На основу Закона о информационој безбједности („Службени гласник Републике Српске“ број 70/11), члана 82, став 2, Закона о републичкој управи („Службени гласник Републике Српске“ број 118/08, 11/09, 74/10, 86/10, 24/12 I 121/12), Правилника о стандардима информационе безбједности број: 19/6-010/91-23/12 (којим се утврђују минимални стандарди информационе безбједности и обезбјеђује основна заштита података на физичком, техничком и организационом нивоу), Правилника о општим условима чувања документарне грађе у дигиталном облику и посебним условима чувања специфичне документарне грађе („Службени гласник Републике Српске“ број 64/12), захтјева стандарда серије ISO/IEC 27001:2005 (тачка 4.2.1 б) и А 15.1.1, Одлуке о почетку активности на обухвату и похрањивању података у дигиталној форми и изради безбједносне политике информационог система број 16-051-158-1/15 од 11.03.2015.године и Рјешења министра о именовању лица одговорних за функцију безбједности информационог система и чланова радне групе за информациону безбједност број 16-051-158/15 од 11.03.2015.године, министар рада и борачко-инвалидске заштите доноси сљедећи документ:

Политика система управљања информационом безбједности

I.

Овим документом утврђује се смјер, принципи и основна правила везана за систем управљања информационом безбједности у Министарству рада и борачко-инвалидске заштите а сваки документ који има обавезујућу снагу уписује се на начин исказан у табелама које слиједе.

Табела 1. (Статус верзије документа)

Верзија документа:	0.1
Датум верзије:	23.03.2015.
Израдио:	
Одобрио:	
Степен тајности:	Интерно

Табела 2. (Евиденција промјена на документу)

Датум	**Верзија**	**Израдио**	**Опис промјена**
18.03.2015.	0.1		Радни нацрт документа

II.

У складу са тачком 1. Овог документа утврђује се начин смјер, принципи и основна правила везана за систем информационе безбједности, а кроз разраду садржаја.

1. Сврха, подручје примјене и корисници

Сврха ове политике је да се пропише смисао, смјер, принципи и основна правила везана за систем управљања информационом безбједности на начин да:

- заштити информације као реусрс и имовину Министарства од свих опасности и пријетњи како спољашњих, тако и унутрашњих, било да је ријеч о случајним или намјерним пријетњама,
- обезбједи сигурну подјелу информација,
- омогући цјеловиту и прифесионалну употребу информација,
- обезбједи да сваки корисник информација разумије своју улогу у процесу употребе и заштите информација,
- обезбједи континуитет пословања и могућу штету сведе на минимум,
- заштити министарство од законске одговорности и неодговарајуће употребе информација.

Овај документ представља оквир за управљање информационом безбједности унутар Министарства рада и борачко инвалидске заштите Републике Српске (у даљем тексту: Министарство) и примјењује се на цјелокупан систем управљања информационом безбједности у Министарству.

Политика система управљања информационом безбједности је документ највишег нивоа у СУБИ, високог степена повјерљивости, која је усвојила одређени број контролних механизама како би омогућила безбједност информација. Овим документом су утврђена мининална обавезујућа правила и прописи који се односе на општа начела поступања, доступа, обраде, чувања, преноса и уништења информационим података унутар Министарства, што укључујњ на примјер, податке о запосленима, податке о корисницима, уговоре, планове, статистичке податке итд.

Корисници овог документа су сви запослени радници министарства, као и све спољне стране које имају одређену улогу у процесима везаним за дјелатност министарства и сва друга лица која учествују у процесу успостављања и имплементације система информационе безбједности. Све одредбе које се односе на лица, а записана су у мушком облику, користе се као неутрална, тј. односе се и на женски и на мушки пол.

2. Референтни документи

- Стандарди серије ISO/IEC 27001 тачка 4.2.1 б) и А 15.1.1,
- Одлука о обиму и границама система информационе безбједности,
- Методологија за процјену ризика,
- Попис статутарних, регулаторних и уговорних обавеза
- Процедура за управљање инцидентима.

3. Основни појмови информационе безбједности

Повјерљивост – карактеристика информација да нису доступне неовлаштеном кориснику, ентитету или процесу;

Расположивост – карактеристика информација и ресурса да су доступни и употребљиви за овлаштене кориснике, онда када су потребни;

Цјеловитост- особнина информација да је осигурана њихова тачност и потпуност;

Информациона безбједност – обезбјеђење повјерљивости, доступности (расположивости) и цјеловитости (интегритета) информација;

Систем управљања информационом безбједности – дио цјелокупног система управљања у некој организацији, заснован на управљању пословним ризицима, који има задатак да се брине о успостављању, имплементацији, редовном управљању, контроли, одржавању и побољшавању безбједности информација (информационе безбједности);

Ресурс – нешто што је важно и вриједно за неку организацију;

Ризик – комбинација вјероватноће неког догађаја и његових посљедица;

Пријетња – потенцијално изазивање нежељеног инцидента, који може резултирати оштећењем система, организације, или неког њиховог дијела;

Рањивост – слабост неког ресурса која може бити искоришћена од стране једног или више извора пријетње;

3.1 Циљеви

Циљеви политике система управљања информационом безбједности су:

- спречавање неовлаштеног доступа до информационих средства и информација, њиховог уништења, отуђења или откривања неовлашћеним лицима усљед неукости или немара,

- обезбјеђење повјерљивости и цјеловитости информација, програмске опреме, мрежних услуга и подршке инфраструктуре,

- стављање на располагање информација и ресурса потребних овлашћеним лицима,

- обезбјеђење примјереног нивоа безбједности цјелокупне инфраструктуре, запослених и информација, односно доступа до њих,

- подизање нивоа свијести запослених и њихово стално оспособљавање у вези са информационом безбједношћу,

- смањивање опасности од људских грешака, крађе, преваре или злоупотребе уређаја, бебједносних инцидената и кварова,

- обазбјеђење усаглашености са захтјевима позитивног законодавства Републике Српске, БиХ и законодавства ЕУ,

- усвајање и провођење добре праксе у области заштите информација.

Усвајањем Политике система управљања информационом безбједности пословодство Министарства је показало запосленима и осталим заинтересованим странама опредјељеност за рјешавање безбједносних питања. Сви запослени морају бити упознати са овом Политиком и њеним циљевима, оспособљени да правилно и ефикасно извршавају своје задатке у вези са безбједношћу информационих ресурса Министарства.

3.2 Захтјеви везани за информациону безбједност

Ова политика и цјелокупан систем информационе безбједности морају бити усаглашени са примјенљивим законским прописима из области информационе безбједности, као и уговорним обавезама.

Захтјеви за информационом безбједношћу произилазе из потребе за заштитом свеукупне информационе имовине од свих пријетњи, било спољашњих или унутрашњих, немјерних или случајних, у контексту заштите њеног интегритета, тајности и доступности, као и правних и пословних интереса Министарства.

Политика система управљања информационом безбједности је усклађена са Уставом Републике Српске, Законом о информационој безбједности („Службени гласник Републике Српске“, број 70/11, Уредбом Владе Републике Српске о мјерама информационе безбједности („Службени гласник Републике Српске“, број 91/12) и другим законским и подзаконским актима, ратификованим међународним уговорима, те с примарним и секундарним законодавством ЕУ. Такође, политика система управљања информационом безбједности прати важеће стандарде и најновија достигнућа различитих струка. Министарство се стара да политику система управљања информационом безбједности усклађује са свим наведеним актима за шта се стара лице одговорно за функцију безбједности информационог система. Поред осталог, он се стара да сви безбједносни поступци буду усклађени са политиком система управљања информационом безбједности и проведени у сладу с њом, о томе неспосредно извјештава пословодство Министарства, а по потреби се консултује и са другим лицима укљученим у пројектовање, провођење, развој и унапређење система управљања информационом безбједности.

3.3 Управљање информационом безбједности и ризицима на стратешком нивоу

Поступак избора начина управљања (мјере заштите) дефинише се у Методологији процјене и обраде ризика.

Одабрани начини управљања и њихов статус имплементације прописани су и Извјештају о примјенљивости.

3.4 Критерији за евалуацију ризика

Основни критерији које је потребно примјенити у процесу анализе и обраде ризика у систему управљања информационом безбједности у министарству су:

- критерији процјене ризика,

- критерији утицаја и

- критерији прихватања ризика.

Критерији процјене ризика вреднују се у односу на стратешку вриједност пословних информација, вриједност информационе имовине, правне, регулаторне и уговорне обавезе, оперативну и пословну вриједност доступности, повјерљивости и интегритета, као и евентуалне негативне посљедице по министарство.

Процјена критерија утицаја ставља у однос степен оштећења или трошкове који су узроковани неким догађајем повезаним са информационом безбједности, а њихов развој се базира на: нивоу класификације информационе имовине која је обухваћена, повреде информационе безбједности, спречавању негативних трендова у пословању, поремећаја у планирању и поштовању рокова и могуће повреде законских, регулаторних и уговорних захтјева.

Критерји прихватања ризика најчешће зависи од политике, циљева и интереса организације.

Овај критерј ће бити примјењен уз поштовање правних и регулаторних аспеката, организацију и технологију пословања, као и друштвених и хуманитарних фактора.

Поступци обраде ризика укључују:

- Примјену одговарајучих контрола како би се ризик елиминисао, или довео у границе прихватљивости;
- Свјесно и објективно прихватање ризика како би се испоштовала политика информационе безбједности и критерији за прихватање ризика;
- Избјегавање ризика спречавањем акција које могу да проузрокују његову појаву;
- Преношење ризика на друге стране;

Доношењем одлуке о имплементацији одабране контроле (контролних механизама) обазбјеђује се редуковање ризика на прихватљив ниво узимајући у обзир захтјеве и ограничења националних и међународних закона и прописа и циљеве министарства.

Трошак имплементације одабраних контрола мора бити пропорционалан захтјевима и ограничењима који су постављени у оквиру циљева министарства, као и штети коју евентуални безбједносни пропуст може узроковати.

3.5 Одговорности за провођење

Сви запослени и спољни сарадници Министарства и други који долазе у контакт са информационим ресурсима Министарства, обухваћеним Системом за управљање

безбједношћу информација одговорни су за провођење Политике система управљања информационом безбједности, зато им је она достављена у писаној форми. Систем за управљање безбједношћу информација (СУБИ) обухвата све информационе ресурсе у сједишту и на другим локацијама Министарства.

Политика система управљања информационом безбједности је потврђена од пословодства Министарства, које је одговорно за њено провођење. Организациона јединица надлежна за кадровске послове је од пословодства овлашћена да, с обзиром на тип кршења политике система управљања информационом безбједности, проводи прописани поступак.

За координисање мјера информационо-безбједносне контроле и провођење мјера политике система управљања информационом безбједности одговорна је јединица за информатику (одјељење за информатику). Оно помаже организационој јединици за кадровске послове код доношења одлуке да ли је због кршења безбједносног поступка потребно покренути дисциплински поступак. За информациону безбједност на појединим подручјима одговорна су лица задужена за та подручја, односно системе. Одговорности су одлукама пословодства документоване и формално потврђене. Стручне савјете у вези са заштитом информација могу давати и спољни сарадници. Њихови савјети се усклађују унутар Министарства.

У случајевима кршења Политике система управљања информационом безбједности прекршилац може да изгуби право коришћења одређене опреме (нпр. приступ интернету или бази података корисника накнада), а у случајевима тежег кршења се, у складу са прописима, може покренути поступак утврђивања дисциплинске и материјалне одговорности те изрећи одговарајуће дисциплинске мјере у сладу са Уредбом о дисциплинској и материјалној одговорности („Службени гласник Републике Српске“ број 104/09 и 77/12) мјера престанка радног или уговорног односа, као и покренути питање кривичне одговорности.

Поновљена кршења безбједносних поступака морају бити забиљежена у персоналном досијеу запосленог и могу имати за посљедицу његову суспензију. Организациона јединица надлежна за кадровске послове је, заједно са таквим запосленим, непосредно одговорна.

Са спољним сарадницима или уговорним партнерима који не проводе Политику система управљања информационом безбједности или је крше, Министарство ће раскинути даљњу сарадњу. У случају тежих кршења може против таквих правних или физичких лица бити покренут одговарајући поступак у сладу са законом.

Осим тога, пословодство Министарства је одговорно да се имплементација СУБИ проводи у складу са овом Политиком, те да су обезбјеђени сви потребни ресурси, да се преглед система управљања информационом безбједности обавља барем једном годишње (или након сваке веће промјене унутар система) да се континуирано планира, проводи и прати обучавање и подизање свијести запослених о важности управљања системом информационе безбједности.

3.6 Комуникација политике

Организациона јединица за кадровске послове и лице одговорно за функцију безбједности информационог система задужени су да сви запослени у Министарству, као и све спољне стране које учествују у успостављању и провођењу система управљања информационом

безбједности буду упознати са овом Политиком. Основно оспособљавање се изводи одмах по заснивању радног односа, а пословодство након тога обезбјеђује да се новозапослени у току 12 мјесеци по запошљавању осособи у области информационе безбједности.

Комуникација Политике система управљања информационом безбједности мора бити отворена, подржана разним видовима комуникације (усмено и писаним путем).

4. Подршка провођењу система управљања информационом безбједности

Овим документом пословодство Министарства даје подршку провођењу, имплементацији, развоју и континуираном унапређењу система управљања информационом безбједности, како би се постигли циљеви утврђени овим документом и задовољили сви утврђени захтјеви.

5. Примјена и управљање документом

Овлашћено лице именовано за функцију безбједности информационог система је одговорно је да врши контролу адекватности ове политике, по потреби га ревидује. Осим тога, лице за именовано за функцију безбједности информационог система прати примјену овог документа и о свим неусаглашеностима писаним путем обавјештава секретара Министарства који оцјењује потребу упознавања министра и стручног колегија.

Када се врши оцјена адекватности и ефективности овог документа потребно је узети у обзир сљедеће критерије:

- Број запослених и ванјских сарадника Министарства који имају одређена овлашћења или одговорности у оквиру система информационе безбједности, а који нису упознати са овим документом,
- Евентуалну неусаглашеност система информационе безбједности са законима и прописима, уговорним обавезама или другим интерним документима министарства,
- Неефективност имплементације и одржавања система информационе безбједности,
- Недовољно јасно одређене одговорности за провођење система информационе безбједности.

Овај документ ступа на снагу од дана његовог усвајања.

Достављено:

- Министар,
- Огласне табле министарства,
- Помоћници министра,
- Секретар,
- а/а.

Министар:

Миленко Савановић

10-051-206/15