На основу члана 15. Закона о информационој безбједности („Службени гласник Републике Српске“, број 70/11) и члана 82. став 2. Закона о републичкој управи („Службени гласник Републике Српске“, бр. 118/08, 11/09, 74/10 и 86/10), а на приједлог Агенције за информационо друштво Републике Српске, министар науке и технологије доноси

ПРАВИЛНИК
О СТАНДАРДИМА ИНФОРМАЦИОНЕ БЕЗБЈЕДНОСТИ

I - ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим правилником утврђују се минимални стандарди информационе безбједности којима се обезбјеђује основна заштита података на физичком, техничком и организационом нивоу.

Члан 2.

Стандарди из члана 1. овог правилника односе се на републичке органе, органе јединица локалне самоуправе, правна лица која врше јавна овлашћења 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 (у даљем тексту: субјекти).

Члан 3.

Поједини изрази који се користе у овом правилнику имају сљедеће значење:

а) хардвер - физичка компонента информационог система,

б) криптографска заштита - систем заштите података и информационих система који осигурава безбједан 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 субјекта, 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,

и) безбједни податак – податак који у складу са прописаним безбједносним мјерама није доступан неовлаштеним лицима у процесу управљања тим податком (управљање = обрада, измјена, пренос, складиштење тј архивирање, копирање, брисање, уништавање),

ј) ОИБ – Одјељење за информациону безбједност – одјељење унутар Агенције за информационо друштво које врши непосредан надзор и контролу над провођењем информационе безбједности,

к) Политика безбједности информационог система - представља скуп правила, смјерница и поступака који дефинишу на који начин информациони систем учинити сигурним, укључујући сигурност технологије, као и информација које информациони систем садржи.

Члан 4.

(1) Подаци у информационом систему субјеката имају један од сљедећих степена безбједности:

а) "1. степен безбједности" – одређује се ради спречавања настанка непоправљиве штете по интересе субјекта,

б) "2. степен безбједности" – одређује се ради спречавања настанка изузетно штетне посљедице по интересе субјекта,

в) "3. степен безбједности" – одређује се ради спречавања настанка штете по интересе субјеката,

г) "4. степен безбједности" – одређује се ради спречавања настанка штете за рад, односно обављање задатака и послова субјекта који их је одредио,

д) „5. степен безбједности (у даљем тексту: јавни подаци)“ – подаци за које се сматра да не могу узроковати настанак било какве штете за субјекат који их је одредио.

(2) Субјекти су дужни извршити процјену ризика информационог система која ће као резултат дати класификацију података по нивоима безбједности.

(3) Процјена ризика и класификација података морају бити задокументовани у склопу документа „Политика безбједности информационог система“.

Члан 5.

(1) Административне зоне класификују се на:

а) јавне и

б) сигурне

(2) Као јавним класификују се административне зоне у којима се или у чијој се непосредној близини налазе само јавни подаци.

(3) Као сигурним класификују се административне зоне које нису јавне.

Члан 6.

(1) Сигурне административне зоне додатно се класификују по степену безбједности.

(2) Степени безбједности сигурних административних зона су:

а) 1. степен безбједности,

б) 2. степен безбједности,

в) 3. степен безбједности,

г) 4. степен безбједности.

Члан 7.

Степен безбједности административне зоне одређује податак, опрема или ресурс највишег степена безбедности који се у тој зони налази и то:

а) 1. степен безбједности – ако садржи макар један податак, опрему или ресурс 1. степена бједности,

б) 2. степен безбједности – ако садржи макар један податак, опрему или ресурс 2. степена бједности,

в) 3. степен безбједности – ако садржи макар један податак, опрему или ресурс 3. степена бједности,

г) 4. степен безбједности – ако садржи макар један податак, опрему или ресурс 4. степена бједности.

Члан 8.

(1) Субјекти могу интерним правилником или одлуком да повећају степен безбједности административних зона у односу на степен дефинисан чланом 7. овог правилника ако то сматрају оправданим и потребним.

(2) Снижавање степена безбједности административних зона није дозвољено.

II - ФИЗИЧКА ЗАШТИТА

1. Успостављање административних зона

Члан 9.

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

(2) 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.

(3) Субјекти успостављају једну или више административних зона одговарајућег степена безбједности сходно обиму, количини, степену безбједности и просторном размјештају података, опреме и ресурса.

Члан 10.

(1) Број, величину, размјештај и степен безбједности административних зона субјекти дефинишу интерним актом, а на основу усвојене Политике безбједности информационог система.

(2) Приликом доношења одлуке о броју, величини, размјештају и степену безбједности административних зона потребно је извршити што већу оптимизацију те број сигурних административних зона смањити на најмању могућу мјеру, а посебно зона степена безбједности 1 и 2.

Члан 11.

(1) Јавне и сигурне зоне потребно је колико је то год могуће и технички изводљиво физички раздвојити.

(2) Ако је субјекат физички смјештен у више објеката (зграда), сигурне зоне степена безбједности 1, 2 и 3 потребно је успоставити у одвојеним објектима.

(3) Ако је субјекат физички смјештен у само једном објекту (згради), сигурне зоне степена безбједности 1, 2 и 3 потребно је успоставити у одвојеном сегменту објекта и то што удаљенијем од јавних зона.

(4) Због додатне безбједности, гдје је то физички могуће, сигурне зоне је пожељно формирати у циљу формирања више безбједносних баријера.

(5) Ово се постиже формирањем сигуних зона вишег степена безбједности унутар сигурних зона нижег степена безбједности.

Члан 12.

(1) Субјекти могу, ако је то економски оправдано, користити административне зоне одговарајућег степена безбједности других субјеката.

(2) У случајевима из става 1. овог члана, сви безбједни подаци, опрема и ресурси смјештени у сигурној административној зони која није у власништву субјекта морају остати у њеном пуном власништву.

2. Физичка заштита околине објекта и објекта

Члан 13.

Подручје око објекта у власништву субјекта (у даљем тексту: околина објекта) у којем се налази јавна и/или сигурна зона потребно је да задовољава сљедеће безбједносне стандарде:

а) околина објекта мора да буде организована и уређена на начин да се обезбједи добра прегледност и да се формирају јасне зоне уласка, изласка и кретања,

б) на добру прегледност утиче добро освјетљење те постојање, врста и распоред растиња, путева, инсталација, мањих помоћних објеката и слично,

в) околина објекта мора да буде добро освјетљена, односно расвјета мора да буде тако распоређена да елиминише слабо освјетљена мјеста (сјене) и тзв. слијепа мјеста,

г) поглед са прозора објекта треба да буде неометан,

д) ако у околини објекта постоји дрвеће и друго високо растиње, крошње се морају формирати тако да не ометају поглед на околину објекта и да не праве тзв. слијепа мјеста,

ђ) стабла и друго високо растиње не смије да има гране на висини нижој од 2,5 метара, мјерено од тла,

е) ниже растиње (живице, жбуње, грмље и сл.) не смије да буде више од 1 метар, мјерено од тла.

Члан 14.

Околина објекта у којем се налази сигурна зона 4. степена безбједности поред услова из члана 13. додатно треба да задовољава и сљедеће безбједносне стандарде:

а) околина објекта треба да буде ограђена адекватном оградом која врши функцију примарне контроле приступа лица усмјеравајући их на јасно означене улазе и излазе.

б) поред ограда могу се користити и зидови који, осим креирања зона сигурног кретања лица, ограничавају видљивост у унутрашњост објеката установе, а могу да штите и од појединих природних или вјештачки изазваних пријетњи као што су поплаве, пожари и експлозије у непосредној околини.

в) без обзира на изведбу ограде/зида, ограда/зид требају бити чврсте конструкције, без прекида изузев на мјестима улаза/излаза.

Члан 15.

Околина објекта у којем се налази сигурна зона 3. степена безбједности поред услова из члана 14. додатно треба да задовољава и сљедеће безбједносне стандарде:

а) изведба ограде/зида треба бити чврсте конструкције, без прекида изузев на мјестима улаза/излаза и таква да онемогућује лаку провалу, прескакање или други вид заобилажења,

б) ванjска ограда/зидови на себи требају да имају улазна/излазна врата која су одговарајућа за онемогућавање неовлаштеног приступа те са свим потребним сигурносним механизмима (катанац, брава, људска контрола (потрир/чувар) и слично),

в) сва улазна/излазна врата морају бити закључана када нису под надзором и/или када субјекти не раде.

Члан 16.

Околина објекта у којем се налази сигурна зона 2. степена безбједности поред услова из члана 15. додатно треба да задовољава и сљедеће безбједносне стандарде:

а) ако се у објекту налазе зоне са јавним приступом, прилаз тим зонама потребно је физички раздвојити,

б) раздвајање се врши формирањем посебних улаза/излаза и ако је неопходно, коришћењем додатних ограда/зидова за раздвајање,

в) улазна и излазна врата морају бити покривена видео надзором,

г) инсталација надзорних камера мора да буде таква да онемогућује лаку саботажу, премошћавање, ометање, оштећивање или уништење,

д) улази и излази који својим габаритима омогућавају пролазак моторних возила категорије Б и више морају имати инсталиране баријере за спречавање неовлашћеног проласка возила (рампа, покретни стуб, покретна бетонска или челична баријера и сл.).

Члан 17.

Објекат у којем се налази сигурна зона 2. степена безбједности треба да задовољава сљедеће безбједносне стандарде:

а) улазна и излазна врата објекта морају бити противпровална,

б) улазна и излазна врата објекта морају бити покривена видео надзором,

в) инсталација надзорних камера мора да буде таква да онемогућује лаку саботажу, премошћавање, ометање, оштећивање или уништење,

г) ванjски прозори, минимално на приземним нивоима и на таквим мјестима на којима им је могућ лак приступ из вана, морају да буду заштићени од провале а заштита се може реализовати употребом противпровалних стакала, монтажом заштитних противпровалних шипки или мрежа и слично,

д) ванjска врата и прозори морају да имају инсталиран противпровални алармни систем, гласни или тихи,

ђ) алармни противпровални систем мора редовно да се тестира, а најмање сваких 12 мјесеци те обавезно у случајевима надоградње или реконфигурисања алармног система и/или случаја активирања аларма,

е) улази и излази из објекта морају бити обезбјеђени портиром/чуваром минимално сво радно вријеме субјекта, а пожељно нон-стоп тј. на бази 24/7,

ж) ако портир/чувар из тачке е) овог члана обезбјеђује субјекат само у току радног времена тада алармни противпровални систем мора бити увезан са одговарајућом установом за заштиту / сигурност (полиција, професионална заштитарска фирма) те у случају активирања извршити алармирање портира/чувара и установе са којом је систем увезан (пожељно је да се додатно алармирају и друге одговорне особе субјекта).

Члан 18.

Околина објекта у којем се налази сигурна зона 1. степена безбједности поред услова из члана 16. додатно треба да задовољава и сљедеће безбједносне стандарде:

а) улазна и излазна врата ограде/зида морају бити противпровална,

б) ограда/зид морају бити непрозирни тако да онемогућавају поглед из вана,

в) ограда, својом цијелом дужином, те улазна и излазна врата на њој морају имати инсталиран противпровални алармни систем, гласни или тихи,

г) алармни противпровални систем мора редовно да се тестира, а најмање сваких 6 мјесеци те обавезно у случајевима надоградње или реконфигурисања алармног система и/или случаја активирања аларма,

д) алармни противпровални систем мора бити увезан са одговарајућом установом за заштиту / сигурност (полиција, професионална заштитарска фирма) те у случају активирања извршити алармирање портира/чувара и установе са којом је систем увезан. (пожељно је да се додатно алармирају и друге одговорне особе субјекта),

ђ) осим улазних и излазних врата, видео надзором мора бити покривена ванјска ограда/зид угључујући простор изван ограде/зида те са обавезним преклапањем зона видео надзора тако да је свака тачка покривена видео надзором са најмање двије надзорне камере.

Члан 19.

Објекат у којем се налази сигурна зона 1. степена безбједности поред услова из члана 17. додатно треба да задовољава и сљедеће безбједносне стандарде:

а) улазна и излазна врата објекта морају бити противпровална са механичком и електронском бравом,

б) улази и излази морају бити опремљени уређајем за детекцију метала и других опасних средстава. (монтажа уређаја мора бити таква да је код уласка односно изласка обавезан пролаз лица кроз уређај),

б) улази и излази из објекта морају бити обезбјеђени портиром/чуваром 24 часа дневно,

в) пожељно је да број портира/чувара који обезбјеђују улазе и излазе објекта буде минимално 2 по улазу/излазу,

г) ако је на улазима/излазима формирана портирница, тада свака портирница мора бити опремљена системом за ручно активирање алармног система (скривени паник тастер или слично).

д) ако не постоје формиране портирнице тада сваки портир за вријеме обављања дужности мора бити опремљен одговарајућим мобилим/преносивим системом за ручно активирање алармног система,

д) алармни противпровални систем мора бити увезан са одговарајућом установом за заштиту / сигурност (полиција, професионална заштитарска фирма) те у случају активирања извршити алармирање те установе (пожељно је да се додатно алармирају и друге одговорне особе субјекта).

3. Физичка контрола приступа (улазак и излазак)

Члан 20.

(1) Физичка контрола приступа како објектима и просторијама унутар објеката тако и околини објекта неопходна је како би се обезбједило да приступ објектима и просторијама имају само овлашћена лица и особље.

(2) Улазак трећих лица и посјетилаца треба бити ограничен те дозвољен само када је то заиста неопходно.

(3) Боравак трећих лица и посјетилаца у сваком тренутку мора бити надзиран од стране одговорног запосленог лица.

Члан 21.

(1) Сваки улазак и излазак из објекта или дијела објекта било којег степена безбједности мора бити евидентиран.

(2) Евиденција мора да садржи најмање датум, вријеме, име и презиме лица.

(3) Приликом уласка трећих лица и посјетилаца, прије уласка треће лице односно посјетилац мора да на увид дâ лични документ са фотографијом ради идентификације.

(4) У евиденцију улазака и излазака се тада осим основних података мора унијети и податак о идентификационом документу лица, а најмање врста и број документа.

(5) Идентификациони документ се трећем лицу односно посјетиоцу враћа тек приликом изласка, а након евидентирања изласка.

Члан 22.

Свако треће лице односно посјетилац, прије приступа безбједној зони, мора да буде упознат са свим безбједносним захтјевима те зоне те свим постојећим процедурама за хитне случајеве који важе за ту зону.

Члан 23.

Сваки улазак и излазак из објекта или дијела објекта степена безбједности 3. и вишег треба да буде ограничен само на овлашћена лица и само када је њихов приступ неопходан.

Члан 24.

(1) Сви радници, трећа лица и посјетиоци за вријеме боравка у зонама било којег степена безбједности морају да носе неку форму јасне идентификације која мора да буде видљиво истакнута и читка.

(2) Идентификација мора да буде израђена на такав начин да је лака израда фалсификата или промјена података на легитимним идентификацијама изузетно тешка, а пожељно готово немогућа.

(3) Изглед идентификације радника и посјетилаца/трећих лица мора да буде различит те јасно и недвосмислено распознатљив.

(4) Сва лица која се налазе унутар безбједних зона морају бити обавезна да ако примијете лице или лица без видљиво истакнуте одговарајуће идентификације обезбјеђењу одмах пријаве тај случај.

(5) Идентификације лица која имају приступ зонама степена безбједности 1. и 2. морају да садрже фотографију те, пожељно, додатне елементе заштите од кривотворења као што су употреба чипова, идентификаторе радио фреквенције (енг. RFID) технологије, холограма и сл.

Члан 25.

Прије уласка у зоне или просторије које захтијевају одржавање посебних и стриктних амбијенталних услова (нпр. чисте собе), прије одобравања приступа лицима потребно је осигурати да лица претходно задовоље све тражене безбједносне стандарде (нпр. облачење натикача, чистих одијела и капуљача).

Члан 26.

(1) Гдје је потребно, улаз у зоне/просторије са посебним амбијенталним условима треба формирати у форми улазних/излазних комора са постојањем најмање двоје улазних/излазних врата од којих у једном тренутку само једна могу бити отворена.

(2) Међузона (комора) може бити потребна због постизања одговарајућег степена чистоће, изједначавања атмосферског притиска или обезбјеђивања додатне контроле уласка/изласка.

Члан 27.

(1) Приступ зони 2. степена безбједности додатно мора да буде контролисан коришћењем додатних савремених механизама контроле приступа.

(2) За утврђивање и одобравање права приступа, осим котроле од стране овлашћених портира/чувара потербно је користити минимално паметне RFID или чип картице за контролу приступа са ПИН-ом.

Члан 28.

(1) Приступ зони 1. степена безбједности додатно мора да буде контролисан коришћењем минимално једног биометријског читача.

(2) Зона мора бити организована као зона без индивидуалног приступа.

(3) Приступ и боравак у зони може се одобрити само паровима овлашћених лица те све критичне операције које се обављају у зони морају захтијевати паралелну интервенцију најмање 2 лица уз механизме који обезбјеђују да једно лице не може физички самостално извршити те операције.

Члан 29.

(1) Зона 1. и 2. степена безбједности морају се налазити под сталним видео надзором.

(2) Аудио и видео записи снимљени опремом из става 1. овог члана означавају се степеном безбједности у складу са степеном безбједности административне зоне, те се са њима поступа на исти начин као и са подацима одговарајућег степена безбједности.

Члан 30.

(1) Сва права приступа лицима, без обзира о којој врсти лица и степену безбједности зоне се ради, морају редовно да се ревидирају и контролишу те, у случају потребе, проширују, ограничавају или скроз укидају.

(2) Права приступа за појединo лице требају да се ревидирају сваки пут када долази до промјене статуса лица (нпр. запошљавање, промјена радног мјеста, одлазак на годишњи одмор, напуштање установе и сл.), а генерална провјера права приступа свих лица требала би се вршити најмање једном на сваких 6 мјесеци.

4. Физичка заштита канцеларија, просторија и постројења

Члан 31.

Циљ обезбјеђивања физичке заштите канцеларија, просторија, постројења и других простора од значаја јесте заштита од пожара, поплава, експлозија и других видова природних или вјештачки изазваних несрећа, детекција неовлашћеног приступа и сл.

Члан 32.

(1) Све просторије, канцеларије, постројења и други простори морају бити опремљени системом за детекцију пожара са функцијом алармирања у складу са Законом о заштити од пожара Републике Српске.

(2) Сходно противпожарним стандардима Републике Српске, на одговарајућим мјестима те у одговарајућем броју потребно је поставити и јасно означити системе за борбу против пожара (противпожарни апарати, хидранти, активни аутоматски системи за гашење пожара).

Члан 33.

(1) Гдје год је то могуће објекти, просторије, канцеларије, постројења и други простори од значаја требају да буду ненаметљиви и да дају што мању индикацију о њиховој сврси и/или да се у њима налази осјетљива опрема и/или подаци и/или да се у њима врши обрада осјетљивих података.

(2) Не би требало да постоје очигледне ознаке, вањске или унутрашње, које би идентификовале присуство активности прикупљања/обраде/смјештања података.

Члан 34.

(1) Посебно битне просторије требају да буду позициониране тако да им неовлашћено особље не може једноставно прићи.

(2) Такве просторије морају да буду смјештене у својим зонама безбједности што даље од зона нижег нивоа безбједности.

Члан 35.

(1) Све канцеларије, просторије, постројења и други простори од значаја требају бити опремљени противпровалним алармним системом.

(2) У зонама у којима се не очекује присуство људи алармни систем мора бити константно активиран, а зона додатно периодично физички провјеравана.

Члан 36.

(1) Све опасне и запаљиве материје морају да буду смјештене на сигурној удаљености од сигурних зона, а посебно од просторија од посебне важности.

(2) Потрошни и канцеларијски материјали не би требало да буду смјештени у сигурним зонама већ у за то предвиђеним складишним просторима.

Члан 37.

Ако је објекат, па самим тим и просторије у њему, на локацији са високим ризиком од поплава, сигурне зоне морају бити обезбјеђене водонепропусним (противпоплавним) вратима.

Члан 38.

(1) Рачунари и друга информатичка опрема морају бити тако постављени да посјетиоци не могу да виде садржај на њима нити њихово коришћење.

(2) Рачунари и друга информатичка опрема мора да буде закључана када није у употреби и када је не користи неко од радника установе.

Члан 39.

Гдје за то постоји потреба, просторије је потребно покрити видео надзором (просторије са јавним приступом, просторије од високог значаја, серверске и комуникационе сале и сл.).

Члан 40.

Сав запримљени материјал и опрема прије пребацивања са мјеста пријема (утовара/истовара) на мјесто складиштења и коришћења треба да буде прегледана против потенцијалних пријетњи (опасне и запаљиве материје, експлозиви, електромагнетна радијација и др.).

Члан 41.

(1) Запослени у субјекту не смију користити приватне фотографске уређаје, уређаје за аудио или видео снимање, приватну ИТ опрему, те преносне медије у просторијама у којима се користе подаци означени степеном безбједности 3. и више.

(2) Употреба службених фотографских уређаја, те уређаја за аудио или видео снимање у просторијама у којима се користе подаци означени степеном безбједности 3 и вишег степена безбједности дозвољено је само уз писани налог руководиоца субјекта у чијим се просторијама желе користити наведени уређаји.

Члан 42.

Интерни телефонски именици, тлоцрти, листе просторија те други материјали који могу да идентификују локације од значаја не би требало да буду јавно доступне ни генералној јавности нити посјетиоцима.

Члан 43.

(1) Ако просторије због своје примјене захтијевају испуњавање посебних физичко-техничких услова (чисте собе, биосигурне собе и сл.) те услове је потребно поштовати, а безбједносне стандарде наведене у претходним члановима примјењивати у броју и обиму у којем је то могуће и неопходно.

(2) Ако просторија из става 1. овог члана припада зони 1. или 2. степена безбједности тада приступ и простор око те просторије мора да задовољи све услове овог правилника прописане за зону 1. односно 2. степена безбједности.

5. Смјештај и физичка заштита опреме

Члан 44.

Сва опрема, како за вријеме складиштења тако и за вријеме редовне експлоатације, треба да буде заштићена од физичких пријетњи те пријетњи радне средине.

Члан 45.

(1) За вријеме складиштења опрема мора да се складишти на начин и у просторије које задовољавају амбијенталне складишне услове средине прописане од стране произвођача опреме (температура, влажност ваздуха, механичко оптерећење, изложеност електро-магнетном зрачењу и сл.).

(2) За вријеме експлоатације опрему је потребно смјестити на начин и у просторије које задовољавају радне услове средине прописане од стране произвођача опреме.

(3) Потребно је обезбиједити све прописане техничке и амбијенталне услове радне средине дефинисане од стране произвођача као што су температура, влажност ваздуха, класа чистоће ваздуха, механичко оптерећење опреме, начин монтаже опреме, изложеност електромагнетном зрачењу, адекватно напајање електричном енергијом, коректно уземљење и др.

Члан 46.

Опрема мора да буде смјештена у просторије и на начин који онемогућава непотребни и/или неовлашћени приступ опреми.

Члан 47.

Опрема која врши прикупљање/обраду/смјештање осјетљивих података мора да буде тако позиционирана и угао погледа на опрему редукован тако да се максимално умањи ризик да неовлашћено лице може да види податке у току њиховог коришћења/обраде од стране овлашћених лица.

Члан 48.

(1) Опрема за смјештање података мора да буде осигурана од неовлашћеног приступа.

(2) Осим смјештање у просторије са строго контролисаним приступом, опрема би требало да буде смјештена и закључана у сигурним ормарима намијењеним за ту сврху.

Члан 49.

Опрема која захтјева посебну безбједност и пажњу мора да буде смјештена одвојено и изоловано од остатка опреме како би се постигла додатна заштита.

Члан 50.

(1) Просторије у којима је смјештена посебно значајна опрема (сервери, активни комуникациони чворови и др.) требају бити прилагођене да минимизују ризик од потенцијалних физичких пријетњи као што је неовлашћен приступ, крађа, пожар, поплава, вибрације, прашина, електрична и електромагнетна интерференција, радијација и сл.

(2) Такве просторије морају да:

а) буду лоциране изван зона које су подложне поплавама и другим потенцијалним негативним утицајима (електромагнетно зрачење, близина опасних или запаљивих материја и сл.),

б) имају противпровална и противпожарна врата са механичком и електронском бравом,

в) имају антистатички под израђен од незапаљивих материјала,

г) имају инсталиран видео надзор,

д) имају инсталиран систем аутентификације лица и контроле приступа коришћењем једне од или више модерних технологија (смарт картице са ПИН кодом, РФИД картице, биометрија и сл.),

ђ) имају инсталиран систем за детекцију пожара, поплаве и провале са функцијом алармирања и дојаве,

е) имају инсталиран активни систем за гашење пожара базиран на нетечним и непроводљивим средствима за гашење која не оштећују електронске компоненте,

ж) имају инсталиране климатске уређаје за одржавање константног нивоа влажности и температуре,

з) имају инсталиране уређаје за филтрирање/пречишћавање ваздуха за одржавање неопходног нивоа чистоће ваздуха.

Члан 51.

Просторије у којима је посебно значајна опрема (сервери, активни комуникациони чворови и др.) не би смјело да садрже ванјске зидове објекта.

Члан 52.

(1) Носивост подова просторија у којима је посебно значајна опрема по јединици површине мора да буде најмање 30% већа од бруто тежине по јединици површине опреме која је у просторији постављена.

(2) Материјали од којих су у просторијама израђени подови, плафони, полице, ормари, носачи и др. морају бити одговарајућих противпожарних карактеристика.

(3) Осим ако опрема смјештена у просторији технички то не захтијева, зидови, подови и плафони просторија не смију да садрже водове воде, гаса или других опасних и запаљивих материја.

(4) У случајевима када су такве инсталације неопходне, потребно је обезбиједити да квар на инсталацијама неће довести до оштећења опреме смјештене у просторији.

Члан 53.

(1) Постављање климатизационих уређаја те уређаја за филтрирање и пречишћавање ваздуха мора да буде изведено на начин којим се елиминише појава врућих зона.

(2) Климатизациони и уређаји за филтрирање и пречишћавање ваздуха морају бити редунданти тако да отказ било којег од уређаја значајно не ремети услове радне средине док се не изврши сервисирање или замјена поквареног уређаја.

Члан 54.

(1) Унутрашње компоненте климатизационих и других уређаја које сарже течност или друге опасне или корозивне материје морају бити бар 1 метар удаљене од електронске опреме.

(2) Директно испод унутрашњих компоненти поменутих уређаја не смије да се налази смјештена електронска опрема.

Члан 55.

(1) Сва посебно значајна опрема која захтијева напајање електричном струјом мора да има обезбјеђен извор напајања кроз непрекидни извор напајања (УПС) одговарајуће називне снаге.

(2) Непрекидни извори напајања морају редовно да се котролишу како би се утврдило да имају одговарајући капацитет.

Члан 56.

(1) Просторија у којој се налази посебно значајна опрема мора да има обезбјеђено адекватно снабдијевање електричном енергијом.

(2) Електричне инсталације и снабдијевање електричном енергијом мора да буде у складу са произвођачким спецификацијама опреме и предвиђеним електричним оптерећењима.

(3) Алтернативни извор напајања (нпр. агрегат) за случај дуготрајнијег нестанка напајања електричном енергијом мора да буде обезбијеђен те редовно тестиран.

(4) Просторија мора да има доступне и јасно обиљежене прекидаче за хитно прекидање електричног напајања цијеле просторије који требају да буду позиционирани код излаза за случај нужде.

Члан 57.

Постављање, мијењање, премјештање, одржавање и уклањање опреме треба да врши само овлашћено особље уз обавезно евидентирање свих радњи.

Члан 58.

(1) Планирани радови одржавања опреме морају бити извршени са максималном могућом контролом процеса одржавања.

(2) Ако одржавање опреме врше трећа лица тј. лица која нису запослени радници субјекта, уколико је то потребно, са опреме је прије почетка процеса одржавања/надоградње/ сервисирања потребно уклонити све осјетљиве информације.

6. Сигурност и физичка заштита опреме ван просторија

Члан 59.

Без обзира на власништво над опремом, коришћење било које опреме за обраду података или телекомуникације која се налази ван просторија субјекта мора претходно бити одобрено од стране руководиоца субјекта.

Члан 60.

Само они уређаји и они подаци за које је ризик те штета у случају оштећења, губитка или компромитације прихватљива могу добити дозволу за изношење из просторија установе и мобилно коришћење.

Члан 61.

(1) Ако је опрема која се користи ван просторија субјекта стационарна (на примјер телекомуникациона опрема), потребно је обезбиједити да установа у чијим просторијама се та опрема налази поштује захтијеване сигурносне стандарде.

(2) Сходно подацима који се на опреми из претходног става налазе, преносе или обрађују, опрема мора бити смјештена у зони одговарајућег степена безбједности.

(3) Опреми се мора ограничити приступ неовлашћеним лицима закључавањем у посебне сигурне ормаре.

7. Безбједност и физичка заштита енергетских и телекомуникационих водова

Члан 62.

Енергетски и телекомуникациони водови кроз које се врши пренос података морају бити заштићени од пресретања, оштећења или уништења.

Члан 63.

(1) Енергетски и телекомуникациони водови који улазе у објекте и просторије у којима се налази заштићени информациони систем, у објекат морају буду проведени подземним путем.

(2) Ако такав начин увођења водова није физички могућ, онда се морају користити оклопљени водови.

(3) Мрежни водови морају да буду заштићени од неовлашћеног приступа и пресретања коришћењем одговарајућих проводних/инсталационих путева те избјегавањем полагања водова кроз јавне зоне.

(4) Електрични водови морају бити раздвојени од комуникационих како би се избјегла интерференција.

(5) Сви мрежни водови од посебног значаја морају да буду проведени блиндираним/ оклопљеним водовима а сва терминална и мјеста за инспекцију морају бити смјештена у закључаним просторијама/ормарима.

Члан 64.

Просторије у којима се налазе *patch* панели морају имати контролисан приступ, а сами *patch* панели морају да се налазе у одговарајућим закључаним ормарима.

8. Физичка заштита меморијских медија на којима се налазе безбједни подаци и резервних копија података

Члан 65.

(1) Сви меморијски медији за складиштење података, те медији за пренос истих морају бити контролисани и физички заштићени.

(2) Сви меморијски медији те медији за пренос података морају бити евидентирани.

(3) Свако задужење меморијског медија и медија за пренос података од стране запослених мора бити евидентирано.

(4) Евиденција минимално мора да садржи датум и вријеме задужења, врсту, капацитет и серијски број медија те име, презиме радника и период задужења.

Члан 66.

(1) Сви меморијски медији који служе за смјештање резервних копија података морају да буду смјештени на безбједној локацији ван објекта/просторије у којој се налазе оригинали тих података.

(2) Удаљеност и позиција локације за смјештај резервних копија треба да је таква да може да преживи сваку природну или вјештачки изазвану катастрофу која би могла да уништи локацију на којој се налазе оригинални подаци, минимално у другој тектонској зони, на удаљености од минимално 300 километара ваздушне линије.

(3) Просторије у којима се смјештају меморијски медији са резервним копијама података морају да буду степена безбједности која одговара степену безбједности података који се на медијима налазе.

(4) Просторије те начин смјештаја меморијских медија морају да задовоље спецификације произвођача медија за њихово сигурно складиштење (ограничено присуство свјетлости, влаге, електромагнетног зрачења, вибрација и др.).

Члан 67.

Сви меморијски медији на којима су снимљени подаци 3. степена безбједности и више морају бити додатно заштићени методама енкрипције података.

Члан 68.

(1) Медији за складиштење безбједних података (тврди дискови, дискете, CD-ROM, DVD-ROM, траке и др.) морају на себи имати јасно видљиву сигурносну ознаку степена безбједности, машински или ручно исписану.

(2) Заштитни оквир медија, ако постоји, мора бити означен у складу са ставом 1. овог члана.

Члан 69.

(1) За медије који се износе из установе, потребно је посебно документовано овлаштење за износ медија.

(2) Овлашћење из става 1. овог члана мора бити издано и документовано због вођења евиденције и евентуалне будуће ревизије.

Члан 70.

(1) Приликом транспорта/слања меморијских медија између пословних јединица субјекта или субјекта и клијената, морају се користити обезбјеђени транспортни канали.

(2) Медији који се транспортују/шаљу морају бити евидентирани у одговарајућу евиденцију.

(3) Транспорт/доставу када год је то могуће требају да изврше овлаштена лица субјекта.

(4) Када је медије потребно достављати/слати коришћењем услуга доставе, потребно је користити само сигурне и поуздане достављаче.

(5) Пожељно је да субјекат формира списак одобрених достављача.

Члан 71.

Код транспорта/слања медија потребно је користити све доступне и економски оправдане методе обезбјеђивања пошиљке као што је коришћење закључаних контејнера, коришћење паковања са детекцијом покушаја неовлашћеног отварања, раздвајање пошиљке на два или више дијелова те слање путем различитих достављача и различитим рутама.

9. Физичка контрола људских ресурса

Члан 72.

Начин спровођења физичке контроле људских ресурса мора бити описан у склопу Политике безбједности информационог система.

III – ЗАШТИТА ПОДАТАКА И ИНФОРМАЦИОНОГ СИСТЕМА

1. Принцип минималности и минималних привилегија

Члан 73.

Само функционалности, уређаји и сервиси неопходни за успостављање функционалног информационог система субјеката треба да буду имплементирани, у циљу избјегавања непотребних ризика.

Члан 74.

(1) Корисницима информационог система субјеката биће дате само привилегије неопходне за приступ подацима неопходним за обављање њиховог посла, а у циљу ограничавања штете која може настати усљед безбједносних инцидената, грешака или неауторизоване употребе података и ресурса информационог система.

(2) Исто важи и за процесе и сервисе информационог система.

2. Сепарација дужности

Члан 75.

Обавезна је сепарација дужности администратора информационог система, као и корисника информационог система који раде с подацима степена безбједности 3. и више.

Члан 76.

Сви витални дијелови информационог система субјекта (физички и виртуелни сервери, комуникациона опрема, апликативни сервери, системи за управљање базама података и др.) морају имати задужене администраторе у складу са чланом 75. овог Правилника који су одговорни за поузданост и расположивост предметних дијелова информационог система.

3. Управљање безбједним подацима

Члан 77.

Ако се на једном медију или у једној колекцији података налазе подаци различитог степена безбједности, онда је медије, односно колекцију података, потребно заштитити као податке највишег степена безбједности предметних података.

Члан 78.

Копирање безбједних података мора се вршити на начин који осигурава да неће доћи до неовлаштеног копирања безбједних података или нарушавања интегритета података који се копирају.

Члан 79.

Уништавање безбједних података на медијима за складиштење података чији је животни вијек истекао или који ће се надаље користити у друге сврхе, обавља се одговарајућим рачунарским програмима доступним у регистру сертификоване опреме, уређаја и софтверских алата.

Члан 80.

(1) Физичко уништавање медија за складиштење безбједних података (тврди дискови, дискете, CD-ROM, DVD-ROM, траке и др.) обавља се због њихове неисправности, дотрајалости, након истека животног вијека опреме.

(2) Физичко уништавање медија за складиштење безбједности података обавља се дробљењем или на други сигуран начин на који се обезбјеђује да накнадна реконструкција података или битних компоненти уређаја није могућа.

(3) Уништавање обавља лице одговорно за функцију безбједности информационог система.

Члан 81.

Прије доставе на уништавање, с медија за складиштење безбједних података морају бити уклоњени сви безбједни подаци, њихови трагови, као и трагови ранијих активности.

Члан 82.

Свако уништавање медија за складиштење безбједних података мора да буде евидентирано, а евиденција мора да садржи најмање датум, вријеме, врсту медија, ознаку медија, начин уништавање те идентификације лица која су извршила његово уништавање.

4. Повјерљивост, цјеловитост, аутентичност и непорецивост података

Члан 83.

(1) Субјекти су дужни да, за потребе обезбјеђивања повјерљивости, цјеловитости, аутентичности и непорецивости података користе акредитоване криптографске алгоритме.

(2) Одјељење за информациону безбједност Агенције за информационо друштво (у даљем тексту: ОИБ) формира листу акредитованих криптографксих алгоритама.

(3) Листа акредитованих криптографских алгоритама формира се на основу препорука одговарајућих међународних организација или властитом акредитацијом у складу с одговарајућим међународним стандардима, нормама и препорукама.

(4) Листа акредитованих криптографских алгоритама мора да се састоји, минимално, од:

а) листе акредитованих алгоритама за креирање електронског сажетка (енг. hash),

б) листе симетричних и асиметричних криптографских алгоритама,

в) листе алгоритама за креирање електронског потписа.

Члан 84.

Сви информациони системи који се користе за пренос и размјену безбједних података морају бити осигурани средствима који обезбјеђују адекватну криптографску заштиту, у складу са чланом 83. овог Правилника.

5. Безбједносна акредитација информационог система

Члан 85.

(1) Безбједносна акредитација информационог система може се проводи се за информациони систем у којем се користе подаци 2. степена безбједности и вишег.

(2) Особе које учествују у процесу из става 1. овога члана требају посједовати сертификат за приступ подацима 1. степена безбједности или за један степена више од највишег степена безбједности података који се обрађују, похрањују или преносе у информационим системима под њиховом надлежности.

(3) Безбједносну акредитацију информационог система врши ОИБ.

6. Регистар сертификоване опреме, уређаја и софтверских алата

Члан 86.

(1) Регистар сертификоване опреме, уређаја и софтверских алата који се користе у информационом систему 3. степена безбјености и више формира ОИБ.

(2) Регистар сертификоване опреме и уређаја формира се преузимањем одговарајућих регистара међународних тијела задужених за стандарде у области безбједности или властитом акредитацијом у складу с одговарајућим међународним нормама.

7. Политика безбједности

Члан 87.

(1) Субјекти су дужни усвојити и имплементирати Политику безбједности информационог система, у складу са овим Правилником, која представља основ за управљање безбједношћу информационог система субјеката, и која као минимум треба да:

а) садржи јасно дефинисану класификацију података по нивоима безбједности,

б) садржи начела и принципе управљања безбједношћу ресурса информационог система,

в) дефинише одговорности које се односе на подручје управљања безбједношћу информационог система,

г) обухвати подручја управљачке, логичке и физичке заштите ресурса информационог система, у складу са величином и комплексношћу информационог система.

(2) Политика безбједности информационог система треба, минимално, да садржи сљедеће документе, ако се исти могу примијенити на информациони систем субјеката, и то:

а) Политика класификације информација односно података (Information Classification Security Policy),

б) Политика управљања ризицима (Risk Management Policy)

в) Политика контроле приступа (Access Control Policy),

г) Политика прихватљивог коришћења(Acceptable Use Policy),

д) E-mail политика (E-mail Policy),

ђ) Политика енкрипције (Acceptable Encryption Policy),

е) Екстранет политика (Extranet Policy),
ж) Политика приступа интернету (Internet Access Policy),
з) Политика креденцијала за аутентикацију (Authentication Credentials Policy),
и) Политика физичке безбједности (Physical Security Policy),
ј) Политика удаљеног приступа (Remote Access Policy),
к) Безбједносна политика сервера (Server Security Policy),
л) Безбједносна политика мрежних уређаја (Network Devices Security Policy),
љ) Безбједносна политика опреме и ДМЗ (DMZ Security Policy),
м) VPN политика (VPN Policy),
њ) Политика бежичне комуникације (Wireless Policy),
о) Политика IP телефоније (IP Telephony Policy),
п) Политика радних станица (Workstations Policy),
р) Политика провјере рањивости (Audit Vulnerability Scan Policy),
с) Политика одговора на безбједносне инциденте (Incident Handling Policy),
ш) Безбједносна политика мобилних уређаја (Mobile Security Policy),
т) Анти-Вирус политика (Anti-Virus Policy).
у) Политика контроле људских ресурса (Human Resources Control Policy)

(3) Детаљи креирања политике безбједности информационог система из ставова 1. и 2. овог члана треба да буду дати у смјерницама које прописује ОИБ.

8. Лице одговорно за функцију безбједности информационог система

Члан 88.

(1) Субјекти су дужни именовати лице одговорно за функцију безбједности информационог система, те дефинисати његова овлашћења и одговорности.

(2) Ова функција треба бити независна од функције организационе јединице за управљање информационим системом.

(3) Лице одговорно за функцију безбједности информационог система треба бити компетентно лице са минимално 5 година радог искуства на пословима из области безбједности информационих система.

Члан 89.

Лице одговорно за функцију безбједности информационог система треба, као минимум, да надзире и координира активности везане уз безбједност информационог система, те да редовно извјештава руководиоца о стању и активностима везаним за безбједност информационог система.

9. Интерна и екстерна ревизија

Члан 90.

Субјекти су дужни спроводити интерну ревизију безбједносних аспеката информационог система.

Члан 91.

(1) Субјекти су дужни ОИБ-у поднијети захтјев за издавање одобрења за именовање независног екстерног ревизора за ревизију безбједносних аспеката информационог система (у даљем тексту: екстерни ревизор).

(2) Субјекти су дужни да, уз захтјев из става 1. овог члана, доставе ОИБ-у сљедеће документе:

а) приједлог одлуке о именовању екстерног ревизора,

б) нацрт уговора са екстерним ревизором,

в) референце екстерног ревизора о обављеним ревизијама,

г) референце и стручне квалификације запослених екстерног ревизора који ће обављати ревизију.

Члан 92.

ОИБ ће рјешење по захтјеву за издавање одобрења за избор екстерног ревизора донијети у року од 30 дана од дана пријема захтјева са комплетном документацијом.

Члан 93.

(1) Одговорно лице субјекта дужно је, по добијању одобрења од ОИБ, донијети одлуку о именовању екстерног ревизора, те са изабраним екстерним ревизором потписати уговор о изради извјешаја о ревизији информационог система.

(2) Субјекат је дужан ОИБ-у доставити усвојену одлуку о избору екстерног ревизора и потписани уговор са изабраним екстерним ревизором, у року од 10 дана од дана усвајања, односно потписивања.

Члан 94.

(1) Екстерни ревизор дужан је сачинити ревизорски извјештај о обављеној ревизији.

(2) Извјештај о обављеној ревизији информационог система је посебан извјештај који усваја руководеће тијело субјекта и доставља га ОИБ, одмах по усвајању истог.

Члан 95.

Субјекти су дужни да екстерну ревизију безбједносних аспеката информационог система обаве у року од годину дана од дана ступања на снагу овог Правилника, а затим да је обављају периодично:

а) најмање једном годишње, у случају да се ради о информационом систему у којем се користе тајни подаци 2. степена безбједности и вишег,

б) најмање једном у три године, у случају да се ради о информационом систему у којем се користе подаци 3. степена безбједности изузев у случају значајних промјена у информационом систему, када су субјекти дужни да у најкраћем могућем року изврше ревизију безбједносних аспеката информационог система.

10. Апликативне контроле

Члан 96.

Субјекти су дужни обезбједити да апликативни софтвер има уграђене контроле исправности, потпуности и конзистентности података који се уносе, мијењају, обрађују и генеришу.

11. Документација

Члан 97.

(1) Субјекти су дужни да дефинишу и имплементирају процедуре управљања документацијом (техничком, функционалном, корисничком и др.) која се односи на информациони систем.

(2) Субјекти су дужни да, као минимум, обезбиједе:

а) постојање тачне, потпуне и ажурне документације изведеног стања свих сегмената информационог система,

б) постојање тачних, потпуних и ажурних корисничких упутстава за све сегменте информационог система,

в) приступ запослених документацији, а у складу са њиховим пословним потребама и класификацији безбједности.

12. Повезивање информационих система

Члан 98.

(1) Повезивање информационих система субјеката дозвољено је само:

а) ако за то постоји оправдани пословни разлог,

б) ако постоји писмена сагласност руководиоца субјеката чији се информациони системи требају повезати,

в) ако су предметни информациони системи пројектовани и имплементирани према одредбама овог Правилника,

г) и ако су акредитовани за рад са безбједним подацима истих степена тајности.

(2) Повезивање информационих система субјеката акредитованих за рад са безбједним подацима различитих степена безбједности дозвољено је само уз обавезну примјену сигурносног рјешења које ће омогућити пренос података одређеног степена безбједности у информациони систем акредитован за рад са безбједним подацима истог или вишег степена безбједности.

13. Управљање приступом ресурсима информационог система

Члан 99.

Субјекти су дужни да успоставе адекватан систем управљања приступом ресурсима информационог система који ће, као минимум, обухватити:

а) дефинисање одговарајућих управљачких, логичких и физичких контрола,

б) управљање корисничким правима приступа који обухвата процесе евидентирања, ауторизације, идентификације и аутентификације, те надзора права приступа,

в) управљање удаљеним приступима.

14. Записи - логови

Члан 100.

(1) Субјекти су дужни, у складу са процјеном ризика, да обезбиједе израду, редовно праћење и чување апликативних и системских записа у сврху откривања неовлашћених приступа и радњи у информационом систему, идентификације проблема, реконструисања догађаја, те утврђивања одговорности.

(2) Апликативни и системски записи морају се чувати централизовано, а у складу са члановима 75. и 76. овог Правилника гдје администратори појединог система немају привилегије надзора над апликативним и системским записима тог систему.

(3) Апликативни и системски записи морају се чувати најмање двије године.

15. Едукација и стручно усавршавање запослених

Члан 101.

(1) Субјекти су дужни да успоставе процес едукације и стручног усавршавања запослених.

(2) У процесу едукације и стручног усавршавања запослених могу се уочити двије карактеристичне групе:

а) група крајњих корисника ресурса информационог система код којих ће бити извршена основна обука о безбједном понашању и коришћењу ресурса информационог система на безбједан начин,

б) група администратора система и инжењера безбједности код којих ће се извршити специјалистичка обука из домена информационе безбједности.

16. Сигурносне копије

Члан 102

(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) Субјекти воде евиденцију информатичких медија на којима су подаци ускладиштени.

Члан 103

(1) Подаци информационог система дневно ускладиштени на информатичке медије одлажу се у најмање једно безбједно складиште у радној просторији субјекта или на другој безбједној локацији.

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

Члан 104.

Субјекти су дужни да успоставе процес управљања сигурносним копијама (енг. *backup*) који укључује процедуре израде сигурносних копија, њиховог складиштења, тестирања рестаурације података са сигурносних копија података, као и адекватан транспорт и предају сигурносних копија, а како би се обезбиједила расположивост података у случају потребе, те омогућио опоравак односно поновна успостава критичних (виталних) пословних процеса у захтијеваном времену.

Члан 105.

(1) Сваки овлашћени администратор обавезан је свакодневно провјеравати исправност дневних сигурносних копија података означених степеном безбједности 3. и више.

(2) Мјесечне, квартално, полугодишње и годишње сигурносне копије података морају се провјеравати најмање једном у периоду до израде нове мјесечне, квартално, полугодишње и годишње сигурносне копије, респективно.

Члан 106.

Подаци снимљени на медијима који требају да буду доступни дуже од животног вијека медија (гледано по спецификацији произвођача) морају да се на истеку половине специфицираног животног вијека медија преносити на други адекватан меморијски медиј да би се осигурало да не дође до губитка података због деградације и/или дезинтеграције меморијског медија.

17. Безбједносни инциденти

Члан 107.

(1) Субјекти су дужни да успоставе процес управљања безбједносним инцидентима, који обухвата дефинисање одговорности и процедура, а који треба омогућити брз и ефикасан одговор у случају нарушавања безбједности информационог система.

(2) Субјекти су дужни, као минимум, да пропишу процедуре за пријављивање, класификацију, праћење и извјештавање о безбједносним инцидентима.

Члан 108.

(1) Субјекти су дужни, у случају тежих безбједносних инцидената, да одмах обавијесте ОИБ о инциденту, његовим посљедицама и предузетим активностима.

(2) Извјештај о безбједносном инциденту, минимално, мора садржавати сљедеће:

а) ако је дошло до компромитације података – опис компромитованих података, укључујући њихову класификацију, датум креирања и аутора,

б) кратак опис околности под којим се безбједносни инцидент догодио, укључујући датум почетка, трајање безбједносног инцидента, као и број и локацију нападача који су безбједносни инцидент узроковали (ако је исте могуће утврдити).

18. Вишеслојна заштита

Члан 109.

(1) Ради ублажавања ризика за информациони систем, низ техничких и нетехничких мјера, организоавних у више слојева заштите, треба бити имплементиран.

(2) Ови слојеви укључују:

а) застрашивање – скуп поступака намијењених за одвраћање потенцијалног нападача,

б) превенцију – скуп поступака намијењених да ометају и блокирају напад на информациони систем,

в) детекцију – скуп поступака намијењених откривању напада на информациони систем,

г) еластичност – скуп поступака намијењених за ограничавање ефекта напада на што је могуће мањи скуп информација и што је могуће мањи дио информационог система,

д) и опоравак – поступци намијењени успостављању сигурне ситуације за информациони систем.

19. Механизми за осигурање података

Члан 110.

(1) Рачунарска опрема која се користи у процесу прикупљања, уноса, обраде, употребе, складиштења, преноса и уништавања безбједних података мора посједовати:

а) механизам за сигурно пријављивање за рад на рачунарској опреми, с могућношћу похране података о пријављивању за рад, како би се приступ рачунарској опреми и подацима могао ограничити и надзирати,

б) механизам за онемогућавање неовлаштеног износа и уноса података употребом преносних медија (дискете, ZIP дискете, CD-ROM, DVD-ROM, USB меморије и др.), комуникационих прикључака и прикључака за испис података,

в) механизам континуираног осигурања и заштите од дјеловања рачунарских вируса и других врста малициозних програма,

г) механизме обезбјеђења безбједних података на тврдим дисковима, на медијима за складиштење података, као и у току размјене истих података на преносним путевима, и то употребом акредитованих криптографских алгоритама и техника, а у складу са члановима 83. и 84. овог Правилника,

д) механизме којима се обезбјеђује јасно видљива ознака степена безбједности података приликом исписа, приказа на монитору, складиштења, преноса и његовог уништавања.

(2) Поред механизама наведених у ставу 1. овог члана, преносни рачунари који се користе у сврхе наведене у ставу 1. овог члана, морају посједовати и мехнизам енкрипције тврдог диска.

Члан 111.

Подаци смјештени на преносним рачунарима морају да буду криптовани те да имају актуелну резервну копију података смјештену у безбједној просторији у субјекту.

20. Коришћење кредендијала за приступ информационом систему

Члан 112.

Запослени у субјекту одговоран је за све активности извршене на рачунарској опреми на радном мјесту употребом његових кредендијала за приступ информационом систему (корисничко име и лозинка, дигитални сертификат на паметној каритци и др.)

Члан 113.

(1) Запослени су обавезни да кредендијале за приступ информационом систему:

а) чувају у тајности,

б) мијењају према дефинисаној Политици безбједности информационог система,

в) мијењају или затраже њихову промјену од надлежног администатора, уколико постоји сумња да је њихова тајност нарушена,

г) користе за потребе за које су им и издати.

(2) Запослени у субјекту не смију користити кредендијале за приступ информационом систему других запослених.

Члан 114.

Запослени у субјекту дужни су извршити одјаву са рачунарске опреме коју користе, уколико престају с радом било на дуже или на краће вријеме, а у складу са Политиком безбједности информационог система.

21. Допуштено и недопуштено коришћење информационог система

Члан 115.

Запослени у субјекту не смију користити информациони систем у сврхе за које он није предвиђен, а посебно за обављање:

а) незаконитих активности,

б) активности противних моралу и друштвеним нормама,

в) активности које могу нанијети штету другим корисницима информационог система,

г) активности за властите или потребе других особа.

Члан 116.

(1) Запослени у субјекту не смију користити приватне фотографске уређаје, уређаја за аудио или видео снимање, приватну ИТ опрему, те преносне медије у просторијама у којима се користе подаци означени 3. степеном безбједности и више.

(2) Употреба службених фотографских уређаја, те уређаја за аудио или видео снимање у просторијама у којима се користе подаци означени 3. степеном безбједности и вишег степена тајности дозвољено је само уз писани налог руководиоца субјекта у чијим се просторијама желе користити наведени уређаји.

(3) Политика безбједности информационог система субјекта може прописати изузетке који се односе на став 1. и став 2. ако се за то укаже потреба.

22. Приступ Интернету

Члан 117.

Приступ Интернету забрањен је на рачунарској опреми која се користи у процесу прикупљања, уноса, обраде, употребе, складиштења, преноса и уништавања безбједних података означених 3. степеном безбједности и више.

Члан 118.

(1) За приступ Интернету запослених у субјекту неопходно је изградити одговарајућу инфраструктуру са могућношћу централизованог надзора и управљања саобраћајем.

(2) Ова инфраструктура мора бити у складу с међународним стандардима и препорукама за исто технолошко подручје.

(3) Забрањено је избјегавати инфраструктуру из става 1. овог члана ради приступа Интернету, успостављањем директне везе с даваоцем услуга приступа Интернету.

Члан 119.

Приступ Интернету дозвољен је запосленим у субјекту у складу с члановима 73., 74., 115. и 116. овог Правилника.

Члан 120.

ИТ опрема субјекта може користити Интернет за повезивање са другим информационим системима у складу с чланом 98. овог Правилника, само уз обавезну примјену рјешења која ће на адекватан начин задовољити све аспекте безбједности података који се размјењују.

23. Коришћење модемских уређаја и телефона

Члан 121

Није дозвољена инсталација и употреба модемских уређаја на рачунарској опреми, уколико постоји могућност прослијеђивања безбједних података похрањених са дате рачунарске опреме или ако постоји могућност слања поменутих података заобилажењем сигурносних механизама информационог система.

Члан 122.

(1) Током телефонског разговора забрањено је размјењивати безбједне податке са саговорником уколико говорна комуникација није заштићена одговарајућим криптографским механизмом.

(2) За потребе осигуране говорне комуникације користе се телефони са криптографском подршком у оквиру постојеће телефонске мреже.

(3) Уколико се телефонским разговором размјењују безбједни подаци забрањено је укључивање разгласа на телефону.

(4) На уређајима за аутоматско примање говорних порука забрањено је остављати поруке које садрже безбједне податке.

IV – ЗАВРШНЕ ОДРЕДБЕ

Члан 123.

Правилник ступа на снагу даном доношења а доставља се свим субјектима из члана 2. овог правилника.

Број:19/6-010/91-23/12
Дана:10.05.2013.године
Бања Лука

МИНИСТАР
Проф. др Јасмин Комић