На основу члана 4. став 2. Закона о информационој безбједности („Службени гласник Републике Српске“, број 70/11) и члана 43. став 2. Закона о Влади Републике Српске („Службени гласник Републике Српске“, број 118/08), Влада Републике Српске, на 82 сједници, одржаној 20.09.2012. године, донијела је

УРЕДБУ
О МЈЕРАМА ИНФОРМАЦИОНЕ БЕЗБЈЕДНОСТИ

I - ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овом уредбом утврђују се мјере информационе безбједности којима се обезбјеђује основна заштита података на физичком, техничком и организационом нивоу.

Члан 2.

Мјере из члана 1. ове уредбе односе се на републичке органе, органе јединица локалне самоуправе, правна лица која врше јавна овлашћења (у даљем тексту: органи) и друга правна и физичка лица која остварују приступ или поступају са подацима у електронском облику републичких органа, органа јединица локалне самоуправе и правних лица која врше јавна овлашћења.

Члан 3.

Поједини изрази који се користе у овој уредби имају сљедеће значење:

а) хардвер - физичка компонента информационог система,

б) криптографска заштита - систем заштите података и информационих система који осигурава сигуран пренос података кроз рачунарску и телекомуникациону мрежу,

в) информатички медиј - сваки медиј на којем је могуће преносити или складиштити податке у електронском облику,

г) безбједно складиште - сеф, каса или други простор за складиштење података опремљен уређајем који спрјечава неовлашћени приступ ускладиштеним подацима,

д) софтвер - сваки оперативни систем, програм, корисничка и сервисна апликација,

ђ) ризик - потенцијални узрок који може нанијети штету податку или информационом систему у којем се користе подаци,

е) безбједна локација - мјесто за чување података складиштених на информатичком медију у или изван радних просторија органа, правног или физичког лица из члана 2. ове уредбе, опремљен техничким уређајима, којима се спрјечава неовлашћени приступ уређајима и подацима,

ж) административна зона - простор или просторија у објекту у којем се чувају подаци и уређаји на којима су смјештени подаци и који захтијева одговарајућу физичку заштиту,

з) криптована заштита података - примјена програмских рјешења или уређаја за заштиту података који осигуравају повјерљивост, цјеловитости и доступност података.

II - ФИЗИЧКА ЗАШТИТА

Члан 4.

Мјере информационе безбједности физичке заштите су:

а) успостављање административне зоне,
б) израда плана физичке заштите,
в) процјена ефикасности мјера физичке заштите,
г) контрола лица,
д) складиштење података,
ђ) физичка заштита информационих система.

Члан 5.

(1) Мјере информационе безбједности физичке заштите спроводе се ради спрјечавања неовлашћеног или насилног уласка лица у објекте и просторије у којима се налазе подаци односно уређаји са подацима, спрјечавања и откривања злоупотреба података од стране запослених као и откривања и реаговања на ризике.

(2) Мјере информационе безбједности физичке заштите одређују се зависно од врсте, броја, облика и начина складиштења података, овлашћења за приступ подацима, као и безбједносне процјене могућих ризика.

Члан 6.

Административна зона се успоставља за коришћење података у контролисаном, видљиво означеном простору унутар којег је могуће контролисати приступ лица.

Члан 7.

(1) Органи, правна и физичка лица из члана 2. ове уредбе, за објекат или простор у којем имају приступ, односно поступају са подацима, израђују план физичке заштите којим се утврђује потреба спровођења мјера физичке заштите, у складу са стандардима информационе безбједности.

(2) Органи, правна и физичка лица из члана 2. ове уредбе, најмање једном годишње, процјењују ефикасност мјера информационе безбједности физичке заштите објеката и просторија у којима се налазе подаци, као и кад дође до промјене намјене локације или елемената у информационом систему.

(3) Органи, правна и физичка лица из члана 2. ове уредбе, дужни су да спроводе контролу лица на улазима и излазима из објекта или простора у којима се налазе подаци и о томе воде евиденцију, ради спрјечавања неовлашћеног изношења података или спрјечавања уношења недозвољених предмета, којима се може угрозити безбједност података.

Члан 8.

Податак се складишти на одговарајућем информатичком медију, који се одлаже и чува у безбједном складишту.

Члан 9.

Простор у којем се налазе рачунари за вођење базе података и централни рачунар информационог система (сервери), мрежна или комуникациона опрема информационог система, организује се као административна зона.

III - ЗАШТИТА ПОДАТАКА

Члан 10.

Рачунар за вођење базе података и централни рачунар информационог система (сервер) мора бити опремљен:

а) системом за безбједно пријављивање за рад са могућношћу евидентирања остварених приступа, како би се приступ серверу могао контролисати и ограничити,

б) механизмом за спрјечавање неовлашћеног изношења и уношења података употребом преносивих информатичких медија, комуникационих прикључака и прикључака за испис података,

в) механизмом заштите од рачунарских вируса и других штетних програма.

Члан 11.

(1) Приступ бази података дозвољен је само лицима задуженим за одржавање и развој информационог система.

(2) Приступ телекомуникационом, рачунарском и апликативном систему за обраду података, дозвољен је уз употребу одговарајућег корисничког имена и припадајуће лозинке.

(3) Корисничко име и припадајућа лозинка не смију се открити и дати на употребу другом лицу.

Члан 12.

Управљање системом корисничког приступа подразумијева развој, примјену и одржавање информационог система, на начин који омогућава једнозначно идентификовање и поуздано гарантовање идентитета корисника.

Члан 13.

Органи, правна и физичка лица из члана 2. ове уредбе дужни су да складиште све податке из инфомационих система на информатичке медије употребом метода који гарантују безбједност, повјерљивост, цјеловитост и доступност ускладиштених података.

Члан 14.

(1) Базе података обавезно се складиште на преносиве информатичке медије најмање једном дневно, седмично, мјесечно и годишње, за потребе обнове базе података.

(2) Подаци информационог система складиште се у онолико дневних примјерака колико има радних дана у седмици.

(3) Седмично складиштење података информационог система врши се посљедњег радног дана у седмици, након спровођења дневног складиштења података, у онолико седмичних примјерака колико у мјесецу има посљедњих радних дана у седмици.

(4) Мјесечно складиштење података информационог система врши се посљедњег радног дана у мјесецу, за сваки мјесец посебно.

(5) Годишње складиштење података информационог система врши се посљедњег радног дана у години.

(6) Сваки примјерак годишње ускладиштених података чува се за вријеме одређено прописима којима се уређује архивска дјелатност.

(7) Сваки примјерак преносивог информатичког медија са ускладиштеним подацима мора бити означен бројем, врстом (дневно, седмично, мјесечно, годишње), датумом складиштења, као и именом лица које је извршило складиштење података.

(8) Органи, правна и физичка лица из члана 2. ове уредбе воде евиденцију информатичких медија на којима су подаци ускладиштени.

Члан 15.

(1) Подаци информационог система дневно ускладиштени на информатичке медије одлажу се у најмање једно безбједно складиште у радној просторији органа, правног или физичког лица из члана 2. ове уредбе или на другој безбједној локацији.

(2) Подаци информационог система седмично, мјесечно и годишње ускладиштени на информатичке медије одлажу се на безбједну локацију.

Члан 16.

Употребљивост сигурносне копије података провјерава се најмање сваких шест мјесеци, уз провјеру поступка повраћаја база података ускладиштених на информатичком медију, тако да враћени подаци након извршене провјере буду цјеловити, повјерљиви и доступни за употребу.

Члан 17.

Подаци ускладиштени годишње на информатичком медију морају се обновити након истека половине гарантованог рока трајања записа на тој врсти медија.

Члан 18.

Органи, правна и физичка лица из члана 2. ове уредбе успостављају систем криптоване заштите података у преносу тих података информационим и телекомуникационим системом.

IV - ЗАШТИТА ИНФОРМАЦИОНОГ СИСТЕМА

Члан 19.

(1) Рачунар за вођење базе података и централни рачунар информационог система (сервер) и рачунарску мрежу поставља и уграђује стручно лице, у складу са пројектном документацијом, важећим нормама, стандардима и техничким упутствима.

(2) По један примјерак пројектне документације из става 1. овог члана чува се у радним просторијама органа, правног или физичког лица из члана 2. ове уредбе, на безбједном мјесту, а доставља се на увид на захтјев органа управног и стручног надзора.

Члан 20.

Контрола повезивања информационих система обухвата дефинисање услова повезивања информационих система, као и евидентирање и надзор повезивања.

Члан 21.

Контрола употребе информационог система подразумијева евидентирање активности корисника информационог система, као и мјере за спрјечавање злоупотребе информационог система кроз инсталирање система за откривање неовлашћеног упада у рачунарску мрежу, дефинисање, прегледање и анализирање записа рада информационог система и спровођење анализа рањивости информационог система.

Члан 22.

(1) Сваки приступ информационом систему за обраду и складиштење података мора бити аутоматски забиљежен корисничким именом, датумом и временом пријаве и одјаве.

(2) Сваки покушај неовлашћеног приступа информационом систему мора бити аутоматски забиљежен корисничким именом, датумом и временом, а ако је то могуће и мјестом са којег је такав приступ покушан.

(3) Лице из члана 11. став 1. ове уредбе дужно је да обавијести старјешину органа, руководиоца правног лица, односно физичко лице о сваком покушају неовлашћеног приступа информационом систему.

Члан 23.

(1) Информациони систем мора бити смјештен у просторијама које имају уређаје за откривање пожара и аутоматско обавјештавање о избијању пожара.

(2) Просторије у којима је смјештен информациони систем морају имати уређаје за гашење пожара, а у близини, испред и у тим просторијама, на видљивим и лако уочљивим мјестима морају бити истакнута упутства о поступању у случају избијања пожара.

Члан 24.

У близини рачунарске и телекомуникационе опреме не смије се постављати:

а) извор јаког електричног или магнетског поља,
б) извор електростатичког електрицитета,
в) извор јонизирајућег зрачења.

Члан 25.

У просторијама у којима је смјештен информациони систем мора се одржавати одговарајућа влажност ваздуха и температура.

Члан 26.

У просторијама и у близини просторија у којима је смјештена опрема информационог система, не смију се налазити нагризајућа и лакозапаљива течност, експлозивна средства и слична опасна или штетна хемијска једињења.

Члан 27.

Повјерљивост, цјеловитост и доступност података обезбјеђује се коришћењем криптографских метода одобрених од стране надлежног органа.

Члан 28.

(1) Органи, правна и физичка лица из члана 2. ове уредбе успостављају безбједносна правила ради обезбјеђивања информационе безбједности података којима та лица имају приступ, односно која поступају са њима.

(2) Безбједносна правила из члана 1. ове уредбе подразумијевају:

а) интерна правила за запослене;

б) едукацију и стручно усавршавање запослених.

Члан 29.

(1) Планирање дјеловања у ванредним ситуацијама подразумијева анализу потенцијалних ризика у раду информационог система и утврђивање поступака за рјешавање тих ризика, као и других метода коришћења ресурса информационог система у случају недоступности информационог система, а у циљу одржавања непрекидног функционисања, односно пословања органа, правног и физичког лица из члана 2. ове уредбе.

(2) Планирање дјеловања у ванредним ситуацијама обухвата:

а) израду плана непрекидног функционисања, односно пословања органа, правног и физичког лица из члана 2. ове уредбе,

б) израду процедура за поступање у случају инцидената.

Члан 30.

План непрекидног функционисања, односно пословања обухвата успостављање и тестирање адекватне процедуре безбједног складиштења података, ради враћања информационог система и података у првобитно стање након инцидента, који подразумијева испад информационог система, природне непогоде и дјеловање рачунарских вируса.

Члан 31.

Израда процедура за поступање у случају инцидента подразумијева планирање и дефинисање активности, спрјечавања, детекције и опоравка од посљедица инцидента, који утичу на повјерљивост, цјеловитост и доступност податка или информационог система, укључујући и извјештавање о инцидентима.

V - УПРАВЉАЊЕ РИЗИКОМ ИНФОРМАЦИОНЕ БЕЗБЈЕДНОСТИ

Члан 32.

(1) Управљање ризиком информационе безбједности подразумијева планирање, организовање и усмјеравање активности, ради обезбјеђивања услова да ризици не угрозе непрекидно функционисање, односно пословање органа, правног и физичког лица из члана 2. ове уредбе.

(2) Планирање из става 1. овог члана подразумијева утврђивање степена прихватљивости ризика, ради његовог прихватања, смањивања или избјегавања (у даљем тексту: анализа ризика).

Члан 33.

(1) Ризик се може прихватити уколико би настала штета била мања од штете која би настала усљед неспровођења одређене активности.

(2) Смањивање ризика спроводи се примјеном мјера дефинисаних у плану активности из члана 34. ове уредбе, ради спрјечавања уништења, отуђења, губитка и неовлашћеног приступа подацима.

(3) Избјегавање ризика подразумијева предузимање организационих и других неопходних мјера у циљу избјегавања радњи које би могле изазвати ризик.

Члан 34.

Након анализе ризика, органи, правна и физичка лица из члана 2. ове уредбе, обавезни су да сачине план активности у којем се утврђује спровођење потребних мјера.

Члан 35.

Резултати анализе ризика редовно се преиспитују, сагласно потребама органа, правног и физичког лица из члана 2. ове уредбе, условљеним унутрашњим или ванјским промјенама.

VI – ПРОВОЂЕЊЕ ИНФОРМАЦИОНЕ БЕЗБЈЕДНОСТИ

Члан 36.

(1) Информациону безбједност проводе сви органи из члана 2. ове уредбе.

(2) Стручни надзор и контролу провођења информационе безбједности врши Агенција за информационо друштво Републике Српске (у даљем тексту: Агенција).

(3) За реализацију става 2. овог члана Агенција формира посебан стручни орган – Одјељење за информациону безбједност – ОИБ (у даљем тексту: ОИБ).

Члан 37.

(1) ОИБ ће вршити стручно–специјалистичке послове успостављања, заштите и одржавања информационе безбједности као и непосредан надзор и контролу над њеним провођењем.

(2) Припадници ОИБ имају овлашћења вршења информационе безбједности у складу са одредбама Закона о информационој безбједности.

(3) У сврху доказивања припадности ОИБ, а ради лакшег и ефикаснијег рада припадници ОИБ имају право на службену легитимацију и значку.

(4) Полицијски службеници, органи републичке управе и други органи надлежни за провођење закона у Републици Српској дужни су лицима из става 4. овог члана пружити помоћ у раду.

(5) Изглед, облик и садржај службене легитимације и значке припадника ОИБ, те услове за њихово коришћење прописује директор Агенције посебним правилником.

VII - ЗАВРШНЕ ОДРЕДБЕ

Члан 38.

Ступањем на снагу ове уредбе престаје да важи Уредба о мјерама заштите података и информација у информационом систему републичких органа и организација (Службени гласник Републике Српске", број 25/04).

Члан 39.

Ова уредба ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Српске".

Број:04/1-012-2-2259/12
Датум: 20.09.2012. године

ПРЕДСЈЕДНИК ВЛАДЕ

Александар Џомбић

.