



**РЕПУБЛИКА СРБИЈА**  
**МИНИСТАРСТВО ФИНАНСИЈА**

**ДИРЕКТИВА**

**за правилно коришћење информационе имовине**

---

Београд, 09. јун 2020. године  
верзија 1



На основу члана 44. став 1. Закона о државној управи („Службени гласник РС”, бр. 79/05, 101/07, 95/10, 99/14, 30/18 -др. закон и 47/18),

министар финансија издаје,

## **Директиву за правилно коришћење информационе имовине**

### **Уводне одредбе**

#### **Члан 1.**

Овом Директивом ближе се уређује додељивање рачунара, задужење, коришћење, раздужење и вођење евиденције о рачунарској опреми, антивирусна заштита, коришћење електронске поште и интернета, коришћење лаптоп рачунара и преносивих медија, коришћење мобилних телефона, поступање са поверљивим документима (у циљу унапређења безбедности података у Министарству финансија) (у даљем тексту: Министарство).

### **Додела рачунарске опреме и стандардног софтвера**

#### **Члан 2.**

Рачунар који је инсталиран радно ангажованим лицима у Министарству мора бити конфигурисан на начин који испуњава минималне услове неопходне за његово функционисање, тј. да је:

- а) Инсталиран оперативни систем;
- б) Учлањен у домен;
- в) Додељено одговарајуће корисничко име на мрежи;
- г) Инсталиран корпоративни антивирус програм;
- д) Инсталиран Office пакет;
- ђ) Инсталиран претраживач;
- е) Инсталиран софтвер за читање pdf фајлова;
- ж) Инсталиран програм за архивирање и компресовање фајлова.

### **Додатни софтверски програми**

#### **Члан 3.**

Уколико постоји оправданост захтева, могуће је извршити инсталацију других софтвера, по захтеву руководиоца надлежне организационе јединице, уз претходну сагласност министра, односно лица на које је министар пренео овлашћење.

Сви софтвери који су инсталирани на рачунарима и рачунарској опреми морају бити лиценцирани.

Корисник не сме да врши самоницијативно инсталирање софтвера или мењање конфигурације рачунара и остале рачунарске опреме.

## **Рачунарска опрема која није у власништву Министарства**

### **Члан 4.**

Рачунарска опрема која није у јавној својини Републике Србије (у даљем тексту јавна својина РС) односно Министарства, Управе за заједничке послове државних органа и Канцеларије за информационе технологије и електронску управу (у даљем тексту: Канцеларија за ИТ) или управа у саставу Министарства, не сме се учинити у домену

Самоиницијативно прикључење рачунара и рачунарске опреме од стране корисника на мрежу Министарства је забрањено.

### **Задужење, рачунарске опреме од стране запослених**

#### **Члан 5.**

Поступак за инсталацију рачунарске опреме покреће организациона јединица за људске ресурсе, на основу електронског обавештења, којим доставља информацију организационој јединици за ИТ, са подацима о новозапосленим лицима који су примљени у радни однос на неодређено и одређено време, као и за лица са којима је потписан уговор о привременим и повременим пословима.

Када је лице ангажовано у Министарству по основу радног односа на неодређено или одређено време или уговора о привременим или повременим пословима, опремом се задужење лице које ту опрему користи.

Приликом задужења рачунарске опреме, реверс о задужењу потписују запослени у организационој јединици за ИТ који је опрему издао и новозапослени у Министарству, и то у 2 (два) примерка.

### **Задужење опреме од стране лица ангажованих на пројектима**

#### **Члан 6.**

Уколико се опрема задужење за потребе лица које је у Министарству ангажовано по неком другом основу (који није радни однос или ангажовање по уговору о привременим и повременим пословима, нпр. ангажовање лица преко пројеката, волонтерског рада, студентске праксе итд.), опремом која се том лицу даје на коришћење, задужење се руководиоца надлежне организационе јединице, који је поднео захтев за задужење рачунарске опреме за то лице.

Приликом задужења рачунарске опреме, реверс о задужењу потписују запослени у организационој јединици за ИТ који је опрему издао и руководиоца у чијој организационој јединици су ангажована лица преко пројеката, волонтерског рада, студентске праксе итд.), и то у 2 (два) примерка.

### **Замена рачунарске опреме**

#### **Члан 7.**

Уколико је потребно рачунарску опрему, која је дата на коришћење, заменити другом опремом, сачињава се захтев о замени опреме, који потписују лице које се задужење старом и задужење новом опремом и запослени у организационој јединици за ИТ. Нова опрема се задужење путем реверса.

## **Раздужење рачунарске опреме**

### **Члан 8.**

Када лицу престаје радно ангажовање у Министарству, организациона јединица за људске ресурсе је у обавези да дан пре завршетка ангажовања обавести запослене у организационој јединици за ИТ, како би се обавио поступак раздужења рачунарске опреме.

Када лицу које ради у организационој јединици која се налази ван Београда, престане радно ангажовање у Министарству, поступак раздужења може да обави и руководицац надлежне организационе јединице.

Раздужена опрема посебно се евидентира и сва опрема се чува у просторијама које се увек закључавају, а кључеви од тих просторија се налазе само код руковођа опремом.

Потписани примерак реверса о раздужењу рачунарске опреме чува се у евиденцији организационе јединице за ИТ.

### **Члан 9.**

Организациона јединица за ИТ, по потреби а на основу захтева секретара, креира извештај о стању опреме која се налази у службеној згради у Улици кнеза Милоша број 20, у просторијама Агробанке у Сремској улици бр. 3-5, као и у организационим јединицама које се налазе ван Београда.

## **Однос запослених према рачунарској опреми и сервисима**

### **Члан 10.**

Радно ангажовано лице би требало, као корисник информационе имовине, да буде свесно својих одговорности у смислу заштите опреме и медија са подацима који се налазе на тој опреми.

Запослени су дужни да свој рачунар заштите од крађе, илегалног приступа, малициозног кода који за резултат могу имати оштећење опреме и неовлашћене употребе. Осетљиве и поверљиве информације морају бити заштићене од неовлашћеног приступа.

Добијени информатички ресурси се користе искључиво у службене сврхе

Запослени је дужан да води рачуна да опрема која му је додељена буде безбедна од неовлашћеног приступа и отуђивања.

Корисник не сме да спроводи активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање рачунарске мреже Министарства.

Имплементиране сервисе на рачунарској мрежи Министарства, запослени су дужни да користе у складу са даним упутствима и дефинисаним нивоима приступа

## **Кориснички налози за приступ информацијама**

### **Члан 11.**

Акредитиви за приступ подразумевају корисничко име и лозинку за приступ. Поред тога, као додатна мера заштите приступа осетљивим системима могу се захтевати додатни код, токен, или картица.

Запослени и трећа лица којима је одобрен приступ рачунарској мрежи морају чувати акредитиве својих корисничких налога.

Кориснички е-mail налози су формата ime.prezime@mfin.gov.rs. У случају да постоји кориснички е-mail налог са истим именом и презименом, отвара се кориснички е-mail налог: prvoslovoimena.prezime@mfin.gov.rs.

### **Антивирусна заштита**

#### **Члан 12.**

На сваком рачунару у мрежи мора бити инсталиран антивирусни софтвер. Ажурирање, конфигурација, инсталација нових верзија антивирусне заштите на корисничким рачунарима и слично, врши се централизовано, коришћењем централног антивирусног сервера.

Уколико повезивање са централним сервером није могуће, подешава се ажурирање преко интернет конекције.

За рачунаре који немају приступ интернету, ажурирање и инсталација нових верзија ради се ручно.

Радно ангажовано лице не сме да покушава да онемогући рад антивирусне заштите и ажурирање рачунара са антивирусном заштитом.

Инсталацију, конфигурисање и одржавање централног антивирусног сервера обавља организациона јединица за ИТ у сарадњи са Канцеларијом за ИТ.

### **Управљање са лозинкама**

#### **Члан 13.**

Почетну лозинку сваком од запослених креира и у непосредном контакту саопштава организациона јединица за ИТ.

Запослени је дужан да приликом првог пријављивања на мрежу креира нову лозинку и периодично је мења, у складу са добијеним упутствима.

О потреби и тачном времену периодичног ажурирања лозинке запослени се обавештава путем аутоматски генерисане поруке.

Лозинка мора да има најмање 8 (осам), а највише 16 (шеснаест) карактера. Лозинка треба да садржи најмање по један карактер из све четири наведене групе:

- а) Велика слова енглеског алфабета
- б) Мала слова енглеског алфабета
- ц) Цифре
- д) Специјални знаци

Лозинка не сме садржати било какве податке о личности запосленог и њему блиских лица, погрдне речи, имена кућних љубимаца и сл. Није дозвољено користити идентитет и лозинку другог корисника. Лозинка не може бити идентична ни једној од претходно шест креираних лозинки.

### **Поступање са лозинкама**

#### **Члан 14.**

Лозинка и ПИН код за картице су строго лични и не саопштавају се другом лицу. Лозинке и ПИН код треба памтити или чувати на сигурној локацији, ван домашаја за друге запослене и трећа лица.

Није дозвољено записивање и одлагање лозинке и ПИН кода тако да буду доступни другим лицима (на стикерима, на радном столу, у мобилном телефону и сл.).

Лозинка и ПИН код који се користи на корисничком налогу у било кој сервису на рачунарској мрежи не смеју бити исти са лозинком и/или ПИН кодом корисничког налога који запослени користи у приватне сврхе.

Ако посумња да су лозинка и ПИН код злоупотребљени или постали познати неовлашћеном лицу, запослени ће о томе одмах обавестити руководиоца организационе јединице за ИТ или лице које он одреди.

## **Недозвољено коришћење рачунарске опреме и сервиса**

### **Члан 15.**

Инсталацију посебних софтвера одобрава непосредни руководиоца, или лице које га замењује. Запослени могу на рачунарима да инсталирају само софтвер који се користи за потребе пројеката и извршења радних задатака.

Коришћење рачунарске опреме и сервиса не сме бити у сукобу са одредбама ове Директиве, преузетим уговорним обавезама, не сме се угрожавати поверљивост информација, морају се поштовати прописане процедуре које се тичу информационе безбедности система.

Недозвољено коришћење рачунарске опреме и сервиса на рачунарској мрежи, представља:

- неовлашћено коришћење или покушај неовлашћеног коришћења рачунарске опреме и сервиса;
- вршење измена на хардверу или инсталираном софтверу који је власништво Министарства, без претходне писане дозволе организационе јединице за ИТ;
- предузимање активности које угрожавају или могу да угрозе нормално функционисање и безбедност рачунарске мреже (ширење малициозног програмског кода, недозвољена употреба интернета и сл.);
- неовлашћено преузимање или слање службених докумената, података о личности других лица, корисника Министарства и других података означених одређеним степеном тајности, осим уколико се не ради о преносу у функцији обављања радног задатка у конкретним предметима;
- коришћење нелиценцираних и неауторизованих рачунарских програма и рачунарске опреме чија употреба није одобрена од стране руководиоца

Рачунаре којима остварују приступ рачунарској мрежи Министарства запослени не смеју давати на коришћење (на услугу, сервисирање и сл.) лицима која за то немају одобрење руководиоца организационе јединице за ИТ.

## **Коришћење електронске поште**

### **Члан 16.**

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

- забрањено је коришћење налога службене електронске поште у приватне сврхе;
- приватни налози електронске поште не смеју се користити у пословне сврхе;
- корисник, без одобрења, не сме да врши слање мејлова целој групи прималаца мејла;
- не смеју се слати подаци о корисничким именима и лозинкама, или други приступни подаци рачунарској опреми и сервисима,
- од корисника електронске поште се очекује да буду учтив и уљудни у комуникацији;
- текст и прилози у мејловима не смеју имати непримерене садржаје;
- за непоштовање правила могуће је покренути дисциплинске мере.

## **Мере безбедности приликом примања електронске поште**

### **Члан 17.**

Службени мејлови и поверљиви документи се не смеју преузимати са бежичних WiFi мрежа на јавним местима, ако немају лозинком заштићен приступ.

У случају примања електронске поште пошиљаоца изван домена „mfin.gov.rs“ запослени је дужан да пажљиво провери назив и тачну мејл адресу пошиљаоца, пре отварања прилога, или клика на линк у мејлу, уколико тачни подаци о пошиљаоцу нису од раније познати.

Електронска пошта са прилозима (документи са екстензијама „exe“, „zip“, „rar“, „doc“ и сл.) не сме се отворати ако долази са сумњивих и непознатих адреса, сви се мора избрисати, или преко мејл адресе admin@mfin.gov.rs проследити организационој јединици за ИТ на проверу.

### **Поступање запослених са поверљивом поштом која је стигла електронским путем**

### **Члан 18.**

Уколико запослено или по другом основу радно ангажовано лице у Министарству, путем електронске поште прими документ који се према пропису којим се уређује тајност података сматра поверљивим документом, такав документ не сме даље да се дистрибуира електронским путем.

У том случају лице је дужно да о поверљивом документу обавести непосредног руководиоца те организационе јединице и овлашћено лице за поступање са поверљивом поштом ради даљег поступања, а све у складу са Уредбом о канцеларијском пословању, Уредбом о начину и поступку означавања тајности података као и Законом о тајности података.

## **Коришћење интернета**

### **Члан 19.**

Корисници рачунарске мреже који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у систем, а сваки рачунар чији се корисник прикључује на интернет мора бити одговарајуће подешен и заштићен

Приликом коришћења интернета треба избегавати сумњиве веб странице, с обзиром да то може проузроковати проблеме - не приметно инсталирање малициозних програма и слично.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави руководиоцу организационе јединице и организационој јединици за ИТ.

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" веб страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

Недозвољена употреба интернета обухвата:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
- коришћење друштвених мрежа и других интернет сервиса забавног садржаја (Фејсбук, Јутјуб, Фоурсквер, Снепчет, Твитер, Инстаграм и сл.);
- регистровање и остављање личних података на онлајн платформама (онлајн трговина, форуми, интернет сервиси, онлајн курсеви и сл.);
- 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);
- преузимање велике количине података које проузрокује “загушење” на мрежи;
- преузимање, пренос и на други начин чињење доступним садржаја заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, спортских догађаја, аудио и видеостреаминг и сл.);
- коришћење сервиса за анонимно претраживање на интернету;
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета;
- размена информација или докумената преко интернет платформи које се користе за делове информација и докумената, без одобрења руководиоца организационе јединице и руководиоца организације јединице за ИТ.

На образложени захтев о којем одлучују руководилац организационе јединице и руководилац организационе јединице за ИТ, запосленом се на радној станици може омогућити коришћење друштвених мрежа и интернет сервиса за објављивање и дељење видео-садржаја уколико су у функцији посла и проактивне комуникације Министарства (Фејсбук, Јутјуб, Твитер, Инстаграм, Линкдин и сл.).

Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже, може се одузети право приступа и могу се дисциплински казнити.

### **Коришћење друштвених мрежа**

#### **Члан 20.**

На друштвеним мрежама није дозвољено објављивање било каквих информација, које се тичу рада Министарства, службених података, фотографија лица, података о личности радно ангажованих и трећих лица.

### **Коришћење преносивог рачунара**

#### **Члан 21.**

Ако радно ангажовано лице задужи преносиви рачунар ради извршења радних задатака ван Министарства, дужан је да се стара о безбедности истог, на начин да неовлашћени приступ и/или крађа буду онемогућени.

Преносиви рачунар се не сме остављати без непосредног надзора. Посебно, не сме се остављати без непосредног присуства:

- у кафићу, ресторану, хотелском јавном простору, оредству јавног превоза, на аеродрому;
- у незакључаној просторији нпр. у хотелској соби, просторијама друге организације и сл.;
- у аутомобилу остављеном на јавном или приватном паркингу.

Забрањено је давати пантон деци и другим члановима породице или трећим лицима на коришћење.

### **Заштита података на преносивом рачунару и мобилном уређају**

#### **Члан 22.**

Документи и подаци који се налазе на преносивом уређају морају бити заштићени од неовлашћеног приступа.

Подаци који су класификовани одређеним степеном тајности, као и лични подаци, морају бити на кодираном (енкриптованом) делу уређаја, са откључавањем са шифром.

Током коришћења преносивог рачунара запослени је дужан да кодира све фајлове који садрже податке о личности или податке означене степеном тајности.

### **Коришћење мобилних телефона**

#### **Члан 23**

Мобилни телефони и таблет рачунари се не могу користити у оквиру рачунарске мреже Министарства.

Запослени могу да за приступ интернету користе бежичну (WiFi) мрежу за госте, издвојену од других информационих ресурса Министарства.

На мобилним телефонима се не смеју чувати поверљиве информације (нпр. лозинке за приступ), слике екрана, или поверљива документа Министарства.

Корисник мобилног телефона или таблет рачунара који има приступ службеној електронској пошти, мора заштити мобилни телефон уз примену следећих мера:

- строго контролу апликација које инсталира на телефон, уз обавезан претходни преглед којим типовима података апликација захтева приступ;
- не смеју да се инсталирају апликације које нису на Листи одобрених апликација за мобилне телефоне, а које захтевају приступ некој од нпр. следећих група података: контакти, документи на телефону, слике, електронска пошта, и др.

Уколико се службени мобилни уређај користи за одређене сервисе Министарства (нпр. Електронску пошту и др), неопходно је:

- да приступ уређају буде заштићен са лозинком;
- да постоји инсталиран и ажуран антивирусни софтвер на мобилном уређају;
- за мобилне уређаје који на себи чувају осетљиве податке, потребно је да поседују могућност обављања кодирања (криптовања) осетљивих података;
- у случају губитка службеног мобилног телефона, одобрава се удаљено брисање података са уређаја.

### **Поступање са преносивим медијима**

#### **Члан 24**

Преносиви медији који обухватају ЦД, ДВД, УСБ флеш меморије, екстерне хард дискове, меморијске картице и друге медијуме, које запослени користе за чување и пренос података насталих у функцији обављања послова за Министарство, дозвољено је користити само уз одобрење непосредног руководиоца

Неопходно је да се примењују следећа правила за чување података на преносивим медијима:

- документа класификована као поверљива, није дозвољено снимати на преносивим медијима, осим у случају одобрења од стране руководиоца;
- у случају снимања поверљивих података, потребно их је додатно обезбедити кодирањем, закључавањем са лозинком и сл;

- пре започињања копирања или отварања фајлова са преносивих медија, неопходно је да се обави анти-вирусна провера складишта података;
- копије података са преносивих медија треба да се сниме на десктоп или лаптоп, како би се онемогућио неповратни губитак података;
- уништавање покретних медија: пре одбацивања медија (ЦД, ДВД и других носача података) потребно је физички уништити носач података (на пример гребанем, бушењем и сл.);
- није дозвољено покретање инсталације апликација са спољних медија. Инсталација је једино дозвољена уз претходно одобрење руководиоца организационе јединице и руководиоца организационе јединице за ИТ;
- запослени може користити само оне преносиве медије којима је задужен од стране непосредног руководиоца;
- уколико запослени изгуби преносиви медиј о томе одмах обавештава руководиоца организационе јединице;
- запослени је дужан да преносиве медије заштити од неовлашћеног приступа и/или крађе, чувањем на сигурном и заштићеном месту.

### **Приватно коришћење услуга облака**

#### **Члан 25.**

Није дозвољено копирање службених и приватних података са рачунара на приватне налоге на облаку за складиштење података (нпр. Dropbox, Google Drive, One Drive и др.).

Такође, није дозвољено слање службених докумената путем јавних сервиса за слање докумената као што је “wetrasfer” и др.

### **Правила празног стола и празног екрана**

#### **Члан 26.**

Ових неколико правила ће Вам омогућити да сачувате поверљиве информације од неовлашћеног приступа или крађе

- немојте остављати ниједан документ са поверљивим садржајем на свом радном столу без надзора, током радног времена или након завршетка радног времена;
- обавезно је да се сва поверљива документа чувају закључана у орману;
- на крају радног времена, поверљива документа се одлажу у орман и закључавају;
- резервни кључ од ормана или касете мора бити под контролом запосленог;
- на десктопу Вашег рачунара не сме да се налазе поверљива документа или документа из чијег назива би могла да се наслути његова садржина;
- приликом удаљавања од рачунара који је укључен, обавезно закључајте екран рачунара;
- забрањено је штампати, без одобрења, документа са ознаком поверљивости или документа за које знате да имају одређен статус поверљивости;
- поверљиве или осетљиве информације се морају правилно уништавати;
- уништите документа од папира и индиго - папира, коришћењем машине за резање папира;
- пријавите одмах сумњиве радње са поверљивим документима или неувобичајене догађаје свом претпостављеном или особи задуженој за безбедност.

## **Размена информација и докумената са клијентима и трећим странама**

### **Члан 27.**

Клијент или трећа страна (физичко или правно лице ангажовано од стране Министарства), мора строго поштовати правила, прописе и обавезе у вези са поверљивошћу које је прописало Министарство:

- Изричито је забрањено да запослени прича, дискутује или открива на било који начин информације у вези са плановима, пројектима, запосленима, клијентима, начинима рада или сличне релевантне податке и поверљиве информације Министарства. Уколико клијент од запосленог затражи да открије такве податке, захтев усмерити на руководиоца;
- Када се процени да клијенту треба дати одређене поверљиве информације, неопходно је да трећа страна потпише Споразум о поверљивости информација и примерак доставити Секретаријату који га одлаже у архиву;
- Забрањено је да клијент користи било какве ресурсе Министарства као што су: десктоп рачунари, лаптоп рачунари, сервери, телефони, електронска пошта, веб услуге или било која друга средства осим оних средстава која су клијенту додељена за рад;
- Није дозвољено да клијент или трећа страна износи било какву врсту штампане документације, информације на УСБ-у или ЦД-у или на било који други начин, а за које се зна да су поверљивог карактера, осим уколико постоји одобрење одговорног руководиоца;
- Свим клијентима који бораве у просторијама Министарства потребно је омогућити слободан приступ интернету преко посебне WiFi мреже за госте. За сва упутства о коришћењу ове мреже контактирати организациону јединицу за ИТ;
- Клијент не сме боравити сам у просторијама Министарства;
- Забрањено је копирати писану кореспонденцију, директоријуме или инструкције лицима изван Министарства, осим ако за то имате одобрење непосредног руководиоца;
- Ако су запосленом потребне додатне информације у вези са испуњавањем ових захтева, обратите се особи задуженој за информациону безбедност или непосредном руководиоцу;
- Уколико постоје било какви проблеми везани за непоштовање горе наведених правила, запослени мора одмах обавестити особу задужену за информациону безбедност.

### **Захтеви за интервенције и инциденти**

### **Члан 28.**

У случајевима када постоји потреба за хитним интервенцијама запослених из организационе јединице за ИТ, запослени у Министарству је у обавези да путем електронске поште контактира организациону јединицу за ИТ на адресу [itpodrska@mfin.gov.rs](mailto:itpodrska@mfin.gov.rs), и да је обавести о проблему са којим се сусрео у раду користећи рачунарску опрему. Само у случају да је дошло до прекида рада рачунарске мреже или да постоји проблем са мејлом, дозвољено је контактирати организациону јединицу за ИТ путем телефона.

Након поштања у рад апликативног решења, сви захтеви за интервенцијама и обавештења о инцидентима упућених организационој јединици за ИТ, биће креирани преко апликације, која ће бити доступна на интранет порталу Министарства.

У случају оштећења или губитка рачунарске опреме са којом је задужено (десктоп рачунар, лаптоп, таблет, мобилни телефон, смарт картица, УСБ меморија и сл.) или проблема са коришћењем сервиса на рачунаrescoј мрежи Министарства, радно ангажовано лице је о томе дужно одмах да обавести организациону јединицу за ИТ.

## **Обавеза потписивања изјаве радно ангажованог лица**

### **Члан 29.**

Након примопредаје рачунарске опреме и добијања дефинисаног права приступа инсталираним сервисима на рачунарској мрежи Министарства, запослени својеручно потписује Изјаву о правилном коришћењу информационе имовине, чији су изглед и садржај део ове Директиве и других директива које се односе на заштиту информација.

Образац се попуњава у 3 (три) примерка од којих један запослени задржава за себе, други се улаже у његов персонални досије, док се трећи чува у евиденцији организационе јединице за ИГ.

Својеручно датим потписом на обрасцу Изјаве запослени потврђује тачност унетих података и чињеницу да је прочитао и разумео садржину дате Директиве.

### **Прелазне и завршне одредбе**

### **Члан 30.**

Ступањем на снагу ове Директиве, престају да важе и да се примењују: Директива о конфигурацији опреме, дељеним фолдерима и антивирусној заштити, задужењу, коришћењу, раздужењу и вођењу евиденције о рачунарској опреми број: 030-03-30/2018 од 6. новембра 2018. године.

### **Члан 31.**

Ова Директива ступа на снагу наредног дана од дана издавања.

**МИНИСТАРСТВО ФИНАНСИЈА**

**Број: 030-01-00019/2020-08**

**Београд, 09. јун 2020. године**

**МИНИСТАР**

**Синиша Мали**



