Члан 2.

Накнаде за послове из члана 1. ове одлуке (у даљем тексту: накнаде) МКО, односно друго правно или физичко лице уплаћују на рачун Агенције.

Члан 3.

Управни одбор и директор МКО, односно друго правно или физичко лице које подноси захтјев за издавање дозволе за рад МКО или захтјев за друге сагласности или мишљења одговорни су за плаћање накнаде.

Члан 4.

(1) Накнаде Агенција наплаћује по сљедећој тарифи:

1) Накнаде које је МКО дужна да плаћа за надзор свог пословања састоје се од сљедећих елемената:

1. годишњег линеарног дијела, који је једнак за сва микрокредитна друштва (у даљем тексту: МКД) у износу од 6.000,00 КМ, а за микрокредитне фондације (у даљем тексту: МКФ) у износу од 3.000,00 КМ, које се уплаћују у једнаким тромјесечним (календарским) ратама најкасније до посљедњег дана текућег тромјесечја за текуће тромјесечје, и

2. тромјесечног варијабилног дијела у висини од 0,15 промила износа укупне активе биланса стања МКО на посљедњи дан претходног тромјесечја, који се уплаћује заједно са дијелом из подтачке 1. ове тачке.

2) Накнада за обраду захтјева за издавање дозвола за рад и друге сагласности и мишљења наплаћује се како слиједи:

1. за оснивање и рад МКД у износу од 6.000,00 КМ,

2. за оснивање и рад МКФ у износу од 3.000,00 КМ,

3. за издавање дозволе за статусну промјену МКО (спајање, припајање и подјела) у износу од 3.000,00 КМ,

4. за оснивање и промјену адресе сједишта организационих дијелова МКО у износу од 500,00 КМ,

5. за издавање сагласности Агенције за именовање спољног ревизора за ревизију годишњих извјештаја, за МКД у износу од 500,00 КМ, а за МКФ у износу од 200,00 КМ,

6. за издавање сагласности на оснивачке акте МКО у износу од 1.000,00 КМ, а накнада за на измјене и допуне истих аката износи 500,00 КМ,

7. накнаде за издавање осталих сагласности, мишљења, те вршење других сличних послова за МКД у износу од 400,00 КМ и за МКФ у износу од 200,00 КМ.

Члан 5.

Даном ступања на снагу ове одлуке престаје да важи Одлука о висини накнада које се плаћају у поступку пред Агенцијом за банкарство Републике Српске ("Службени гласник Републике Српске", број 3/07).

Члан 6.

Ова одлука објавиће се у "Службеном гласнику Републике Српске" по добијању сагласности Владе Републике Српске и ступа на снагу осмог дана од дана објављивања.

Број: УО-41/18
24. септембра 2018. године
Бањалука

Предсједник
Управног одбора,
Братољуб Радуловић, с.р.

Фонд здравственог осигурања Републике Српске

На основу члана 30. Статута Фонда здравственог осигурања Републике Српске ("Службени гласник Републике Српске", бр. 6/04, 19/05, 63/08, 64/09, 105/09, 119/11, 113/14 и 30/16), а у складу са чланом 7. став 3. Уредбе о Интегрисаном здравственом информационом систему ("Службени гласник Републике Српске", број 30/17), в.д. директора Фонда здравственог осигурања Републике Српске д о н и о ј е

У П У Т С Т В О

О ФУНКЦИОНИСАЊУ, УПРАВЉАЊУ РИЗИКОМ И БЕЗБЈЕДНОШЋУ ИНТЕГРИСАНОГ ЗДРАВСТВЕНОГ ИНФОРМАЦИОНОГ СИСТЕМА

I - ОСНОВЕ ОДРЕДБЕ

1. Овим упутством утврђују се начин функционисања, те управљање ризиком и безбједношћу ИЗИС-а којима се обезбјеђује основна заштита података на физичком, техничком и организационом нивоу.

2. Поједини изрази који се користе у овом упутству 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 спречава 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, опремљено техничким уређајима којима се спречава 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 неовлашћеним 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 спровођењем информационе безбједности,

13) Фонд, ФЗО - Фонд здравственог осигурања Републике Српске,

14) ИЗИС - Интегрисани здравствени информациони систем.

II - ФУНКЦИОНИСАЊЕ ИЗИС-а

II - 1 - Основна структура система

3. Интегрисани здравствени информациони систем (ИЗИС) чине информациони системи:

1) здравствених установа,

2) Фонда и

3) других правних лица која у свом пословању сарађују са системом здравствене заштите и са Фондом успостављају сарадњу у овом питању.

4. ИЗИС се дјели на сљедеће подсистеме:

1) Централни апликативни система са подсистемима:

- подсистем примарне здравствене заштите,

- подсистем консултативно-специјалистичке заштите (примарни и ванболнички),

- болничко-клинички подсистем;

2) Централни интеграциони систем са подсистемима:

- подсистем електронског здравственог картона (подсистем за електронску размјену здравствених података),

- подсистем електронских упутница,

- подсистем електронских рецепата,

- подсистем за електронску размјену немедицинских података;

3) подсистем за приступ медицинским подацима од стране пацијента;

4) подсистем за администрацију ИЗИС-а, који чине:

- подсистем управљања ресурсима и шифарницима,

- подсистем управљања и подршке корисницима здравствене заштите,

- подсистем за извјештаје и бизнис интелигенцију,

- подсистем лабораторијске и радиолошке дијагностике,

- подсистем електронске здравствене картице и картице здравственог радника.

II - 2 - Администрација и управљање ИЗИС-ом

5. Администрацију, управљање и развој ИЗИС-а врши Фонд, који представља централно мјесто за размјену медицинских података те обављања кључних улога као што су генерисање, похрањивање те размјена медицинских података између свих установа које ће користити ИЗИС.

6. Задаци при администрацији и управљању ИЗИС-ом су:

1) управљање Дата центром - примарном и секундарном локацијом,

2) обезбјеђивање поузданости и доступности цјелокупног система,

3) обезбјеђивање функционалности, капацитета и перформанси система неопходних за пружање адекватне подршке пословним процесима здравствених установа,

4) централизовано управљање апликацијама, регистрима и шифарницима,

5) контрола приступа, поступања и коришћења медицинских података,

6) обезбјеђивање сервиса за размјену медицинских и осталих података,

7) пружање неопходне стручне помоћи корисницима ИЗИС-а.

II - 3 - Колектовање података

7. Извор података су здравствене установе, које у склопу свог рада колектују неопходне податке. Начин колектовања, тј. прикупљања података, могућ је на два начина:

1) користећи апликације Централног апликативног система,

2) користећи сервисе Централног интеграционог система.

8. Централни апликативни систем састоји се од одређеног броја апликација које у склопу рада појединих подсистема омогућавају колектовање података. Апликације Централног апликативног система ИЗИС-а намијењене су здравственим установама које немају или имају неадекватне постојеће информационе системе.

9. За установе које задржавају сопствени информациони систем у употреби Фонд обезбјеђује адекватне сервисе за интеграцију са ИЗИС-ом те сву неопходну стручну помоћ путем Централног интеграционог система ИЗИС-а.

II - 4 - Формирање и управљање регистрима

10. Систем обезбјеђује успостављање и одржавање сљедећих регистара и шифарника, који представљају основ система и формирају се на нивоу цјелокупног здравственог система:

1) јединствени регистар корисника здравствене заштите, који укључује све резиденте (engl. Master Patient Index),

2) јединствени регистар здравствених установа са организационом структуром - укључујући и приватне здравствене установе и установе које обезбјеђују здравствену заштиту у складу са Законом о извршењу кривичних санкција Републике Српске,

3) јединствени регистар здравствених радника,

4) јединствени регистар тимова породичне медицине,

5) јединствени регистар обољелих од болести од већег јавно-здравственог значаја,

6) јединствени регистар уплатилаца доприноса,

7) јединствени регистар тимова специјалиста,

8) јединствени регистар занимања у здравству,

9) јединствени регистар медицинских услуга и процедура (DRG ACHI),

10) јединствени регистар медицинских уређаја и апарата,

11) јединствене класификационе системе (шифарнике) лијекова (ATC), медицинског и санитетског материјала,

12) јединствени класификациони систем (шифарник) дијагноза МКБ-10,

13) шифарник основа осигурања,

14) шифарник пројеката у здравству.

11. За регистре и шифарнике за које је могуће системско повезивање омогућени су аутоматизован унос, креирање и ажурирање података путем веб-сервиса, док за остале регистре систем обезбјеђује унос, креирање и ажурирање ових података кроз апликативни модул ИЗИС система.

12. Регистри и шифарници треба да буду документовани релевантном пратећом документацијом која описује њихов садржај и структуру.

13. Свака ставка у регистру или шифарнику мора да има један и само један јединствени код који је идентификује. Уколико се шифарник или регистар преузима од надлежне институције, саставни дио регистра је и јединствени идентификатор институције из које се преузима.

II - 5 - Функционисање Централног апликативног система

14. Централни апликативни систем ИЗИС-а састоји се од апликација:

1) примарне здравствене заштите,

2) консултативно-специјалистичке заштите (примарни и ванболнички),

3) болничко-клиничког подсистема,

4) подсистема за администрацију.

II - 5.1 - Функционисање апликација

15. За функционисање, даљи развој и унапређење апликација Централног апликативног система ИЗИС-а, те техничку администрацију апликативних сервера врши Фонд.

II - 5.2 - Приступ апликацијама и идентификација корисника

16. Омогућавање приступа здравствених установа апликацијама врши Фонд на основу писменог захтјева установе, а у складу са Процедуром за размјену података Фонда.

17. Омогућавање приступа састоји се од комуникационог увезивања, те креирања приступних параметара надлежног администратора.

18. Даље управљање приступом корисника здравствене установе појединим апликацијама врши надлежни admini-

стратор здравствене установе уз дефинисање и додјељивање јасних права над појединим апликацијама, а све у складу са Упутством за делегирану администрацију.

19. Приступ корисника апликацијама могућ је на два начина:

1) преко корисничког имена и шифре и

2) користећи картицу здравственог радника.

20. Обје врсте приступа засноване су на тзв. SSO приступу (Single sign-on), односно процесу аутентикације сесије корисника који дозвољава да се само једним уношењем приступних параметара изврши логовање у више апликација.

II - 5.3 - Размјена података кроз апликације

21. Права на податке, те даља размјена података, између подсистема Централног апликативног система ИЗИС-а врши се на основу надлежности корисника и здравствене установе уз дефинисање јасних права на податке на основу којих се врши сва даља размјена.

22. Права на податке, демографске и медицинске има изабрани доктор породичне медицине. Даља права, у процесу лијечења на наведене податке, имају надлежна установа и доктори унутар наведене установе у коју је пацијент упућен, а на основу важеће и активне електронске упутнице у подсистему е-Упутнице.

II - 6 - Функционисање Централног интеграционог система

23. Централни интеграциони систем ИЗИС-а састоји се од сљедећих подсистема:

1) подсистем електронског здравственог картона (подсистем за електронску размјену здравствених података),

2) подсистем електронских упутница,

3) подсистем електронских рецепата,

4) подсистем за електронску размјену немедицинских података.

II - 6.1 - Приступ систему и интеракција са независним системима

24. Омогућавање приступа систему од стране здравствених установа које задржавају сопствени информациони систем у употреби врши Фонд на основу писменог захтјева институције, а у складу са Процедуром за размјену података Фонда.

25. Омогућавање приступа састоји се од комункационог увезивања, евидентирања здравствене установе у јединственом регистру здравствених установа, одређујући при томе јединствени идентификатор здравствене установе на нивоу система. Евидентирање установе у регистру врше администратори Фонда.

26. За идентификацију здравствене установе при размјени података користи се јединствени идентификатор.

II - 6.2 - Размјена података

27. Размјена података између Центра за размјену здравствених информација и здравствене институције врши се преко подсистема електронског здравственог картона.

28. Све здравствене институције које користе локалне здравствене информационе системе преносе информације у ИЗИС путем централног подсистема за електронску размјену здравствених информација коришћењем HL7 стандарда (CDA R2).

29. Подсистем електронског здравственог картона подржава спремање и обраду минимално сљедећих клиничких докумената:

1) извјештај о прегледу на примарном нивоу,

2) извјештај о ванболничком/амбулантном лијечењу,

3) извјештај о хоспитализацији,

4) упутница,

5) рецепт.

30. Подсистем електронског здравственог картона подржава преузимање сажетка медицинских података пацијента из EZK у реалном времену (eng. On-demand option).

31. Подсистем електронског здравственог картона подржава претрагу и преузимање појединачних докумената регистрованих у Регистру докумената (Document Registry).

32. Подсистем електронског здравственог картона омогућава дохватање појединачних докумената из Регистра докумената (Document Repository).

II - 6.3 - Приступ пацијента подацима

33. Приступ подацима од стране пацијента врши се путем Подсистема за приступ медицинским подацима од стране пацијента.

34. Подсистем за приступ медицинским подацима пацијента омогућава:

1) веб базиран приступ порталу те приступ кроз мобилну апликацију,

2) приступ свим веб-страницама кроз јединствено пријављивање на систем (SSO - Single Sign On),

3) слање информација осигураницима путем e-mail порука,

4) приступ носиоцу осигурања својим члановима уже породице (дјеца и супружници), те претрагу и преглед свих медицинских података за своје чланове породице,

5) портал са веб базираним интерфејсом, компатибилан са тренутно најзаступљенијим веб-претраживачима: IE, Google Chrome, Mozilla Firefox i Safari.

35. Омогућавање приступа наведеном подсистему врши се пријавом за наведени подсистем од стране пацијента. Пријавом се одређују приступни параметри који се достављају на e-mail пацијента.

III - УПРАВЉАЊЕ БЕЗБЈЕДНОШЋУ

36. Подаци у ИЗИС-у 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.

37. Фонд је дужан да изврши процјену ризика података ИЗИС-а. Процјена ће као резултат дати документ под називом Политика класификације података, која ће бити укључена у Политику безбједности ИЗИС-а, са посебном пажњом на заштиту личних података корисника који се користе у раду ИЗИС-а. Лични подаци корисника квалификују се као подаци 3. степена безбједности.

38. Административне зоне класификују се на:

1) јавне и

2) сигурне.

39. Јавним се класификују административне зоне у којима се или у чијој се непосредној близини налазе само јавни подаци. Као сигурним класификују се административне зоне које нису јавне.

40. Сигурне административне зоне додатно се класификују по степену безбједности.

41. Степени безбједности сигурних административних зона су:

1) 1. степен безбједности,

2) 2. степен безбједности и

3) 3. степен безбједности.

42. Степен безбједности административне зоне одређују 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.

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

44. Степен безбједности ових зона одређују податак, опрема или ресурс који се у тој зони налази.

III - 1 - Физичка заштита

45. 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.

46. 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.

47. 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.

48. Надлежни из Фонда 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.

49. 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.

50. 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 - 2 - Заштита података и информационог система

51. Корисницима ИЗИС-а биће дате само привилегије неопходне за приступ подацима неопходним за обављање њиховог посла, а с циљем ограничавања штете која може настати услед безбједносних инцидената, грешака или неауторизоване употребе података и ресурса информационог система.

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

53. Сви витални дијелови информационог система ИЗИС-а (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.

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

55. 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.

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

57. Фонд је дужан усвојити и имплементирати Политику безбједности ИЗИС-а (у даљем тексту: Политика безбједности). Политика безбједности као Прилог бр. 1 овог упутства је јавно објављена и доступна на веб-страници Фонда.

Фонд је дужан упознати све запослене са Политиком безбједности.

58. Политика безбједности представља основ за управљање безбједношћу ИЗИС-а.

59. Политика безбједности треба, минимално, да садржи сљедеће документе:

1) политика класификације информација, односно података (Политика класификације 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 DMZ,

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) антивирус политика.

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

61. 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.

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

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

64. 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.

65. 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.

66. 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. Апликативни и системски записи морају се чувати најмање двије године.

67. Фонд је дужан да успостави процес едукације и стручног усавршавања администратора унутар Фонда и здравствених установа.

68. У процесу едукације и стручног усавршавања могу се уочити двије карактеристичне групе:

1) група администратора здравствених установа код којих ће бити извршена основна обука о безбједном понашању и коришћењу ресурса информационог система на безбједан начин и

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

69. Базе података обавезно се складиште на преносиве информатичке медије најмање једном дневно, седмично, мјесечно и годишње за потребе обнове базе података. Фонд води евиденцију информатичких медија на којима су подаци ускладиштени.

70. Фонд је дужан да успостави процесе управљања сигурносним копијама (eng. 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.

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

72. 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.

73. Фонд прописује процедуре за пријављивање, класификацију, праћење и извјештавање о безбједносним инцидентима.

74. Корисници ИЗИС-а приликом повезивања морају обезбиједити минимум сљедећих захтјева:

1) усвајање Политике информационе безбједности од стране других лица,

2) именовање особе задужене за информациону безбједност других лица,

3) усалгашеност Политике информационе безбједности других лица са Политиком безбједности ИЗИС-а.

75. Корисници ИЗИС-а су дужни усагласити Политике информационе безбједности са Политиком безбједности ИЗИС-а у сљедећим политикама:

1) политика класификације података – подаци које екстерни информациони системи размјењују са информационим системом Фонда морају бити класификовани у исте степене безбједности,

2) политика прихватљивог коришћења,

3) политика управљања ризицима,

4) политика одговора на безбједносне инциденте.

76. Корисници ИЗИС-а 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 картици и др.).

77. Корисници ИЗИС-а 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 администратора уколико постоји сумња да је њихова тајност нарушена,

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

5) корисници ИЗИС-а не смију користити креденцијале за приступ информационом систему других запослених.

78. Корисници ИЗИС-а 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.

III - 3 - Спровођење информационе безбједности

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

80. Фонд је дужан спроводити интерну ревизију безбједносних аспеката информационог система.

81. 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).

82. 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 и

4) референце и стручне квалификације запослених екстерних ревизора који ће обављати ревизију.

IV - УПРАВЉАЊЕ РИЗИКОМ

IV - 1 - Управљање сигурносним ризиком

83. Сигурносни ризик представља могућност реализације неког нежељеног догађаја, који може негативно утицати на повјерљивост, интегритет и расположивост информационих ресурса ИЗИС-а (хардвер, софтвер, људски ресурси, подаци и сл.). Управљање ризиком дефинише се као процес идентификације оних фактора који могу негативно утицати на повјерљивост, интегритет и расположивост рачунарских ресурса и њихова анализа у смислу вриједности појединих ресурса и трошкова њихове заштите.

84. Процес управљања сигурносним ризицима састоји се и спроводи у три фазе:

1) процјена ризика,

2) умањивање ризика и

3) испитивање и анализа.

85. Фонд именује лица задужена за процес управљања сигурносним ризицима те дефинише њихова овлашћења и одговорности. Лица одговорна за процес управљања сигурносним ризицима треба да редовно извјештавају руководиоца о стању и активностима везаним за наведени процес.

IV - 2 - Процјена ризика

86. Лица одговорна за управљање ризиком процес процјене ризика спроводе у девет корака:

1) идентификација и класификација ресурса,

2) идентификација пријетњи,

3) идентификација рањивости,

4) анализа постојећих контрола,

5) вјероватноћа појаве нежељених догађаја,

6) анализа посљедица,

7) одређивање ризика,

8) препоруке за умањивање и

9) документација.

87. Након спроведених наведених корака добијени резултати у форми извјештаја предају се менаџменту Фонда, који на темељу изнесених резултата доноси одлуке о томе који ће се ризик умањивати и на који начин, а који ће се прихватити онаквим какав јесте.

88. Извјештај се предаје у јасној и пажљиво структурираној форми, како би резултати били што прегледнији и једноставнији за интерпретацију.

IV - 3 - Умањивање ризика

89. Након процеса процјене ризика, на основу добијеног извјештаја, стручне службе Фонда врше даљу анализу и евалуацију те имплементацију одговарајућих сигурносних контрола.

90. Опције за управљање ризиком су:

1) умањивање ризика - подразумијева имплементацију одговарајућих сигурносних контрола с циљем умањивања идентификованог ризика,

2) трансфер ризика - ризик и трошкови у случају његове реализације пребацују се некој другој организацији,

3) прихватање ризика - поступак којим се ризик прихвата као такав без имплементације икаквих сигурносних контрола. Уколико cost/benefit анализе покажу да је већи трошак улагати у заштиту ресурса него што представља његов губитак, тада се примјењује овај приступ. Одлука о прихватању ризика повлачи велику одговорност и редовно захтијева писмено извјештавање о томе ко је одговоран и зашто контроле нису имплементиране,

4) одбацивање ризика - приступ који подразумијева потпуно занемаривање сигурносног ризика. Оповргавање или свјесно игнорисање ризика у нади да он никада неће бити реализован потпуно је неприхватљив приступ и не смије се спроводити нити у једном случају.

91. О примјени неких од описаних приступа одлучује менаџмент Фонда. Умањивање ризика приступ је који се примјењује у већини ситуација. Имплементацијом одговарајућих сигурносних контрола и механизама, прихватљивих са финансијског и техничког становишта, сигурносни ризик своди се на прихватљив ниво. Ризик који остаје након имплементације сигурносних контрола назива се резидуалним ризиком и он подразумијева све оне пријетње и рањивости за које се сматра да не захтијевају додатни третман у погледу умањивања постојећег ризика. Присутност резидуалног ризика посљедица је спроведених cost/benefit анализа којима је установљено да су трошкови заштите већи од трошкова у случају његове реализације.

IV - 4 - Методологија руковања ризицима

92. Ризик се уклања по приоритету. Приоритет ризика одређује се на основу степена безбједности података који могу бити погођени и на основу cost/benefit анализе.

Прво се имплементирају рјешења која су финансијски најприхватљивија, а резултоваће што квалитетнијим поузданим сигурносним контролама са минималним утицајем на мисију и пословне процесе.

93. Умањивању ризика потребно је приступити методолошки, са добро разрађеним и еволуираним рјешењима и спроводи се у седам фаза, чије спровођење резултира квалитетнијом и ефикаснијом имплементацијом сигурносних контрола:

1) одређивање приоритетних акција,

2) евалуација препоручених сигурносних контрола,

3) анализа добијеног и уложеног,

4) одабир сигурносних контрола,

5) подјела одговорности,

6) израда плана за имплементацију сигурносних контрола,

7) имплементација контрола.

IV - 5 - Испитивање и анализа

94. Испитивање и анализу, односно процјену ризика потребно је радити једном годишње. У случају учесталих промјена на систему или у току периода имплементације, процјену ризика потребно је радити чешће, односно сваких шест мјесеци.

V - ЗАВРШНЕ ОДРЕДБЕ

95. Ово упутство ступа на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Српске".

Број: 01/004-8477/18
7. септембра 2018. године
Бањалука

В.д. директора,
Дејан Кустурић, с.р.

Друштво за управљање Пензијским резервним фондом Републике Српске а.д. Бања Лука

На основу члана 31. Закона о Пензијском резервном фонду ("Службени гласник Републике Српске", бр. 73/08, 50/10, 120/12 и 20/18), члана 12. Закона о министарским, владиним и другим именовањима Републике Српске ("Службени гласник Републике Српске", број 41/03) и чл. 22. и 24. Статута Друштва за управљање Пензијским резервним фондом Републике Српске а.д. Бања Лука ("Службени гласник Републике Српске", бр. 65/10, 62/11, 111/12 и 83/18), те члана 10. Пословника о раду Надзорног одбора Друштва за управљање Пензијским резервним фондом Републике Српске а.д. Бања Лука, Надзорни одбор Друштва за управљање Пензијским резервним фондом Републике Српске а.д. Бања Лука, на сједници одржаној 18.10.2018. године, д о н о с и

Р Ј Е Ш Е Њ Е

О РАЗРЈЕШЕЊУ ВРШИОЦА ДУЖНОСТИ ЧЛАНА УПРАВЕ ДРУШТВА ЗА УПРАВЉАЊЕ ПЕНЗИЈСКИМ РЕЗЕРВНИМ ФОНДОМ РЕПУБЛИКЕ СРПСКЕ АД БАЊА ЛУКА (ДИРЕКТОРА) И ИМЕНОВАЊУ ЧЛАНА УПРАВЕ ДРУШТВА ЗА УПРАВЉАЊЕ ПЕНЗИЈСКИМ РЕЗЕРВНИМ ФОНДОМ РЕПУБЛИКЕ СРПСКЕ АД БАЊА ЛУКА (ДИРЕКТОРА)

1. Разрјешава се вршиоца дужности члана Управе - директора Друштва за управљање Пензијским резервним фондом Републике Српске а.д. Бања Лука Милош Грујић, због окончања поступка избора и коначног именовања директора Друштва за управљање Пензијским резервним фондом Републике Српске а.д. Бања Лука.

2. За члана Управе Друштва за управљање Пензијским резервним фондом Републике Српске а.д. Бања Лука - директора Друштва за управљање Пензијским резервним фондом Републике Српске а.д. Бања Лука именује се Милош Грујић.

3. Мандат лица из тачке 1. овог рјешења врши се на период од пет година, почевши од дана ступања на снагу овог рјешења.

4. Ово рјешење ступа на снагу наредног дана од дана објављивања у "Службеном гласнику Републике Српске".

Број: 01-НО9Р-4/18
18. октобра 2018. године
Бањалука

Предсједник,
Сања Рашевић, с.р.

Казнено-поправни завод Фоча

На основу члана 15. став 1. Закона о извршењу кривичних санкција Републике Српске ("Службени гласник Републике Српске", број 63/18), в.д. директора Казнено-поправног завода Фоча, уз Сагласност министра правде Републике Српске, број: 08.030/020-2853/18, од 9.10.2018. године, д о н о с и