



Република Србија
МИНИСТАРСТВО КУЛТУРЕ И
ИНФОРМИСАЊА

Број: 110-00-16/2020-07
Датум: 13.03.2020. године
Влајковићева 3
Београд

ПРАВИЛНИК

о начин употребе рачунарско-комуникационих ресурса у Министарству културе и информисања

Предмет

Члан 1.

Овим правилником се прописује начин употребе рачунарско-комуникационих ресурса на мрежи органа државне управе (мрежа), коју користи Министарство културе и информисања.

Примена

Члан 2.

Правилник се примењује на све запослене (кориснике) у државном органу којима је омогућен приступ мрежи.

Изрази – значење

Члан 3.

Изрази и њихово значење у правилнику:

1. **Рачунарско-комуникациони ресурси** су рачунари, рачунарска опрема, мрежна опрема и сервиси на мрежи;
2. **Корисничко име** представља име корисника које је јединствено у систему;

3. **Лозинка** представља шифру коју одређује корисник;
4. **Кориснички налог** омогућава приступ ресурсима и сервисима мреже путем корисничког имена и лозинке;
5. **Администратор** је овлашћено техничко лице које пружа техничку подршку у вези корисничких налога на мрежи;
6. **Интернет** је јавно доступна глобална мрежа за пренос података која заједно повезује рачунаре и рачунарске мреже коришћењем интернет протокола (IP-Internet protocol);
7. **Антивирусна заштита** је рачунарски програм који се користи за спречавање, откривање и уклањање злонамерног софтвера (програма);
8. **Електронска пошта** је начин службене комуникације и представља сервис који омогућава слање и примање порука електронским путем;
9. **Меил клиент (mail client)** представља програм за коришћење електронске поште.

Рачунарско – комуникациони ресурси

Члан 4.

Рачунарско – комуникациони ресурси на мрежи обухватају:

1. Рачунаре и рачунарску опрему (радне станице, преносне рачунаре, сервере, штампаче, скенере, мрежно комуникациону опрему и тд).
2. Сервиси на мрежи: систем за управљање корисничким налозима, употреба интернета, електронска пошта на домену мреже и ван мреже, антивирусна заштита.

Заштита рачунара и рачунарске опреме

Члан 5.

Неопходни кораци које корисник мора да испуни како би спречио злоупотребу података на рачунарима и рачунарској опреми:

1. Заштити рачунар лозинком (одјављивањем са корисничког налога) када се не користи или када корисник није у канцеларији;
2. Онемогући приступ рачунару и рачунарској опреми неовлашћеним лицима;
3. Обезбедити све предуслове како не би дошло до физичког оштећења рачунара и рачунарске опреме (Влага, сметње у електричном напајању, утицај температуре и слично);
4. Пријава свих сазнања о могућој злоупотреби приступа рачунара и рачунарској опреми.

Члан 6.

Рачунар мора бити конфигуриран на прописан начин како би испуњавао минималне услове неопходне за његово функционисање. А то су:

1. Инсталиран оперативни систем;
2. Учлањен на домен;
3. Додељивање одговарајућег корисничког имена;
4. Инсталиран доступан Office пакет;
5. Активан и ажуриран антивирусни програм;
6. Инсталиран програм за читање ПДФ (PDF) фајлова;
7. Конфигурисана мрежна картица неопходним параметрима како би се омогућио приступ интернету, изузев у случају где рачунар не сме бити повезан на интернет из сигурности разлога.

Сви програми који се инсталирају на рачунарима и рачунарској опреми морају бити лиценцирани.

Корисник не може вршити самоиницијативно инсталирање програма или мењање конфигурације рачунара.

Чување, управљање и безбедност дигитализоване грађе

Члан 7.

Министарство културе и информисања за потребе чувања података насталих дигитализацијом културног наслеђа и савременог стваралаштва и управљања дигитализоване грађе у промотивне и едукативне сврхе има сопствене ресурсе у виду серверске платформе.

У циљу испуњавања стандарда и обезбеђивања услова за смештај рачунарско-комуникационе опреме и препоруке о њиховој примени, ресурси могу бити смештени и изван просторија Министарства културе и информисања.

О безбедности сета података, приступу базама и функционисању апликација Министарство културе и информисања се стара у сарадњи са државним органом надлежан за те послове: Академска мрежа Републике Србије (АМРЕС) и Канцеларија за информационе технологије и електронску управу.

Администратор система намењеног чувању, управљању и безбедности дигитализоване грађе

Члан 8.

Администратор система из члана 7 намењеног чувању, управљању и безбедности дигитализоване грађе је особа из сектора у чијој је надлежности дигитализација културног наслеђа и савременог стваралаштва и која обезбеђује функционалност свих рачунарских система и сервиса. Остале дужности могу укључити управљање пројектима, надзор и обуку корисника и помоћ у решавању

проблема у свакодневном функционисању а све у циљу обезбеђења максималне поузданости и доступности система општим корисницима.

Коришћење приватних преносних меморија (усб, цд и др.)

Члан 9.

Корисницима није дозвољено коришћење приватних преносних меморија на рачунарима и другим уређајима у Министарству.

Корисницима је дозвољено коришћење приватних преносних меморија под условом да је претходно извршена провера од стране администратора органа.

Запослени који на преносној меморији преносе податке из Министарства морају за то имати сагласност Руководиоца органа или од лица које он овласти.

Коришћење корисничког налога

Члан 10.

Отварање, укидање, ажурирање или привремено уклањање корисничког налога на домену врши администратор.

Преко корисничког налога корисник врши идентификацију (преко корисничког имена и лозинке) и приступа мрежи.

Корисник од овлашћеног администратора добија податке о корисничком имену и лозинки, преко којег се врши активација налога, након чека је корисник дужан да промени лозинку.

Корисник је одговоран за све активности на мрежи које се врше употребом његовог корисничког налога.

Корисник употребљава кориснички налог искључиво у пословне сврхе, на начин утврђен радним задацима и пријављује све уочене неправилности или злоупотребе корисничког налога од стране другог лица.

Ограничења приликом употребе корисничког налога

Члан 11.

Корисник не може да:

1. Користи туђи кориснички налог;

2. Саопштава податке о свом корисничком налогу другом лицу;
3. Користи мрежне ресурсе на начин који није одобрен од стране Руководиоца органа;
4. Злоупотребљава кориснички налог на начин којим би се угрозила тајност података на мрежи.

Заштита лозинке

Члан 12.

Како би се заштитила лозинка неопходно је да:

1. Се иницијална лозинка мења приликом првог пријављивања;
2. Лозинка која се користи на корисничком налогу не сме се користити и у приватне сврхе;
3. Се лозинка не саопштава другом лицу;
4. Уколико постоји сумња да је лозинка угрожена, неопходно је да се лозинка промени и да се случај пријави администратору;
5. Се врши промена лозинке на сваких 60 дана;
6. Не треба користити опцију „ЗАПАМТИ ЛОЗИНКУ“ ;
7. Се лозинка не пише на месту које је доступно другим лицима;
8. Уз одобрење Руководиоца органа лозинка се може чувати на безбедном месту којем могу да приступе само овлашћена лица.

Антивирусна заштита корисника

Члан 13.

Корисник треба да:

1. Има инсталиран и активан антивирусни програм;
2. Периодично врши скенирање фајлова успомоћ антивирусног програма;
3. Пријави неадекватно функционисање антивирусног програма или сумњу на постојање вируса на рачунару корисника.

Корисник не сме самоиницијативно брисати или мењати конфигурацију антивирусног програма.

Приступ интернету

Члан 14.

Приступ интернету је дозвољен ради обављања пословних активности изизев у случају ако Руководилац органа није другачије одлучио.

Недозвољена употреба интернета

Члан 15.

Недозвољена употреба интернета обухвата:

1. Нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
2. Намерно ширење програма који могу да наруше сигурност на интернету (вируси, малициозни програми и др.)
3. Преузимање података велике „тежине“ који проузрокују „загушење на мрежи“;
4. Преузимање материјала заштићених ауторским правима;
5. Коришћење интернета у приватне сврхе.

Корисници који неадекватним коришћењем доведу до загушења протока, прекида у раду или нарушавање безбедности мреже може се ограничити право приступа.

Употреба електронске поште

Члан 16.

Сервис електронске поште доступан је путем посебних програма (mail client) који су инсталирани и конфигурисани на рачунарима.

Сервис електронске поште је доступан и путем интернет адресе <https://mail.gov.rs> путем корисничког имена и лозинке.

Употребом доменског налога се аутоматски омогућује приступ сервису електронске поште тог корисничког налога.

Сервис електронске поште обезбеђује примање/слање електронских порука, дељење именика, календара, антивирусну заштиту и архивирање електронске поште.

Неопходни кораци које корисник треба преузети ради ефикасније употребе електронске поште:

1. Због ограничене величине поштанског сандучета неопходно је вршити редовно архивирање електронских порука;
2. Редовно брисање непотребне поште;
3. Обезбеђује да садржај поруке буде у складу са препорукама пословне комуникације.

Ограничења приликом употребе електронске поште

Члан 17.

Недозвољена употреба електронске поште обухвата:

1. Креирање или прослеђивање ланчаних мејлова, као и слање нежељених масовних порука без икаквог критеријума;
2. Коришћење службеног мејла у приватне сврхе, рекламирање производа и узнемиравање других запослених.

Корисник који злоупотребљава приступ мрежи и ресурсима мреже, право приступа ће бити укинута и биће обавештен Руководилац органа.

Употреба рачунарско – комуникационих ресурса

Члан 18.

Корисник треба да употребљава рачунарско – комуникационе ресурсе савесно и одговорно, искључиво у пословне сврхе да не би угрозио безбедност функционисања мреже.

Корисник треба да обавести администратора и Руководиоца органа ако има информацију о злоупотреби рачунарско – комуникационих ресурса од стране других лица.

Уништавање података и опреме

Члан 19.

Отписана опрема (Е-отпад) се враћа Управи за заједничке послове републичких органа ради уништавања опреме и података.

У случају када се Е-отпад не враћа Управи за заједничке послове републичких органа, управљање отпадом у оквиру сакупљања, транспорта, складиштење, третмана и одлагања отпада врши се у складу са прописима који регулишу ову област.


МИНИСТАР
Владан Вукосављевић