Република Северна Македонија
Министерство за информатичко
општество и администрација

Бр. 13-23/34
05.01.2022 год.
Скопје

	ПЛАН ЗА ТРЕТМАН НА РИЗИКОТ	**ПЛ 8.3**
ISO 27001:2013	**RISK TREATMENT PLAN**	**Ревизија-01**

	Должност	*Име*	*Дата*	*Потпис*
Утврдил:	Министер	**Doc.D-r Jeton Shaqiri**	11.06.2021	
Одобрил:	Државен секретар	Елена Манчева	11.06.2021	
Изработил:	Тим за безбедност на информации	Солза Ковачевска Димитар Манчев	11.06.2021	

Дата на регистрација на документот:	11.06.2021
Оригиналот се чува кај	Тим за безбедност на информации

Вид на примерокот и реден број

Оригинал	x	Контролирана копија		Информационен	

Распределба на документот:	*Корисник*
Внатрешна:	
Надворешна:	

Регистрирање на извршените промени во документот:

Ред. Бр.	Причина за промена	Променети, Отстранети и Додадени Страници	ИМЕ Должност	Потпис Дата

Регистрирање на проверките на документот:

Бр. и дата на проверката		Потврда за валидност	Продолжен рок на дејствување до:	ИМЕ Должност	Потпис Дата

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА - REPUBLIKA E MAQEDONISË SË VERIUT
МИНИСТЕРСТВО ЗА ИНФОРМАТИЧКО ОПШТЕСТВО И АДМИНИСТРАЦИЈА
MINISTRIA E SHOQËRISË INFORMATIKE DHE ADMINISTRATËS
Бр.-Nr. 13-23/34
05.01 2022 год.-viti
СКОПЈЕ - SHKUP

1. ЦЕЛ:

Целта на овој план е преземање на навремени активности и мерки за намалување на ризикот во однос на безбедноста на информацискиот систем и средствата на МИОА, кои се подложни на многу висок и висок ризик.

Координација на активностите за намалување на високите нивоа на ризик и воведување на средства за контрола, неопходни за заштита на информациите.

Информирање на вработените и утврдување на ефикасно управување со ризиците во однос на безбедноста на информациите.

2. ОПФАТ:

Планот се применува за целокупниот информациски систем и сите средства (assets), кои се подложни на многу висок и висок ризик.

3. ОДГОВОРНОСТИ:

Претставниците на раководството за квалитет на ИМС, заедно со врвното раководство (Министер) даваат целосна поддршка за почитување и примена на овој план.

Одговорноста за почитување на правилата наведени во овој план ја носат следните вработени:

- Министер;
- Државен секретар;
- Тим за безбедност на информации;
- Претставници на раководството за ИМСч;
- Офицер за безбедност на информации;
- Персонал за поддршка на ИКТ (администратори на системи);
- Останати одговорни вработени во МИОА.

4. ТЕРМИНОЛОГИЈА И КРАТЕНКИ:

- МИН - Министер
- ПР – Претставници на раководството
- ОБИ – Офицер за безбедност на информациите
- ИС – Информациски систем
- ИМС – Интегриран менаџмент систем
- СУБИ – Систем за управување со безбедност на информации

- МИОА - Министерство за информатичко општество и администрација

Забелешка: *Документите и податоците се во форма на секаков запис, како во тврда копија, така и во електронска и друга форма.*

5. АКТИВНОСТИ И МЕТОДИ

5.1. ПЛАНИРАЊЕ НА ПРОЦЕСОТ ЗА НАМАЛУВАЊЕ НА РИЗИКОТ

По идентификацијата на ризиците во однос на безбедноста на информациите и нивно евидентирање во ФК 6.1/1 Регистер на ризици, се преминува кон следниве активности во однос на управување со ризиците:

1. Евалуација/оценка на ризик (согласно утврдена методологија ФК 6.1/2 Критериуми и методологија за проценка на ризици).
2. Определување на прифатливо ниво на ризик (согласно утврдена методологија – ФК 6.1/2 Критериуми и методологија за проценка на ризици).
3. Идентификација на средствата (assets) со висок и многу висок ризик.
4. Избор на метода за намалување на ризикот.
5. Дефинирање на контролни мерки, кои што треба да бидат воведени.
6. Определување на дополнителни средства за контрола (ако е неопходно).
7. Определување на временската рамка, во која соодветните контролни мерки ќе бидат воведени и ќе се спроведуваат.
8. Избор на соодветни активности за третман на ризиците:
   a) решение да се прифати ризикот;
   b) избегнување на ризикот;
   c) префрлување (трансфер) на ризикот;
   d) намалување на ризикот до прифатливо ниво.

За секој идентификуван ризик во ФК 6.1/1 Регистер на ризици, согласно утврдената оценка/ниво на ризик, се утврдуваат постоечките контролни мерки, и се планираат дополнителните контроли и активности кои треба да се преземат за управување со ризикот.

5.2. ИСПОЛНУВАЊЕ НА ПЛАНОТ ЗА НАМАЛУВАЊЕ НА РИЗИКОТ

Исполнувањето на планот обезбедува ефективна примена на избраните контролни мерки и активности, како и помош во управувањето со ризиците поврзани со безбедноста на информациите, согласно решенијата превземени во фазата на планирање.

Во оваа фаза потребно е да се преземат планираните контролни мерки и активности (ФК 6.1/1 Регистер на ризици) за секој идентификуван ризик и да се следи нивното спроведување во однос на дадените рокови и одговорности.

5.3. ОБЕЗБЕДУВАЊЕ НА РЕСУРСИ ЗА ИСПОЛНУВАЊЕ НА ПЛАНОТ ЗА ТРЕТМАН НА РИЗИЦИТЕ

5.3.1. Обезбедување на човечки ресурси

За спроведување на Планот за третман на ризици се инволвираат вработени на МИОА, согласно своите овластувања и одговорности.

По потреба може да се ангажираат надворешни советници и консултанти во однос на конкретни ризици со висок приоритет.

Спроведувањето на Планот за третман на ризици се следи од страна на Претставниците на раководството за ИМС, кои на редовна основа го информираат раководството во однос на управувањето и третманот на идентификуваните ризици.

5.3.2. Обезбедување на финансиски ресурси

Во рамките на подготовка на годишниот буџет на МИОА се планираат потребните финансиски средства за активностите за обезбедување на информацискатa безбедност и управување со ризиците.

5.3.3. Обезбедување на материјални ресурси

Врз основа на планираниот и утврден буџет, се обезбедуваат сите неопходни материјални ресурси (информациски, софтверски, хардверски, физички и слично).

5.4 ТРЕТМАН НА РИЗИКОТ

Во однос на утврденото ниво на ризик се применува соодветна стратегија за третман на ризикот, согласно дадената табела:

Проценка на ризик	Објаснување	Стратегија
Незначителен ризик	Многу мала веројатност за настанување на ризикот; Занемарливо влијание доколку се случи	**Не е потребна акција**
Прифатлив ризик	Мала веројатност за настанување на ризикот; Мало влијание доколку се случи	**Реактивен/ корективен пристап-** **Прифаќање и следење на ризикот, доколку се случи ќе се преземат соодветни мерки**
Умерен ризик	Реална можност за настанување на ризикот; Умерени последици од појава на ризикот	**Реактивен/ корективен пристап-** **Да се преземат активности за намалување на ризикот во планиран временски период.**
Значаен ризик	Голема веројатност за настанување на ризикот; Значителни последици од негово настанување	**Проактивен/ превентивен пристап-** **Во краток временски рок се преземат мерки за отстранување на ризикот.**
Неприфатлив ризик	Многу голема веројатност/ сигурност за настанување на ризикот; Фатални последици од настанување на ризикот	**Проактивен/ превентивен пристап-** **Ризикот не смее да се прифати.** **Не смее да се започне, ниту да се продолжи со работа.** **Потребна е итна акција за отстранување на ризикот.**

За ризиците, кои се оценени како прифатливи (незнечителен ризик и прифатлив ризик), не се неопходни дополнителни дејствија.

За ризиците кои се оценети како умерени, потребно е да се следат и за истите да се преземат активности во планиран временки период.

За ризиците кои се оценети како значајни и неприфатливи, потребно е да се преземе итна акција за отстранување на ризикот или негово намалување на прифатливо ниво.

5.5. ПРОВЕРКА НА ЕФЕКТИВНОСТА НА ПЛАНОТ ЗА ТРЕТМАН НА РИЗИЦИТЕ

5.5.1. Општо

Проверката на ефективноста на планот за третман на ризиците треба да докаже дека контролните мерки и преземените активности се ефективни. Заедно со проверката се извршува преглед на сите измени кои се дефинирани или опфатени со оценката на ризикот.

Доколку контролните мерки и активности се недоволни, треба да се преземат други мерки и да се следи нивната ефективност во однос на третманот на ризиците.

Резултатите (документираните информации) добиени за време на проверката обезбедуваат податоци, кои можат да бидат искористени за определување и мерење на ефективноста на СУБИ при исполнување на документираните политики и цели по безбедноста на МИОА.

КРИТЕРИУМИ И МЕТОДОЛОГИЈА ЗА ОЦЕНКА НА РИЗИЦИ И МОЖНОСТИ

Содржина

1. Критериуми за прифаќање на ризик 3

2. Методологија за евалуација на ризик 4

2.1 Табела 1 - Методологија/ табела за проценка на ризикот 5

2.2 Табела 2- Евалуација и третман на ризикот 6

3. Методологија за евалуација на можности 7

3.1 Табела 1 - Методологија за проценка на можности 7

3.2 Табела 2 - Евалуација и третман на можности 8

1. Критериуми за прифаќање на ризик

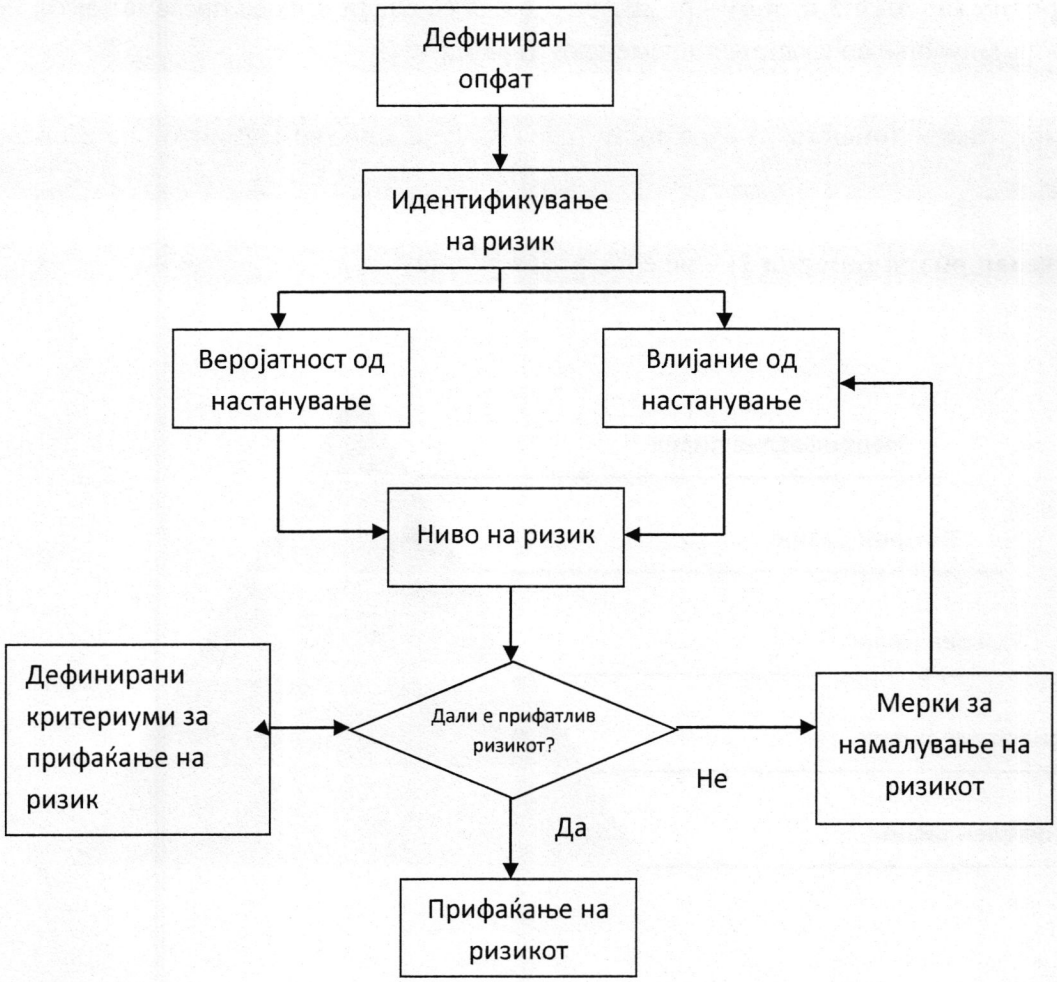
Идентификуваните ризици во МИОА може да се поделат во следниве **пет категории**:

- **Неприфатлив ризик (оценка 9)** – потребна е итна акција за отстранување на ризикот.
- **Значаен ризик (оценка 6)** - може да се преземат само во исклучителни околности. Потребно е во краток временски рок да се преземат мерки за отстранување на ризикот.
- **Умерен ризик (оценка 3 или 4)** – ризикот треба да се следи и да се преземат активности за негово намалување во планиран временски период.
- **Прифатлив ризик (оценка 2)** – ризикот треба да се следи, во моментот не е потребна акција.
- **Незнечителен ризик (оценка 1)** – не е потребна акција.

2. Методологија за евалуација на ризик

По идентификувањето на ризиците потребно е да се изврши нивна евалуација, согласно утврдените критериуми за прифаќање на ризиците.

Евалуацијата на ризиците се врши согласно прикажаниот дијаграм:



2.1 Табела 1 - Методологија/ табела за проценка на ризикот

Влијание / Веројатност	**Малку Штетно (1)**	**Штетно (2)**	**Многу штетно (3)**
Скоро невозможно (1)	**Незначителен ризик (1)**	**Прифатлив ризик (2)**	**Умерен ризик (3)**
Малку веројатно (2)	**Прифатлив ризик (2)**	**Умерен ризик (4)**	**Значителен ризик (6)**
Веројатно (3)	**Умерен ризик (3)**	**Значителен ризик (6)**	**Неприфатлив ризик (9)**

2.2 Табела 2- Евалуација и третман на ризикот

Проценка на ризик	Објаснување	Стратегија
Незначителен ризик	Многу мала веројатност за настанување на ризикот; Занемарливо влијание доколку се случи	**Не е потребна акција**
Прифатлив ризик	Мала веројатност за настанување на ризикот; Мало влијание доколку се случи	**Реактивен/ корективен пристап-** **Прифаќање и следење на ризикот, доколку се случи ќе се преземат соодветни мерки**
Умерен ризик	Реална можност за настанување на ризикот; Умерени последици од појава на ризикот	**Реактивен/ корективен пристап-** **Да се преземат активности за намалување на ризикот во планиран временски период.**
Значаен ризик	Голема веројатност за настанување на ризикот; Значителни последици од негово настанување	**Проактивен/ превентивен пристап-** **Во краток временски рок се преземат мерки за отстранување на ризикот.**
Неприфатлив ризик	Многу голема веројатност/ сигурност за настанување на ризикот; Фатални последици од настанување на ризикот	**Проактивен/ превентивен пристап-** **Ризикот не смее да се прифати.** **Не смее да се започне, ниту да се продолжи со работа.** **Потребна е итна акција за отстранување на ризикот.**

3. Методологија за евалуација на можности

3.1 Табела 1 - Методологија за проценка на можности

Влијание / Веројатност	Малку позитивно (1)	Позитивно (2)	Многу позитивно (3)
Скоро невозможно (1)	Неприфатлива можност (1)	Незначителна можност (2)	Прифатлива можност (3)
Малку веројатно (2)	Незначителна можност (2)	Прифатлива можност (3)	Значајна можност (6)
Веројатно (3)	Прифатлива можност (3)	Значајна можност (6)	Исклучително значајна можност (9)

3.2 Табела 2 - Евалуација и третман на можности

Проценка на можност	Објаснување	Стратегија
Неприфатлива можност	Многу мала веројатност за настанување на можноста. Занемарливо влијание доколку се случи.	**Не е потребна акција**
Незначителна можност	Мала веројатност за настанување на можноста. Мало влијание доколку се случи.	**Не е потребна акција во моменот, но сепак може да се следат околностите и евентуална промена на веројатноста и влијанието.**
Прифатлива можност	Постои веројатност за реално настанување на можноста и умерени позитивни ефекти од нејзино искористување.	**Реактивен пристап во случај на промена на околностите од аспект на веројатност на настанување и влијание да се преземе соодветна акција во планиран временски период.**
Значајна можност	Голема веројатност за настанување на можноста, значајни придобивки од нејзино искористување.	**Проактивен пристап, во краток временски период да се преземат активности за искористување на можноста.**
Исклучително значајна можност	Многу голема веројатност/ сигурност за настанување на можноста. Многу значајни придобивки од искористување на можноста.	**Проактивен пристап, можноста не смее да се пропушти. Потребно е да се преземе итна акција за искористување на можноста.**

Република Северна Македонија Министерство за информатичко општество и администрација Republika e Maqedonisë së Veriut Ministria e Shoqërisë Informatike dhe Administratës	РЕГИСТЕР НА РИЗИЦИ И МОЖНОСТИ - ISMS ISO 27001:2013	ФК 6.1/1-36 Верзија:01 Датум: 20.07.2021

	1	2	3	4	5	6	7
Бр.	Идентификуван ризик (опис)	На коголшто се однесува ризикот (процес, работно	Веројатност за настанување	Влијание од појава на ризик	Оценка на ризикот	Постоечки контроли/ мерки	Потребни дополнителни мерки/ активности/ планови
1	Истекување на сензитивни информации преку мобилни уреди и телекомуникациски врски	Комуникација преку мобилни уреди/ телекомуникации			0	Следење на Правилник за деловна тајна	
2	Проток на сензитивни информации од страна на вработените	Сите вработени	2	3	6	Физичка и електронска контрола на пристап до клучни документи и	Обука на вработените за воведената документација и безбедност на информациониот систем
3	Недоволна едукација/ обука на вработените за безбедност на информации	Сите вработени			0	Воведување на соодветни политики и правила на	Обука на вработените за воведената документација и безбедност на информациониот систем
4	Несоодветно чување и управување со средствата / опрема	Управување со средства / опрема			0	Опремата се чува во деловните простории со контрола на	
5	Несоодветна класификација на сензитивни информации и неконтролиран пристап до истите	Информациски систем			0	Воведување на процедура за класификација на информации	Класификација на информации и примена на соодветен начин на чување и користење на информациите согласно утврден степен на класификациіа
6	Несоодветна заштита и управување со информации складирани на USB и други медиуми	Управување со информации складирани на USB и други медиуми			0	Складираните информации на екстерни медиуми се заштитени со	

7	Неовластен пристап на вработени до одредени информации	Информациски систем			0	Политика за контрола на пристап до информации и документи во	
8	Неконтролиран физички пристап до деловни простории	Безбедност на просториите			0	Систем за контрола на пристап и регистрирање на работно време/	Систем за видео надзор на објекот и деловни простори на МИОА / Компанија за обезбедување
9	Загуба на податоци и документи складирани на Cloud	Безбедност на информации			0	Правење на backup на клучни документи во електронска форма	
10	Корумпираност на податоци и документи при нивно креирање, електронски пренос и складирање	Безбедност на информации			0	Имплементиран и заштитни механизми (софтвер за антивирус, огнен зид, заштитени	
11							

Република Северна Македонија Министерство за информатичко општество и администрација	Република е Македонисë së Veriut Ministria e Shoqërisë Informatike dhe Administratës	РЕГИСТЕР НА РИЗИЦИ И МОЖНОСТИ - ISMS ISO 27001:2013	ФК 6.1/1-36 Верзија:01 Датум: 20.07.2021

	1	2	3	4	5	6	7
Бр.	Идентификуван ризик (опис)	На кого/што се однесува ризикот (процес, работно	Веројатност за настанување	Влијание од појава на ризик	Оценка на ризикот	Постоечки контроли/ мерки	Потребни дополнителни мерки/ активности/ планови
1	Истекување на сензитивни информации преку мобилни уреди и телекомуникациски врски	Комуникација преку мобилни уреди/ телекомуникации			0	Следење на Правилник за деловна тајна	
2	Проток на сензитивни информации од страна на вработените	Сите вработени	2	3	6	Физичка и електронска контрола на пристап до клучни документи и	Обука на вработените за воведената документација и безбедност на информациониот систем
3	Недоволна едукација/ обука на вработените за безбедност на информации	Сите вработени			0	Воведување на соодветни политики и правила на	Обука на вработените за воведената документација и безбедност на информациониот систем
4	Несоодветно чување и управување со средствата / опрема	Управување со средства / опрема			0	Опремата се чува во деловните простории со контрола на	
5	Несоодветна класификација на сензитивни информации и неконтролиран пристап до истите	Информациски систем			0	Воведување на процедура за класификација на информации	Класификација на информации и примена на соодветен начин на чување и користење на информациите согласно утврден степен на класификација
6	Несоодветна заштита и управување со информации складирани на USB и други медиуми	Управување со информации складирани на USB и други медиуми			0	Складираните информации на екстерни медиуми се заштитени со	

7	Неовластен пристап на вработени до одредени информации	Информациски систем			0	Политика за контрола на пристап до информации и документи во	
8	Неконтролиран физички пристап до деловни простории	Безбедност на просториите			0	Систем за контрола на пристап и регистрирање на работно време/	Систем за видео надзор на објекот и деловни простори на МИОА / Компанија за обезбедување
9	Загуба на податоци и документи складирани на Cloud	Безбедност на информации			0	Правење на backup на клучни документи во електронска форма	
10	Корумпираност на податоци и документи при нивно креирање, електронски пренос и складирање	Безбедност на информации			0	Имплементиран и заштитни механизми (софтвер за антивирус, огнен зид, заштитени	
11							

Република Северна Македонија Министерство за информатичко општество и администрација Republika e Maqedonisë së Veriut Ministria e Shoqërisë Informatike dhe Administratës	РЕГИСТЕР НА РИЗИЦИ И МОЖНОСТИ - ISMS ISO 27001:2013	ФК 6.1/1-36 Верзија:01 Датум: 20.07.2021

	1	2	3	4	5	6	7
Бр.	Идентификуван ризик (опис)	На кого/што се однесува можноста (процес, работно	Веројатност за настанување	Влијание од појава на можноста	Оценка на можноста	Постоечки контроли/ мерки	Потребни дополнителни мерки/ активности/ планови
1	Подобра заштита и безбедност на информациите	Информациски систем			0	Воведување на Систем за управување со безбедност на информации, согласно ISO 27001	
2	Унапредување на имиџот на институцијата	МИОА			0	Примена на воведените процедури и правила, согласно стандардот ISO 27001	Објавување на сертификат за ISO 27001 на веб страната на МИОА

Република Северна Македонија Министерство за информатичко општество и администрација Republika e Maqedonisë së Veriut Ministria e Shoqërisë Informatike dhe Administratës	РЕГИСТЕР НА РИЗИЦИ И МОЖНОСТИ - ISMS ISO 27001:2013	ФК 6.1/1-36 Верзија:01 Датум: 20.07.2021

	1	2	3	4	5	6	7
Бр.	Идентификуван ризик (опис)	На кого/што се однесува можноста (процес, работно	Веројатност за настанување	Влијание од појава на можноста	Оценка на можноста	Постоечки контроли/ мерки	Потребни дополнителни мерки/ активности/ планови
1	Подобра заштита и безбедност на информациите	Информациски систем			0	Воведување на Систем за управување со безбедност на информации, согласно ISO 27001	
2	Унапредување на имиџот на институцијата	МИОА			0	Примена на воведените процедури и правила, согласно стандардот ISO 27001	Објавување на сертификат за ISO 27001 на веб страната на МИОА