ISMS – ПРОЦЕДУРЕ ИКТ СИСТЕМА МТО

ISMS.01

- **ПОСТУПАК УПРАВЉАЊА РИЗИЦИМА ПО БЕЗБЕДНОСТ ИКТ СИСТЕМА 01.**
- **ПОПИС ИТ ИМОВИНЕ 01.01**
- **КАТЕГОРИЗАЦИЈА РИЗИКА 01.02**
- **АНАЛИЗА РИЗИКА ПО БЕЗБЕДНОСТ ИКТ СИСТЕМА 01.03**
- **ЕВАЛУАЦИЈА ПОСТОЈЕЋИХ СИСТЕМА ЗАШТИТЕ 01.04**
- **ПЛАН УПРАВЉАЊА РИЗИКОМ**

ISMS.02

- **УПУТСТВО ЗА ОБЕЗБЕЂЕЊЕ ОБЈЕКАТА 02.**

ISMS.03

- **ПОСТУПАК УПРАВЉАЊА ЉУДСКИМ РЕСУРСИМА 03.**
- **ИЗЈАВА О ПРИХВАТАЊУ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА 03.01**
- **ЗАПИС О ОБУЦИ 03.02**

ISMS.04

- **КОНТРОЛА ПРИСТУПА 04.**
- **ТАБЕЛА ЗА РЕГИСТРАЦИЈУ ДОДЕЉЕНИХ ПРИСТУПА 04.01**
- **ЗАХТЕВ ЗА ДОДЕЉИВАЊЕ/ПРОМЕНУ/УКИДАЊЕ ПРАВА ПРИСТУПА ИКТ СИСТЕМУ 04.02**
- **ЕВИДЕНЦИЈА ДОПУНСКИХ ПРАВА ПРИСТУПА 04.03**

ISMS.05

- **УПУТСТВО ЗА УПРАВЉАЊЕ ОДНОСИМА СА ИСПОРУЧИОЦИМА**

ISMS.06

- **УПУТСТВО ЗА УПРАВЉАЊЕ БЕЗБЕДНОСНИМ ИНЦИДЕНТИМА 06.**
- **ЕВИДЕНЦИЈА БЕЗБЕДНОСНОГ ИНЦИДЕНТА 06.01**
- **РЕАКЦИЈА НА БЕЗБЕДНОСНИ ИНЦИДЕНТ 06.02**
- **ПРОЦЕНА УТИЦАЈА БЕЗБЕДНОСНОГ ИНЦИДЕНТА 06.03**

ISMS.07

- **ПОСТУПАК ДЕФИНИСАЊА ПЛАНА КОНТИНУИТЕТА ПОСЛОВАЊА 07.**
- **АНАЛИЗА РИЗИКА ПО КОНТИНУИТЕТ ПОСЛОВАЊА 07.01**
- **ПЛАН УПРАВЉАЊА РИЗИЦИМА ПО КОНТИНУИТЕТ ПОСЛОВАЊА 07.02**
- **ИНФОРМАЦИЈЕ ОД ЗНАЧАЈА ЗА ПОСТУПАЊЕ У ВАНРЕДНИМ СИТУАЦИЈАМА 07.03**
- **ИЗВЕШТАЈ О ПРОВЕРИ КОНТИНУИТЕТА БЕЗБЕДНОСТИ ИКТ СИСТЕМА 07.04**

ISMS.08

- **УПУТСТВО ЗА БЕЗБЕДНО КОРИШЋЕЊЕ МОБИЛНИХ УРЕЂАЈА 08.**

ISMS.09

- **УПУТСТВО ЗА ОДРЖАВАЊЕ ИКТ СИСТЕМА 09.**

ISMS.10

- **УПУТСТВО ЗА КОРИШЋЕЊЕ ИКТ СИСТЕМА - ОПШТА ПРАВИЛА 10.**

ISMS.11

- **УПУТСТВО ЗА ПОСТУПАЊЕ СА РЕЗЕРВНИМ КОПИЈАМА 11.**

ISMS.12

- **УПУТСТВО ЗА КОРИШЋЕЊЕ ИНТЕРНЕТА И Е-ПОШТЕ 12.**

ISMS.13

- **УПУТСТВО ЗА ОЦЕЊИВАЊЕ РИЗИКА ПО БЕЗБЕДНОСТ ИКТ СИСТЕМА 13.**

ISMS.14

- **УПУТСТВО ЗА ОПОРАВАК ИКТ СИСТЕМА У СЛУЧАЈУ ХАВАРИЈЕ 14.**

ISMS.15

- **УПУТСТВО ЗА ПРИКЉУЧЕЊЕ НА ИКТ СИСТЕМ 15.**

ISMS.16

/- ПРОЦЕДУРА НЕ ПОСТОЈИ – МТО НЕ ПОСЕДУЈЕ КРИПТИЗАШТИТУ

ISMS.17

- **УПУТСТВО ЗА ЗАШТИТУ И ТЕСТИРАЊЕ ИКТ СИСТЕМА**

ISMS.01

- ISMS.01.01
- ISMS.01.02
- ISMS.01.03
- ISMS.01.04
- ISMS.01.05

Република Србија
МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

Поступак управљања ризицима по безбедност ИКТ система
ISMS.01

Садржај:

1. Сврха и подручје примене

Сврха овог документа је да дефинише начин идентификације ризика по безбедност ИКТ система, вредновања и управљања истим.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Управљање ризицима

Поступак управљања ризицима по безбедност ИКТ система описан је у ***Табели 1***.

4. Прилози и записи

РБ	Назив	Ознака	Начин идентификације записа	Одлагање на електронском медију	Одлагање на папирном медију	Период чувања
1.	Попис ИТ имовине	ISMS.01.01	Према називу ОЦ и датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Popis IT imovine/ Naziv OC-Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
2.	Категоризација информација у односу на безбедносни ризик	ISMS.01.02	Према називу ОЦ и датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Kategorizacija informacija/ Naziv OC-Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
3.	Анализа ризика по безбедност ИКТ система	ISMS.01.03	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Analiza rizika/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
4.	Евалуација постојећих система заштите	ISMS.01.04	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Evaluacija sistema zaštite/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
5.	План управљања ризиком	ISMS.01.05	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Plan upravljanja rizikom/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно

5. Дефиниције и ознаке

Информација - подаци од значаја. За сваки организациони систем може се извршити класификација информација на:
• поверљиве (највиши степен поверљивости);

• ограничене (средњи степен поверљивости);
• за унутрашњу употребу (најнижи степен поверљивости) и
• јавне (информације доступне свима).

Имовина - имовина Министарства која се користи за функционисање ИКТ система

Безбедност ИКТ система - очување поверљивости, интегритета (целовитости) и расположивости информација; поред тога, могу такође бити обухваћене и друге особине као што су веродостојност, надлежност, непорецивост и поузданост.

Оцењивање ризика - свеобухватни процес анализе и вредновања ризика.

Анализа ризика - систематска употреба информација у циљу идентификације извора и процене ризика.

Вредновање ризика - процес упоређивања процењених ризика у односу на критеријуме ризика, како би се одредио значај тог ризика.

Управљање ризицима - координисане активности у циљу усмеравања и контролисања ризика.

Поступање са ризицима - процес избора и имплементације мера да би се обезбедила превенција од настанка инцидента.

Поверљивост - обезбеђивање да информација не буде доступна или откривена неовлашћеним лицима.

Интегритет - очуваност изворног садржаја и комплетности података.

Доступност - подразумева да је податак на располагању и употребљив када овлашћено лице тражи приступ.

Табела 1

РБ	Улаз	Назив активности	Излаз	Опис активности	Носилац/ Одговорни
1.	• Пописне листе • Рачуни/отпремнице добављача у вези ИТ имовине	**ПОПИС ИМОВИНЕ**	• *Попис ИТ имовине (ISMS:01-01)*	Одговорно лице је у обавези да води и ажурира листу имовине и да пријави одговорном лицу за спровођење анализе ризика по безбедност ИКТ система *(активност под ред. бр. 4)* сваку промену имовине како би се ажурирала анализа претњи и рањивости. Имовину организације чине: • ***Хардвер*** - нпр. лаптопови, сервери, штампачи, али и мобилни телефони или УСБ меморијски уређаји. • ***Софтвер*** - подразумевајући не само купљени софтвер, већ и бесплатан. • ***Информације*** - не само у електронским медијима (базе података, датотеке у PDF-у, Word-у, Excel-у и други формати), али и на папиру и другим облицима. • ***Инфраструктура*** - нпр. канцеларије, струја, клима - јер та средства могу изазвати недостатак доступности информација. Сва имовина укључена у обраду, пренос и складиштење информација мора имати задужено лице које је одговорно за безбедност, поузданост и расположивост предметне имовине.	Руководилац ОЦ
2.	• Спецификација информација • Опис послова • Списак докумената • Прописи и одлуке који се	**КАТЕГОРИЗАЦИЈА ИНФОРМАЦИЈА**	• *Категоризација информација у односу на безбедносни ризик (ISMS.01-02)*	Подаци за које је неопходан висок ниво заштите су подаци који се налазе у ИКТ систему и представљају тајну ако су тако дефинисани сходно важећем Закону о тајности података и у Каталогу докумената, података и информација који треба да буду означени степеном тајности «Интерно» и «Поверљиво» у МТО (бр. 82-00-1/2023-02 од 16.03.2023.)) и Каталогу докумената, података и информација који треба да буду означени	Руководилац ОЦ

	односе на поверљивост података			степеном тајности «Државна тајна» и «Строго поверљиво» у МТО (бр. 82-00-2/2023-02 од 16.03.2023). Подаци за који је неопходан висок ниво заштите су и нарочито осетљиви подаци о личности, као и пословне тајне. Подаци који се означе као тајни, морају бити заштићени у складу са важећим одредбама: ▪ Закона о тајности података, ▪ Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима, ▪ Уредбе о посебним мерама физичко-техничке заштите тајних података, ▪ Уредбе о начину и поступку означавања тајности података, односно докумената, ▪ Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа.	
3.	• *Категоризација информација у односу на безбедносни ризик (ISMS.01-02)* • *Попис ИТ имовине (ISMS:01-01)*	**ИДЕНТИФИКАЦИЈА ИМОВИНЕ КОЈА ЈЕ НОСИЛАЦ ИНФОРМАЦИЈА**	• *Анализа ризика по безбедност ИКТ система (ISMS.0103) ИКТ система*	За све информације чија је заштита прописана законом, подзаконским актима и актима Министарства, или где је процењен високи или веома висок ефекат у случају настанка ризика, идентификује се имовина за обраду, пренос и складиштење таквих информација.	Руководилац ОЦ
4.	• *Анализа ризика по безбедност ИКТ система (ISMS.0103) ИКТ система*	**ОЦЕЊИВАЊЕ РИЗИКА ПО БЕЗБЕДНОСТ ИКТ СИСТЕМА**	• *Анализа ризика по безбедност ИКТ система (ISMS.0103)ИКТ система*	За идентификовану имовину спроводи се анализа претњи и рањивости у циљу оцењивања ризика по безбедност ИКТ система.	Именовано лице

	• Упутство за оцењивање ризика по безбедност ИКТ система			***Претња*** је потенцијални ризик који може довести до нарушавања информационе безбедности ИКТ система Министарства. ***Рањивост*** је слабост имовине (ресурса) или групе имовине која може бити искоришћена од стране једне или више претњи. Анализа претњи и рањивости се ажурира приликом сваке промене у организацији, пословним процесима, опреми за обраду, пренос и складиштење информација и система који имају утицај на безбедност ИКТ система. Такође, сваки инцидент по безбедност ИКТ система треба да покрене преиспитивање и по потреби ажурирање анализе претњи и рањивости.	
5.	• *Анализа ризика по безбедност ИКТ система (ISMS.0103)*	**ЕВАЛУАЦИЈА ПОСТОЈЕЋИХ СИСТЕМА ЗАШТИТЕ**	• *Евалуација постојећих система заштите (ISMS.01.04)*	Управљање ризиком подразумева евалуацију постојећих система заштите и доношење одлука у вези нових мера заштите за оне ризике који су у фази анализе претњи и рањивости процењени као ризици код којих постојећи системи заштите не могу елиминисати претње или свести на прихватљив ниво.	Именовано лице
6.	• *Анализа ризика по безбедност ИКТ система (ISMS.0103)* • *Евалуација постојећих система заштите (ISMS.01.04)*	**ДЕФИНИСАЊЕ ПЛАНА УПРАВЉАЊА РИЗИКОМ**	• *План управљања ризиком (ISMS.01.05)*	У плану управљања ризиком дефинишу се све радње које треба предузети у правцу елиминисања или свођења на прихватљиви ниво свих ризика за које су у претходном кораку донете одлуке о потреби имплементације додатних мера. План треба да дефинише рокове, одговорности и потребне ресурсе за остварење истог, узимајући у обзир политику и циљеве система менаџмента безбедношћу информација, као и финансијске могућности организације у посматраном периоду. Пожељно је да план дефинише и период и када је то могуће методе за оцену ефективности спроведених мера, како би се потврдило да предузете мере дају жељене резултате.	Именовано лице

7.	• *План управљања ризиком (ISMS.01.05)*	**УСВАЈАЊЕ ПЛАНА УПРАВЉАЊА РИЗИКОМ**	• *План управљања ризиком (ISMS.01.05)*	Руководилац МТО-а на основу дефинисаног предлога Плана управљања ризицима преиспитује и усваја исти.	Руководилац МТО-а
8.	• *План управљања ризиком (ISMS.01.05)*	**РЕАЛИЗАЦИЈА ПЛАНА УПРАВЉАЊА РИЗИКОМ**	• *План управљања ризиком (ISMS.01.05)*	Реализација свих активности из плана управљања ризиком у надлежности је именованих лица у сарадњи са организационом јединицом за безбедност ИКТ система.	Именована лица Планом
9.	• *План управљања ризиком (ISMS.01.05)*	**ОЦЕНА ЕФЕКТИВНОСТ И ПРЕДУЗЕТИХ МЕРА**	• *План управљања ризиком (ISMS.01.05)* • *Евалуација постојећих система заштите (ISMS.01.04)*	Након реализације плана управљања ризиком спроводи се оцена ефективности мера. У случају незадовољавајуће оцене ефективности предузетих мера врши се допуна Плана управљања ризиком и понавља се поступак од активности 6 *(Дефинисање плана управљања ризиком)*. Уколико је спроведена мера оцењена као ефективна, ажурира се листа постојећих система заштите тако што се евидентира новоспроведена мера.	Именовано лице

ПОПИС ИТ ИМОВИНЕ

Сервер

Произвођач	*Модел*	*Серијски број*	*Бр. CPU*	*CPU*	*RAM*	*Капацитет Диска*	*Оперативни систем*	*Напомена*

Уређаји за складиштење - *Storage*

Редни број	*Ид број*	*Власник/Локација*	*Произвођач*	*Модел*	*Серијски број*	*Капацитет Диска*	*Тип storage*	*Напомена*

ПОПИС ИТ ИМОВИНЕ

Мрежна опрема

Редни број	*Ид број*	*Власник/Локација*	*Серијски број*	*Произвођач*	*Тип уређаја*	*Модел*	*Тип порта*	*Бр. порта*	*Напомена*

ПОПИС ИТ ИМОВИНЕ

Десктоп рачунар

Редни број	*Ид број*	*Власник/ Локација*	*Произвођач*	*Модел*	*Серијски број*	*CPU*	*RAM*	*Капацитет Диска*	*Оперативни систем*	*Софтвери од значаја*	*Анти Вирус*	*Напомен*

ПОПИС ИТ ИМОВИНЕ

Лаптоп и *notebook*

Редни број	***Ид број***	***Власник/ Локација***	***Произвођач***	***Модел***	***Серијски број***	***CPU***	***РАМ***	***Капацитет Диска***	***Оперативни систем***	***Софтвери од значаја***	***Анти Вирус***	***Напомена***

ПОПИС ИТ ИМОВИНЕ

UPS

Редни број	*Ид број*	*Власник/Локација*	*Произвођач*	*Модел*	*Серијски број*	*Капацитет*	*Напомена*

Принтери

Редни број	*Ид број*	*Власник/Локација*	*Произвођач*	*Модел*	*Серијски број*	*Тип везе*	*Напомена*

ПОПИС ИТ ИМОВИНЕ

Software

Редни број	*Ид број*	*Власник/Локација*	*Произвођач*	*Назив*	*Верзија*	*Серијски број*	*Лиценца*	*Број лиценци*	*Напомена*

ПОПИС ИТ ИМОВИНЕ

Backup driver

Редни број	Ид број	Власник/Локација	Произвођач	Модел	Серијски број	Капацитет	Напомена

ПОПИС ИТ ИМОВИНЕ

Остало – додати по потреби

Редни број	*Ид број*	*Власник/Локација*	*Произвођач*	*Модел*	*Серијски број*	*Напомена*

Министарство трговине, туризма и телекомуникација:

Р БР.	**Документ/податак/ информација**	**Класа информација**	**Безбедносни ризици у вези информација и ефекат у случају настанка ризика**
1.	Интерно	*Веома висок ниво заштите*	Настанак штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио
2.	Поверљиво		Настанак штете по интересе Републике Србије
3.	Строго поверљиво		Настанак тешке штете по интересе Републике Србије
4.	Државна тајна		Настанак неотклоњиве тешке штете по интересе Републике Србије
5.	Нарочито осетљиви подаци о личности		Отицање података, неовлашћен приступ и коришћење нарочито осетљивих података о личности
6.	Пословна тајна		Незаконито прибављање и коришћење информације која представља пословну тајну

АНАЛИЗА РИЗИКА ПО БЕЗБЕДНОСТ ИНФОРМАЦИЈА ИКТ СИСТЕМА

Организациона јединица:

Р. бр.	**Информације/ Безбедносни ризици у вези ИКТ система**	**Подручје настанка ризика**	**Имовина**	**Претње**	**Рањивост**	**Ризик**	**Вероватноћа претње**	**Оцена рањивости**	**Вредност ризика***
1.		*Обрада*							
		Пренос							
		Складиштење							
2.		*Обрада*							
		Пренос							
		Складиштење							
3.		*Обрада*							
		Пренос							
		Складиштење							
4.		*Обрада*							
		Пренос							
		Складиштење							

**НАПОМЕНА: Уколико се за једну имовину везује више ризика различитог интензитета, за коначан ризик се узима највећа вредност процењеног ризика.*

Р. бр.	Информације	Безбедносни ризик	Лице које је одговорно[1]	Систем заштите који је тренутно у употреби	Захтев за додатном мером ДА/НЕ
1.				*За превенцију ризика:* *За детекцију ризика:* *За опоравак система:*	
2.				*За превенцију ризика:* *За детекцију ризика:* *За опоравак система:*	
3.				*За превенцију ризика:* *За детекцију ризика:* *За опоравак система:*	
4.				*За превенцију ризика:* *За детекцију ризика:* *За опоравак система:*	
5.				*За превенцију ризика:* *За детекцију ризика:* *За опоравак система:*	
6.				*За превенцију ризика:* *За детекцију ризика:* *За опоравак система:*	
7.				*За превенцију ризика:* *За детекцију ризика:* *За опоравак система:*	

[1]Под „*лице које је одговорно*" се подразумева особа или ентитет са одговорностима и овлашћенима да управљању ризиком, односно особа која је заинтересована за поступање са ризиком и која је довољно високо позиционирана у организационом систему да може да уради нешто по том питању.
Пример и разлика између „*власника имовине*" и „*власника ризика*" (није искључено да „*власник имовине*" и „*власник ризика*" могу бити иста особа):
Власник имовине сервера може бити ИТ администратор, а власник ризика може бити шеф/руководилац ИТ сектора. ИТ администратор врши одређена управљања на и у вези са сервером свакодневно, док ће се шеф/руководилац ИТ сектора побринути да нпр. улаже у бољу заштиту сервера, обезбеди обуке за ИТ администратора, итд.

ПЛАН УПРАВЉАЊА РИЗИКОМ

Р. БР.	**Безбедносни ризик за ИКТ систем**	**Циљеви**	**Програм за реализацију циљева**				
			Задатак	**Потребни ресурси**	**Одговорно лице**	**Рок**	**Оцена ефективности предузетих мера**
1.							
2.							
3.							
4.							
5.							

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Упутство за обезбеђење објеката
ISMS.02

Упутство за обезбеђење објеката

Садржај:

1. Сврха и подручје примене

Документ дефинише начин обезбеђења објеката у циљу заштите ИКТ система МТО.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Обезбеђење објеката

3.1 Систем видео надзора

У оквиру Министарства туризма и омладине НИЈЕ имплементиран систем видео надзора, ни на једној од три локације на којима послује Министарство туризма и омладине. Обзиром да се пословне просторије министарства налазе у оквиру објеката које су у државном власништву и да је министарство "закупац" тих просторија, нема потребе да се министарство бави питањима физичког обезбеђења простора, већ је то на УЗЗПРО и служби безбедности.
Систем видео надзора није имплементиран у деловима објекта (спратовима) које користи Министарство туризма и омладине.
Систем видео надзора је имплементиран од стране "Управе за заједничке послове републичких органа" на улазима објекта и око објекта. Ова управа такође врши и одржавање система видео надзора.
Министарство туризма и омладине нема директан приступ систему видео надозора и нема податке о техничким карактеристикама видео камера и видео снимача.

Систем контроле приступа

У оквиру ИТ система Министарства туризма и омладине НИЈЕ имплементиран систем за контролу приступа као ни систем за евиденцију уласка/изласка запослених из објеката.
У оквиру ИТ система Министарства туризма и омладине НИЈЕ имплементиран систем за евиденцију радног времена.

3.2 Против–пожарни аларм

У просторије МТО уграђен је против-пожарни алармни систем који се састоји од:

Ручних јављача пожара

Намена ручних јављача пожара је да омогуће запосленима, или другим лицима која се налазе у просторијама МТО, да ручно активирају против-пожарни аларм у случају да примете пожар.

Алармне централе са системом даљинског мониторинга

Намена алармне централе је да управља радом и контролише рад система. Централа је опремљена системом даљинског мониторинга који омогућава аутоматско обавештавање овлашћених запослених о алармирању и статусу система.

Сирена

Намена сирена је да звучним путем сигнализирају на алармирање система. Сирене су распоређене тако да се могу чути у свим просторијама објекта.

Блицера

Намена блицера је да визуелним путем сигнализирају на алармирање система.

У случају алармирања против-пожарног аларма запослени поступају у складу са Правилима заштите од пожара и Планом евакуације.

Против-пожарни алармни систем је у функцији 24 сата дневно. У случају губитка напајања из градске мреже, систем аутоматски прелази на напајање из сопствених батерија и дизел-електричног агрегата.

За исправан рад и организацију одржавања против-пожарног аларма стара се одговорно лице. Против-пожарни аларм се одржава и редовно тестира од стране квалификоване екстерне организације, у складу са Законом.

3.3 Уговорна организација за обезбеђење

МТО ангажује екстерну организацију за пружање услуга даљинског надзора против-провалног алармног система и интервенције у алармним ситуацијама, као и физичко обезбеђење (портир) у току радног времена МТО.

Екстерна организација 24 сата дневно врши даљински надзор над против-провалним алармним системом.

У случају активације аларма, употребе тихе дојаве на аларму од стране запослених или по позиву запослених - екстерна организација одмах упућује интервентни тим обезбеђења, обавештава овлашћене запослене телефоном о алармној ситуацији и интервенцији, у случају потребе обавештава територијално надлежну јединицу полиције, те предузима друге радње.

3.4 Пријем посетилаца

Лица која нису запослена у МТО се по доласку у просторије јављају портиру на улазу у објекат.

Портир податке о посетиоцима евидентира у Евиденцији посета, а потом позива лице код кога посетиоци имају најављен долазак. Пожељно је, посетиоце након најаве дочека у холу и даље спроведе кроз објекат, што важи и за напуштање објекта након завршетка састанка.

Посетиоци се у пословном простору могу кретати само у пратњи запослених.

3.5 Приступ серверском простору

Самосталан приступ серверском простору дозвољен је администратору. Други запослени могу приступити простору само у присуству и по одобрењу администратора. Приступ административној зони може имати и запослени/а на пословима одржавања хигијене уз писано одобрење и присуство надлежног лица.

Посетиоцима који нису запослени у МТО није дозвољен приступ серверском простору, осим радника квалификованих екстерних организација за техничко одржавање – који простору приступају само у присуству и по одобрењу администратора.

Просторија мора бити видљиво обележена и у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима. Прозори и врата на овој просторији морају увек бити затворени.

3.6 Поверљивост информација о безбедности објекта

Информације о безбедности објекта представљају поверљиву информацију.
Следеће информације и документа не смеју се саопштавати или давати лицима која нису запослена у МТО, осим надлежним државним органима у складу са законом и лицима одређеним за техничко одржавање система уз претходну сагласност руководства:

- Технички подаци, ознаке, карактеристике алармних система, видео надзора, система за контролу приступа;
- Информације о броју, распореду, зонама покривања сензора, камера или других компоненти алармних-система, система видео надзора и система контроле приступа;
- Шифре или било какви подаци о шифрама или начину приступа и контроле алармних-система, система видео надзора и система контроле приступа;
- Инструкција за поступање у случају алармирања против-провалног аларма или детекције покрета у објекту ван радног времена;
- Снимци система видео-надзора и приступ систему видео надзора;
- Евиденције система за контролу приступа, и приступ систему за контролу приступа;
- Списак запослених овлашћених за стављање у функцију/ искључивање против-провалног аларма;
- Стандардна радна процедура екстерне организације за обезбеђење.

4. Прилози и записи

Документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине.

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.03

- ISMS.03.01
- ISMS.03.02

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Поступак управљања људским ресурсима са аспекта безбедности ИКТ система

ISMS.03

Садржај:

1. Сврха и подручје примене

Сврха овог поступка је обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност као и заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система. Овај поступак се односи на све запослене у МТО без обзира на начин ангажовања.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Управљање људским ресурсима

3.1 Услови запошљавања

Министарство треба да обезбеди да се сви запослени, без обзира на начин ангажовања, сложе са правима и обавезама који су везани за безбедност ИКТ система. Права и обавезе требају да буду одговарајући за природу посла и правима приступа над информационом имовином Министарства (информациони системи и ИТ сервиси). Приликом заснивања радног односа, запослени је у обавези да потпише *Изјаву о прихватању политике безбедности ИКТ система (ISMS.03.01)* и да се упозна са њеним садржајем. Након потписивања ове изјаве попуњава се реверс.

Одговорности које се помињу у правима и обавезама запошљавања би требало дефинисати на период до прекида радног односа и по потреби након тога..

3.2 Свест о безбедности информација, едукација и обуке

Сви запослени у Министарству морају да се редовно обучавају и да редовно обнављају знања о политикама и процедурама, на начин који одговара њиховој пословној функцији, чиме се подиже свест запослених о:

- политици безбедности ИКТ система,
- свом доприносу ефективности система менаџмента безбедношћу ИКТ система, укључујући користи од побољшаних перформанси безбедности ИКТ система и
- последицама неусаглашености са захтевима система менаџмента безбедношћу ИКТ система.

Уводна обука о безбедности ИКТ система је конципирана тако да се запослени упознају са политикама и очекивањима Министарства пре него што корисник добије приступ информационом систему. Подизање свести о безбедности ИКТ система, едукација и обука треба да садрже теме у вези познатих и реалних претњи као и информације коме треба запослени да се обрати за савет или пријави безбедносно-информациони инцидент. Додатна обука за подизање свести о безбедности ИКТ система је намењена да омогући појединцима да препознају проблеме и инциденте безбедности ИКТ система, као и како да реагују на њих.

План обуке у вези безбедности ИКТ система саставља одговорно лице (именовано одлуком) на почетку године на захтев руководиоца организационих целина

министарства. Елементи плана обуке уносе се у *Запис о обуци запосленог (ISMS.03.02)* за сваког запосленог у делу „Планирање обуке".

По завршетку обуке у вези безбедности ИКТ система, одговорно лице (именовано одлуком) попуњава *Запис о обуци запосленог (ISMS.03.02)* у делу „Реализација обуке" који се чува у досијеу запосленог. Потврде о обучавању у вези безбедности ИКТ система запослени могу да добију преко праћења семинара или обучавања од стране спољног стручног лица итд. Ове потврде се такође чувају у досијеу запосленог.

Након извесног временског периода и уколико се то сматра неопходним врши се процена ефективности обуке. Циљ ове процене је утврђивање да ли је знање пружено на обуци довољно и да ли постоји неопходност за додатним обучавањем. Резултати вредновања ефективности се евидентирају у *Запису о обуци запосленог (ISMS.03.02)* у делу „Реализација обуке - Вредновање ефективности".

3.3 Дисциплински поступак

Уколико запослени поступа супротно прописима, Акту о безбедности, процедурама и правилима, против њега се покреће дисциплински поступак.

3.4 Престанак радног односа и промена посла

Одговорности и обавезе које су на снази и након престанка радног односа дефинисане су у *Изјави о прихватању политике безбедности ИКТ система (ISMS.03.01)*.

Сви запослени или сарадници Министарства треба да врате сву имовину Министарства која је у њиховом поседу, након престанка радног односа, уговора или споразума. Окончање процеса треба формализовати да укључују повратак свих претходно издатих софтвера, корпоративних докумената и опреме. Остала имовина, у виду организационе имовине као што су екстерни рачунарски уређаји, мобилни телефони, приступне картице, софтвери, приручници и подаци који се налазе на електронским медијима, такође треба да се врате.

Списак информационо-комуникационе опреме наведен у реверсу се ажурира и тек тада лице може да напусти Министарство. Овај запис потврђује да ће сав инвентар, опрема и сва друга средства за коју је лице одговорно бити враћена. Ова изјава је потписана од стране запосленог одмах након запослења. У изјави се наводи да је запослени извршио правилно коришћење и одржавање свих средстава за које је задужен. Наведени запис се архивира у личном досијеу запосленог.

3.5 Додела и уклањање приступних права

Право приступа свих запослених и сарадника у Министарству који су корисници ИКТ система треба уклонити по престанку радног односа, уговора или споразума, односно прилагодити их променама ако су се изменила права приступа.

Право приступа на имовину у оквиру информационог система и ИТ сервиса, треба да буду онемогућени након престанка радног односа. Исто тако се морају онемогућити у случају прераспоређивања са једног на друго радно место.

Права приступа се морају уклонити или прилагодити, укључују физички и логички приступ, кључеве, идентификационе картице, опрему за обраду информација, чланарине и уклањање лица из било које документације која их идентификује као тренутног члана Министарства. Ако је одлазећем запосленом из Министарства позната лозинка за преостале активне рачуне, они треба да буду уклоњени по престанку или промени запослења, уговора или споразума.

У одређеним околностима право приступа може бити додељено већем броју лица, извођачу или трећој страни (нпр. групни ИД). У таквим околностима, појединци који напуштају Министарство треба да буду уклоњени са свих листа и група. Након спровођења овог поступка кооперанти треба да се обавесте да не деле никакве информације са особом која напушта Министарство.

Додела и уклањање приступних права спроводи се према *Упутству за контролу приступа (ISMS.04)*.

4 Прилози и записи

РБ	Назив	Ознака	Начин идентификације записа	Одлагање на електронском медију	Одлагање на папирном медију	Период чувања
1.	Изјава о прихватању политике безбедности ИКТ система	ISMS.03.01	Према имену корисника	C(D):/ Dokumentacija/ Zapisi/ Izjava o prihvatanju politike/ Ime korisnika.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
2.	Запис о обуци запосленог	ISMS.03.02	Према имену и презимену запосленог	C(D):/ Dokumentacija/ Zapisi/ Zapis o obuci/ Ime i prezime zaposlenog.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно

5 Дефиниције и ознаке

Овај документ не садржи дефиниције и ознаке.

ИЗЈАВА О ПРИХВАТАЊУ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА

Дајем изјаву да сам прочитао доле наведену политику безбедности ИКТ система и обавезујем се да се придржавам њеног садржаја, као и свих осталих релевантних политика информационе безбедности прописаних од Министарства туризма и омладине (у даљем тексту: Министарство) које су обавезујуће за запослене.

1. Поступаћу у складу са Актом о безбедности ИКТ система Министарства, прописаним процедурама и правилима.
2. Упознат сам да се моја употреба компјутера и комуникационих система можда надзире и /или бележи у законите сврхе.
3. Прихватам да сам одговоран за коришћење и заштиту свих креденцијала који су ми додељени (кориснички налог и лозинку, токен за приступ или друге ставке које су ми додељене).
4. Изјављујем да нећу користити туђи кориснички налог и лозинку како би приступио системима Министарства.
5. Изјављујем да нећу покушати приступити ниједном другом компјутерском систему за који немам одобрен приступ.
6. Заштитићу сваки поверљиви материјал који ми је послат, примљен, спремљен и обрађен, у складу са степеном поверљивости који има, како електронске, тако и папирне копије.
7. Сваки поверљиви материјал који креирам означићу у складу са смерницама за објављивање, како би он остао прикладно заштићен.
8. Нећу слати поверљиве информације интернетом путем емаил-а или било којим другим методом осим ако нису коришћени одговарајући методи (нпр. енкрипција) који ће их заштитити од неовлашћеног приступа.
9. Водићу рачуна да сам унео/ла тачну емаил адресу примаоца, како поверљиве информације не би биле компромитоване.
10. Обезбедићу да ме не надгледају неовлашћена лица док радим и предузећу одговарајуће мере предострожности када штампам поверљиве информације.
11. Поверљив одштампан материјал ћу пажљиво да архивирам и побринућу се да је исправно уништен, када више не буде потребан.
12. Нећу остављати свој компјутер без надзора и омогућити неовлашћен приступ информацијама путем мог налога док сам одсутан.
13. Упознаћу се са свим политикама и процедурама безбедности у Министарству и свим посебним упутствима повезаним са мојим послом.
14. Одмах ћу обавестити свог надређеног ако приметим, посумњам или будем сведок инциденту који може да проузрокује повреду безбедности.
15. Нећу покушати да избегнем систем безбедносних контрола.
16. Нећу уклањати опрему или информације из просторија Министарства без одговарајућег одобрења.
17. Водићу рачуна о компјутерским медијима или преносивим компјутерима када их будем носио ван просторија Министарства.
18. Нећу унети вирусе или друге злонамерне програме у систем или мрежу.
19. Нећу покушати да искључим антивирус заштиту која ми се налази на компјутеру.
20. Усагласићу се са законским, правним и уговорним обавезама о којима ме Министарство обавести.
21. Приликом напуштања Министарства, пре одласка обавестићу свог непосредног руководиоца о свим важним информацијама које се налазе на мом налогу.

ИЗЈАВА О ПРИХВАТАЊУ ПОЛИТИКЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА

Име корисника:

Потпис корисника:

Датум:

Ова изјава израђује се у два примерка, један примерак задржаће корисник, а други Министарство.

ЗАПИС О ОБУЦИ ЗАПОСЛЕНОГ

Име и презиме запосленог	
Радно место	

ПЛАНИРАЊЕ ОБУКЕ			**РЕАЛИЗАЦИЈА ОБУКЕ**					
Тема обуке	**Планирани термин**	**Начин вредновања ефективности**	**Датум реализације**	**Извођач обуке**	**Трајање обуке**	**Сертификат/ уверење**	**Вредновање ефективности**	
							датум:	*реализовао:*
							датум:	*реализовао:*
							датум:	*реализовао:*
							датум:	*реализовао:*

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.04

- ISMS.04.01
- ISMS.04.02
- ISMS.04.03

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Упутство за контролу приступа

ISMS.04

Садржај:

1. Сврха и подручје примене

Сврха овог упутства је да дефинише контроле приступа које Министарство туризма и омладине имплементира у свом информационом систему, са циљем омогућавања безбедности ИКТ система, система за обраду информација и пословних процеса, а који морају бити контролисани на бази пословних и безбедносних захтева. Ово упутство се односи на све запослене, као и на све ауторске процесе, испоручиоце услуга, консултанте, привремено запослене, тј. лица који на било који начин морају уз одговарајуће одобрење приступати ИКТ систему.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Контрола приступа

3.1. Увод

МТО контролише приступ информационим системима на три нивоа: физичком, административном и техничком.

Физичка заштита је остварена контролом приступа безбедносним зонама, уз чување записа о свакоме ко улази и остаје унутар ових зона. Физичка заштита је постављена за документацију (на папирном и електронском медију), сервере, компјутере, мрежну опрему и осталу имовину која има утицај на безбедност ИКТ система (ингеренција МУП-а)

Административна заштита је остварена усвајањем политика, процедура и документације за сва корисничка права приступа на нивоу целог система. Заштита је имплементирана од стране ИТ подршке.

Техничка заштита је остварена у сваком делу информационог система употребом свих технолошких средстава и могућности. Заштита је надгледана употребом најновијих софтверских решења, хардвером и мрежним протоколима.

3.2. Додела права приступа

Права приступа могу бити **основна** и **допунска**.

Основна права приступа су права које запослени има по основу именовања на одређено радно место за које су дефинисана права приступа. Основна права за радна места утврђује руководилац организационе целине којој припада радно место, а верификује лице одговорно за безбедност ИКТ система. Основ за утврђивање права приступа за одређена радна места представља спроведена анализа ризика по безбедност ИКТ система. Утврђена права приступа за радна места специфицирају се у *Табели за регистрацију додељених приступа (ISMS.04.01)*.

У случају пријема новозапослених, кад је запослени прераспоређен са једног радног места на друго или напушта МТО, основна права приступа информационим системима морају бити додељена, промењена или укинута. Руководилац организационе целине

упућује *Захтев за доделу/промену/укидање права приступа ИКТ систему (ISMS.04.02)* лицу одговорном за безбедност ИКТ система које је даље одговорно за реализацију захтева. Након реализације захтева лице одговорно за безбедност писаним путем обавештава руководиоца организационе целине да су права запослених додељена/промењена/укинута што лице одговорно за безбедност ИКТ система евидентира у *Табели за регистрацију додељених приступа (ISMS.04.01)*.

Допунска права приступа су права запослених или лица која су одређена посебним одобрењима ради реализације одређених задатака и послова. За остваривање допунских права приступа, директно претпостављени у чијој надлежности је реализација одређених задатака и послова ће доставити лицу одговорном за безбедност ИКТ система *Захтев за доделу/промену/укидање права приступа ИКТ систему (ISMS.04.02)* тачно наводећи кориснички ниво приступа сваком систему за сваког корисника.

Након одобравања допунских права приступа, одговорно лице за безбедност ИКТ система издаје налог одговорном лицу за контролу приступа да омогући дозвољене приступе. Након истека рока за допунска права приступа обавеза је лица одговорног за безбедност ИКТ система **да укине** сва додељена права. Одговорно лице за безбедност ИКТ система води *Евиденцију допунских права приступа (ISMS.04.03)*.

У случају додељених права приступа просторијама, мора се успоставити листа особа којима је издата дозвола за улазак у безбедносно подручје и ажурирати када год се додели или укине право приступа корисницима. Листа лица којима је издата дозвола за улазак у безбедносно подручје мора бити видно истакнута на улазу у безбедносно подручје.

3.3. Ревизија корисничких привилегија приступа

Лице одговорно за безбедност ИКТ система редовно врши проверу додељених корисничких права приступа и листу лица којима је издата дозвола за улазак у безбедносно подручје најмање два пута годишње или у краћим интервалима, посебно када долази до напуштања радног места, пријема нових запослених, промена радних позиција итд.

Преиспитивање корисничких права приступа се спроводи редовно како би се омогућила ефективна контрола приступа информацијама и ИТ сервисима и позитивно потврдили сви корисници. О спроведеном преиспитивању корисничких права приступа одговорно лице сачињава *Извештај о ревизији корисничких права приступа* који мора да садржи као минимум: датум ревизије, промене радног статуса запослених у периоду за који се израђује извештај, вишемесечна одсуства запослених, промене права приступа, закључак у вези ефективности дефинисаног система контроле приступа.

3.4. Неактивне сесије (Session time out)

Неактивне сесије се аутоматски искључују након одређеног периода неактивности на систему/апликацији. Ограничена форма sessio time out-a је дефинисана на радним станицама, која закључава екран и не дозвољава неовлашћен приступ али не затвара апликације или мрежне сесије. Сесије су угашене да би се спречио неовлашћен приступ и други хакерски напади на систем. Лимитирање времена трајања сесије спречава кориснике да држе отворене сесије.

4. Прилози и записи

РБ	Назив	Ознака	Начин идентификације записа	Одлагање на електронском медију	Одлагање на папирном медију	Период чувања
1.	Табела за регистрацију додељених приступа	ISMS.04.01	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Tabela za registraciju dodeljenih pristupa/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	3 године
2.	Захтев за доделу/промену/укидање права приступа ИКТ систему	ISMS.04.02	Према датуму и запосленом	C(D):/ Dokumentacija/ Zapisi/ Zahtev za kontrolu prava pristupa/ Datum-zaposleni.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	3 године
3.	Евиденција допунских права приступа	ISMS.04.03	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Evidencija dopunskih prava pristupa/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	3 године
4.	Извештај о ревизији корисничких права приступа		Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Izveštaj o reviziji korisničkih prava pristupa / Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	3 године

5. Дефиниције и ознаке

ИСМС – Систем менаџмента безбедношћу информација
МТО – Министарство, туризма и омладине

ТАБЕЛА ЗА РЕГИСТРАЦИЈУ ДОДЕЉЕНИХ ПРИСТУПА

Организациона целина:

Ред. бр.	Радно место	Приступ[1]	Ниво[2]	Име и презиме запосленог	Датум доделе приступа	Корисничко име	Лозинка
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							
13.							
14.							
15.							
16.							
17.							

	Име и презиме	Датум	Потпис
Израдио:			
Верификовао:			

[1] *А - Апликацијама, Ф - Фолдерима, Р - Рачунарима, П - Просторијама, РС - Радним станицама, Д - Домаин ресурсима, Б - Базама података.*
[2] *А – Администратор, К – Корисник, И – Измена, П – Преглед, У – Унос, Ш – Штампање.*

ЗАХТЕВ ЗА ДОДЕЉИВАЊЕ/ПРОМЕНУ/УКИДАЊЕ ПРАВА ПРИСТУПА ИКТ СИСТЕМУ

Захтев за	Доделу ☐	Промену ☐	Укидање ☐
Име и презиме запосленог/лица коме се одобрава приступ			
Сектор / екстерна организација			
Организациона јединица			
Радно место			
Датум доделе/промене/укидања права приступа			
Период важења права приступа			
Разлози за одобравање допунских права приступа			

Приступ		**Ниво**		**Захтев**	
Апликацијама	☐	Администратор	☐	Омогући	☐
Фолдерима	☐	Корисник	☐	Забрани	☐
Рачунарима	☐	Измена	☐	Суспендуј	☐
Просторијама	☐	Преглед	☐	Укини суспензију	☐
Радним станицама	☐	Унос	☐		☐
Domain ресурсима	☐	Штампање	☐		☐
Базама података	☐		☐		☐
	☐		☐		☐
	☐		☐		☐

ОПИС		

На основу спроведене анализе ризика по безбедност информација захтев се: **ОДОБРАВА – НЕ ОДОБРАВА** *(прецртати сувишно).*

ЗАХТЕВ ЗА ДОДЕЉИВАЊЕ/ПРОМЕНУ/УКИДАЊЕ ПРАВА ПРИСТУПА ИКТ СИСТЕМУ

Напомена у вези права приступа:

	Име и презиме	**Датум**	**Потпис**
Захтев поднео:			
Захтев одобрио:			
Налог за доделу права приступа примио:			

ЕВИДЕНЦИЈА ДОПУНСКИХ ПРАВА ПРИСТУПА

Ред. бр.	Име и презиме	Радно место/ Организација	Приступ[1]	Ниво[2]	Корисничко име	Лозинка	Датум доделе права	Датум укидања права
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								
14.								
15.								
16.								
17.								

	Име и презиме	Датум	Потпис
Израдио:			

[1] *А - Апликацијама, Ф - Фолдерима, Р - Рачунарима, П - Просторијама, РС - Радним станицама, Д - Домаин ресурсима, Б - Базама података.*

[2] *А – Администратор, К – Корисник, И – Измена, П – Преглед, У – Унос, Ш – Штампање.*