивирају по процедури за израду копија - архива осталих података у ИКТ систему, у складу са чланом 22. овог правилника.

Систем за контролу и дојаву о грешкама и неовлашћеним активностима, мора бити подешен тако да одмах обавештава запослене са администраторским овлашћењима, руководиоца уже унутрашње организационе јединице надлежне за послове ИКТ и помоћника директора Сектора за ИК, о свим нерегуларним активностима запослених-корисника, о покушајима упада и упадима у систем.

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 Завода, односно Freeware i Opensource верзије.

Инсталацију и подешавање софтвера може да врши само запослени са администраторским овлашћењима у Служби и Сектору за ИК, односно запослени 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 безбедносних слабости ИКТ система

Члан 25.

Запослени са администраторским овлашћењима у Служби и Сектору за ИК најмање једном месечно, а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и друго), у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, запослени са администраторским овлашћењима у Служби и Сектору за ИК, су дужни да одмах изврше подешавања, односно инсталацију софтвера који ће отклонити уочене слабости.

Запослени са администраторским овлашћењима у Служби и Сектору за ИК треба да подешавањем корисничких полиса, онемогуће неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

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 запослених-корисника.

Уколико то није могуће у радно време, онда се врши након завршетка радног времена запослених-корисника, чији би пословни процес био ометан, уз претходну сагласност непосредног руководиоца запосленог-корисника.

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.

Запослени са администраторским овлашћењима у Служби, Сектору за ИК и Одељењу за ИП су дужни да стално врше контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коју могу да користе посетиоци објеката у надлежности Завода мора бити одвојена од интерне мреже коју користе запослени-корисници у Заводу 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 државним органима, органима локалних самоуправа, правним и физичким лицима се врше у складу са важећим прописима и унапред дефинисаним и потписаним уговорима.

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

Члан 29.

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

Запослени из Сектора за ИК су задужени 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 запослени из Сектора за ИК воде документацију.

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

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

Члан 30.

За потребе тестирања ИКТ система односно делова система запослени из Сектора за ИК могу користити податке који нису осетљиви, које штите, чувају и контролишу на одговарајући начин.

Приликом тестирања система, подаци који су означени ознаком тајности, односно поверљивости или представљају податке о личности, запослени из Сектора за ИК одговарају за податке у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

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

Члан 31.

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.

Запослени из Сектора за ИК су одговорни 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 32.

Запослени из Сектора за ИК су одговорни за надзор над поштовањем уговорених обавеза од стране трећих лица-пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система.

У случају непоштовања уговорених обавеза запослени из Сектора за ИК су дужни да одмах обавесте помоћника директора Сектора за ИК и директора Завода, како би он могао да предузме мере у циљу отклањања неправилности.

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

Члан 33.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени је дужан да одмах, без одлагања обавести непосредног руководиоца.

По пријему пријаве, информацију о инциденту руководилац је дужан да исту одмах проследи запосленима са администраторским овлашћењима у Служби и Сектору за ИК како би се одмах предузеле 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), помоћника директора Сектора за ИК дужан је да поред директора завода обавести и надлежни орган дефинисан наведеном уредбом.

Запослени у Сектору за ИК воде евиденцију о свим инцидентима, као и пријавама инцидената, у складу са наведеном 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 34.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из просторија РГЗ-а, запослени са администраторским овлашћењима у Служби и Сектору за ИК, су дужни да у најкраћем року пренесу делове ИКТ система (или обезбеде 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.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује Сектор за ИК, и то у три примерка, од којих се један налази код помоћника директора Сектора за ИК, други код запосленог надлежног за послове одбране и ванредне ситуације а трећи примерак код директора Завода.

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

Складиштење 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 Провера ИКТ система

Члан 35.

Проверу ИКТ система врши запослени са администраторским овлашћењима у Служби и Сектору за ИК.

Проверу ИКТ система може вршити и лице изабрано у складу са законом којим се уређује поступак јавних набавки.

Провера ће се вршити последњег месеца у години.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности информационо-комуникационих система у Републичком геодетском заводу, са прописаним условима, односно проверава да ли су 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;

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 помоћнику директора Сектора за ИК.

IV Садржај извештаја о провери ИКТ система

Члан 36.

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 информационо-комуникационих система у Републичком геодетском заводу, 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.

V Прелазне и завршне одредбе

Члан 37.

У случају настанка промена које могу наступити услед техничко - технолошких, кадровских и организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, помоћник директора Сектора за ИК је дужан да о томе обавести директора Завода, ради издавања налога да се формира радно тело која ће приступити измени овог правилника.

Члан 38.

Даном ступања на снагу овог правилника престаје да важи Директива о безбедности информационо-комуникационих система у Републичком геодетском заводу 01 Број:021-64/2016 од 20. маја 2016. године.

Члан 39.

Овај правилник ступа на снагу наредног дана од дана објављивања на интернет страни Завода.

07Број: 110-7/2017
У Београду, дана 12. јуна 2017. године

В.Д. ДИРЕКТОРА

Борко Драшковић, дипл. геод. инж.