Република Србија
МИНИСТАРСТВО НАУКЕ,
ТЕХНОЛОШКОГ РАЗВОЈА И ИНОВАЦИЈА
Број: 002395648 2024 13440 004 001 020 092 04 001
Датум: 09.08.2024. године
Београд
Немањина 22-26

На основу члана 44. Закона о државној управи („Службени гласник РС“, бр. 79/05, 101/07, 95/10, 99/14, 30/18 – др. закон и 47/18), и члана 8. Закона о информационој безбедности („Службени гласник РС“, бр. 6/16, 94/17 и 77/19), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационог система од посебног значаја („Службени гласник РС“, бр. 94/16), министар науке, технолошког развоја и иновација, 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 одржавање адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система (у даљем тексту: ИКС) Министарства науке, технолошког развоја и иновација (у даљем тексту: Министарство).

Мере прописане овом Директивом се односе на све организационе јединице Министарства, на све запослене, радно ангажоване, као и на трећа лица која користе информатичке ресурсе Министарства (у даљем тексту: корисници ресурса).

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 ИК систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хадверских компонената, техничку и корисничку документацију, унутрашње акте и правилнике који се односе на ИКС и сл.

Члан 2.

Поједини термини у смислу ове директиве имају следеће значење:

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

- *електронске комуникационе мреже* у смислу закона који уређује електронске комуникације;

- уређај или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
- податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачке (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКС;

2) *информациона безбедност* представља скуп мера које омогућавају да подаци којим се рукује путем ИКС 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 података;
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 ИКС;
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 ИКС* су техничке и организационе мере за управљање безбедоносним ризицима ИКС;
12) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
13) *ИКС за рад са тајним подацима* је ИКС 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) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;
17) *криптоматеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
18) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
19) *информациона добра* обухватају податке у датотекама и базама података, програмски код, конфигурацију хадверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
20) *VPN (Virtual Private Network)* – је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
21) *MAC адреса (Media Access Control Address)* је јединствени број, којим се врши индентификација уређаја на мрежи;
22) *Freeware* је бесплатан софтвер;

23) *Opensource софтвер* отвореног кода;
24) *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;
25) *USB* или флеш меморија је спољашњи медијум за складиштење података;
26) *CD-ROM (Compact disk – read only memory)* се користи као медијум за снимање података;
27) *DVD* је оптички диск високог капацитета који се користи као медујум за складиштење података.

II МЕРЕ ЗАШТИТЕ

Члан 3.

Мерама заштите ИКС 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 ИКС је одговоран за безбедност ресурса ИКС које користи ради обављања послова.

За контролу и надзор над обављањем послова корисника, у циљу препознавања опасности по заштиту и безбедност ИКС Министарства надлежан је запослени у Одсеку за кадровске и опште послове и подршку управљању (у даљем тексту: Администратор ИКС Министарства) и шеф Одсека за кадровске и опште послове и подршку управљању, 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 ИКС, 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 ИКС, у складу са прописима (као нпр. Министарства унутрашњих послова, Канцеларију и др.).

Члан 6.

Корисници ресурса, могу путем мобилних уређаја, који су у власништву Министарства, и који су подешени од стране Администратора ИКС Министарства, да приступају само оним деловима ИКС који им омогућавају обављање радних задатака (електронска пошта).

Приступ информационим добрима Министарства са удаљених локација од стране користинка ресурса, у циљу обављања радних задатака, омогућен је само путем заштићене VPN/интернет конекције.

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

Администратор ИКС Министарства, је дужан да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради *фабрички ресет*, и обавести корисника ресурса о последицама истог.

Уколико овлашћено лице – администратор система Канцеларије (у даљем тексту овлашћено лице Канцеларије) установи неовлашћени приступ (инцидент) о томе се путем електронске поште одмах, а најкасније сутрадан обавештава Администратор ИКС Министарства, које о томе одмах обавештава секретара Министарства.

Члан 7.

Администратор ИКС Министарства је дужан да сваког новог корисника ресурса упозна са одговорностима и правилима коришћења ИКС ресурса Министарства.

Члан 8.

У случају промене услова односно радног места корисника ресурса, Администратор ИКС Министарства, ће извршити промену привилегија које је користник ресурса 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 ресурса, кориснички налог се укида, на основу захтева предпостављеног (прилог 2.).

Корисник ресурса, након престанка радног ангажовања у Министарству, не сме да отрива податке који су од значаја за иформациону безбедност ИКС.

Члан 9.

Евиденцију о информационим добрима води Администратор ИКС Министарства, у писаној и електронској форми.

Предмет заштите су:

- хадверске софтверске компоненте ИКС;
- подаци који се обрађују или чувају на компонентама ИКС;
- користнички налози и други подаци о корисницима информатичких ресурса ИКС.

Члан 10.

Подаци који се налазе у ИКС представљају тајну, ако су тако дефинисани просебним 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 53/11).

Члан 11.

Администратор ИКС Министарства, 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 Администратор ИКС Министарства. Носачи морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

---

[1] Закон о слободном приступу информацијама од јавног значаја („Сл. гласник РС“, број 120/04, 54/07, 104/09, 36/10 и 105/21), Закон о заштити података о личности („Сл. Гласник РС“, број 87/18), Закон о тајности података („Сл. Гласник РС“, број 104/09), као и Уредба о начину и поступку означавања тајности података, односно докумената („Сл. Гласник РС“, број 8/11)

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

Члан 12.

Приступ информационим добрима Министарства одређен је врстом налога, односно додељеном улогом коју корисник ИКС има.

Администратор ИКС Министарства, има права приступа свим информационим добрима Министарства (софтверским и хадверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања информационим добрима Министарства.

Корисник ресурса може да користи само свој кориснички налог који је добио од Администратора ИКС Министарства и не сме да омогући другом лицу коришћење његовог корисничког налога, сем Администратору ИКС Министарства.

Корисник ресурса је дужан да поштује следећа правила безбедног и примереног коришћења информационих добра Министарства, 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 упутству Канцеларије;
6) пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу;
7) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
8) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
9) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
10) израђује заштитне копије (backup) података у складу са прописаним процедурама;
11) користи интернет и електронску пошту у Министарству у складу са утврђеним правилима понашања државних службеника;
12) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија и сл.) обављају по распореду плана Администратора ИКС Министарства;
13) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
14) прихвати да техничке сигурности (анти вирус програми, *firewall*, системи за детекцију упада, средстава за шифрирање, средстава за проверу интегритета и др.) спречавају потенцијалне претње ИКС;
15) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

Члан 13.

Право приступа ИКС имају само корисници ресурса.

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

Администраторски налог има само запослени на пословима ИКС.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу којих се врши аутентификација – провера индентитета и ауторизација – провера права приступа, односно права коришћења информационих добра Министарства од стране корисника ресурса.

Кориснички налог додељује Администратор ИКС Министарства, на основу захтева руководиоца организационих јединица Министарства.

У случају одсуства са посла дуже од месец дана, кориснику ресурса се привремено укида право да приступа систему до повратка на посао. У случајевима када је због потреба посла неопходан приступ документима и електронској пошти одсутног корисника ресурса, Администратор ИКС Министарства дозвољава приступ другом кориснику ресурса на основу писаног захтева руководиоца организационе јединице 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 ресурса посумња да је друго лице открило његову лозинку дужан је да одмах промени лозинку.

Члан 15.

Приступ информационим добрима Министарства не захтева посебну криптозаштиту.

Члан 16.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКС, организује се као административна зона. Административна зона се успоставља за физички приступ ресурсима информациним добрима Министарства, видљиво означеном простору, који је обезбеђен. Простор мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и њему треба да буде одговарајућа температура (климатизован простор).

Министарство науке, технолошког развоја и иновација користи заједничку просторије у сарадњи са Министарсвом просвете, у згради Немањина 22-26, у Београду.

Члан 17.

Осим Администратора ИКС Министарства, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених информационих добара Министарства, а по претходном одобрењу секретара Министарства уз присуство и Администратора ИКС система Министарства.

Просторија мора бити видљиво обележена и у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у који се налази ИКС 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-a*, Администратор ИКС Министарства у сарадњи са овлашћеним лицем испред Министарства просвете је дужно да искључи опрему у складу са порцедурама произвођача опреме.

ИКС опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети.

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 ИКС ресурса Министарства.

Члан 18.

Запослени на пословима ИКС континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКС 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 ИКС.

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.

Корисници ресурса министарства пролазе обуке које се спроводе 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.

Под обуком се сматра и достављена информација о заштити из става.1 овог члана (усмена или путем имејла од стране Администратора ИКС Министарства).

За успешну заштиту од вируса на сваком рачунару је потребно 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 ИКС Министарства са интернета администратор информационих система Канцеларије је дужан да одржава систем за спречавање упада.

Корисницима ресурса који су прикључени на ИКС је забрањено самостално прикључивање на интернет, при чему Администратор ИКС Министарства, може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ресурса који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКС, а сваки рачунар чији се корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши Администратор ИКС Министарства.

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 ресурса примети необично понашање рачунара, запажање треба без одлагања да пријави Администратору ИКС Министарства.

Недозвољена употреба интернета обухвата:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступних „пиратских“ или других софтверских производа који нису лиценцирани на одговорајући 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 приватиних налога електонске 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 ИКС ресурсима, могуће је само за обављање послова из надлежности Министарства подешених од стране Администратор ИКС Министарства у периоду када није могуће користити уређај у власништву Министарства.

Корисницима који неадекваним 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.

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

Сваки примерак годишње копије-архиве чува се у року који је дифинисан Упутсвом о канцеларијском пословању органа државне управе („Сл. гласник РС“, број 10/93, 14/93-испр., 67/16, 3/17 и 20/22 – др. упутство).

Члан 21.

Систем за контролу и дојаву о грешкама, неовашћеним активностима и др (систем Канцеларије), мора бити подешен тако да одмах обавештава Администратора ИКС Министарства о свим нерегуларним активностима корисника ресурса, покушајима упада и упадима у систем. Администратор ИКС Министарства мора да поступи по обавештењу и отклони нерегуларне активности.

Члан 22.

У ИКС 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 ИКС Министарства.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера сходно Упутству за управљање односима са 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 ИКС Министарства, по потреби врши анализу потенцијалних слабости ИКС.

Уколико се идентификују слабости које могу да угрозе безбедност ИКС, Администратор ИКС Министарства, је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

Администратор ИКС Министарства, треба да подешавањем корисничких налога, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКС.

Члан 24.

Ревизија ИКС система се мора вршити тако да има што мањи утицај на пословне процесе корисника ресурса. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника ресурса, чији би пословни процес био ометен, уз обавештење руководиоца организационе јединице о активностима у њиховим просторијама ван радног времена.

Члан 25.

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

Члан 26.

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

Члан 27.

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

Администратор ИКС Министарства је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКС, односно увођењу нових делова и изменама постојећих делова ИКС, Администратор ИКС Министарства води документацију.

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

Члан 28.

Приликом тестирања система, за податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су лични подаци, Администратор ИКС Министарства, 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 Упутсву за управљање односима са испоручиоцима.

Лице за чије потребе је јавна набавка извршена са Администратором ИКС Министарства и лицем које је задужено за послове јавних набавки у Министарству је одговорно за контролу приступа и надзор над извршењем уговорних обавеза, као и за поштовање одредаба ове директиве којима су такве активности дефинисане.

Члан 30.

Физичко техничко обезбеђење зграде Министарства се врши се на јединствен начин за целу зграду у Немањиној 22-26, Немањиној 11, Булевару Михајла Пупина 2, у Београду, од стране Министарства унутрашњих послова – Одељења за обезбеђење објеката и личности.

Физичко техничко обезбеђење зграде у Његошевој 12, Београд, врши се на јединствен начин којим се обезбеђује објекат у Његошевој.

Члан 31.

У случају било каквог инцидента који може да угрози безбедност информационог добра Министарства, корисник ресурса је дужан да одмах обавести Администратора ИКС Министарства.

По пријему пријаве, Администратор ИКС Министарства, је дужан да одмах обавести секретара Министарства и предузме мере у циљу заштите информационог добра Министарства.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, („Сл. гласник РС“, бр. 11/20), Администратор ИКС Министарства, ја дужан да осим секретара Министарства обавести и надлежни орган дефинисан наведеном уредбом.

Администратор ИКС Министарства, води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом.

Члан 32.

У случају ванредних околности, које могу да доведу до измештања ИКС из зграде Министарства, Администратор ИКС Министарства, је дужан да у најкраћем року организује пренос делова ИКС, неопходних за функционисање у ванредној ситуацији. Делове ИКС који нису неопходни за функционисање у ванредним ситуацијама складиште се на резервну локацију коју одреди министар или други овлашћени орган.

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

III ПРОВЕРА ИКС

Члан 33.

Проверу ИКС врши Администратор ИКС Министарства у сарадњи са овлашћеним лицима Канцеларије.

Члан 34.

Извештај о провери ИКС садржи:

1) назив оператора ИКС 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 Директиве о безбедности ИКС са прописаним условима;
6) закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
7) закључке по питању евентуалних безбедоносних слабости на нивоу техничких карактеристика компоненти ИКС;
8) оцена укупног нивоа информационе безбедности;
9) предлог евентуалних корективних мера;
10) потпис одговорног лица које је спровело проверу ИКС.

IV ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 35.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКС и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, шеф Одсека за кадровске и опште послове и подршку управљању у сарадњи са Администратором ИКС Министарства, дужан је да предложи измену ове Директиве у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКС, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКС.

Члан 36.

Приликом заснивања радног односа, односно радног ангажовања корисника ресурса, Министарство науке, технолошког развоја и иновација је дужно да га упозна са политиком безбедности ИКС а корисник ресурса је у обавези да потпише изјаву о прихватању политике безбедности ИКС, која се потом улаже у његов персонални досије (Прилог 1.)

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

Датум објављивања 12.08. 2024. године
Датум ступања на снагу 20.08. 2024. године

МИНИСТАР

др Јелена Беговић

Република Србија
МИНИСТАРСТВО НАУКЕ,
ТЕХНОЛОШКОГ РАЗВОЈА И
ИНОВАЦИЈА

ИЗЈАВА О ПРИХВАТАЊУ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИКС

Дајем изјаву да сам прочитао/ла доле наведену политику безбедности ИКС и обавезујем се да се придржавам њеног садржаја, као и и свих осталих релевантних политика информационе безбедности прописаних од Министарства науке технолошког развоја и иновација (у даљем тексту: Министарство) које су обавезујуће за запослене.

1. Поступаћу у складу са Директивом о безбедности ИКС Министарства, прописаним процедурама и правилима.
2. Прихватам да сам одговоран/а за коришћење и заштиту свих креденцијала који су ми додељени (кориснички налог и лозинку, токен за приступ или друге ставке које су ми додељене).
3. Изјављујем да нећу користити кориснички налог и лозинку у приватне сврхе, како би приступио системима Министарства.
4. 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.
5. Сваки поверљиви материјал који креирам означићу у складу са смерницама за објављивање, како би он остао прикладно заштићен.
6. Нећу слати поверљиве информације интернетом путем емаил-а или било којим другим методом осим ако нису коришћени одговорајући методи (нпр. енкрипција) који ће их заштити од неовлашћеног приступа.
7. Водићу рачуна да сам унео/ла тачну емаил адресу примаоца, како поверљиве инфорамације не би биле компромитоване.
8. Обезбедићу да ме не надгледају неовлашћена лица док радим и предузећу одговорајуће мере предострожноти када штампам поверљиве информације.
9. Поверљив одштампан материјал ћу пажљиво да архивирам и побринућу се да је исправно уништен, када више не буде потреба.
10. Нећу остављати свој компјутер без надзора и омогућити неовлашћен приступ инфорамцијама путем мог налога док сам одсутан/одсутна.
11. Упознаћу се са свим политикама и процедурама безбедности у Министарству и овим посебним упутствима повезаним са мојим послом.
12. Одмах ћу обавестити свог надређеног и Администратора ИКС Министарства ако приметим, посумњам или будем сведок инциденту који може да проузрокује повреду безбедности.

Република Србија
МИНИСТАРСТВО НАУКЕ,
ТЕХНОЛОШКОГ РАЗВОЈА И
ИНОВАЦИЈА

ИЗЈАВА О ПРИХВАТАЊУ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИКС

13. Нећу уклањати опрему или инфорамције из просторија Министарства без одговарајућег одобрења.
14. Водићу рачуна о компјутерским медијима или преносивим компјутерима када их будем носио/ла ван просторија Министарства.
15. Нећу намерно унети вирусе или друге злонамерне програме у систем или мрежу.
16. Нећу покушати да искључим антивирус заштиту која ми се налази на компјутеру.
17. Редовно ћу вршити *backup* података, као и проверу снимљених података у складу са потребама организационих јединица.
18. Приликом напуштања Министарства, пре одласка обавестићу свог непосредног руководиоца о свим важним информацијама које се налазе на мом налогу.

Име корисника: _____

Потпис корисника: _____

Датум: _____. године

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

Република Србија
МИНИСТАРСТВО НАУКЕ,
ТЕХНОЛОШКОГ РАЗВОЈА И
ИНОВАЦИЈА

Прилог 2.

ЗАХТЕВ ЗА ДОДЕЉИВАЊЕ/ПРОМЕНУ/УКИДАЊЕ ПРАВА ПРИСТУПА ИКС

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			
Разлози за одобравања 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		

Република Србија
МИНИСТАРСТВО НАУКЕ,
ТЕХНОЛОШКОГ РАЗВОЈА И
ИНОВАЦИЈА

Прилог 3.

ТАБЕЛА ЗА РЕГИСТРАЦИЈУ ДОДЕЉЕНИХ ПРИСТУПА

Организациона целина: _____

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

	Име и презиме	Датум	Потпис
Израдио:			
Верификовао			

[2] А-Апликацијама, Ф-Фолдерима, Р-рачунарима, П-Просторијама, РС – Радним станицама, Д-Домаин ресурсима, Б-Базама података
[3] А-Администратор, К-Корисник, И-Измена, П-Преглед, У-Унос, Ш-Штампање.