Фонд здравственог осигурања
Републике Српске
Бања Лука

ПРАВИЛНИК
О МЈЕРАМА ИНФОРМАЦИОНЕ БЕЗБЈЕДНОСТИ У ФОНДУ ЗДРАВСТВЕНОГ ОСИГУРАЊА РЕПУБЛИКЕ СРПСКЕ

Бања Лука, фебруар, 2015. године

На основу члана 2. Закона о информационој безбједности („Службени гласник Републике Српске“, број 70/11) Управни одбор Фонда здравственог осигурања Републике Српске, на I сједници одржаној дана 19.02.2015. године, донио је

ПРАВИЛНИК
О МЈЕРАМА ИНФОРМАЦИОНЕ БЕЗБЈЕДНОСТИ
У ФОНДУ ЗДРАВСТВЕНОГ ОСИГУРАЊА РЕПУБЛИКЕ СРПСКЕ

I - ОСНОВНЕ ОДРЕДБЕ

Члан 1.

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

Члан 2.

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

1) Хардвер - физичка компонента информационог система,
2) Криптографска заштита - систем заштите података и информационих система који осигурава безбједан пренос података кроз рачунарску и телекомуникациону мрежу,
3) Информатички медиј - сваки медиј на којем је могуће преносити или складиштити податке у електронском облику,
4) Безбједно складиште - сеф, каса или други простор за складиштење података опремљен уређајем који спрјечава неовлашћени приступ ускладиштеним подацима,
5) Софтвер - сваки оперативни систем, програм, корисничка и сервисна апликација,
6) Ризик - потенцијални узрок који може нанијети штету податку или информационом систему у којем се користе подаци,
7) 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,
8) 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,
9) Криптована заштита података - примјена програмских рјешења или уређаја за заштиту података који осигуравају повјерљивост, цјеловитости и доступност података,
10) 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),

11) 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,
12) ОИБ - Одјељење за информациону безбједност - одјељење унутар Агенције за информационо друштво које врши непосредан надзор и контролу над провођењем информационе безбједности, и
13) Фонд - Фонд здравственог осигурања Републике Српске.

Члан 3.

(1) Подаци у информационом систему могу имати један од сљедећих степена безбједности:

1) "1. степен безбједности" - одређује се ради спречавања настанка непоправљиве штете по интересе субјекта,
2) "2. степен безбједности" - одређује се ради спречавања настанка изузетно штетне посљедице по интересе субјекта,
3) "3. степен безбједности" - одређује се ради спречавања настанка штете по интересе субјеката,
4) "4. степен безбједности" - одређује се ради спречавања настанка штете за рад, односно обављање задатака и послова субјекта који их је одредио, и
5) "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) Фонд је дужан извршити процјену ризика информационог система која ће као резултат дати класификацију података по нивоима безбједности.

Члан 4.

(1) Административне зоне класификују се на:

1) јавне и
2) 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 5.

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

(2) Степени безбједности сигурних административних зона су:

1) 1. степен безбједности,
2) 2. степен безбједности, и
3) 3. степен безбједности.

Члан 6.

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

1) 1. степен безбједности - ако садржи макар један податак, опрему или ресурс 1. степена безбједности,

2) 2. степен безбједности - ако садржи макар један податак, опрему или ресурс 2. степена безбједности,

3) 3. степен безбједности - ако садржи макар један податак, опрему или ресурс 3. степена безбједности.

Члан 7.

(1) Простор у коме се налазе сервери, мрежна или комуникациона опрема информационог система, организује се као безбједносна и административна зона.

(2) Степен безбједности ових зона одређује податак, опрема или ресурс који се у тој зони налази.

II - ФИЗИЧКА ЗАШТИТА

Члан 8.

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

Члан 9.

(1) Фонд израђује план физичке заштите којим се утврђује потреба спровођења мјера физичке заштите, у складу са стандардима информационе безбједности и у склопу Политике безбједности информационог система.

(2) Надлежни из Фонда 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) Надлежни из Фонда 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 спречавања неовлашћеног изношења података или спречавања уношења недозвољених предмета, којима се може угрозити безбједност података.

Члан 10.

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

(2) Просторије у којима се смјештају меморијски медији са резервним копијама података морају да буду степена безбједности који одговара степену безбједности података који се на медијима налазе, те да задовољавају спецификације произвођача медија за њихово сигурно складиштење.

III - ЗАШТИТА ПОДАТАКА И ИНФОРМАЦИОНОГ СИСТЕМА

Члан 11.

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.

Члан 12.

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

Члан 13.

Сви витални дијелови информационог система Фонда (физички и виртуелни сервери, комуникациона опрема, апликативни сервери, системи за управљање базама података и др.) морају имати задужене администраторе који су одговорни за поузданост и расположивост информационог система.

Члан 14.

(1) 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.

(2) 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, уређајима и софтверским алатима.

Члан 15.

Сви информациони системи који се користе за пренос и размјену безбједних података морају бити осигурани средствима који обезбјеђују адекватну криптографску заштиту.

Члан 16.

(1) Фонд је дужан усвојити и имплементирати Политику безбједности информационог система (у даљем тексту: Политика безбједности) која се налази у Прилогу број 1 и чини саставни дио овог правилника.

(2) Политика безбједности представља основ за управљање безбједношћу информационог система субјеката.

(3) Политика безбједности треба, минимално, да садржи сљедеће документе и то:

1) Политика класификације информација односно података,
2) Политика управљања ризицима,
3) Политика контроле приступа,
4) E-mail политика,
5) Политика енкрипције,
6) Политика приступа интернету,
7) Политика креденцијала за аутентикацију,
8) Политика физичке безбједности,
9) Политика удаљеног приступа,
10) Безбједносна политика сервера,
11) Безбједносна политика мрежних уређаја,
12) Безбједносна политика опреме и ДМЗ,
13) VPN политика,
14) Екстранет политика,
15) Политика бежичне комуникације,
16) Политика радних станица,
17) Политика провјере рањивости,
18) Политика одговора на безбједносне инциденте,
19) Безбједносна политика мобилних уређаја, и
20) Анти-Вирус политика.

Члан 17.

Фонд је дужан именовати лице или лица одговорна за функцију безбједности информационог система, те дефинисати њихова овлашћења и одговорности.

Члан 18.

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.

Члан 19.

Фонд је дужан обезбједити да апликативни софтвер има уграђене контроле исправности, потпуности и конзистентности података који се уносе, мијењају, обрађују и генеришу.

Члан 20.

(1) Фонд је дужан да дефинише и имплементира процедуре управљања документацијом (техничком, функционалном, корисничком и др.) која се односи на информациони систем.

(2) Фонд је дужан да, као минимум, обезбиједи:

1) постојање тачне, потпуне и ажурне документације изведеног стања свих сегмената информационог система,
2) постојање тачних, потпуних и ажурних корисничких упутстава за све сегменте информационог система, и
3) приступ запослених документацији, а у складу са њиховим пословним потребама и класификацији безбједности.

Члан 21.

Фонд је дужан да успостави адекватан систем управљања приступом ресурсима информационог система који ће, као минимум, обухватити:

1) дефинисање одговарајућих управљачких, логичких и физичких контрола,

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

3) управљање удаљеним приступима.

Члан 22.

(1) Фонд је дужан, у складу са процјеном ризика, да обезбиједи 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 најмање 2 године.

Члан 23.

(1) Фонд је дужан да успостави процес едукације и стручног усавршавања запослених.

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

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

2) група администратора система и инжењера безбједности код којих ће се вршити континуирано специјалистичка обука из домена информационе безбједности.

Члан 24.

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

(2) Фонд води евиденцију информатичких медија на којима су подаци ускладиштени.

Члан 25.

Фонд је дужан да успостави процесе управљања сигурносним копијама (eng. kaskir) 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 26.

Сваки овлашћени администратор обавезан је свакодневно провјеравати исправност дневних сигурносних копија.

Члан 27.

(1) Фонд је дужан да успостави 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) Фонд је дужан, као минимум, да пропише процедуре за пријављивање, класификацију, праћење и извјештавање о безбједносним инцидентима.

Члан 28.

Запослени у Фонду одговорни су за све активности извршене на рачунарској опреми на радном мјесту употребом његових креденцијала за приступ информационом систему (корисничко име и лозинка, дигитални сертификат на паметној каритци и др.)

Члан 29.

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

1) чувају у тајности,

2) мијењају према дефинисаној Политици безбједности,

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

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

(2) Запослени у Фонду не смију користити креденцијале за приступ информационом систему других запослених.

Члан 30.

Запослени у Фонду 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.

Члан 31.

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

1) незаконитих активности,
2) активности противних моралу и друштвеним нормама,
3) активности које могу нанијети штету другим корисницима информационог система, и
4) активности за властите или потребе других особа.

IV - СПРОВОЂЕЊЕ ИНФОРМАЦИОНЕ БЕЗБЈЕДНОСТИ

Члан 32.

Стручни надзор и контролу спровођења информационе безбједности врши Агенција за информационо друштво Републике Српске.

Члан 33.

Фонд је дужан спроводити интерну ревизију безбједносних аспеката информационог система.

Члан 34.

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

(2) Фонд је дужан да, уз захтјев, достави ОИБ-у сљедеће документе:

1) Приједлог одлуке о именовању екстерног ревизора,
2) Нацрт уговора са екстерним ревизором,
3) Референце екстерног ревизора о обављеним ревизијама,
4) Референце и стручне квалификације запослених екстерног ревизора који ће обављати ревизију.

V - ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 35.

Измјене и допуне овог правилника врше се на начин и по поступку који је предвиђен за његово доношење.

Члан 36.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли Фонда, а објавиће се и на Интернет страници Фонда.

Члан 37.

Ступањем на снагу овог правилника престаје да важи Правилник о сигурности информационог система Фонда здравственог осигурања Републике Српске, број 01/015-1308/09 од 03.03.2009. године.

Број: 02/002-1228-11/15
19. фебруара 2015. године
Бања Лука

Предсједник Управног одбора

Оливера Марковић, дипл. економиста