Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.05

Упутство за управљање односима са испоручиоцима

ISMS.05

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Управљање односима са испоручиоцима 2
3.1. Оцена ризика 2
3.2. Уговарање 2
3.3. Контрола приступа 2
3.4. Истек рока трајања уговора 2
4. Прилози и записи 3
5. Дефиниције и ознаке 3

1. Сврха и подручје примене

Сврха овог документа је да дефинише политику безбедности ИКТ система у односу на испоручиоце са којима Министарство туризма и омладине има уговорне односе.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Управљање односима са испоручиоцима

3.1. Оцена ризика

Потребно је спровести оцену ризика у вези поверљивости, интегритета и доступности информација уколико се за реализацију неког процеса ангажују екстерне организације („outsource“) или се дозвољава трећој страни да приступи ИКТ систему. На основу резултата анализе да ли је потребно дефинисање додатних клаузула о обавези поштовања политике безбедности ИКТ система у уговору, односно у захтевима конкурсне документације.

3.2. Уговарање

Потребно је у конкурсној документацији предвидети захтеви које испоручилац мора да испуни у вези безбедности ИКТ система.

Испоручилац мора да се обавеже уговором да ће обезбедити предузимање мера заштите у складу са прописима из области информационе безбедности и Актом о безбедности ИКТ система Министарства.

3.3. Контрола приступа

Потребно је да Министарство осигура да је испоручиоцу дат приступ само информацијама, односно деловима ИКТ система који су неопходни за реализацију посла. Контрола приступа се спроводи сходно одредбама документа *Упутство за контролу приступа (ISMS.04)*.

3.4. Истек рока трајања уговора

Након истека рока трајања уговора мора бити обезбеђено да је испоручилац вратио сву опрему и да су му укинута сва додељена права приступа.

4. Прилози и записи

РБ	Назив	Ознака	Начин идентификације записа	Одлагање на електронском медију	Одлагање на папирном медију	Период чувања
1.	План управљања испоручиоцима	ISMS.05.01	Према датуму и испоручиоцу	C(D):/ Dokumentacija/ Zapisi/ Plan upravljanja isporučiocima/ Datum-isporučilac.doc	Регистратор: Записи ИСО – Безбедност ИКИ система	3 године

5. Дефиниције и ознаке

ИСМС – систем менаџмента безбедношћу информација

МТО - Министарство туризма и омладине

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.06

- ISMS.06.01
- ISMS.06.02
- ISMS.06.03

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Упутство за управљање безбедносним инцидентима

ISMS.06

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Управљање безбедоносним инцидентима 2
   3.1. Пријава безбедоносних инцидената 2
   3.2. Процедуре за управљање безбедоносним инцидентима 2
   3.3. Реакција на безбедоносни инцидент 3
   3.4. Сакупљање доказа у случају безбедоносних инцидената 3
   3.5. Врсте инцидената 4
   3.6. Одговорности и овлашћења 5
4. Прилози и записи 5
5. Дефиниције и ознаке 5

1. Сврха и подручје примене

Циљ ове процедуре јесте ублажити негативне последице безбедносних инцидената те обезбедити брже реаговање на њих и успостављање нормалног функционисања операција погођених инцидентима. Процедура омогућава брзо додељивање одговорности за пријаву и решавање инцидената, чиме је омогућено брзо и професионално реаговање на њих као и праћење и решавање датих инцидентних ситуација.

2. Веза са другим документима

Овај документ се позива на важећу *Уредбу о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја.*

3. Управљање безбедносним инцидентима

3.1. Пријава безбедносних инцидената

Уколико инциденте открију запослени у Министарству, одмах након откривања пријављују их непосредном руководиоцу и лицу именованом за координацију активности у случају инцидента у ИКТ систему. Руководилац сектора унутар којег је инцидент пријављен одговоран је да у сарадњи са лицем именованом за координацију у случају инцидента преиспита озбиљност пријаве и, по потреби, организује тим за брзо и адекватно реаговање у датој ситуацији. Пријава инцидента се обавља помоћу формулара за пријаву безбедносног инцидента – *Евиденција безбедносног инцидента (ISMS.06.01)*. Попуњена пријава се шаље путем Емаил адресе или редовном поштом.

Уколико је пријава инцидента извршена усменим-телефонским путем, најкасније у року од два дана надлежном руководиоцу се треба доставити формулар за пријаву безбедносног инцидента који се потом прослеђује лицу именованом за координацију у случају инцидента.
Када запослени пријави безбедносни инцидент потребно је да се поступи на следећи начин:

- Престати са радом на компјутеру, односно средству рада у оквиру ИКТ система
- Не искључивати компјутер или било коју активну апликацију
- Не настављати управљање системом или апликацијом док се не добије службено овлашћење од стране ИТ да је могуће наставити са нормалним радом
- Не преносити информације о безбедносном инциденту осим овлашћеним лицима која су укључења у његово отклањање

3.2. Процедуре за управљање безбедносним инцидентима

Лице одговорно за координацију активности у случају инцидента је води и координише активностима у случају инцидента. Уколико је потребан тим за реаговање на инциденте, њега ће чинити:

- Лице одговорно за координацију активности у случају инцидента,
- Надлежни руководилац организационе целине унутар које је идентификован инцидент,
- Друга лица по потреби

Тим именује министар, односно надлежни државни секретар, а на предлог руководиоца.

У зависности од озбиљности инцидента тиму се могу прикључити и додатни чланови, као што су екстерни консултанти и сарадници или представници корисника.

У случају инцидента потребно је предузети следеће активности:

- Анализа и идентификација узрока инцидента,
- Ограничење непосредног утицаја инцидената,
- Категоризација инцидента,
- Увођење ограничења рада и забрана које произилазе из инцидента,
- Пружање упутстава крајњим корисницима за рад у датим условима,
- Планирање и имплементација превентивних контрола у случају грешке или сумње у решење,
- Планирање и имплементација корективних мера како би се спречило понављање инцидента,
- Комуницирање са укљученима или погођенима датим инцидентом,
- Извештавање о предузетим активностима приликом управљања инцидентом,
- Обавештење надлежних институција уколико је потребно (полиција, тужилаштво,..).

У случају појаве безбедносног инцидента, запослени је одговоран да прикупи и заштити све доказе и трагове који би могли да послуже интерној анализи инцидента као истражни материјал.

3.3. Реакција на безбедносни инцидент

Решење инцидента мора се евидентирати у облику *Извештаја о реакцији на безбедносни инцидент (ISMS.06.02)*. Лице одговорно за координацију активности у случају инцидента у обавези је да припреми извештај о догађају и да га достави надлежном руководиоцу. Надлежни руководилац је у обавези да анализира утицај инцидента на Министарство. Анализа се спроводи на обрасцу *Процена утицаја безбедносног инцидента (ISMS.06.03)*.

Надлежни руководилац подноси комплетан извештај о безбедносним инцидентима министру/државном секретару.

3.4. Сакупљање доказа у случају безбедносних инцидената

Кад год је то могуће морају се водити тачни записи о свим предузетим активностима и прикупити докази о истим.

То може подразумевати:

- Screenshot свих релевантних порука или информација,
- Аудит дневнике,
- Ручни запис хронологије инцидента,
- Оригиналне документе, укључујући записе о томе ко их је нашао, где и када,
- Детаље о сведоцима.

Једном прикупљени, докази се морају чувати на безбедном месту где се не могу мењати.

3.5. Врсте инцидената

Сви запослени дужни су да пријаве следеће инциденте:

- инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;
- инциденти који утичу на велики број корисника услуга;
- инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;
- инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;
- инциденти који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе.

Примери безбедносних инцидената које запослени треба да пријаве су: губитак поверљивости, интегритета или расположивости информација, тј. губитак сервиса, опреме, простора, ресурса или средстава због:

- Прекида у телекомуникацијама;
- Искључења провајдера ИТ сервиса;
- Прекида рада / нестанка струје;
- Инцидената / несрећа проузроковане природним катастрофама;
- Инцидената у случају избијања пожара.

Системске сметње / преоптерећења, квар софтвера, хардвера или комуникационих система:

- Стално смањене перформанси апликација;
- Дужи прекиди у софтверских решења;
- Грешке у обради података.

Људске грешке, злоупотребе, одстрањивања и откривања информација и ресурса:

- Намерно погрешно руковање опремом;
- Неовлашћено објављивање поверљивих информација;
- Откривање лозинке, коришћење лозинке друге особе;
- Објављивање података о личности трећим, неовлашћеним лицима;
- Грешке које су резултат непотпуних података;
- Кршење одредби физичке безбедности.

Крађа кључних информационих система (хардвера, софтвера, комуникационих система):

- Присуство неовлашћених особа у просторијама министарства;
- Неконтролисане промене у систему и напади;
- Хакерски напади;
- Напади вируса;
- Злонамерни програмски код;
- Самовољна инсталација неодобрених софтвера или уређаја;
- Неконтролисане промене услед промена у производњи и конфигурацији;

- Неправилно понашање система - индикација напада.

Неовлашћени приступ ресурсима и информацијама:
- Неовлашћени приступ компјутерским мрежама / апликацијама;
- Неовлашћени приступ деловима апликације за које запослени нема овлашћење.

3.6. Одговорности и овлашћења

Надлежни руководилац је одговоран за планирање и организовање активности *Процедуре за управљање безбедносним инцидентима (ISMS.06)*.

4. Прилози и записи

РБ	Назив	Ознака	Начин идентификације записа	Одлагање на електронском медију	Одлагање на папирном медију	Период чувања
1.	Евиденција безбедносног инцидента	ISMS.06.01	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Evidencija bezbednosnog incidenta/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
2.	Реакција на безбедносни инцидент	ISMS.06.02	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Reakcija na BI/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
3.	Процена утицаја безбедносног инцидента	ISMS.06.03	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Procena uticaja BI/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно

5. Дефиниције и ознаке

Овај документ не садржи дефиниције и ознаке.

ЕВИДЕНЦИЈА БЕЗБЕДНОСНОГ ИНЦИДЕНТА

За: Одговорно лице (именовано одлуком) Email: _____

Извештај о безбедносном инциденту			
Особа која извештава о инциденту			
Презиме		Име	
		Email	
Опис посла			
Датум избијања инцидента		Време избијања инцидента	
Датум пријаве инцидента		Време пријаве инцидента	

Информације о безбедносном инциденту			
ИТ инциденти		**Намерно изазвани инциденти**	
☐	Неовлашћени приступ	☐	Угрожена физичка безбедност
☐	Квар мреже (switch, ruter, modem, firewall)	☐	Крађа опреме / провала
☐	Квар система (кластер, сервер, складиштење, диск)	☐	Превара
☐	Квар софтвера(ОС, базе података или апликације)		
☐	Софтверски bug-ови		
☐	Мрежни сервиси нису доступни		
☐	Вируси / Worm/ Тројанци/е-маил напади		
☐	Adware / Spyware / злонамерни код / Спам		
Инциденти настали због губитка ресурса и/или сервиса		**Инциденти узрокованим природним непогодама и катастрофама**	
☐	Телецомуникациони проблеми	☐	Земљотрес
☐	Прекид напајања струјом или беспрекидно напајање	☐	Поплава
☐	Проблеми са климатизацијом	☐	Пожар
☐	Прекид рада опреме (не укључујући ИТ хардвера)	☐	Олуја
Инциденти узроковани људском грешком		**Инциденти узроковани употребом медија**	
☐	Програмерска грешка	☐	Телефон /факс
☐	Грешке у конфигурационој опреми	☐	Е-маил
☐	Грешке у документацији	☐	Интернет / chat, IRC...
☐	Игнорисање безбедносних прописа	☐	Компјутерски медији (CD, DVD, Floppydisk, HDD, USB Flash drive, меморијске картице)
☐	Неправилно коришћење		

Детаљи о безбедносном инциденту (кратак опис):					
Да ли су неки јавни сервиси и установе обавештени о инциденту?					
☐	Да (Ко?)	☐	Не	☐	Није познато
Остале особе обавештене о инциденту					
☐		☐			

ЕВИДЕНЦИЈА БЕЗБЕДНОСНОГ ИНЦИДЕНТА

☐		☐			
☐		☐			
Да ли је било инцидената ове врсте у прошлости?					
☐	Да (детаљи)	☐	Не	☐	Није познато
Детаљи:					
Да ли су узроци инцидента идентификовани?					
☐	Да	☐	Не		
Да ли су неке поверљиве информације угрожене?					
☐	Да (детаљи)	☐	Не	☐	Није познато
Детаљи:					
Да ли је дошло до прекида нормалног рада Министарства?					
☐	Да (детаљи)	☐	Не	☐	Није познато
Детаљи:					

Потпис подносиоца извештаја

_____

РЕАКЦИЈА НА БЕЗБЕДНОСНИ ИНЦИДЕНТ

Извештај о реакцији на безбедносни инцидент			
Лице одговорно за координацију активности у случају инцидента			
Име		Телефон	
Презиме		Email	
Сектор Група/одсек/одељење		Радно место	
Датум избијања инцидента		Време избијања инцидента	
Датум реаговања на инцидент		Време реаговања на инцидент	
Опис инцидента			
Остале контакт особе у случају избијања инцидента			
Име		Телефон	
Презиме		Email	
Сектор Група/одсек/одељење		Радно место	
Име		Телефон	
Презиме		Email	
Сектор Група/одсек/одељење		Радно место	
Име		Телефон	
Презиме		Email	
Сектор Група/одсек/одељење		Радно место	
Да ли је било инцидената ове врсте у прошлости?			
Да ☐	Не ☐	Није познато ☐	
Детаљи:			
Да ли су узроци инцидента идентификовани?			
Да ☐	Не ☐		
Да ли су неке поверљиве информације угрожене?			
Да ☐	Не ☐		

РЕАКЦИЈА НА БЕЗБЕДНОСНИ ИНЦИДЕНТ

Детаљи:		
Да ли је дошло до прекида нормалног рада Министарства?		
Да ☐	Не ☐	Није познато ☐
Детаљи:		
Време трајања инцидента		
Детаљи:		
Компјутерски системи, хардвери / или софтвер погођени инцидентом		

Предузете мере у случају избијања инцидента			
Нису предузете мере	☐	Обнављање помоћу backup-а	☐
Сервер / PC искључен из мреже	☐	Backup и заштита података	☐
Чишћење од вируса/ злонамерних софтвера	☐	Реинсталирани ОС	☐
Промена конфигурације	☐	Техничка подршка	☐
Замена опреме или делова опреме	☐	Друге	

Додатне информације о предузетим мерама

Лица укључена у решавање инцидента			
Име и презиме		Потпис	
Име и презиме		Потпис	
Име и презиме		Потпис	

Да ли је проблем решен		
Да ☐	Не ☐	Потребна истрага ☐

Датум

_____

Извештај саставио:

_____

ПРОЦЕНА УТИЦАЈА БЕЗБЕДНОСНОГ ИНЦИДЕНТА

Кратак опис инцидента и утицај који је изазвао:

Предузете активности ради ублажавања последица инцидента:

Оцена утицаја безбедносног инцидента		
Време трајања инцидента*	Опис штете**	Оцена безбедносног инцидента***

*унети број из табеле „Време трајања инцидента“
** унети број из табеле „Опис штете“
*** Оцена безбедносног инцидента је једнака највећој додељеној оцени у било којој од 3 категорије

Време трајања инцидента		**Опис штета**		
Ознака приоритета	**Рок за обнову и рестаурацију пословања у сатима**	**Оцена штете**	**Опис штете**	
1	1 сат	1	Занемарљива штета	
2	4 сата	2	Мала штета	Краткорочна штета
3	24 сата	3	Средња штета	Материјална штета
4	72 сата	4	Велика штета	Значајна штета са последицама
5	>72 сата	5	Штета је катастрофална	Престанак функционисања ИКТ система

Датум: _____

Одговорно лице (именовано одлуком)

_____

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.07

- ISMS.07.01
- ISMS.07.02
- ISMS.07.03
- ISMS.07.04

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Поступак дефинисања плана континуитета пословања

ISMS.07

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. План континуитета пословања 2
   3.1 Анализа ризика 2
   3.2 План управљања ризицима 3
   3.3 Опште мере 3
   3.4 Верификација и унапређење 4
4. Прилози и записи 4
5. Дефиниције и ознаке 5

1. Сврха и подручје примене

Документ описује начин поступања МТО у случају настанка ванредних ситуација, као и активностима које је потребно спровести пре, у току и након ванредне ситуације како би се смањила могућност настанка ванредне ситуације, потенцијалне последице свеле на минимум.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. План континуитета пословања

3.1 Анализа ризика

Пре израде *Плана континуитета пословања (ISMS.07.01)* министарство врши анализу ризика, која подразумева идентификацију и анализу могућих ризика којима је МТО изложена и израђује се на обрасцу *Анализа ризика по континуитет пословања (ISMS.07.01)*. Ова анализа обухвати све потенцијалне ванредне ситуације које могу озбиљно угрозити пословање МТО и изазвати привремену обуставу рада. Предмет анализе нису одступања мањег обима која се могу јавити у свакодневном пословању и која се решавају на оперативном нивоу без већих последица на рад (на пример привремени прекиди интернет комуникације, застоји на појединачним деловима система и сл.). Анализа подразумева и идентификацију ефеката ванредне ситуације на рад МТО, вероватноћу настанка и јачину ефеката ванредне ситуације. Да би се адекватно оценила ванредна ситуација, у обзир треба узети и мере које су предузете у тренутку оцене ризика.

За потребе анализе користи се следећи систем оцене и класификације ванредних ситуација:

Вероватноћа

1 – вероватноћа настанка ванредна ситуација је минимална; ванредна ситуација се никада раније није појављивала или се појављивала под таквим околностима да није имала утицај; МТО предузима адекватне мере тако да је ризик минималан.
2 – постоји реална вероватноћа појаве ванредне ситуације, ванредна ситуација се у мањем обиму јављала у претходном периоду; предузете су одговарајуће мере, али откази или сличне аномалије у систему, могу умањити ефективност предузетих мера.
3 – ванредна ситуација се готово редовно јавља; не постоје ефективне мере превентивног деловања или ране детекције.

Ефекат

1 – настала ванредна ситуација има веома мале последице на МТО; ванредна ситуација не изазива дужи прекид рада или је прекид ограничен на поједине процесе који нису кључни за МТО; последице по имовину МТО су минималне; не постоји могућност оштећења имовине корисника.

2 – ефекат ванредне ситуације је умерен; изазива краћи прекид у раду кључних активности, или дужи прекид активности које нису од већег значаја за МТО;

последице по имовину МТО су ограничене, постоји могућност брзог опоравка и замене оштећене имовине; постоје ограничени ефекти на имовину корисника.

3 – ванредна ситуација оставља озбиљне последице по имовину МТО, онемогућава одвијање процеса на нивоу читавог МТО; има озбиљне последице на имовину корисника; без предузимања системских и превентивних мера ванредна ситуација би могла да изазове трајан прекид у раду МТО.

Све ванредне ситуације чија је укупна оцена већа од 4 спадају у категорију ванредних ситуација за које је потребно дефинисати додатне мере у циљу минимизирања ефеката. У зависности од расположивости ресурса и планираних инвестиција у наредном периоду, могу се предузети и додатне мере за ванредне ситуације чија је укупна оцена испод 4.

Анализу ризика је потребно ревидирати минимум једном у 3 године, а по потреби и чешће и то минимум сваки пут када се појави ванредна ситуација, као и када се после симулације ванредне ситуације утврди да постоје пропусти у планом предвиђеним мерама.

3.2 План управљања ризицима

Узимајући у обзир утврђене ванредне ситуације и њихов укупни утицај на МТО, потребно је планирати (на обрасцу *План управљања ризицима по континуитет пословања (ISMS.07.02)*) и реализовати мере које имају за циљ свођење ефеката ванредне ситуације на прихватљив ниво. Ове мере не замењују већ предузете мере и не елиминишу ниједан од успостављених система превенције, осим ако није другачије наведено.

Циљно време опоравка подразумева временски период за који се предвиђа да ће МТО бити у могућности да настави са реализацијом свакодневних активности са ограниченим капацитетима и процењује се на основу процена спремности МТО за реаговање у ванредним ситуацијама, расположивих капацитета и процењених ефеката ванредне ситуације.

3.3 Опште мере

Општа процедура поступања у ванредним ситуацијама подразумева следеће:

- Обавестити сва лица чланове кризног штаба о насталој ситуацији, без одлагања.
- У зависности од настале ситуације позвати хитне службе (хитна помоћ, ватрогасно спасилачка јединица итд.) и дати информације о насталој ситуацији и потребама деловања. Свако давање додатних информација трећим лицима без одобрења руководиоца именованог за координацију ванредне ситуације је строго забрањено.
- Руководилац именован за координацију ванредне ситуације окупља чланове на договореној локацији, формира оквирни план реаговања, процену штете и начин даљег поступања и информисања заинтересованих страна.
- Контактирати кључне институције и направити план опоравка - приоритет је оспособљавање кључне информационо комуникационе опреме. Прикупити све информације о расположивим ресурсима кључних институција и роковима одзива (нпр. за колико времена је могуће оспособити информационо комуникациони систем и сл.). У оквиру ових активности морају се предузети све мере за обезбеђење

информационих добара (заштита од оштећења, заштита од случајног/намерног отуђења итд.)
- Обезбедити људске и материјалне ресурсе потребне за минималан процес рада.
- Минималну опрему и запослене потребне за наставак рада упутити на секундарну локацију (претходно договорену са кључним институцијама са којима је успостављен договор о коришћењу ресурса у случају ванредна ситуација, уколико су ванредна ситуација захваћене све секундарне локације МТО).
- Обезбедити услове за повратак на примарну локацију.
- Наставак уобичајеног пословања.

3.4 Верификација и унапређење

За потребе верификације ефективности плана континуитета пословања, потребно је минимум једном у 3 године извршити ревизију комплетног плана, по потреби ажурирати, поновити обуку свих запослених и симулирати бар једну ванредну ситуацију како би се утврдила ваљаност овог плана.

План је потребно ревидирати и након сваке појаве ванредне ситуације или битнијих промена у систему које могу утицати на спремност МТО за реаговање у, и након ванредна ситуација.

4. Прилози и записи

РБ	Назив	Ознака	Начин идентификације записа	Одлагање на електронском медију	Одлагање на папирном медију	Период чувања
1.	Анализа ризика по континуитет пословања	ISMS.07.01	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Analiza rizika po kontinuitet poslovanja / Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
2.	План управљања ризицима по континуитет пословања	ISMS.07.02	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Plan upravljanja rizicima po kontinuitet poslovanja / Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно
3.	Информације од значаја за поступање у ванредним ситуацијама	ISMS.07.03	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Informacije za postupanje u vanrednim situacijama / Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно

4.	Извештај о провери континуитета безбедности информација	ISMS.07.04	Према датуму креирања	C(D):/ Dokumentacija/ Zapisi/ Izveštaj o proveri kontinuiteta BI/ Datum.doc	Регистратор: Записи ИСО – Безбедност ИКТ система	Трајно

5. Дефиниције и ознаке

ИСМС – систем менаџмента безбедношћу информација

Ванредна ситуација - стање када су ризици и претње или последице катастрофа ванредних догађаја и других опасности по људе, животну средину, материјална добра и пословне процесе, таквог обима и интензитета да њихов настанак или последице није могуће спречити или отклонити редовним деловањем, због чега је за њихово ублажавање и отклањање неопходно употребити посебне мере, снаге и средства уз појачан режим рада.

МТО – Министарство туризма и омладине

АНАЛИЗА РИЗИКА ПО КОНТИНУИТЕТ ПОСЛОВАЊА

Ванредна ситуација	Ефекти - опис	Предузете мере	Вероватноћа настанка ВС	Ефекти ВС	Укупно

	Име и презиме	Датум	Потпис
Израдио:			
Одобрио:			

ПЛАН УПРАВЉАЊА РИЗИЦИМА ПО КОНТИНУИТЕТ ПОСЛОВАЊА

Ванредна ситуација	Укупна оцена	Циљно време опоравка	Мере које је потребно предузети	Одговорност за реализацију	Рок за реализацију

	Име и презиме	Датум	Потпис
Израдио:			
Одобрио:			

Контакти учесника у ванредној ситуацији:		
Име и презиме	**Функција**	**Контакт телефон**
	Руководилац	
	Члан	
	Члан	
	Члан	
	Члан	

Локација окупљања чланова кризног штаба:

Хитне службе:	
Назив	**Контакт телефон**
Хитна помоћ	
Ватрогасна јединица	
Полиција	
.....	

Контакти екстерних организација значајних за поступање у ванредним ситуацијама:	
Назив	**Контакт телефон**

Људски ресурси потребни за минималан процес рада	
Име и презиме	**Радно место**

Материјални ресурси потребни за минималан процес рада		
Назив	**Спецификација**	**Количина**

	Име и презиме	**Датум**	**Потпис**
Израдио:			
Одобрио:			

ИЗВЕШТАЈ О ПРОВЕРИ КОНТИНУИТЕТА БЕЗБЕДНОСТИ ИКТ СИСТЕМА

Назив процеса:	
Назив вежбе за управљање континуитетом	
Датум вежбе:	
Припремио:	<ИмелицакојејеприпремилоИзвештај>
Одговорност за спровођење вежбе	<Име>
Унос плана и циљева извршио:	<Име>
Унос у вези са исходом извршења извршио:	<Име извршне стране>
Одобрио:	
Достављено:	

1. Опис и циљеви

Објашњење: .Одредите врсту вежбе, време, улогу сваког учесника, који планови се примењују и који су мерљиви циљеви вежбе. У зависности од сложености вежбе неопходно је укључити више учесника. Сами можете да реализујете једноставнију вежбу (планирање/ извршавање/ извештавање)
Савет 1: Проверите да ли сте усклађени са учесницима по питању планирања, извршавања, извештавања и праћења.
Савет 2: Ако је вежба сложена или ако никад раније није извођена, препоручује се да се у сали за састанке „прође кроз" штампану документацију вежбе да би проверило да ли је јасно шта треба урадити.

1.1 Опис вежбе:

Следеће тачке треба да буду укључене у опис вежбе, у оквиру кога је, на пример, планирано премештање апликације MSMail (Exchange) на сервер за израду резервних копија:

Предмет	Опис
Модалитет:	Планирана/непланирана.
Објава:	Објављена или необјављена
Сценарио:	Нпр. Резервна копија за маил не функционише отказа сервера.
Опис вежбе: (главни кораци)	• Премештање функције сервера за маил ради опоравка и покретања на хосту за резервне копије на резервној локацији. • Оставити систем да ради на хосту за резервне копије током периода од недељу дана. • Преместити сервер за електронску пошту
Коришћени планови/процедуре/документација: назив/верзија плана/процедура)	
Неопходна припрема састанка на коме се „пролази кроз" штампану документацију	да/не

1.2 Циљеви:

Овде треба навести мерљиве циљеве:

Број циља	Опис циља
1	Дефинисано време потребно за опоравак
2	Обезбедите доказе о оспособљености да извршите опоравак система за израду резервних копија у непредвиђеним ситуацијама.
3	Контрола квалитета, валидација (без грешака) механизама и процедура за непредвиђене ситуације.
4	Текућа документација треба да буде 100% ажурирана; верификација + (по потреби) ажурирање процедура за непредвиђене ситуације.
5	Циљ је вежба/обука.

Резултат вежбе се дефинише током вежбе или непосредно након вежбе

2. Резултат вежбе

Објашњење: резултати реализоване вежбе/обуке. Молимо Вас да изаберете једну од опција наведених у наставку.

- **Успешно** (нису се јавили проблеми, осим мањих процедуралних проблема)
- **Делимично успешно** (проблем се јавио, нпр. Временски циљеви нису испуњени или је дошло до преузимања или опоравка)
- **Неуспешно** (вежба/обука се морају одбацити).

2.1 Резултат вежбе: успешно, делимично успешно или неуспешно.

- Вежба је била: ...
- Ако циљеви НИСУ испуњени, навести их у наставку:

Број циља.	Шта није испуњено у оквиру овог циља? (кратка спецификација)

2.2 Откривени проблеми/изузеци

О свим проблемима, такође и у оквиру процедура, морају се поднети извештаји. Молимо Вас да у наставку наведете референце и описе (у само једној линији) проблема који се јављају, укључујући и проблеме у вези са документацијом.

Р. бр	Опис проблема

2.3 Резиме руководства

Дефинишите кључне кораке (не све кораке) вежбе. Наведите време које је било потребно за опоравак уколико је опоравак извршен, а ради поређења са дефинисаним временом за поновно успостављање процеса.

- Укупно време опоравка: сати ..... минута.

Време	Опис

Напомене:

- .....

3. Праћење (попотреби)

Објашњење: Овде се наводе активности праћења. Као резултат ове вежбе, да ли морају да се прате елементи хардвера, софтвера, процеса, документације? Ко шта ради?

Р.бр	Акција о проблему или документацији/процесу коју треба пратити	Одговорно лице	Рок

Израдио: _____ **(потпис)** **Датум:**_____
Одобрио: _____ **(потпис)** **Датум:**_____

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.08

Упутство за безбедно коришћење мобилних уређаја

ISMS.08

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Коришћење мобилних уређаја 2
3.1 Како се користе мобилни уређаји 2
3.2 Подешавање мобилних уређаја 2
3.3 WLAN корисници 2
3.4 Извршна правила 2
3.5 Упутство за оператере 3
3.6 Упутство за WLAN оператере 3
4. Прилози и записи 3
5. Дефиниције и ознаке 3

1. Сврха и подручје примене

Документ дефинише правила која се морају поштовати приликом употребе мобилних уређаја или других уређаја који користе бежичну интернет конекцију.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Коришћење мобилних уређаја

3.1 Како се користе мобилни уређаји

- Губљење или крађа мобилних уређаја мора се одмах пријавити и писмено евидентирати.
- Мобилни уређаји који се пронађу, а власништво су МТО треба да се пријаве и писмено евидентирају.
- Сваки мобилни уређај на ком се обављају пословни задаци мора да се чува и употребљава у складу са безбедносним правилима.
- Строго је забрањено коришћење мобилних уређаја који нису власништво МТО за извршавање пословних задатака који се тичу министарства.
- Сигурносна копија се мора редовно правити за уређаје на којима се обављају пословне активности.

3.2 Подешавање мобилних уређаја

- Сигурносна подешавања на мобилном уређају се не смеју мењати ни под каквим околностима.
- Уколико је уређај власништво МТО сигурносна подешавања се морају извршити пре уступања уређаја на коришћење.
- Сигурносна подешавања се морају редовно проверавати за познате уређаје.

3.3 WLAN корисници

- WLAN конекција се мора прекинути када се не користи.
- Екстерном мрежном инфраструктуром поверљиви подаци се могу преносити само преко VPN (Vitrual Private Network) конекције.
- Незаштићени SSID се не смеју објавити, потребно је користити макар минималну аутентификацију (нпр. сигурносни ниво WPA2-PSK).
- Поверљиви и строго поверљиви подаци не смеју се транспортовати кроз екстерну мрежну инфраструктуру.

3.4 Извршна правила

- Враћање уређаја од стране запослених се мора спровести у складу се процедуром.
- Размена или примопредаја уређаја између запослених мора се спровести уз одобрење руководиоца унутрашње организационе јединице.

3.5 Упутство за оператере

Односи се на све мобилне уређаје који су власништво МТО:

- Морају бити инсталирана и подешена сва сигурносна подешавања.
- Заштитни приступни софтвери морају бити инсталирани.
- Антивирусна заштита мора бити инсталирана и подешена.
- Уколико је потребно да уређај сервисима приступа преко VPN конекције, онда сва подешавања морају бити извршена у складу са упутствима и процедурама УЗЗПРО која омогућава VPN приступ.
- На свим уређајима редовно морају бити ажуриране све сигурносне системске надградње.
- Уређајима који су власништво МТТ треба да садрже контакт информације, које би помогле враћању уређаја у случају губитка.
- Анонимни приступ свим подацима од значаја мора бити онемогућен.

3.6 Упутство за WLAN оператере

- SSID не сме имати назив који може да указује да се ради о мрежи МТО .
- Бежичне мреже МТО морају се редовно осматрати и контролисати.
- Административни приступ мрежном уређају мора бити онемогућен за приступ споља и мора бити заштићен јаком лозинком, треба размотрити и могућност промене подразумеваног корисничког имена.
- Административни приступ вршити само преко кабла.
- Бежична мрежа мора бити строго одвојена од LAN мреже.
- Потребно је извршити реконфигурацију украдене WLAN опреме која приступа мрежи.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине.

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.09

Упутство за одржавање ИКТ система
ISMS.09

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Одржавање ИКТ система 2
   3.1 Полазне основе 2
   3.2 Пуштање у рад, одржавање и расходовање опреме 3
   3.3 Тестирање, инсталирање и одржавање софтвера 3
   3.4 Управљање локалном рачунарском мрежом (LAN) 4
   3.5 Заштита од вируса 5
   3.6 Резервне копије 5
   3.7 Едукација корисника 6
4. Прилози и записи 6
5. Дефиниције и ознаке 6

1. Сврха и подручје примене

Документ дефинише основна правила одржавања ИКТ система унутар МТО.

2. Веза са другим документима

Овај документ се позива на:
- Упутство за поступање са резервним копијама,
- Упутство за управљање безбедносним инцидентима,
- Поступак управљања људским ресурсима са аспекта безбедности информација.

3. Одржавање ИКТ система

3.1 Полазне основе

Искључива намена опреме у ИКТ систему МТО је да служи као средство за рад и није допуштено коришћење исте за обављање приватних послова.

Евиденција о опреми и софтверу води се путем докумената:
- Преглед опреме (електронски документ), који садржи ажуран списак рачунарске и телекомуникационе опреме у МТО и основне податке о опреми.
- Картон опреме (електронски документ), који је отворен за опрему, а садржи основне податке о опреми и податке о одржавању опреме.
- Евиденција одржавања, где се воде све „интервенције“ на опреми,
- Евиденцију дозвољених приступа појединим деловима информационог система,
- Евиденција преносивих медијума и удаљених локација на којима се чувају подаци.

Опрема се означава у складу са важећим системом означавања у МТО.

За вођење евиденције о опреми и софтверу задужен је администратор који се именује на нивоу МТО-а и/или његових сектора.

При томе се изричито забрањује коришћење рачунарске мреже са циљем неовлашћеног уласка у делове информационог система или друге системе путем заобилажења сигурносних механизама. Такође, забрањује се коришћење помоћних средстава (хардверских и софтверских) за анализу мреже којима се откривају сигурносни параметри и поверљиве информације других корисника или система. Корисници за које се установи да су прекршили наведена правила сносе одговорност за извршене радње сходно закону и другим актима.

Обавеза администратора подразумева свакодневно праћење рада информационог система, анализу архивских (лог) фајлова и проверу рада мрежних сервиса.

Задатак администратора је и надгледање функционисања система, како би се открили недопуштене активности. У случају инцидента, тј. активности корисника које нису у оквиру прихватљивог коришћења информационог система, администратор је дужан да о томе писаним путем обавести руководство сходно документу *Управљање безбедносним инцидентима (ISMS.06)*.

Администратор је дужан да у своме раду поштује приватност корисника и поверљивост информација с којима долази у додир при обављању посла.

Администратор је обавезан да води евиденцију свих преносивих медијума који су део информационог система МТО и медијума на удаљеним локацијама на којима се чувају

подаци.

3.2 Пуштање у рад, одржавање и расходовање опреме

Опрема се мора поставити или заштитити тако да се смање ризици од претњи и опасности из окружења, као и могућности за неовлашћени приступ. Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система. Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку за информационе услуге морају да буду заштићени од пресретања, ометања или оштећења тј. морају бити постављени у зиду или каналицама, и на друге начине извршена изолација од могућег оштећења.

Сервери и активна мрежна опрема (switch, modem, router, firewall), морају стално бити прикључени на уређаје за непрекидно напајање – UPS и мора се налазити у закључаном rack орману. Администратор је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности. У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, дужан је да искључи опрему у складу са процедурама произвођача опреме

У случају расходовања преносивих медијума, администратор је дужан да све податке уклони са истих, пре него што се изврши уништење/расходовање медијума. Исти принцип важи и за све рачунаре на којима су складиштени подаци.

Опрема, информације похрањене на одговарајућим медијумима, као и софтвер не смеју се измештати без претходног одобрења. На измештену имовину морају се применити механизми безбедности, узимајући у обзир различите ризике при раду изван просторија МТО. У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење одговорног лица који ће одредити услове, начин и место изношења опреме. ИКТ опрема се из просторије у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења. Ако се опрема износи ради сервисирања, поред одобрења, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Када је из било ког разлога потребно извршити транспорт медијума, администратор је обавезан да обезбеди да се то реализује на начин који неће имати негативан утицај на безбедност података (лични транспорт у циљу заштите од приступа трећих лица, закључавање одговарајућим шифрама, адекватно транспортно паковање у циљу заштите од физичких оштећења и сл.)

По добијању информација о престанку ангажовања запосленог, администратор је дужан да онемогући приступ и остале привилегије свим деловима ИКТ, запосленом чији радни однос/ангажовање је престао.

3.3 Тестирање, инсталирање и одржавање софтвера

При тестирању софтвера потребно је обезбедити неометано функционисање ИКТ система, а пре самог увођења у рад неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију. За тестирање се морају користити искључиво сервери и подаци који су намењени тестирању и развоју. Приликом

тестирања система, подаци који су означени као поверљиви морају бити на адекватан начин заштићени, како не би били злоупотребљени или на други начин компромитовани.

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије, мора се вршити на начин који не омета оперативни рад запослених-корисника.

У случају да се на новој верзији софтвера који је уведен у оперативни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

3.4 Управљање локалном рачунарском мрежом (LAN)

Систем администратор, односно лице које је одговорно за управљање мрежом, конфигурише мрежне уређаје, додељује адресе, сегментује мрежу, креира виртуелне LAN-ове, успоставља VPN комуникацију преко интернета са другим референтним тачкама који за то имају одобрење. Администратор мора у сваком тренутку имати тачан попис свих мрежних прикључака и мрежних уређаја, укључујући и лаптоп рачунаре. Поред прецизних информација о попису мреже, администратор мора редовно ажурирати логичку мапу мрежне и мрежне инфраструктуре.

Виртуелизација мреже се употребљава због удобнијег рада, штедње постојећих ресурса и сигурности, остварује се употребом VLAN-ова. VLAN дозвољава администратору да групише унутар истог мрежног опсега (broadcast домена) различите мрежне уређаје и портове, без обзира на физичку локацију у локалној мрежи. Рачунарска мрежа МТО подељена је на следеће сегменте:

- Менаџмент мрежу – У овој мрежи се налазе сви административни уређаји којима приступ имају само администратори. Мрежа има строго дефинисана правила приступа, могу јој приступити само познати уређаји којима је дозвољен приступ.
- Сервер мрежу – У овој мрежи се налазе серверски уређаји на којима се размењују подаци са јавним и локалним клијентима. Мрежа има строго дефинисана правила приступа, могу јој приступити само познати уређаји којима је дозвољен приступ, а унутар мреже се налазе само серверски уређаји.
- Корисничку мрежу – Ово је сегмент мреже где се налазе само запослени у МТО са унапред дефинисаним IP адресама и правима приступа који је у складу са политиком коришћења ИКТ система.
- Voice мрежа - Ово је мрежа у којој се налазе ИП телефони. Мониторинг мреже и уређаја у мрежи врши "Телеком Србија".
- WLAN - Ово је изолована мрежа намењена за бежичне кориснике и непознате "гост" кориснике, она је потпуно изолована од и потпуно је онемогућен приступ свим сервисима ИКТ МТО система.

VPN (Virtual Private Network) омогућава удаљеним корисницима да преко интернета приступе локалној мрежи и сервисима који су им неопходни. Администрацију, конфигурисање и креирање налога за приступ VPN мреже врши Канцеларија за информационе технологије и електронску управу (КЕУ), која је такође надпровајдер МТО и омогућава им приступ интернету. Нови налози корисника се издају у складу са процедуром КЕУ по којој је неопходно да се одговорно лице обрати писменим захтевом у ком се тражи отварање новог налога и жељеном сегменту мреже. Онемогућен је VPN приступ Менаџмент мрежи и администрација се не врши преко VPN.

Администратор је обавезан разрадити правила за спајање на мрежу гостујућих рачунара, која доносе са собом спољни сарадници, предавачи, пословни партнери, сервисери, итд. Не сме се дозволити да они сами прикључују рачунаре на мрежу због опасности од ширења вируса, или намерних агресивних радњи попут пресретања мрежног саобраћаја, прикупљања информација, итд. Администратор дефинише прикључна места за гостујуће рачунаре, а конфигурацијом мрежних уређаја спречава да гостујући рачунар улази у локалну рачунарску мрежу МТО. Гостима и спољним сарадницима се омогућује несметано и сигурно коришћење интернета, успостава VPN-а према сопственим системима, као и ограничено коришћење мрежних ресурса МТО, искључиво уз одобрење руководства. При томе се мора водити рачуна да интерни корисници и апликације имају приоритет. Даљински приступ ресурсима LAN-а за запослене и спољне сараднике који су ангажовани због неког пословног процеса је потребно обезбедити на начин да се не угрожава безбедносна политика МТО (обезбедити потребан хардвер и софтвер).

3.5 Заштита од вируса

Заштита локалне рачунарске мреже од разних малициозних напада, споља и изнутра, обезбеђује се firewall уређајем, механизмима енкрипције и заштите интегритета података и централном инсталацијом антивирусног софтвера са разним модулима заштите (File Anti-virus, Mail Anti-virus, Web Anti-virus, Anti-spy, Anti-hacker, Anti-spam).

Администратор је дужан инсталирати антивирусне програме на све корисничке рачунаре и централизовати администрацију тако да се измене у бази вируса и у конфигурацији аутоматски пренесу на све корисничке рачунаре, без активног учествовања корисника.

Корисници не смеју самовољно искључити антивирусну заштиту на свом рачунару и не смеју инсталирати друге врсте антивирусног програма. Уколико из неког разлога морају привремено зауставити антивирусни програм, корисници морају затражити дозволу од администратора.

Уколико се деси да је антивирус детектовао вирус од неког рачунара или медијума које је власништво МТО корисник је дужан да то одмах пријави администратору. Администратор није дужан чувати електронске поруке корисника заражене вирусима.

Обавезно је, у зависности од финансијских могућности и потреба МТО за бољом безбедношћу података, пратити техничко-технолошки развој на овом пољу и примењивати (усвајати) актуелне напредне технике безбедности за LAN.

3.6 Резервне копије

Резервне копије омогућују опоравак информационог система у случајевима губитка података као што су:

- сигурносни инциденти,
- губитак података због случајних или намерних догађаја,
- хаварије,
- остали нежељени и непредвиђени догађаји.

Процес управљања резервним копијама обухвата поступке израде, чувања и тестирања података у складу са *Упутством за поступање са резервним копијама (ISMS.11)*.

3.7 Едукација корисника

Непланирани и нежељени догађаји у ИКТ систему најчешће настају као последица ненамерних радњи као што су грешке или пропусти, а ређе као последица намерних радњи почињених с циљем наношења штете ИКТ систему. Како би се наведени догађаји и њихово штетно деловање свели на прихватљив ниво, потребно је едуковати кориснике ИКТ система.

Едукација корисника треба да садржи следеће елементе:

- едукација потребна за правилно коришћење ресурса ИКТ система, како би на ефикасан и сигуран начин користили ИКТ систем у оквиру обављања пословних задатака,
- потребно је упознати кориснике с интерним актима (политике, процедуре и остали поступци којих корисници треба да се придржавају), како би били упознати са обавезама, оквирима деловања и личним одговорностима.

Горе наведена едукација корисника се може имплементирати:

1. организовањем интерних курсева и презентација у МТО,
2. стручним обукама из области коришћења корисничких апликација,
3. обезбеђењем стручне литературе.

Едукација корисника из области коришћења корисничких апликација треба да буде до нивоа детаљности који захтева извршење њихових пословних задатака сходно документу *Управљање људским ресурсима (ISMS.03)*.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине.

УЗЗПРО – Управа за заједничке послове републичких органа.

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.10

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Упутство за коришћење ИКТ система - Општа правила

ISMS.10

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Општа правила коришћења ИКТ система 2
4. Прилози и записи 4
5. Дефиниције и ознаке 4

1. Сврха и подручје примене

Документ дефинише основна правила за коришћење ИКТ система Министарства туризма и омладине

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Општа правила коришћења ИКТ система

Искључива намена опреме у оквиру ИКТ система МТО је да служи као средство за рад и није допуштено коришћење исте за обављање приватних послова.

Приликом коришћења имовине ИКТ система, корисник се мора придржавати следећих правила:

1) да користи информатичке ресурсе искључиво у пословне сврхе;
2) да прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво МТО и да могу бити предмет надгледања и прегледања;
3) да поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4) да безбедно чува своје лозинке, односно да их не одаје другим лицима;
5) да мења лозинке сагласно утврђеним правилима;
6) да пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу;
7) да захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8) да обезбеди сигурност података у складу са важећим прописима;
9) да приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) не сме на радној станици да складишти садржај који не служи у пословне сврхе;
12) да израђује заштитне копије (backup) података у складу са прописаним процедурама;
13) да користи интернет и електронску пошту у МТО у складу са прописаним процедурама;
14) да прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
15) да прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
16) да прихвати да технике сигурности (анти вирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему.
17) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

Свако кршење горе наведених правила и радњи које намерно оштећују рачунарску мрежу и остале ресурсе ИКТ система, утичу на уобичајене могућности функционисања истих или доводе до поремећаја, сматрају се кршењем овог упутства о коришћењу и представља повреду радне обавезе.

За радње извршене под одређеним корисничким именом и лозинком, одговоран је корисник. Сваки корисник ради под својим корисничким именом уз обавезу коришћења лозинке. Почетну корисничку лозинку одређује Администратор. Предефинисана лозинка (лозинка која се добије од администратора) се мора заменити након првог логовања.

Корисник је обавезан да памти своју лозинку и дужан је при првом пријављивању у систем да је промени, а препоручује се да је мења сваких месец дана, а најмање једном у 6 месеци. Иста лозинка се не сме понављати у временском периоду од годину дана.

Препоруке за креирање јаке лозинке:

- има најмање 8, а идеално је 14 карактера;
- садржи комбинацију великих и малих слова, бројева и знакова као што су #, !, $ итд.;
- не садржи цело или делове корисничког имена, називе организационих целина или њихове скраћенице;
- не садржи датум рођења, број телефона и друге препознатљиве податке;
- не треба да садржи слова из ћириличног писма као што су ш,ч,ћ итд.
- не користи тривијалне речи или фразе које се често понављају не користити исту лозинку за различите нивое сигурности (удаљени приступ, приступ апликацијама, системски приступ);
- PIN мора да садржи насумично одабране бројеве.

Лозинку сме да зна само корисник. Ако запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени и обавести администратора о могућем инциденту.

Лозинке не треба остављати на папирићима који су залепљени на екран, или остављени на столовима, или у незакључаним ладицама. Корисник је одговоран да чува тајност своје лозинке и ни у ком случају је не треба откривати. Ако се лозинка чува у електронском облику на рачунару, фајл се мора шифровати.

Уколико корисник заборави лозинку коју је сам поставио, треба да се обрати Администратору. Администратор ће у том случају поново поставити одређену почетну лозинку, након чега ће корисник моћи даље самостално да мења лозинку

Недозвољеним се сматра свако коришћење рачунара на начин који доводи до повреде важећих закона и етичких норми, а могу да узрокују материјалну или нематеријалну штету за МТО.

Коришћење нелегалног тј. не лиценцираног софтвера представља повреду ауторског права и интелектуалног власништва. Забрањено је инсталирати све врсте софтвера за које не постоје одговарајуће лиценце. Уколико постоји потреба корисника за инсталацијом додатних апликативних програма, захтев се упућује Администратору, који потом обавештава руководство.

Корисници не смеју самовољно искључити антивирусну заштиту на своме рачунару и не смеју инсталирати друге врсте антивирусног програма. Уколико из неког разлога морају привремено зауставити антивирусни програм, корисници морају затражити дозволу од Администратора.

Кориснички рачунари и њима припадајућа периферна рачунарска опрема (нпр. штампач, скенер, итд) се након завршетка радног времена искључују.

Пре сваког напуштања радног места (и у току радног времена), а у циљу онемогућавања приступа информационом систему неовлашћеним лицима, корисник је обавезан да се одјави из радног окружења тј. закључа рачунар – одабирањем опције стање приправности ("Stand by") или одјави се ("Log off") уместо искључи ("Shut down") приликом уобичајене процедуре искључења рачунара. Приликом прикључења корисника у ИКТ систем иницијално се подешава да се рачунар аутоматски „закључа" након 10 минута неактивности. Уколико корисник жели да промени вредност овог временског периода или да у потпуности искључи аутоматско закључавање, треба да се обрати Администратору. У случају искључења аутоматског закључавања, корисник је дужан да се одјави са рачунара путем наведене процедуре.

Политика „чистог стола" и „чистог екрана" мора се поштовати, нарочити када су у питању поверљиве информације. Ово значи да се поверљиви подаци било у електронској форми, било у папиру не смеју оставити незаштићени, на видним местима и доступни другим лицима која немају овлашћење за приступ истим. Сва креирана документа не смеју бити сачувана на Деск-топу, већ у фолдеру my document.

По престанку радног односа или другог вида ангажовања корисник је дужан да изврши примопредају комплетне имовине ИКТ система, укључујући и документацију. Свако умножавање исте и коришћење након престанка радног односа, без писане сагласности МТО и корисника је строго забрањено.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине.

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.11

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Упутство за поступање са резервним копијама

ISMS.11

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Поступање са резервним копијама 2
   3.1 Израда резервних копија 2
   3.2 Чување резервних копија 2
   3.3 Тестирање резервних копија 3
4. Прилози и записи 3
5. Дефиниције и ознаке 3

1. Сврха и подручје примене

Документ дефинише правила поступања са резервним копијама.

2. Веза са другим документима

Овај документ се позива на Упутство о канцеларијском пословању органа државне управе.

3. Поступање са резервним копијама

3.1 Израда резервних копија

Израду и учесталост израде резервних копија података потребно је установити у складу са класификацијом информација по важности. За уређаје који садрже поверљиве податке, информације, подешавања и конфигурације резервне копије се израђују аутоматски и на дневном нивоу. Сви медији који садрже резервне копије морају бити једнозначно и прецизно означени. Информације које су истакнуте означавају назив и датум стварања копије.

Такође, потребно је одржавање пратеће документације о резервним копијама у писаном облику где су наведене детаљније информације као што су информације о садржају, датуму израде, име особе која је направила резервну копију, системском окружењу (нпр. врста и верзија оперативног система), категорији важности података итд.

У општем случају важе следећа правила:

- Базе података обавезно се архивирају на преносиве медије (CDROM, DVD, USB, „strimer" трака, екстерни хард диск- у зависности који преносни медији корисник има а располагању), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података;
- Остали фајлови-документи се архивирају најмање једном недељно, месечно и годишње;
- Подаци о запосленима-корисницима, архивирају се најмање једном месечно.

Динамика копирања је следећа:

- Дневно копирање-архивирање врши се за сваки радни дан у седмици,
- Недељно копирање-архивирање врши се последњег радног дана у недељи, онолико недељних примерака колико има последњих радних дана у месецу.
- Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно.
- Годишње копирање-архивирање врши се последњег радног дана у години.

Потребно је подесити систем да након сваке копије пошаље извештај да детаљима о изради и провери резервне копије. Те извештаје чувати најмање годину дана.

3.2 Чување резервних копија

Аутоматске креиране резервне копије се чувају на мрежним медијумима који искључиво намењени за ту намену и имају високе критеријуме заштите. Припадајућа документација се такође смешта на сигурну локацију (на пр. закључана ладица, ормар или ватро-отпоран сеф).

Дневне, недељне и месечне копије-архиве се чувају у просторији која је физички и у складу са мерама заштите од пожара обезбеђена.

Годишње копије-архиве се израђују у два примерка, од којих се један чува у просторији у којој се чувају дневне, недељне и месечне копије-архиве, а други примерак у згради.

Сваки примерак преносног информатичког медија са копијама-архивама, мора бити означен бројем, врстом (дневна, недељна, месечна, годишња), датумом израде копије-архиве, као и именом запосленог-корисника који је извршио копирање-архивирање.

Резервне копије потребно је чувати прописани временски период. Медији који садрже поверљиве информације не бацају се, већ се уништавају методом која осигурава да се трајно и поуздано уништи садржај, у складу са прописима.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе.

3.3 Тестирање резервних копија

У оквиру процеса управљања резервним копијама потребно је вршити:

- периодично тестирање података како би се потврдило да су резервне копије сачуване на исправан начин, да није нарушен интегритет података, те да је податке могуће обновити,
- периодични опоравак података у тестном окружењу да би се установило колико је времена потребно да се систем опорави.

Исправност копија-архива проверава се најмање на шест месеци и то тако што се изврши повраћај база података које се налазе на медију, при чему враћени подаци након повраћаја треба да буду исправни и спремни за употребу.

За све наведене активности потребно је водити уредну документацију.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине.

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.12

Упутство за коришћење интернета и е-поште

ISMS.12

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Коришћења интернета и електронске поште 2
3.1 Коришћење интернета 2
3.2 Правила коришћења електронске поште (e-mail) 3
4. Прилози и записи 4
5. Дефиниције и ознаке 4

1. Сврха и подручје примене

Документ дефинише правила која се морају поштовати приликом употребе интернета и електронске поште.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Коришћења интернета и електронске поште

3.1 Коришћење интернета

Корисницима ИКТ система је забрањено омогућавање алтернативног интернет приступа за уређаје у оквиру ИКТ система МТО.

Интернет се сматра једним од ресурса ИКТ система МТО. Интернет је средство за рад, чија је основна намена унапређивање пословних токова.

Размена података путем интернета није сигурна по питању заштите података и поверљивости. Поверљиве пословне информације се, у складу са могућностима, морају се преносити у оквиру добро заштићене мреже и шифровано. Корисник се обавезује, да уколико уноси своје личне податке или личне податке трећих лица на веб-у (нпр. ЈМБГ, име, презиме, разне приступне лозинке, бр. лк., информације о банковним рачунима итд.) користи искључиво када је на тој страници примењен HTTPS протокол и SSL сертификат. У супротном случај треба пријавити Администратору који ће поступити у складу са процедуром за управљање ризицима. Уколико корисник примети било какве промене на порталу на ком уноси податке који имају висок степен заштите дужан је да обавести администратора, без одлагања.

Забрањено је:

- користити приступ интернету за пренос музике, видеа и других садржаја забавног карактера, нити за играње компјутерских игара,
- посећивање интернет страница које садрже порнографски и остали недоличан садржај,
- гледање телевизијских садржаја и слушање радио станица који се могу пратити путем интернета,
- вређање људи у интернет комуникацији по верској, расној или некој другој припадности,
- у радно време прегледати садржаје на интернету који нису везани за посао, тј. у приватне сврхе, осим у изузетним случајевима и у оквирима који су уобичајени за ову врсту комуникације.
- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимање (download) података велике “тежине” које проузрокује “загушење” на

мрежи;
- преузимање (download) материјала заштићених ауторским правима;
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.
- приступање другим мрежама кроз VPN или други неки други вид виртуелног умрежавања

Уколико администратор установи да долази до заузимања ресурса интернет линка у приватне сврхе у мери већој од уобичајених оквира, администратор ће о томе писаним путем обавестити руководство.

У случајевима када корисник врши коришћење интернет линка у приватне сврхе у мери да долази до угрожавања несметане електронске размене пословних садржаја, због недостатка времена за писану процедуру, администратор има право да кориснику привремено укине приступ интернету.

3.2 Правила коришћења електронске поште (e-mail)

Сервис електронске поште је део ИКТ система МТО. Електронска пошта се сматра средством за рад и искључиво је намењена коришћењу у пословне сврхе. Уколико корисник добија SPAM поруке или поруке сумњивог садржаја дужан је да о томе обавести администратора.

Максимална величина е-маил поруке је 10 MB. Уколико корисник има потребу да пошаље поруку чија је величина већа од максималне треба да се обрати администратору.

Уколико корисник жели да провери да ли је његова порука успешно послата или разлог евентуалног не достављања очекиване поруке треба да се обрати администратору.

Сваки корисник добија аутоматско обавештење са mail сервера уколико дође до одстрањивања документа у прилогу поруке из разлога што документат није прошао неки од сигурносних критеријума конфигурисаних на mail серверу (нпр. сумња на присуство вируса, спам, забрањени тип документа итд.)

Правила прихватљивог коришћења електронске поште:

- није дозвољено слање ланчаних порука којима се оптерећују мрежни ресурси и запосленима одузима радно време;
- није дозвољено слање порука забавног карактера које садрже музичке и видео садржаје (нпр. "mp3", "avi" датотеке итд.);
- свака написана порука се сматра документом, те припада пошиљаоцу. За прослеђивање примљене поруке требате имати сагласност аутора тј. пошиљаоца;
- пословне поруке које представљају део радног предмета треба да се архивирају и чувају одређени временски период једнако као и документи у папирној форми;
- приватне поруке су дозвољене у умереној количини уколико не ометају редован рад;
- препоручује се да корисник јавно не објављује своју службену е-маил адресу, нити да је наводи као контакт адресу на форумима, мејлинг листама на које се шаљу разна обавештења итд.
- уколико пошиљалац затражи од корисника да пошаље потврду о прочитаној поруци ("read receipt"), корисник треба одмах да прихвати слање потврде. То треба да се уради и у случају када корисник не може одмах дати одговор. Овим начином пошиљалац има потврду да се порука није изгубила;
- препоручује се да корисник не одговара на нежељене поруке рекламног карактера

(спам поруке) нити да отвара веб линкове понуђене у таквим порукама;
- забрањен је сваки покушај читања, брисања, копирања или промене e-mail других корисника без њиховог допуштења.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине.

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.13

Упутство за оцењивање ризика по безбедност ИКТ система

ISMS.13

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Анализа ризика информационих технологија 2
3.1 Идентификација претњи и рањивости (слабости) 2
3.2 Идентификација ризика 5
3.3 Оцењивање ризика 6
3.4 Утврђивање критеријума прихватљивости за добијене резултате оцењивања ризика 7
4. Прилози и записи 7
5. Дефиниције и ознаке 7

1. Сврха и подручје примене

Упутство је намењено свим запосленима у организацији који учествују у реализацији оцењивања ризика по безбедност ИКТ система.

2. Веза са другим документима

- SRPS ISO/IEC 27001:2014 - Систем менаџмента безбедношћу информација - Захтеви;
- SRPS ISO/IEC 27005:2013 - Менаџмент ризицима по безбедност ИКТ система;
- Закон о информационој безбедности („Сл. гласник РС“, бр. 6/2016, 94/17, 77/19).

3. Анализа ризика информационих технологија

3.1 Идентификација претњи и рањивости (слабости)

Идентификација претњи и рањивости (слабости) помаже организацији као помоћ за спровођење процене ризика у оквиру информационих технологија. У оквиру ***Табеле 1*** се налазе неки од претњи и рањивости (слабости) које су заједничке за сваку организацију, а које се могу допунити свим специфичним претњама и рањивостима (варира од организације до организације).

Табела 1 - Неке од могућих претњи и рањивости по безбедност информација организације

Претње	Рањивости (слабости)
Приступ мрежи од стране неовлашћених лица	Компликовани кориснички интерфејс
Кршење уговорних односа	Коришћење уобичајених непромењених лозинки
Кршење закона и прописа	Одлагање медија за складиштење без брисања података
Компромитовање поверљивих информација	Осетљивост опреме на промене у напону
Скривање идентитета корисника	Осетљивост опреме на влагу и загађење
Штете проузроковане од стране трећих лица	Осетљивост опреме на температуре
Уништавање записа	Неадекватно управљање променама
Катастрофе (проузроковане од стране људи)	Неадекватна класификација информација
Катастрофе (природне)	Недовољна контрола физичког приступа
Откривање информација	Неадекватно одржавање
Откривање лозинки	Неадекватно управљање мрежом
Прислушкивање	Недовољно или неправилно управљање “бекап”-ом
Проневера	Неадекватно управљање лозинкама
Грешке у одржавању	Неадекватна физичка заштита
Неуспех у комуникационим везама	Неадекватна заштита од криптографских кључева
Фалсификовање записа	Неадекватна замена старије опреме

Претње	Рањивости (слабости)
Пожар	Неадекватна свест о заштити
Поплаве	Неадекватна подела задатака и одговорности
Преваре	Неадекватан надзор запослених
Индустријска шпијунажа	Неадекватан надзор запослених
Отицање информација	Неадекватна обука запослених
Прекид пословних процеса	Непотпуне спецификације за развој софтвера
Губитак електричне енергије	Недовољно тестирање софтвера
Губитак услуга подршке	Недостатак управљања улазним и излазним подацима
Квар опреме	Недостатак интерне документације
Злонамерни код	Недостатак или слабо спровођење интерне провере
Злоупотреба информационих система	Недостатак политике за употребу криптографије
Злоупотреба алата за проверу	Недостатак заштите за мобилну опрему
Загађење	Недостатак система за идентификацију и проверу идентитета
Софтверске грешке	Недостатак валидације обрађених података
Терористички напади	Локација подложна поплавама
Крађе	Један примерак
Удар грома	Неконтролисано копирање података
Ненамерна промена података у ИС-у	Неконтролисана преузимања са интернета
Неовлашћени приступ информационом систему	Неконтролисана употреба информационих система
Неовлашћена промена записа	Недокументовани софтвер
Неовлашћена инсталација софтвера	Демотивисаност запослених
Неовлашћен физички приступ	Нередовност преиспитивања корисничких права
Неовлашћено коришћење ауторског материјала	Неадекватно управљање капацитетима
Неовлашћено коришћење софтвера	Неадекватно обезбеђена свест
Грешка корисника	Недостатак политике чистог стола и екрана
Вандализам	Превише моћи у једној особи
	Незаштићеност јавно доступне мреже

Све претње се могу сврстати у неколико категорија што је приказано следећом табелом.

Табела 2 - Класификација претњи и узроци јављања

Класификација	Претња	Узроци јављања
Физичка оштећења	Пожар	Н, С, П
	Оштећење водом	
	Загађење	
	Велике несреће	
	Уништење опреме или медија	
	Прашина, корозија, замрзавање	
Природни утицаји	Климатске промене	Н
	Сеизмичке промене	
	Метеоролошки утицаји	
	Поплаве	
Губитак основних услуга	Квар клима уређаја или система за напајање водом	Н, С
	Губитак напајања енергијом	Н, С, П
	Квар телекомуникационе опреме	Н, С
Поремећаји настали услед радијације	Електромагнетно зрачење	Н, С, П
	Топлотно зрачење	
	Електромагнетни импулси	
Компромитовање информација	Пресретање или компромитовање информација	Н
	Даљинско шпијунирање	Н
	Прислушкивање	Н
	Крађа медијума или докумената	Н
	Крађа опреме	Н
	Повраћај рециклираних или одбачених медујума	Н
	Обелодањивање	Н, С
	Подаци од непоузданих извора	Н, С
	Манипулисање хардвером	Н
	Манипулисање софтвером	Н, С
Технички кварови	Квар опреме	С
	Засићење информационог система	Н, С
	Отказ софтвера	С
	Нарушавање одржавања ИС	Н, С
Неовлашћена поступања	Неовлашћено коришћење опреме	Н
	Копирање софтвера ради преваре	Н, С
	Коришћење фалсификованог или копираног софтвера	Н
	Корупција података	Н
	Нелегална обрада података	Н
Компромитовање функција	Грешка у коришћењу	Н
	Злоупотреба права	Н, С
	Фалсификовање права	Н
	Ускраћивање операција	Н
	Нарушавање доступности особља	Н, С, П

- ***Н** - намерно угрожавање безбедности информација;*
- ***С** - случајно угрожавање безбедности информација;*
- ***П** -природно (сви инциденти који су настали утицајем природе, без човековог деловања)*

3.2 Идентификација ризика

За идентификацију ризика, организација се води методологијом коришћења имовине, претњи и рањивости (слабости) организације. Ова методологија функционише тако што између све три компоненте (имовина, претње и рањивости) постоји веза: за сваку имовину или део имовине се утврђују претње које доводе до одређених рањивости (слабости), односно ризика по безбедност ИКТ система организације.

Неки од примера су дати у наставку, у ***Табели 3***.

Табела 3 - Примери идентификације ризика на основу имовине, претњи и рањивости (слабости)

Р. бр.	Имовина	Претња	Рањивост	Ризик
1.	Документ у папирној верзији	Пожар	Документ се не чува у ватросталној просторији	Губитак доступности информација
			Непостојање резервне копије документа	Потенцијални губитак расположивости
		Неовлашћени приступ	Документ није закључан у просторији у којој се чува	Потенцијални губитак поверљивости
2.	Дигитални документ	Квар диска	Непостојање резервне верзије документа	Потенцијални губитак расположивости
		Вирус	Антивирусни програм није исправно ажуриран	Потенцијални губитак поверљивости, интегритета и доступности
		Неовлашћени приступ	Шема контроле приступа информацијама није правилно дефинисана	Потенцијални губитак поверљивости, интегритета и доступности
			Приступ је дат великом броју људи	Потенцијални губитак поверљивости, интегритета и доступности

3.	Систем администратор	Недоступност ове особе	Не постоји замена за ову позицију, радно место	Потенцијални губитак расположивости
		Честе грешке	Недостатак обуке	Потенцијални губитак интегритета и доступности

Обзиром да се за сву имовину или сваки део имовине може наћи велики број претњи, а за сваку претњу велики број рањивости (слабости), а како би се избегла детаљна анализа која би могла да доведе до преоптерећености организације, приликом идентификације ризика, потребно је да се фокусира само на најважније претње и рањивости (слабости). За сву имовину је довољно идентификовати око пет претњи, а за сваку претњу две до три рањивости (слабости).

3.3 Оцењивање ризика

Овај процес подразумева детаљну анализу и вредновање ризика по безбедност ИКТ система укључујући идентификацију имовине, анализу претњи у односу на имовину, као и анализу рањивости (слабости). Резултати ових активности се користе за оцењивање ризика и идентификацију начина поступања са ризицима.

За сваку идентификовану улазну и излазну информацију и безбедносне ризике повезане са основним параметрима безбедности информација: 1) поверљивост, 2) интегритет и 3) доступност оцењују се ризици узимајући у обзир рањивост и вероватноћу настанка претње. Оцена рањивости и вероватноће настанка претње квантификује се на начин како је описано у табели у наставку:

Нумеричка вредност	Опис	Рањивост	Вероватноћа претње
1	Ниска	Рањивости (слабости) које је скоро немогуће искористити како би се утицало на безбедност ИКТ система организационог система	Готово да не постоји вероватноћа појављивања
2	Средња	Рањивости (слабости) које је тешко искористити да би се утицало на безбедност ИКТ система организационог система и које захтевају висок ниво знања о имовини организације	Постоји вероватноћа појаве али се до сада није дешавало
3	Висока	Рањивости (слабости) које могу бити искоришћене уз умерено познавање имовине организације како би се утицало на безбедност ИКТ система	Постоји реална вероватноћа појаве
4	Веома висока	Рањивости (слабости) које се могу лако искористити од стране било кога и лако се може утицати на безбедност ИКТ система	Постоји велика вероватноћа настанка, иста се и раније појављивала

Вредност ризика се одређује на начин који је описано у табели у наставку:

	Вероватноћа претње			
Рањивост	***1***	***2***	***3***	***4***
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

3.4 Утврђивање критеријума прихватљивости за добијене резултате оцењивања ризика

Вредност ризика се тумачи на начин описан у табели:

Нумеричка вредност	**Ризик**	**Опис**
1 – 4	**Мали ризик**	Процењени ризик је низак. Није потребно предузимати даље кораке у вези са наведеним ризиком.
6 – 9	**Средњи ризик**	Процењени ризик је средњи. Потребно га је елеминисати и свести на прихватљив ниво у догледном временском периоду.
12 - 16	**Високи ризик**	Процењени ризик је висок и неопходно га је без одлагања елеминисати и свести на прихватљив ниво.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

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).

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 да се идентификују извори и процени ризик.

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

Управљање ризицима - координисане активности усмеравања и контролисања у некој организацији у погледу ризика.

Поступање са ризицима - процес избора и имплементације мера да би се ризик модификовао.

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.14

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Упутство за опоравак ИКТ система у случају хаварије

ISMS.14

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Упутство за опоравак 2
   - 3.1 Полазне основе 2
   - 3.2 Рад хардверске опреме 3
   - 3.3 Функционисање софтвера 4
   - 3.4 Напајање електричном енергијом 5
   - 3.5 Крађа или физичко оптећење 5
   - 3.6 Утицај више силе 6
   - 3.7 Документовање хаваријског догађаја 6
4. Прилози и записи 7
5. Дефиниције и ознаке 7

1. Сврха и подручје примене

Документ дефинише основне активности које се предузимају у случају појаве хаваријског догађаја, као и општа правила којих се треба придржавати у циљу бржег опоравка ИКТ система МТО, након хаваријског догађаја.

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Упутство за опоравак

3.1 Полазне основе

Хаварија као нежељена ситуација, без обзира на узрок настанка, може оставити озбиљне последице на пословање и привремено онемогућити рад пуним капацитетима или га чак обуставити у одређеном временском периоду. Да би се то избегло МТО предузима одговарајуће мере у складу са утврђеним ризицима и расположивим средствима. Ипак, без обзира на предузете мере постоји вероватноћа појављивања нежељених догађаја који могу оставити веће или мање последице на ИКТ систем, а самим тим на рад МТО делимично или у целости.

Под хаваријом се подразумева онеспособљавање ИКТ система, делимично или у целости, у обиму који угрожава или може угрозити функционисање МТО. Мања одступања каква су кварови појединачних делова (нпр. рачунари, штампачи, тренутни прекид приступа интернету, мрежи и сл.) не сматрају се хаваријама и самим тим се не третирају овим упутством.

Свака потенцијална хаварија је специфична за себе и да би се адекватно реаговало након настанка, неопходно је извршити одговарајуће анализе и дефинисати планове опоравка. Поред мера које се прописују за сваку специфичну ситуацију, општа процедура реаговања у таквим ситуацијама је следећа:

- Администратор и одговорни руководилац се обавештавају о насталој хаварији, без одлагања;
- Администратор врши прелиминарну анализу хаварије, прикупљају неопходне податке, контактирају екстерне организације које пружају услуге одржавања ИКТ и доносе одлуке у ком правцу даље ићи;
- Врши се детаљна анализа хаварије, настале и очекиване будуће штете, процењује време опоравка и дефинишу мере;
- Уколико је неопходно, осигурава се сервер са примарне локације (уколико исти није оштећен) – по потреби се врши измештање на сигурну локацију, врши се израда додатне резервне копије, анализира се степен оштећености;
- Уколико је неопходно, осигурава се документација у папирној форми – премештање на секундарну локацију или у друге просторије унутар примарне локације које задовољавају услове за привремено складиштење;
- Ако је неопходно активира се опрема ускладиштена на секундарној локацији, односно врши се набавка минимално потребне опреме за рад, са средстава са рачуна намењених за те потребе;
- Преузимају се подаци са секундарне локације, уколико су уништени подаци на примарној локацији;
- Организује се наставак рада, по потреби на секундарној локацији;
- Врши се детаљна процена утицаја хаварије на пословање, као и утицај на

заинтересоване стране и исте се по потреби обавештавају. Предлог обавештења сачињава администратор, а одобрава га искључиво одговорни руководилац. Свако давање информација било којој заинтересованој страни, без одобрења одговорног руководиоца је строго забрањено;
- Обавештава се осигуравајуће друштво о насталој штети и врши наплата полисе;
- Покреће се процедура истраге инцидента и утврђивања узрока;
- Предузимају се мере за повратак на ниво рада пре хаварије.

3.2 Рад хардверске опреме

Администратор у сарадњи са спољним организацијама које пружају услуге одржавања и управљања опремом ИКТ система, дефинише мере, поступке и активности за опоравак хардверске опреме неопходне за функционисање ИКТ система.

Интерна техничка документација за опоравак рачунарске и телекомуникационе опреме треба да садржи:

- дефинисане поступке опоравка зависно о врсти хардверског уређаја и његовом утицају на остале ресурсе ИКТ система,
- дефинисане приоритете у опоравку ресурса ИКТ система потребних за његово функционисање,
- дефинисане одговорности и обавезе особа задужених за опоравак,
- контакт податке о свим лицима укљученим у процес опоравка система,
- дефинисане поступке везане за уговорне односе са даваоцима услуга (трећа лица) који се односе на опоравак одређеног дела ИКТ система, за које је исти надлежан.

Опрема која се сматра неопходном за несметано функционисање ИКТ система може се поделити у неколико група:

- пасивна мрежна опрема (утичнице за рачунарску мрежу, РАТСНП панели са UTP модулима, кабели итд);
- активна мрежна опрема (Router, Firewall, Switch, наменски уређаји за спајање са удаљеним системима итд):
- комуникациона опрема (комутациона опрема са припадајућом инсталацијом, мултиплексери –UMUX1500, RR систем, VF опрема, Wireless линк, G.SXDSL опрема, итд);
- сервери;
- кориснички рачунари;
- периферни уређаји (оптичке кутије и спојнице, оптички трансивери, штампачи, скенери, факс апарати, телефонски апарати итд);
- остала опрема (камере, каблови, конектори, читачи картица, резервни делови за рачунаре итд).

Сва горе наведена опрема која подржава обављање основних пословних процеса захтева редовно и интервентно одржавање. Сва опрема се у континуитету надгледа, анализира рад и врши конфигурисање и подешавање исте.

Обавеза Администратора је да благовремено информише надређеног руководиоца и затражи набавку резервних делова и уређаја који омогућавају несметано функционисање ИКТ система како би се смањило време потребно за поновно успостављање пуне функционалности ИКТ система у случајевима када је рад нарушен услед губитка поузданости у раду или отказа уређаја.

Мере које је потребно предузети ради елиминисања кварова или ублажавања штетности ефеката кварова на хардверској опреми су:

- стално надгледање, анализа рада и надоградња сервера, мултиплексне и комутационе опреме, активне мрежне опреме и предвиђање потенцијалних отказа у раду опреме;
- коришћење наменских хардверских конфигурација за опрему;
- креирање интерних писаних процедура опоравка за кључну хардверску опрему, битну за очување пословних процеса, када то има смисла;
- омогућавање довољног броја серверских конфигурација на којима би се могао урадити опоравак пословног процеса (e-mail, интернет, евиденција присуства и контрола приступа у згради итд.) у случају већег хардверског квара на серверу и немогућности опоравка истог;
- обезбеђење алтернативних комуникационих веза за интернет, размену електронске поште и размену података са удаљеним системима, уколико је то у складу са планом опоравка;
- обезбеђење редудантног хардвера за подизање кључних сервиса за опоравак у случају хаварије.

3.3 Функционисање софтвера

Проблеми у функционисању софтвера могу настати као последица:

- неисправности у раду корисничких и серверских оперативних система,
- деловања малициозног кода,
- нестручног руковања рачунаром.

Мере које се могу спровести да би се елиминисали или ублажили ефекти проблема у функционисању софтвера су:

- Коришћење лиценцираних серверских и корисничких оперативних система, што омогућава искоришћавање пуне функционалности софтвера у погледу могућности за опоравак серверских и корисничких оперативних система, те ангажовање овлашћене техничке подршке и коришћење глобалних база знања;
- Конфигурисање мрежног окружења тако да корисници имају приступ само оним ресурсима рачунара и мреже који су им неопходни за обављање посла;
- Употреба лиценцираних софтверских решења за креирање резервних копија (disk image) чврстих дискова кључних сервера и корисничких рачунара;
- Формирање система дуплих података (конфигурисање хард дискова у Raid и Mirror режиму рада) на серверима и обезбеђење резервног сервера (backup сервер), где је то технички изводљиво;
- Спречавање неовлашћене инсталације софтвера;
- Дефинисати упутства за коришћење, опоравак и инсталирање кључних софтверских компоненти, као и места где се чувају оригинали и резервне копије лиценцираног софтвера, када има смисла.

У случају неисправности у раду серверских и корисничких оперативних система, лице/организација задужена за управљање опремом је дужно да отклони проблеме у што краћем периоду. Наведени проблеми могу бити решени на неки од следећих начина:

- Опоравком оперативног система преко алатки за опоравак оперативног система Windows (system restore),

- Опоравком постојеће инсталације Windows са оригиналног инсталационог медијума,
- Инсталацијом новог оперативног система Windows,
- Инсталацијом Windows коришћењем сачуване копије диска (disk image).

За опоравак софтвера у случају специјализованих наменских уређаја као што су конфигурациони фајлови рутера, свичева, firewall уређаја, VF уређаја, G.SXDSL уређаја, wireless уређаја, софтвера за интернет сервис, електронску пошту и антивирусну заштиту, потребно је у процесу опоравка користити последњу исправну верзију софтвера која се чува на алтернативној локацији.

У случају да дође до губитка или смањене функционалности неке пословне апликације (нпр. финансије итд.) потребно је дијагностификовати проблем. Уколико се не ради о проблему системске природе (нпр. функционисање оперативног система, рад мреже, опреме итд.), већ о проблемима пословне апликације треба урадити следеће:

- Уколико је могуће решити проблем са постојећим ресурсима у МТО,
- Ако је за функционисање тог дела ИКТ система задужено треће лице, обавестити га о догађају и у договору са њим предузети одређене активности за превазилажење проблема.

3.4 Напајање електричном енергијом

У случају нестанка електричне енергије ресурси који омогућавају несметано функционисање ИКТ система морају бити обезбеђени алтернативним извором напајања.

Потребно је обезбедити исправљачке уређаје (48V) за напајање телекомуникационе опреме.

Уређаји за које је потребно обезбедити додатни извор напајања су:

- сервери,
- комуникациона опрема (рутер, свич, фирewалл, комутациона опрема, VF уређаји, RR уређаји, G.SXDSL уређаја, wirless уређаја итд),
- уређаји који служе за техничко обезбеђење објекта,
- кориснички рачунари на којима се користе апликације за обављање важнијих пословних процеса.

Додатни извор напајања се обезбеђују коришћењем додатних исправљачких уређаја, квалитетних уређаја за непрекидно напајање (UPS) и агрегата (**ингеренција УЗЗПРО)**

3.5 Крађа или физичко оштећење

Сигурност ИКТ система може бити нарушена неовлашћеним приступом просторијама и опреми која обезбеђује његово функционисање, као и крађом ове опреме.

Како би се ове могућности свеле на најмању могућу меру потребно је увести ограничења у погледу приступа просторијама и опреми за подршку ИКТ система.

Уколико дође до крађе или физичког оштећења опреме за подршку ИКТ система, треба што пре оправити сервер на новој хардверској компоненти. Да би то било могуће, мора се планирати набавку резервних хардверских конфигурација које могу подржати поједине пословне процесе у случају крађе или физичког оштећења које се не може отклонити.

Такође, уколико не постоји резервна хардверска конфигурација која може подржати одређени пословни процес, обустављен због крађе или физичког оштећења, треба се размотрити и уколико је то могуће привремено повратити прекинуте пословне процесе на расположивој хардверској опреми.

3.6 Утицај више силе

Као случајеви више силе сматрају се сви догађаји који се не могу спречити укључујући и случајеве када се могу предвидети. На њихово деловање се може само делимично утицати, у смислу умањења последица, али не и на потпуно елиминисање вероватноће настанка.

У више силе спадају:
- поплаве,
- пожари,
- земљотреси,
- удар грома,
- остали утицаји (температура, влага, прашина, статички електрицитет итд.).

Да би се умањиле последице оваквих појава, предузимају се следеће мере:

- ИТ опрема се поставља тако да је што више удаљена од водоводних чворова и измештена из просторија које су изложене већем ризику од продора воде.
- Пожари, дим и нагризајући плинови могу нанети штету ресурсима ИКТ система. Стога се подаци који су кључни за опоравак система чувају у ватроотпорним ормарима. Све просторије у којима се налази опрема за подршку ИКТ система су обезбеђене алармним уређајима за дојаву пожара.
- Земљотреси, као и пожари могу да делимично или потпуно униште ресурсе ИКТ система, зато се копије значајних података чувају и изван зграде, тј. на алтернативној локацији.
- У циљу спречавања штетних последица које могу настати при удару грома, објекат је опремљен громобранском заштитом, а инсталације се контролишу у редовним трогодишњим интервалима.
  Остали фактори који угрожавају функционисање ИКТ система су температура, влага, прашина и статички електрицитет. Савремена хардверска опрема која служи за подршку ИКТ система осетљива је на радну температуру, влагу, прашину и уопште квалитет ваздуха. За рад хардверских уређаја постоје радни услови тј. радна температура, влага итд. Стога су кључни уређаји смештени у просторије у којима је могуће контролисати температуру и влагу 24 сата дневно. Ове просторије поседују клима уређаје. Просторије се одржавају чистим. Приликом чишћења неопходно се води рачуна да не дође до ненамерног угрожавања опреме од стране лица задужених за одржавање чистоће. Ови послови се обављају под надзором.

3.7 Документовање хаваријског догађаја

Сваки хаваријски догађај је потребно документовати. Документацију о хаваријском догађају израђује администратор.

Документација треба да садржи:

- податке о лицу које је пријавило хаваријски догађај,
- опис хаваријског догађаја (узрок настанка и настала штета),
- све активности предузете у процесу опоравка,

- учињена штета, са посебно издвојеним информацијама о ресурсима који су неповратно изгубљени, и онима који су опорављени,
- закључак (степен опоравка).

Наведена документација се користи за израду препорука ради бржег препознавања или спречавања понављања хаваријског догађаја, као и за статистичке извештаје о учесталости хаваријских догађаја и њихових узрока.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.15

Република Србија
МИНИСТАРСТВО
ТУРИЗМА И ОМЛАДИНЕ

Упутство за прикључење на ИКТ систем

ISMS.15

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Прикључење на ИКТ систем 2
   3.1 Процедура прикључења корисника у ИКТ систем 2
   3.2 Процедура привременог прикључења (госта) у локалну рачунарску мрежу 3
   3.3 Процедура искључења корисника из локалне рачунарске мреже 3
4. Прилози и записи 3
5. Дефиниције и ознаке 3

1. Сврха и подручје примене

Документ дефинише правила која се морају поштовати приликом прикључења корисника на ИКТ систем Министарства туризма и омладине

2. Веза са другим документима

Овај документ се не позива на друга документа.

3. Прикључење на ИКТ систем

3.1 Процедура прикључења корисника у ИКТ систем

Прикључење корисника у локалну рачунарску мрежу, телефонску мрежу, VPN мрежу МТО друге системе Министарства туризма и омладине се врши на основу захтева руководиоца организационе јединице којој припада новозапослени.

Одговорна лица за одржавање ИКТ система обавезана да воде детаљну и ажурну евиденцију корисника ИКТ система (електронски документи).

Пре прикључења рачунара у локалну рачунарску мрежу потребно је обезбедити физичку везу рачунара до пасивне и активне мрежне опреме, а потом администратор система врши припрему рачунара за рад у систему. Припрема рачунара за рад у систему обухвата:

- креирање корисничког налога са одговарајућим корисничким именом и лозинком,
- креирање налога за е-пошту итд
- припрема рачунара за рад у мрежном окружењу,
- поставка анти-вирус програма,
- друге поставке неопходне за рад.

Кориснички налог се састоји од корисничког имена и лозинке по матрици име.презиме, енглеским алфабетом без употребе слова ђ,ж,љ, њ, ћ, ч, џ, ш. Препорука: Уместо ових слова користити слова из табеле.

Ћирилична слова	Латинична слова
Ђ	dj
Ж	z
Љ	lj
Њ	nj
ћ, ч	c
ш	s
џ	dz

Кориснички налог може да се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр. лична карта са чипом и уписаним сертификатом).

Пријављивање у ИКТ систем МТО се врши убацивањем медија са електронским сертификатом у читач картица.

Следећа правила се морају поштовати у вези са лозинкама корисничких налога:

- Систем администратор треба да надгледа како запослени примењују правила поступања са лозинкама;

- систем треба да буде подешен да приморава запослене на унос квалитетне лозинке и да их приморава да лозинку редовно мењају;
- квалитет лозинке потребно је проверавати коришћењем софтвера за контролу лозинки;
- не користити увек исту лозинку приликом отварања налога или ресета лозинке, а администраторске лозинке које имају привилегован приступ се морају мењати на сваких 30 дана.

3.2 Процедура привременог прикључења (госта) у локалну рачунарску мрежу

Привремено прикључење тј. прикључење госта у ИКТ систем се врши преко изоловане WLAN мреже која је потпуно одвојена од LAN мреже. Корисник од овлашћеног лица добија параметре за приступ мрежи у складу са процедуром о коришћењу мобилних уређаја.

Уколико "гост" (корисник који не користи рачунар Министарства туризма и омладине, већ сопствени) има потребу да приступа локалној мрежи и другим интерним сервисима, онда треба писменим захтевом да се обрати надлежном руководиоцу. На основу писаног захтева који одобрава надлежни руководилац, а који садржи информације о сврси прикључења.

Прикључење госта се спроводи по истом принципу, као и интерних корисника, а у складу са нивоима приступа који су дефинисани захтевом.

3.3 Процедура искључења корисника из локалне рачунарске мреже

У случају престанка потребе да корисник користи ИКТ систем, надређени руководилац је дужан да најкасније у року од 2 дана затражи искључење корисника из ИКТ система путем писаног захтева. Такође и корисник WPN налога је дужан да обавести овлашћено лице о престанку радног односа, што укључује обавештење у писаној форми како би лице задужено на овим пословима извршило процедуру молбе ка канцеларији за ИТ за укидање WPN налога.

Захтев за искључење корисника је потребно поднети у случају да је кориснику престао радни однос или из другог разлога.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

ISMS.17

Република Србија

МИНИСТАРСТВО ТУРИЗМА И ОМЛАДИНЕ

Упутство за заштиту и тестирање ИКТ система

ISMS.17

Садржај:

1. Сврха и подручје примене 2
2. Веза са другим документима 2
3. Заштита и тестирање ИКТ система 2
   3.1 Мере заштите и обезбеђења интегритета ИКТ система 2
   3.2 Тестирање ИКТ система 3
4. Прилози и записи 4
5. Дефиниције и ознаке 4

1. Сврха и подручје примене

Документ дефинише основна правила која се примењују у циљу заштите ИКТ система и његовог интегритета, током животног века система, укључујући и начин тестирања.

2. Веза са другим документима

Овај документ се позива на:

- Упутство за одржавање ИКТ система,
- Упутство за поступање са резервним копијама,
- Упутство за управљање односима са испоручиоцима.

3. Заштита и тестирање ИКТ система

3.1 Мере заштите и обезбеђења интегритета ИКТ система

Администратор и други субјекти који учествују у одржавању ИКТ система обавезни су да у свом раду користе:

- Алат за мониторинг апликативних сервиса у реалном времену;
- Алат за идентификација напада у реалном времену;
- Алат за праћење сваке апликативне трансакције "back end-a";
- Алат за снимање, складиштење и индексирање свих трансакција;
- Алат за "Snapshot reporting" детаља трансакција;
- Алат за побољшање перформанси апликација.

О активностима администратора и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и сл.). Ови подаци подлежу обавезном архивирању – чувању резервних копија на начин прописан *Упутством за поступање са резервним копијама (ISMS.11).*

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и сл., мора бити подешен тако да одмах обавештава администратора и надлежна лица, о свим нерегуларним активностима запослених-корисника, покушајима упада и упадима у систем.

Одговорно лице најмање једном месечно а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, одговорно лице је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност надлежних.

У циљу обезбеђења интегритета система, подешавањем корисничких полиса онемогућено је неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система. Такође, израдом и чувањем на безбедном локацијама резервних копија лиценцираних софтвера обезбеђен је брз опоравак у случају инцидента.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у МТО, обавезно се дефинише уговорима и сходно томе се врши технички надзор над њиховим радом од стране одговорног лица.

Омогућавање приступа МТО информационом систему трећим лицима и његовим референтним тачкама преставља велики ризик за безбедност података. Из тог разлога организације којима се уступа посао и приступ морају се бирати према критеријумима и правилима који су ближе уређени *Упутством за управљање односима са испоручиоцима (ISMS.05).*

У циљу спречавања неовлашћеног приступа ИКТ систему од стране трећег лица које пружа услуге развоја и одржавања система, потребно је испунити следеће услови (детаљи могу зависити од врсте услуга која се пружа и од дизајна ИКТ система):

- идентификација и аутентификација корисника;
- овлашћења приступа дефинисана у складу са уговореним обавезама
- адекватно обезбеђен шифровани линк за приступ који је у складу са процедурама МТО, уколико се ради о удаљеном приступу систему;
- употреба јаких лозинки који су у складу са процедурама МТО;
- ревизија за све нивое притупа.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система мора се води документација, како је предвиђено *Упутством за одржавање ИКТ система (ISMS.09).*

3.2 Тестирање ИКТ система

За потребе тестирања ИКТ система односно делова система користе се подаци који се не употребљавају у продукцијском окружењу и не могу ни на који начин компромитовати МТО или нека трећа лица повезана са МТО.

Коришћење продукцијских података у тестном окружењу се никако не препоручује. У случајевима кад је немогуће избећи коришћење оригиналних података, неопходно је применити одговарајуће контроле како би се осигурало да се оригиналне информације не користе од стране неовлашћених лица.

Предуслов за коришћење продукцијских (оригиналних) података у тестне сврхе јесте писано одобрење највишег руководства, коме треба да претходи документовано образложење зашто се користе продукцијске информације у сврхе тестирања, које су то информације и ко ће имати приступ истим за време тестирања. У оваквим ситуацијама морају се поштовати следећа правила:

- подаци који се преузму са продукцијских севера МТО-а, не смеју се користити у неке друге сврхе осим за тестирање које је одобрено у образложењу;
- тестно окружење мора имати ограничен број корисника који приступају подацима;
- за сваког корисника се мора вршити ревизија;
- мора се пратити ток преузимања података и сви логови приступа се морају чувати и анализирати;
- након преузимања продукцијских информација мора се одмах искључити са продукцијског окружења.

Кориснички налози који приступају продукцијским информацијама треба да испуњавају слеће услове:

- треба да има најмање привилегије у продукцијском систему – дозвољава се гледање само оних података који су неопходни за тестирање;
- мора бити јединствен налог, не сме бити дељени налог преко кога се у истом тренутку приступа са више места, при чему се изузетак може направити само ако се преко истог налога приступа у различитим временским терминима, али се у том случају сваки пут мора мењати лозинка.

4. Прилози и записи

Овај документ не садржи прилоге и записе.

5. Дефиниције и ознаке

МТО - Министарство туризма и омладине.