На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16) и члана 44. став 1. Закона о државној управи („Службени гласник РС”, бр. 79/05, 101/07, 95/10 и 99/14),

директор Републичког геодетског завода доноси

ДИРЕКТИВУ
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА РЕПУБЛИЧКОГ ГЕОДЕТСКОГ ЗАВОДА

Предмет директиве
Члан 1.

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

Циљеви директиве
Члан 2.

Циљеви доношења ове директиве су:

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

2) минимизација безбедоносних инцидената;

3) допринос развоју одговарајућих безбедоносних апликација и обезбеђивање конзистентне контроле свих компонената информационо-комуникационог система (у даљем тексту: ИКТ систем).

Обавезност директиве
Члан 3.

Ова директива је обавезујућа за све унутрашње јединице Завода и за све кориснике информатичких ресурса, као и за трећа лица која користе информатичке ресурсе Завода.

Непоштовање ове директиве повлачи дисциплинску одговорност корисника информатичких ресурса.

За праћење примене ове директиве надлежан је Сектор за информатику и комуникације (у даљем тексту: Сектор за ИК).

Појмови
Члан 4.

Поједини изрази употребљени у овој директиви имају следеће значење:

1) *интегритет* је немогућност неовлашћене измене информација;

2) *расположивост* је доступност информација корисницима информатичких ресурса у обиму корисничког овлашћења;

3) *тајност* је обезбеђивање доступности информација само овлашћеним корисницима информатичких ресурса, као и немогућност приступа информацијама лицима која немају таква овлашћења;

4) *администраторско овлашћење* је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;

5) *кориснички налог* јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно овлашћења корисника);

6) *администраторски налог* јесте јединствен налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога.

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 сме бити компромитовани.

Информатички ресурси Завода

Члан 6.

Информатички ресурси 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.

Предмет заштите

Члан 7.

Предмет заштите обухвата:

1) хардверске и софтверске компоненте информатичких ресурса;
2) податке који се обрађују или чувају на информатичким ресурсима;
3) корисничке налоге и друге податке о корисницима информатичких ресурса у Заводу.

Корисник информатичких ресурса

Члан 8.

Корисник информатичких ресурса јесте постављено лице, запослено лице на неодређено или одређено време, лице ангажовано по основу уговора, консултант или друго радно ангажовано лице коме је одобрен приступ неком информатичком ресурсу Завода.

Корисник информатичких ресурса одговоран је за правилну употребу, тачност и сигурност података приликом коришћења информатичких ресурса Завода, односно лично је одговоран за остваривање својстава података у ИКТ систему Завода.

Корисник информатичких ресурса нема имовинска права над информатичким ресурсима Завода.

Дужности корисника информатичких ресурса

Члан 9.

Корисник не сме да спроводи активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система Завода.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне сврхе, а Завод задржава право да информатичке ресурсе повуче у било ком тренутку и у потпуности задржи све податке, без обавезе да их накнадно преда кориснику.

Корисник непреносиве радне станице је дужан да пословне податке смешта на одређене мрежне дискове, односно портале Завода.

Изузетно од става 2. овог члана, због потребе посла, подаци се могу привремено сместити на локални диск непреносиве радне станице, ако се са тим сагласи непосредни руководилац корисника.

Корисник преносиве радне станице има право да привремено смешта пословне податке на локални диск преносиве радне станице, као и обавезу да уради копију докумената са локалног диска на мрежни, односно портале Завода.

Запослено, односно ангажовано лице у Сектору за ИК и у службама за катастар непокретности са администраторским овлашћењима (у даљем тексту: администратор), као и лица која су задужена за израду резервних копија, дужни су да дневно израђују резервне копије података са мрежних дискова и портала.

Корисник информатичких ресурса дужан је да поштује и следећа правила безбедног и примереног коришћења информатичких ресурса, 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 („излогује“), односно закључа радну станицу (CTRL+ALT+DEL+LOCK или WINDOWS L);
7) користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење Сектора за ИК, а на основу образложеног предлога непосредног руководиоца;
8) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
9) обезбеди сигурност података у складу са важећим прописима;
10) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
11) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
12) не сме да на радној станици складишти садржај који не служи у пословне сврхе;
13) израђује заштитне копије (backup) података у складу са прописаним процедурама;

14) користи Internet и Internet e-mail сервис у Заводу у складу са прописаним процедурама;

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

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

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

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

Безбедоносни профил корисника информатичких ресурса

Члан 10.

У зависности од описа задатака и послова радног места на које је распоређен, корисник информатичких ресурса, на предлог непосредног руководиоца, стиче одређена права приступа ИКТ систему Завода.

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

Креирање лозинке

Члан 11.

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

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

Ако корисник информатичких ресурса посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Корисник информатичких ресурса дужан је да мења лозинку најмање једном у три месеца.

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

Употреба корисничког налога

Члан 12.

Кориснички налог може да употребљава само корисник информатичких ресурса коме је исти издат.

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору у случају подешавања радне станице.

Корисник информатичких ресурса је непосредно одговоран за активности које су реализоване на основу његовог корисничког налога.

Кориснички налози са администраторским овлашћењима користе се само за потребе неопходних интервенција којима се обезбеђује несметан рад информатичких ресурса (у даљем тексту: информатичке интервенције).

Употреба администраторског налога

Члан 13.

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 унутрашње јединице.

Право коришћења администраторског налога имају само администратори за потребе информатичких интервенција.

Након сваког отварања коверте и коришћења администраторског налога од стране администратора, руководилац унутрашње јединице је дужан да промени лозинку из административног налога.

Поступци у случајевима сигурносних инцидената

Члан 14.

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 из става 1. овог члана дужан је да одмах проследи администратору, као и Сектору за ИК.

По пријави инцидента мора се поступати адекватно и ефикасно, а по хитном поступку у случајевима:

1) нарушавања поверљивости информација,
2) откривања вируса или грешака у функционисању апликација,
3) вишеструких покушаја неауторизованог приступа,
4) системских падова и престанка рада сервиса.

Сектор за ИК је дужан да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести надлежни орган, у складу са законом којим се уређује информациона безбедност.

Заштита од малициозног софтвера

Члан 15.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена:

1) лиценцираног софтвера, односно забрана коришћења неауторизованог софтвера;

2) правила за заштиту од ризика приликом преузимања фајлова из екстерних извора (података, апликација и сл.).

Приликом преузимања фајлова из става 1. тачка 2) овог члана преносиви медији пре коришћења морају бити проверени на присуство вируса.

Ако се утврди да је преносиви медиј садржи вирусе, врши се чишћење медија од вируса, уз сагласност доносиоца медија.

Ризик од евентуалног губитка података приликом чишћења медија антивирусним софтвером, сноси доносилац медија.

Сигурност електронске поште

Члан 16.

У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

1) електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;

2) забрањено је коришћење електронске поште у приватне сврхе;

3) не смеју се користити приватни налози електронске поште у пословне сврхе;

4) програми који користе сервисе електронске поште морају се искључити када се рачунар не користи;

Поред правила из става 1. ове директиве, приликом коришћења електронске поште морају се поштовати и правила наведена у Упутству о коришћењу Internet и Internet e-mail сервиса у Републичком геодетском заводу (бр. 021-11/04 од 05.04.2004. године).

Поступање са преносивим медијима

Члан 17.

Преносиви медији који садрже податке морају да буду прописно обележени и пописани и да се чувају у заштићеној библиотеци магнетних или електронских медија.

У случају брисања података који се налазе на преносивим медијима, потребно је обезбедити њихово неповратно брисање.

Преносиви медији из става 1. овог члана, пре стављања ван употребе, морају бити физички уништени.

Физичка сигурност информатичких ресурса

Члан 18.

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови**:**

1) сервери, сторици (storage) и комуникационо чвориште у седишту Завода морају бити смештени у посебној просторији (сервер сала) која испуњава стандарде противпожарне заштите и поседује редундантно напајање електричном струјом и адекватну климатизацију;

2) сервери, сторици (storage) и комуникационо чвориште у службама за катастар непокретности морају бити смештени у адекватним просторијама, у којима је забрањен приступ незапосленим лицима;

3) приступ сервер сали, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење помоћника директора Сектора за ИК;

4) радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;

5) просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;

6) штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;

7) медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

Приступ ИКТ систему Завода

Члан 19.

Приступ свим компонентама ИКТ система мора бити аутентификован.

Администратор, на основу прецизног писаног захтева непосредног руководиоца, додељује кориснику информационог ресурса корисничко име, лозинку и привилегије, као и налог за електронску пошту.

Кориснику информатичких ресурса додељују се само привилегије које су неопходне за реализацију његових радних обавеза.

У случају престанка радног односа или радног ангажовања у Заводу кориснику информатичких ресурса укида се право приступа ИКТ систему.

У случају одсуства са посла дуже од месец дана, кориснику информатичких ресурса се привремено укида право приступа ИКТ систему, до повратка на посао.

О престанку радног односа или радног ангажовања, одсуству са посла дуже од месец дана, као и о промени радног места корисника информатичких ресурса, непосредни руководилац је дужан да обавести Сектор за ИК ради укидања, односно измена приступних привилегија тог корисника.

Корисник информатичких ресурса, након престанка радног ангажовања у Заводу, не сме да открива поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система.

Трећем лицу могу се одобрити права приступа ИКТ систему уз претходно склапање 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 уговара, одобрени приступ се одмах укида.

Инсталација и одржавање софтвера

Члан 20.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужени су администратори, који су дужни да поступају у складу са прописаним процедурама и упутствима.

Сектор за ИК обезбеђује запосленом, односно радно ангажованом лицу, коришћење радне станице (десктоп или лап-топ) са преинсталираним и правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачки програми (драјвери), пословно и развојно окружење, софтвер за вирусну заштиту, разне помоћне апликације), који је типски за све радне станице и који представља минимум потребан за обављање стандардних послова.

Администратор врши оцену конзистентности траженог софтвера са постојећим инсталираним софтверима на предметној радној станици и уколико оцени да тражени софтвер неће угрозити или ометати рад, инсталираће захтевани софтвер.

Основна подешавања из става 2. овог члана су:

1) додељивање имена и TCP/IP адреса радној станици и њено придруживање домену или радној групи;
2) подешавање mail-клијента;
3) подешавање Web-претраживача (TCP/IP-адреса прокси сервера);

4) инсталација антивирусног софтвера одобреног од стране Сектора за ИК,

5) инсталација званичног апликативног софтвера који одређене унутрашње јединице Завода користе у свом раду.

У случају да је кориснику потребно да се изврши инсталација одређеног специфичног софтвера на радној станици, непосредни руководилац подноси захтев електронским путем Сектору за ИК, односно начелнику СКН ако је у СКН запослен администратор.

Корисник информатичких ресурса дужан је да сваки проблем у функционисању оперативног система, mail-клијента, Web-претраживача, пословног софтвера (MS Office ili Open Office) и апликативног софтвера, пријави непосредном руководиоцу, који ову информацију прослеђује електронским путем Сектору за ИК, односно начелнику СКН ако је у СКН запослен администратор.

Проблем у функционисању антивирусног и антиспајвер софтвера мора се пријавити без одлагања.

Администратор је дужан да проблеме из ст. 6. и 7. овог члана отклони у најкраћем могућем року на локацији корисника, даљинском конекцијом ка радној станици или доношењем радне станице у Сектор за ИК.

Завршна одредба

Члан 21.

Ова директива ступа на снагу наредног дана од дана објављивања на интернет страници Завода.

01 Број: 021-64/2016
У Београду, 20. маја 2016. године

В.Д. ДИРЕКТОРА

Борко Драшковић, дипл. геод. инж.