Република Србија
МИНИСТАРСТВО ДРЖАВНЕ УПРАВЕ
И ЛОКАЛНЕ САМОУПРАВЕ
Београд, Бирчанинова 6.
Број:021-02-00713/2017-03
Датум: 22. јануар 2018. године

На основу члана 44. Став 1. Закона о државној управи („Сл. гласник РС“, број 79/05, 101/07, 95/10 и 99/14), и члана 8. Закона о информационој безбедности („Сл. гласник РС”, број 6/16), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. гласник РС“, бр. 94/2016) министар државне управе и локалне самоуправе доноси

Директиву
о безбедности информационо-комуникационог система

I ОПШТЕ ОДРЕДБЕ

Члан 1.

Директивом о безбедности информационо-комуникационог система (у даљем тексту: Директива) утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система (у даљем тексту: ИКТ систем) Министарства државне управе и локалне самоуправе (у даљем тексту: Министарство).

Мере прописане овом Директивом се односе на све организационе јединице Министарства, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Министарства.

За праћење примене ове Директиве обавезује се запослени у организационој јединици за опште и информатичке послове.

Члан 2.

Поједини термини у смислу ове директиве 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 подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКТ системом;

2) *информациона безбедност* представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

3) *тајност* је својство које значи да податак није доступан неовлашћеним лицима;

4) *интегритет* значи очуваност изворног садржаја и комплетности податка;

5) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) *аутентичност* је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

7) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

8) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

9) *управљање ризиком* је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

10) *инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

11) *мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

12) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

13) *ИКТ систем за рад са тајним подацима* је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

14) *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

15) *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) Freeware је бесплатан софтвер;
24) Opensource софтвер отвореног кода;
25) 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;
26) USB или флеш меморија је спољњи медијум за складиштење података;
27) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;
28) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

II МЕРЕ ЗАШТИТЕ

Члан 3.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности Министарства.

Члан 4.

Сваки корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова.

За контролу и надзор над обављањем послова корисника, у циљу препознавања опасности по заштиту и безбедност ИКТ система Министарства надлежна је организациона јединица за опште и информатичке послове у сарадњи са Канцеларијом за информационе технологије и електронску управу (у даљем тексту: Канцеларија).

Члан 5.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност;
- послови 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, 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.

Члан 6.

Запослени и друга лица, корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву Министарства, и који су подешени од стране администратора информационог система, организационе јединице за опште и информатичке послове, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака (електронска пошта).

Приступ ресурсима ИКТ система Министарства са удаљених локација, од стране запослених и других корисника, у циљу обављања радних задатака, омогућен је само путем заштићене VPN/интернет конекције (уколико то техничке могућности дозвољавају).

Свим корисницима ИКТ система - забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.)

Запослени у организационој јединици за опште и информатичке послове, је дужан да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради *фабрички ресет*, и обавести корисника ИКТ система о последицама истог.

Уколико овлашћено лице – администратор система Канцеларије установи неовлашћен приступ (инцидент) о томе се путем електронске поште одмах, а најкасније сутрадан обавештава овлашћено лице организационе јединице за опште и информатичке послове, које о томе одмах обавештава секретара Министарства.

Члан 7.

ИКТ системом управљају запослени у складу са важећим Правилником о унутрашњем уређењу и систематизацији радних места.

Извршилац за администрирање система је дужан да сваког новог корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Министарства.

Члан 8.

У случају промене послова, односно радног места корисника ИКТ система, извршилац за администрирање система, организационе јединице за опште и информатичке послове, ће извршити промену привилегија које је корисник ИКТ система имао у складу са описом радних задатака, а на основу захтева претпостављеног, који је саставни део ове Директиве (прилог 2.).

У случају престанка радног ангажовања корисника ИКТ система, кориснички налог се укида, на основу захтева предпостављеног (прилог 2.).

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

Члан 9.

Информациона добра Министарства су сви ресурси који садрже пословне информације Министарства, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације,

конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње акте и правилнике који се односе на ИКТ систем и сл.

Евиденцију о информационим добрима води извршилац за администрирање система, у писаној и електронској форми.

Предмет заштите су:

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

Члан 10.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани посебним прописима [1].

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

Члан 11.

Извршилац за администрирање система ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених лица.

Евиденцију носача на којима су снимљени подаци води извршилац за администрирање система. Носачи морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта носача са подацима секретар Министарства ће одредити одговорну особу и начин транспорта.

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

Члан 12.

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

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

Корисник ИКТ система 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.

---

[1] Закон о слободном приступу информацијама од јавног значаја („Сл. гласник РС“, број 120/04, 54/07, 104/09 И 36/10), Закон о заштити података о личности („Сл. гласник РС“, број 97/08,104/09-ДР. Закон 68/12,-ОДЛУКА УС И 107/2012), Закон о тајности података („Сл. гласник РС“, број 104/2009), као и Уредба о начину и поступку означавања тајности података, односно докумената („Сл. гласник РС“, број 8/2011)

Корисник ИКТ система је дужан да поштује 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 Министарства 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 или електронској форми;
8) обезбеди сигурност података у складу са важећим прописима;
19) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (backup) података у складу са прописаним процедурама;
13) користи интернет и електронску пошту у Министарству у складу са прописаним процедурама;
14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају по захтеву или по распореду организационе јединице за опште и информатичке послове;
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.

Корисник ИКТ система дужан је да користи интернет и е-пошту у складу са Упутством за коришћење интернета и е-поште, које је саставни део ове директиве.

Члан 13.

Право приступа ИКТ систему имају само запослени који имају администраторске или корисничке налоге.

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

Администраторски налог може/могу да користи/е само запослени на пословима ИКТ.

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 врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране корисника.

Кориснички налог додељује администратор, на основу захтева руководиоца организационих јединица Министарства и сагласности секретара Министарства (прилог 2) и води евиденцију о додељеним корисничким налозима на табели за регистрацију додељених приступа која је саставни део ове Директиве (прилог 3.).

У случају одсуства са посла дуже од месец дана, кориснику ИКТ ресурса се привремено укида право приступа систему, до повратка на посао. У случајевима када је због потреба посла неопходан приступ документима и електронској пошти одсутног корисника ИКТ система, администратор ИКТ система дозвољава приступ другом кориснику на основу писаног захтева руководиоца организационе јединице и сагласности секретара Министарства у коме је прецизиран период коришћења наведених информатичких ресурса (прилог 2.).

Члан 14.

Кориснички налог се састоји од корисничког имена и лозинке (***Пример***: корисничко име се креира по матрици име.презиме, латиничним писмом без употребе слова ђ,ж,љ, њ, ћ, ч, џ, ш - ***Препорука***: Уместо ових слова користити слова из табеле)

Ћирилична слова	Латинична слова
Ђ	dj
Ж	z
Љ	lj
Њ	nj
Ћ, Ч	c
Ш	s
Џ	dz

Лозинка мора да садржи минимум осам 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 ИКТ система посумња да је друго лице открило његову лозинку дужан је да одмах промени лозинку.

Корисник ИКТ система дужан је да мења лозинку најмање једном у 45 дана.

Иста лозинка се не сме понављати у временском периоду од 11. месеци односно 10. наредних пута.

Члан 15.

Приступ ресурсима ИКТ система Министарства не захтева посебну криптозаштиту.

Члан 16.

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. 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).

Евиденцију о уласку у ову зону води запослени Канцеларије и Поште Србије.

Члан 17.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу секретара Министарства и овлашћеног лица Канцеларије уз присуство извршиоца организационе јединице за опште и информатичке послове, сходно Упутству за управљање односима са испоручиоцима које је саставни део ове Директиве.

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 носачи са подацима.

Прозори и врата на овој просторији морају увек бити затворени.

Сервери и активна мрежна опрема морају стално бити прикључени на уређаје за непрекидно напајање – UPS.

У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, овлашћено лице Канцеларије и ЈП Пошта Србије је дужно да искључи опрему у складу са процедурама произвођача опреме.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења секретара Министарства, директора Канцеларије и директора Поште Србије.

У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење секретара Министарства.

Ако се опрема износи ради сервисирања, поред одобрења секретара Министарства, 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 део ИКТ ресурса Министарства.

Члан 18.

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 секретару Министарства одговарајуће мере.

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад корисника ИКТ система.

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.

Члан 19.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару је потребно је инсталирати антивирусни програм.

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

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

У циљу заштите, односно упада у ИКТ систем Министарства са интернета, администратор информационих система Канцеларије је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет, при чему администратор информационих система 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 корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши администратор информационог система.

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

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави организационој јединици за опште и информатичке послове.

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 streaming и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета;
- коришћење електронске поште у приватне сврхе;
- коришћење приватних налога електронске поште у службене сврхе;
- отварање електронске поште са прилозима која долази са непознате и сумњиве адресе, као одлазак на интернет адресу која је саставни део те електронске поште.

Коришћење приватних мобилних уређаја (лаптоп и таблет) који приступају ИКТ ресурсима, могуће је само за обављање послова из надлежности Министарства, подешених од стране администратора ИКТ система у периоду када није могуће користити уређај у власништву Министарства.

Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже може се одузети право приступа (ставиће се забрана приступа интернету гледање филмова, аудио и видео streaming и сл.).

Члан 20.

Базе података обавезно се архивирају на преносиве носаче података (CDROM, DVD, USB, „strimer" трака, екстерни хард диск) за потребе обнове базе података.

Подаци о корисницим, архивирају се најмање једном месечно. Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно, од 15 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 („Сл. гласник РС", број 10/93, 14/93-испр. и 67/2016).

Члан 21.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и др. мора бити подешен тако да одмах обавештава администратора система о свим нерегуларним активностима корисника ИКТ ресурса, покушајима упада и упадима у систем.

Члан 22.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Канцеларије, Министарства, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само администратор информационог система, односно корисник ИКТ ресурса који има овлашћење за то.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера сходно Упутству за управљање односима за испоручиоцима.

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.

Члан 23.

Администратор информационог система, најмање једном месечно а по потреби и чешће врши анализу потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, администратор информационог система, је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

Администратор информационог система, треба да подешавањем корисничких налога, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

Члан 24.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника ИКТ ресурса, чији би пословни процес био ометан, уз претходну сагласност секретара Министарства.

Члан 25.

Комуникациони каблови и каблови за напајање морају бити безбедно постављени, тако да се онемогући неовлашћен приступ.

Члан 26.

Министарство врши размену података са органима и организацијама у складу са законима, потписаним уговорима и протоколима у којима су јасно наведена овлашћена лица ИКТ система.

Члан 27.

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

Администратор информационог система је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

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

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

Члан 28.

Приликом тестирања система, за податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су лични подаци, администратор система, одговара у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

Члан 29.

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ сходно Упутству за управљање односима са испоручиоцима.

Организациона јединица за опште и информатичке послове, је одговорна за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредаба ове директиве којима су такве активности дефинисане.

Члан 30.

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

Члан 31.

Физичко техничко обезбеђење зграде Министарства врши треће лице на основу уговора потписаног са Управом за заједничке послове републичких органа и организовано је сходно Упутству за обезбеђење објекта које је саставни део ове директиве.

Члан 32.

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

По пријему пријаве, администратор информационог система, је дужан да одмах обавести секретара Министарства и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, „Сл. гласник РС", број 94/2016), администратор информационог система, је дужан да осим секретара Министарства обавести и надлежни орган дефинисан наведеном уредбом.

Организациона јединица за опште и информатичке послове, води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом.

Члан 33.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Министарства, организациона јединица за опште и информатичке послове, је дужна да у најкраћем року пренесе делове ИКТ система, неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

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

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 34.

Проверу ИКТ система врши администратор информационог система министарства у сарадњи са овлашћеним лицима Канцеларије.

Члан 35.

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 ИКТ система 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.

IV ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 36.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, руководилац организационе јединице за опште и информатичке послове, дужан је да предложи измену ове Директиве у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Члан 37.

Ова Директива ступа на снагу осмог дана од дана објављивања на огласној табли Министарства.

Датум објављивања 26. 01. 2018. године
Датум ступања на снагу 02.02. 2018. године

МИНИСТАР
Бранко Ружић

Република Србија
МИНИСТАРСТВО ДРЖАВНЕ УПРАВЕ И ЛОКАЛНЕ САМОУПРАВЕ

ИЗЈАВА О ПРИХВАТАЊУ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА

Дајем изјаву да сам прочитао/ла доле наведену политику безбедности ИКТ система и обавезујем се да се придржавам њеног садржаја, као и свих осталих релевантних политика информационе безбедности прописаних од Министарства државне управе и локалне самоуправе (у даљем тексту: Министарство) које су обавезујуће за запослене.

1. Поступаћу у складу са Директивом о безбедности ИКТ система Министарства, прописаним процедурама и правилима.
2. Упознат/а сам да се моја употреба компјутера и комуникационих система можда надзире и /или бележи у законите сврхе.
3. Прихватам да сам одговоран/а за коришћење и заштиту свих креденцијала који су ми додељени (корисички налог и лозинку, токен за приступ или друге ставке које су ми додељене).
4. Изјављујем да нећу користити туђи кориснички налог и лозинку како би приступио системима Министарства.
5. Изјављујем да нећу покушати приступити ниједном другом компјутерском систему за који немам одобрен приступ.
6. Заштитићу сваки поверљиви материјал који ми је послат, примљен, спремљен и обрађен, у складу са степеном поверљивости који има, како електронске, тако и папирне копије.
7. Сваки поверљиви материјал који креирам означићу у складу са смерницама за објављивање, како би он остао прикладно заштићен.
8. Нећу слати поверљиве информације интернетом путем смаил-а или било којим другим методом осим ако нису коришћени одговарајући методи (нпр. енкрипција) који ће их заштитити од неовлашћеног приступа.
9. Водићу рачуна да сам унео/ла тачну емаил адресу примаоца, како поверљиве информације не би биле компромитоване.
10. Обезбедићу да ме не надгледају неовлашћена лица док радим и предузећу одговарајуће мере предострожности када штампам поверљиве информације.
11. Поверљив одштампан материјал ћу пажљиво да архивирам и побринућу се да је исправно уништен, када више не буде потребан.
12. Нећу остављати свој компјутер без надзора и омогућити неовлашћен приступ информацијама путем мог налога док сам одсутан/одсутна.
13. Упознаћу се са свим политикама и процедурама безбедности у Министарству и свим посебним упутствима повезаним са мојим послом.
14. Одмах ћу обавестити свог надређеног ако приметим, посумњам или будем сведок инциденту који може да проузрокује повреду безбедности.
15. Нећу покушати да избегнем систем безбедносних контрола.
16. Нећу уклањати опрему или информације из просторија Министарства без одговарајућег одобрења.
17. Водићу рачуна о компјутерским медијима или преносивим компјутерима када их будем носио/ла ван просторија Министарства.
18. Нећу унети вирусе или друге злонамерне програме у систем или мрежу.
19. Нећу покушати да искључим антивирус заштиту која ми се налази на компјутеру.
20. Усагласићу се са законским, правним и уговорним обавезама о којима ме Министарство обавести.

Република Србија
МИНИСТАРСТВО ДРЖАВНЕ УПРАВЕ И ЛОКАЛНЕ САМОУПРАВЕ

ИЗЈАВА О ПРИХВАТАЊУ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА

21. Обавезујем се да ћу редовно вршити backup података, као и проверу снимљених података у складу са упутствима.
22. Приликом напуштања Министарства, пре одласка обавестићу свог непосредног руководиоца о свим важним информацијама које се налазе на мом налогу.

Име корисника:

Потпис корисника:

Датум:

Ова изјава израђује се у два примерка, један примерак задржаће корисник, а други Министарство.

Прилог 2.

Република Србија
МИНИСТАРСТВО ДРЖАВНЕ УПРАВЕ И ЛОКАЛНЕ САМОУПРАВЕ

ЗАХТЕВ ЗА ДОДЕЉИВАЊЕ/ПРОМЕНУ/УКИДАЊЕ ПРАВА ПРИСТУПА ИКТ СИСТЕМУ

Захтев за	Доделу ☐	Промену ☐	Укидање ☐
Име и презиме запосленог/лица коме се одобрава приступ			
Сектор			
Организациона јединица			
Радно место			
Датум доделе/промене/укидања права приступа			
Период важења права приступа			
Разлози за одобравање допунских права приступа			

Приступ		**Ниво**		**Захтев**	
Апликацијама	☐	Администратор	☐	Омогући	☐
Фолдерима	☐	Корисник	☐	Забрани	☐
Рачунарима	☐	Измена	☐	Суспендуј	☐
Просторијама	☐	Преглед	☐	Укини суспензију	☐
Радним станицама	☐	Унос	☐		☐
Domain ресурсима	☐	Штампање	☐		☐
Базама података	☐		☐		☐
	☐		☐		☐
	☐		☐		☐

ОПИС		

Прилог 2.

Република Србија
МИНИСТАРСТВО ДРЖАВНЕ
УПРАВЕ И ЛОКАЛНЕ САМОУПРАВЕ

ЗАХТЕВ ЗА ДОДЕЉИВАЊЕ/ПРОМЕНУ/УКИДАЊЕ ПРАВА ПРИСТУПА ИКТ СИСТЕМУ

На основу спроведене анализе ризика по безбедност информација захтев се: **ОДОБРАВА – НЕ ОДОБРАВА** *(прецртати сувишно).*

Напомена у вези права приступа:	

	Име и презиме	**Датум**	**Потпис**
Захтев поднео:			
Захтев одобрио:			
Налог за доделу права приступа примио:			

Прилог 3.

Република Србија
МИНИСТАРСТВО ДРЖАВНЕ УПРАВЕ И ЛОКАЛНЕ САМОУПРАВЕ

ТАБЕЛА ЗА РЕГИСТРАЦИЈУ ДОДЕЉЕНИХ ПРИСТУПА

Организациона целина:

Ред. бр.	Радно место	Приступ[1]	Ниво[2]	Име и презиме запосленог	Датум доделе приступа	Корисничко име	Лозинка
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							
13.							
14.							
15.							
16.							
17.							

	Име и презиме	Датум	Потпис
Израдио:			
Верификовао:			

[1] *А - Апликацијама, Ф - Фолдерима, Р - Рачунарима, П - Просторијама, РС - Радним станицама, Д - Домаин ресурсима, Б - Базама података.*

[2] *А – Администратор, К – Корисник, И – Измена, П – Преглед, У – Унос, Ш – Штампање.*