На основу члана 7. став 4. Закона о информационој безбедности („Службени гласник РС”, број 6/16) и члана 42. став 1. Закона о Влади („Службени гласник РС”, бр. 55/05, 71/05 – исправка, 101/07, 65/08, 16/11, 68/12 – УС, 72/12, 7/14 – УС и 44/14),

Влада доноси

УРЕДБУ

о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја

"Службени гласник РС", број 94 од 24. новембра 2016.

Предмет Уредбе

Члан 1.

Овом уредбом ближе се уређују мере заштите информационо-комуникационих система од посебног значаја (у даљем тексту: мере заштите).

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја

Члан 2.

Оператор ИКТ система од посебног значаја (у даљем тексту: оператор ИКТ система) је дужан да, у оквиру организационе структуре, у складу са природом, обимом и сложеношћу пословања утврди послове и одговорности запослених у циљу управљања информационом безбедношћу.

Оператор ИКТ система утврђује, у оквиру организационе структуре, послове и одговорности запослених за заштиту информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност, за управљање ризицима у области информационе безбедности, као и за послове предвиђене процедурама у области информационе безбедности.

Подела одговорности запослених треба да се изврши тако да се онемогући неовлашћена или ненамерна измена, оштећење или злоупотреба средстава, односно информационих добара оператора ИКТ система, као и да се онемогући приступ, измена или коришћење средстава без овлашћења и без евиденције о томе.

Оператор ИКТ система успоставља процедуре ради праћења активности, ревизије и надзора у оквиру управљања информационом безбедношћу.

Приликом утврђивања одговорности запослених потребно је предвидети и одговорност за обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

Оператор ИКТ система утврђује процедуре комуникације са другим институцијама у случају инцидента у циљу благовремене пријаве, односно решавања насталог безбедоносног инцидента.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 3.

Оператор ИКТ система који у свом систему дозвољава рад на даљину и употребу мобилних уређаја дужан је да успостави и одржава безбедност рада на даљину и употребе мобилних уређаја, узимајући у обзир ризике који могу постојати услед неадекватног коришћења мобилних уређаја.

Оператор ИКТ система је дужан да дефинише услове и ограничења за рад на даљину тако да се не угрози безбедност ИКТ система, при чему оператор ИКТ система узима у обзир физичку безбедност места и окружења са кога се обавља рад на даљину, услове за безбедност комуникације између ИКТ система оператора и места са којег се ради на даљину, превенцију или свођење на неопходни минимум обраде и чувања информација на личном уређају лица које ради на даљину, превенцију од неовлашћеног приступа, услове за коришћење локалне мреже и бежичних мрежних сервиса, захтеве за заштиту од злонамерних софтвера и друге мере које су потребне за безбедност рада на даљину.

Приликом коришћења мобилних уређаја мора да се обезбеди заштита података од интереса за оператора ИКТ система и смање ризици коришћења мобилних уређаја у незаштићеним окружењима (јавним местима, мрежама са непознатом или недовољном заштитом и слично), при чему оператор ИКТ система узима у обзир следеће:

1) евиденцију мобилних уређаја;

2) мере физичке заштите мобилних уређаја (од уништења, оштећења, губитка или неовлашћеног приступа уређајима и подацима од интереса за оператора ИКТ система);

3) ограничења за инсталацију и ажурирање софтвера;

4) инсталацију адекватних софтвера за мобилне уређаје и њихово редовно ажурирање;

5) ограничење коришћења услуга информационог друштва које би угрозиле информациону безбедност ИКТ система;

6) контроле приступа мобилном уређају и подацима на њему;

7) криптографске технике;

8) заштиту од вируса и других злонамерних софтвера;

9) даљинско управљање мобилним уређајем у случају инцидента, од стране овлашћеног лица оператора ИКТ система, путем којег је могуће да се изврши неповратно брисање података и онемогућавање даљег коришћења уређаја;

10) успостављање и одржавање резервне копије (backup) података;

11) омогућавање безбедног коришћења интернет сервиса и апликација.

Ако оператор ИКТ система дозвољава у свом систему коришћење приватних мобилних уређаја дужан је да обезбеди услове из става 3. овог члана и предузме мере ради раздвајања приватног од пословног коришћења ових уређаја.

Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност

Члан 4.

Лица која управљају ИКТ системом односно запослена лица која користе ИКТ систем морају да имају адекватан ниво образовања и способности, свест о значају послова које обављају и њихове одговорности која се утврђује уговором и другим актима.

Како би лица која користе ИКТ систем односно управљају ИКТ системом разумели своје одговорности, оператор ИКТ система обучава запослене о важности информационе безбедности ИКТ система, мерама и процедурама за заштиту ИКТ система и њиховим обавезама.

Оператор ИКТ система је дужан да покрене одговарајући поступак против лица одговорних за нарушавање безбедности информационог система.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Члан 5.

Оператор ИКТ система је дужан да уговором или другим актом обавеже запослена и по другим основама ангажована лица да након престанка или промене радног ангажовања не откривa поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система. Дужности и обавезе које остају важеће и после престанка ангажовања треба да буду садржане у условима уговора са запосленим односно по другом основу ангажованим лицем.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 6.

Оператор ИКТ система је дужан да идентификује и класификује информациона добра, односно средства и имовину, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, изврши попис информационих добара, односно средстава и имовине, и успостави, одржава и редовно ажурира њихову евиденцију.

Оператор ИКТ система је дужан да класификацију из става 1. овог члана врши према степену осетљивости и критичности, узимајући у обзир могуће последице нарушавања поверљивости, интегритета и расположивости добара, да доследно примењује ту класификацију, као и да, у складу с тим, обезбеди адекватан ниво заштите ових добара.

За свако информационо добро, односно средство и имовину, потребно је одредити задужено лице за њихову заштиту.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности

Члан 7.

Оператор ИКТ система одређује шему класификације података према којој се подаци класификују узимајући у обзир осетљивост, важност података, штету која може да настане услед неовлашћеног откривања, измене или брисање података и прописе који уређују питања заштите података (о тајним подацима, пословној тајни, подацима о личности и сл.).

Оператор ИКТ система у обавези је да дефинише одговарајући скуп процедура за поступање, обраду, складиштење и преношење података у складу са шемом класификације података из става 1. овог члана.

Мере заштите података који су, у складу са законом који уређује област тајности података, означени као тајни, одређују се у складу са прописима који регулишу ову област.

Избор и ниво примене мера заштите података се заснива на процени ризика, потреби за превенцијом ризика и отклањању последица ризика који се остварио, укључујући све врсте ванредних околности.

Заштита носача података

Члан 8.

Оператор ИКТ система дужан је да обезбеди спречавање неовлашћеног разоткривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података, тако што утврђује и примењује процедуре за управљање носачима података у складу са класификацијом из члана 7. ове уредбе.

Приликом дефинисања процедура и поступања са носачима података, треба предвидети неповратно брисање података, у случају када су истекли рокови за њихово чување и када они више нису потребни, поступак одобравања

изношења носача података из просторија оператора ИКТ система, чување носача података на безбедном месту, коришћење криптографских техника за заштиту података када је то предвиђено прописима, односно у другим случајевима када је таква врста заштите потребна, обезбеђивање сигурног преноса података на нови носач података, чување резервних копија на одвојеним носачима података и друге мере и поступке за заштиту носача података.

Оператор ИКТ система треба да предвиди процедуре за безбедно расходовање и уништавање носача података када више нису потребни, а које треба да на минимум сведу ризик од приступа подацима од стране неовлашћених лица.

Носачи података треба да буду заштићени од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта, обезбеђивањем поузданог транспорта и поузданих особа које преносе носаче података и обезбеђивањем адекватне амбалаже у циљу физичке заштите приликом транспорта.

Оператор ИКТ система одређује за које податке, у складу са шемом класификације података, треба водити евиденцију о коришћењу носача података и предузетим поступцима у вези са заштитом података и носача података.

Ограничење приступа подацима и средствима за обраду података

Члан 9.

Ограничење приступа подацима и средствима за обраду података подразумева дефинисање прецизних правила приступа, тако што се дефинише ко има право чему да приступи и која су ограничења приступа подацима и средствима за обраду података, а водећи рачуна о специфичностима података и опреме и одговорностима и радним задужењима лица која приступају подацима и опреми.

Ограничење приступа подразумева хардверско, односно софтверско ограничење приступа подацима и средствима за обраду података, укључујући и физичко ограничење приступа подацима и средствима.

Ограничење приступа врши се у складу са класификацијом података из члана 7. ове уредбе.

Оператор ИКТ система треба да обезбеди приступ мрежи и мрежним услугама само лицима која имају овлашћења за коришћење.

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Члан 10.

Оператор ИКТ система је у обавези да предвиди процедуру за одобравање и укидање овлашћеног приступа ИКТ систему и услугама које ИКТ систем

пружа, тако што предвиђа услове за одобравање и укидање овлашћеног приступа, проверу адекватности одобреног нивоа приступа и доделу јединствене идентификационе ознаке лицу којем се одобрава приступ.

Оператор ИКТ система води евиденцију о додељеним и одузетим ознакама, утврђује услове за коришћење заједничке идентификационе ознаке у случајевима када је то неопходно, дефинише начин и услове онемогућавања и уклањања јединствених идентификационих ознака, као и услове за доделу и коришћење администраторских права.

Лицима којима се одобрава овлашћени приступ омогућује се приступ на основу података за аутентикацију (лозинке, криптографски кључеви, подаци складиштени на токенима и сл.).

Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана.

Оператор ИКТ система дужан је да обезбеди механизам за укидање права приступа у случајевима промене радног места, престанка радног односа и, по потреби, у другим случајевима.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 11.

Оператор ИКТ система прописује начин аутентикације лица коме је одобрен приступ систему, односно корисника.

Лице коме се одобрава овлашћени приступ, односно корисник, мора да се обавеже да неће откривати своје податке за аутентикацију.

Оператор ИКТ система предвиђа начине креирања и чувања података за аутентикацију који обезбеђују висок ниво безбедности и заштите од откривања од стране других лица.

Оператор ИКТ система предвиђа обавезу промене података за аутентикацију у случају да су подаци откривени, или је повећана опасност од њиховог откривања.

Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Члан 12.

Ради заштите тајности, аутентичности и интегритета података, оператор ИКТ система треба да размотри коришћење одговарајућих мера криптозаштите, узимајући у обзир осетљивост информација које треба да се штите, пословне процесе који се спроводе, ниво захтеване заштите, имплементацију примењених криптографских техника и управљање криптографским кључевима.

Управљање криптографским кључевима обухвата њихов целокупан животни циклус, укључујући генерисање, складиштење, архивирање, преузимање, расподелу, повлачење и уништавање кључева.

Оператор ИКТ система треба да посебно води рачуна о заштити средстава криптозаштите од свих облика компромитације.

Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему

Члан 13.

Оператор ИКТ система дужан је да спречи неовлашћен физички приступ објектима, просторима, просторијама односно безбедносним зонама у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему.

У случају када посебним прописима није предвиђена обавеза успостављања безбедносних зона, оператор ИКТ система може да предвиди мере физичко-техничке заштите просторија у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему, као што су уградња алармних уређаја, контрола уласка уз обавезно ношење видљиве идентификације за све време боравка и друге којима се обезбеђује физичко-техничка заштита.

Оператор ИКТ система дужан је да предвиди и примени мере физичке заштите у случају елементарних непогода, злонамерних напада, несрећа или намерног уништавања објеката, просторија, средстава и докумената ИКТ система.

Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем

Члан 14.

Оператор ИКТ система дужан је да заштити средства која чине ИКТ систем од губитка, оштећења, крађе или другог облика угрожавања безбедности.

У циљу заштите средстава, оператор ИКТ система мора да води рачуна о постављању средстава на безбедна места, елиминише непотребан приступ у простор у коме се налазе, врши редовне провере заштићености средстава од крађа, пожара, електромагнетних зрачења и других претњи и прати услове околине (температуру, влажност и др.) који би могли негативно да утичу на рад средстава.

Средства треба да буду заштићена у случају поремећаја у дистрибуцији електричне енергије, телекомуникационих капацитета, воде, гаса, вентилације обезбеђивањем алтернативних решења која омогућују наставак рада ИКТ система.

Измештање имовине ИКТ система може да се врши само уз претходно одобрење овлашћеног лица, уз примену безбедносних механизама,

узимајући у обзир различите ризике приликом рада изван просторија организације.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 15.

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, оператор ИКТ система дефинише процедуре за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевима измештања делова ИКТ система.

Оператор ИКТ система успоставља процедуре за поступање у случају промена у организацији, пословним процесима, средствима за обраду информација и на системима које имају утицај на безбедност информација и предвиђа одговорности за спровођење дефинисаних процедура.

Оператор ИКТ система континуирано надзире и проверава функционисање средстава за обраду података и предвиђа будуће промене које могу утицати на безбедност ИКТ система и, у складу са тим, планира одговарајуће мере.

Оператор ИКТ система мора међусобно раздвојити окружења за развој, тестирање и оперативан рад да би се смањили ризици од неовлашћеног приступа или промена у радном окружењу.

Заштита података и средства за обраду података од злонамерног софтвера

Члан 16.

Заштита података и средстава за обраду података треба да обухвати мере за откривање злонамерног софтвера и за отклањање штете од злонамерног софтвера, укључујући одговарајуће контроле приступа систему, спречавање уношења и извршавања злонамерних софтвера, спречавање приступања ризичним веб сајтовима, континуирано ажурирање софтвера за откривање злонамерних софтвера, управљање рањивостима и проверама ИКТ система, имплементацију процедура као и подизање свести о ризицима од последица деловања злонамерног софтвера.

Заштита од губитка података

Члан 17.

Заштита од губитка података постиже се редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за израду резервних копија.

Оператор ИКТ система дефинише време чувања и заштите резервних копија, обим и учесталост резервних копија, безбедно место чувања резервних копија, обезбеђује физичку заштиту резервних копија и заштиту од спољашњих утицаја, проверава носаче података како би се осигурало њихово исправно функционисање и поузданост у складу са планом израде резервних копија.

Оператор ИКТ система врши израду резервних копија које треба да обухвате све системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Члан 18.

Оператор ИКТ система треба да обезбеди да се у ИКТ систему формирају записи о догађајима (логови) у вези активности корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати.

Средства за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене.

У оквиру ИКТ система записују се активности администратора и корисника и редовно преиспитују у циљу заштите.

У циљу обезбеђивања поузданости записа, времена у свим подсистемима ИКТ система морају бити синхронизована међусобно, као и са референтним тачним временом.

Обезбеђивање интегритета софтвера и оперативних система

Члан 19.

Оператор ИКТ система предвиђа и спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, ажурирање софтвера и оперативних система од стране овлашћеног администратора, односно овлашћеног лица, примена система за контролу конфигурације софтвера, успостављање могућности повратка на претходно стање пре имплементације промена у систему, чување претходних верзија софтвера у случају неочекиваних ситуација и друге мере у циљу смањења ризика од оштећења софтвера и оперативних система.

Заштита од злоупотребе безбедносних слабости ИКТ система

Члан 20.

У циљу заштите ИКТ система од злоупотребе безбедносних слабости, оператор ИКТ система врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и, у

складу са тим, предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену других врста заштите ИКТ система.

Оператор ИКТ система онемогућава неодобрено инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедносним слабостима.

Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Члан 21.

Приликом спровођења ревизије ИКТ система, оператор ИКТ система мора да обезбеди да ревизија има што мањи утицај на функционисање система, тако што планира адекватно време спровођења ревизије и редослед активности који не ометају пословне процесе оператора ИКТ система.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 22.

У циљу заштите података у комуникационим мрежама, уређајима и водовима врши се њихова контрола и заштита од неовлашћеног приступа, при чему се предвиђа успостављање процедура и одговорности за управљање мрежном опремом, одговорност за рад мреже, посебне контроле за заштиту поверљивости и интегритета података који пролазе путем јавних или бежичних мрежа.

Оператор ИКТ система редовно проверава да ли постоји адекватна безбедност мрежних сервиса.

Оператор ИКТ система, у циљу посебне заштите појединих ИКТ сервиса, може извршити сегментирање мреже у циљу изолације ових сервиса и ограничити приступ само овлашћеним лицима.

Каблови за напајање и комуникациони каблови који преносе податке или који представљају подршку информационим услугама треба да буду заштићени од прислушкивања, крађе, ометања или оштећења.

Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система

Члан 23.

Заштита података који се преносе комуникационим средствима унутар оператора ИКТ система, између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се успостављањем процедура и адекватних контрола.

Процедурама се предвиђа заштита од прислушкивања, модификовања, погрешног усмеравања и уништења података, откривање и заштита од

злонамерног софтвера, евентуално коришћење криптографских техника и друге адекватне мере.

Када се пренос података врши између оператора ИКТ система и лица ван оператора ИКТ система, могу се закључити споразуми о преносу података и споразуми о поверљивости или неоткривању који садрже одредбе о безбедности преноса података.

У случају из става 3. овог члана, за пренос података о личности потребно је испунити услове предвиђене законом којим се уређује заштита податка о личности.

Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 24.

Захтеви за информациону безбедност морају да се испуне у свим фазама животног циклуса ИКТ система односно делова система, што подразумева фазу пројектовања ИКТ система, успостављања новог или мењање постојећег ИКТ система, односно делова система, и набавку производа потребних за функционисање ИКТ система.

Успостављање новог ИКТ система, односно мењање постојећег, обухвата спровођење процедуре документовања, дефинисања захтева за информациону безбедност, проверу испуњености захтева, контролисање и управљање поступка увођења новог, односно мењања постојећег ИКТ система.

Захтеви за информациону безбедност морају да се испуне и када се врши пренос информација путем јавних комуникационих мрежа и користе апликативне услуге путем јавних комуникационих мрежа.

Приликом поверавања активности у вези са ИКТ системом трећим лицима, потребно је да оператор ИКТ система надгледа и прати активности развоја ИКТ система.

Заштита података који се користе за потребе тестирања ИКТ система односно делова система

Члан 25.

За потребе тестирања ИКТ система односно делова система оператор ИКТ система користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

Ако се за потребе тестирања користе поверљиве информације, односно лични подаци, потребно их је употребљавати и штитити у складу са прописима и овлашћењима.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 26.

Оператор ИКТ система у својим процедурама предвиђа ниво доступности и врсту информација и средства којима могу да приступе пружаоци услуга, начине приступа информацијама и средствима и надзор над приступом.

Оператор ИКТ система треба да идентификује и успостави процедуре безбедности информација које се конкретно баве приступом информацијама пружаоца услуга унутар организације.

Обавезе пружаоца услуга у вези са информацијама и средствима која су доступна пружаоцима услуга оператора ИКТ система регулишу се споразумом између оператора ИКТ система и пружаоца услуга, чијим одредбама се обезбеђује адекватан ниво заштите информација и средстава, у складу са прописима и техничким стандардима.

Оператор ИКТ система дужан је да обезбеди да пружалац услуга обавља поверене активности у складу са актом о безбедности ИКТ система, односно другим актима којима се уређује безбедност његовог информационог система.

Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга

Члан 27.

У циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, оператор ИКТ система успоставља механизме надзора над пружањем услуга, именује лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности, применом одговарајућих процедура и успоставом надзора.

Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама

Члан 28.

Оператор ИКТ система у обавези је да утврди процедуре којима се дефинишу одговорна лица задужена за превенцију и реаговање, план поступања у случају опасности од настанка безбедносних инцидената или настанка безбедносних инцидената, обавезу вођења евиденције о предузетим активностима, обавезу извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.

Оператор ИКТ система треба да обавеже све запослене и пружаоце услуга да одговорном лицу из става 1. овог члана без одлагања пријављују безбедносне слабости, претње и инциденте у ИКТ систему.

Оператор ИКТ система је у обавези да одреди одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности.

Оператор ИКТ система треба да дефинише и примењује процедуре које требају да обезбеде процесе за идентификацију, прикупљање и чување информација које могу да послуже као доказ ради покретања дисциплинског, прекршајног или кривичног поступка.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 29.

Оператор ИКТ система треба да предвиди мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, дефинисање одговорности, планова, поступака у случају ванредних догађаја и процедура за опоравак ИКТ система, у оквиру редовних процедура за одржавање информационе безбедности или доношењем посебних процедура.

Оператор ИКТ система треба да успостави, документује, имплементира и одржава процесе, процедуре и контроле да би осигурао захтевани ниво континуитета пословања током ванредне ситуације.

Оператор ИКТ система треба да верификује успостављене и имплементиране контроле континуитета пословања у редовним условима рада, како би оне биле важеће и ефективне током ванредне ситуације.

Оператор ИКТ система треба да идентификује захтеве за доступност ИКТ система. Редундантне компоненте треба размотрити онда када се доступност не може гарантовати коришћењем постојећих архитектура система.

Завршна одредба

Члан 30.

Ова уредба ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

05 број 110-9472/2016-1

У Београду, 17. новембра 2016. године

Влада

Председник,

Александар Вучић, с.р.