ПРОЦЕДУРА

УПРАВЉАЊЕ ИНЦИДЕНТИМА

Израдио: Петар Јовановић

Контролисао: Милован Жагрић

Процедура је обавезна за примену. Дужност сваког запосленог на кога се процедура односи је да се са истом упозна и поступа на прописан начин. Обавезна је примена свих упутстава и записа који су дефинисани овом процедуром.

Датум: 30.11.2018.

Директор: Дејан Јонић

Одговоран за примену: **Помоћник директора/Представник руководства за систем менаџмента**

Одговоран за измене у процедури: **Помоћник директора/Представник руководства за систем менаџмента**

1. ПРЕДМЕТ

Предмет ове процедуре је дефинисање поступака и документације у потпроцесима:

2. ПОДРУЧЈЕ ПРИМЕНЕ

Ову процедуру примењују сви запослени у Сектору за информатичку подршку.

3. ДЕФИНИЦИЈЕ И СКРАЋЕНИЦЕ

- „ISMS" – „Information Security Management System" - Систем управљања безбедношћу информација;
- ИТ – информационе технологије;
- УЗЗПРО – Управа за заједничке послове Републичких органа.

4. ВЕЗА СА ДРУГИМ ДОКУМЕНТИМА

Интерна:

- Пословник квалитета;
- Пословник безбедности информација
- Документа QMS-а и ISMS-а;

Екстерна:

- ISO 9000:2015, Системи управљања квалитетом - основе и речник, 2015. година;
- ISO 9001:2015, Системи управљања квалитетом - захтеви, 2015. година;
- ISO 9004:2009, Системи управљања квалитетом - упутства за побољшање перформанси, 2009. година;
- ISO/IEC 27001:2013, Информационе технологије – Технике безбедности – Системи менаџмента безбедношћу информација – Захтеви
- „Recommended International Code of Practice General Principles of Food Hygiene, CAC/RCP 1-1969, Rev. 4 (2003)". (Препоручени међународни кодекс праксе општа начела хигијене хране)

5. ОПИС ПРОЦЕДУРЕ

5.1 Одговорност

Од свих корисника и власника имовине из угла безбедности информација очекује се да следе ову процедуру и да у најкраћем року извештавају о слабостима и догађајима везаним за безбедност информација.

Извештаји о слабостима и догађајима везаним за безбедност информација подносе се Помоћнику директора Сектора за информатичку подршку, у складу с овом процедуром.

Помоћник директора Сектора за информатичку подршку је одговоран за реаговање на информације о угрожавању безбедности.

Руководиоци запослених су одговорни за обучавање и подизање свести о безбедности информација код запослених.

Помоћник директора за Сектора за информатичку подршку је одговоран за координацију и примерено реаговање на сваку пријављену слабост или догађај, укључујући документовање сваког предузетог корака, скупа доказа и решавања проблема.

Од техничког особља и других запослених, потписника уговора или трећих лица, очекује се да пруже подршку Помоћнику директора Сектора за информатичку подршку у поступању са било којим догађајем или слабошћу, везаном за систем безбедности информација.

Помоћник директора Сектора за информатичку подршку ауторизује приступ систему или подацима у случају идентификације инцидентне ситуације.

Помоћник директора Сектора за информатичку подршку је одговоран за прикупљање доказа у случају непредвиђених догађаја.

Помоћник директора Сектора за информатичку подршку је одговоран за сакупљање и чување информација о инцидентима везаним за безбедност информација.

Директор УЗЗПРО мора обезбедити да је Помоћник директора Сектора за информатичку подршку обучен до адекватног нивоа, када су у питању методе сакупљања доказа који су у надлежности УЗЗПРО.

5.2 Идентификација и извештавање о инцидентима по безбедност информација

5.2.1 Дефинисање инцидента нарушавања безбедности информација

Врло је важно да организација благовремено препозна инцидент који може да наруши безбедност њених информација. Неке од ситуација која се могу сврстати у инциденте

по безбедност информација у УЗЗПРО-у, су следеће (али се не ограничавају само на њих):

- Губитак опреме или средства
- Људске грешке
- Неисправно функционисање система
- Преоптерећење делова система
- Кршење физичке сигурности/заштите
- Неусклађеност са политикама, процедурама и/или упутствима
- Неконтролисане промене у систему
- Прекршаји у вези са приступом
- Неисправно функционисање хардвера и/или софтвера

5.2.2 Идентификација и извештавање о слабостима и догађајима везаним за безбедност информација

Слабости и догађаје везане за безбедност информација може идентификовати било ко.

Када се инцидент или слабост везана за безбедност информација идентификује она треба бити документована попуњавањем записа **Извештај о безбедносном инциденту** и моментално послата електронском поштом Начелнику одељења за системско-техничку подршку.

Корисници информација који немају приступ или сопствену маил адресу, дужни су да у најкраћем року ступе у контакт са Начелником одељења за системско-техничку подршку како би известили о инциденту и заједнички израдили запис **Извештај о безбедносном инциденту**.

Корисницима информација није дозвољен даљи рад после идентификовања могуће слабости или догађаја који је везан за безбедност информација.

Начелник одељења за системско-техничку подршку ће проучити извештај о слабости или догађају везаном за безбедност информација и послати (заједно са својим коментарима) електронском поштом Помоћнику директора Сектора за информатичку подршку.

Помоћник директора Сектора за информатичку подршку ће послати повратни извештај, као што је описано у тачки 5.2.3 ове процедуре - Одговор на извештај о безбедносном инциденту, електронском поштом, заједно са копијом, Начелнику одељења за системско-техничку подршку, са описом поступања у вези са догађајем, а Начелник за системско-техничку подршку ће са истим упознати и запосленог који је пријавио инцидент.

5.2.3 Одговор на извештај о безбедносном инциденту

Сви догађај у вези безбедности информација и слабостима заштите се одмах након пријем анализирају, оцењују и категоризују.

Углавном се користе четири категорије идентификовања слабости система:

- Догађаји; то су појаве које после анализе, немају или имају врло малу важност за безбедност информација;
- Инциденти: су појаве које имају (значајну) вероватноћу да ће угрозити безбедност информација УЗЗПРО-а;
- Рањивости: су слабости које, после анализе, јасно постоје као значајне слабости угрожавајући безбедност информација;

Редослед приоритета за одговоре, када постоји извештаји за више догађаја је: инциденти, рањивости, догађаји.

Када у исто време постоји више извештаја из исте категорије, Помоћник директора Сектора за информатичку подршку даје приоритет одговорима узимајући у обзир важност пословних система и информационих вредности, опасност од даљег угрожавања безбедности информација УЗЗПРО и средстава у власништву УЗЗПРО.

О инцидентима који угрожавају пословно критичне ресурсе, Помоћник директора Сектора за информатичку подршку одмах извештава Директора УЗЗПРО-а.

Помоћник директора Сектора за информатичку подршку кад је то потребно може да захтева додатне податке или помоћ од квалификованог техничког или било ког другог особља, да би анализирао и разумео инцидент и да би установио одговарајуће активности како би се уочени инцидент у што краћем року ставио под контролу.

Помоћник директора Сектора за информатичку подршку иницира стандардне поступке или додатне активности које он сматра неопходним да би се инцидент ставио под контролу, у циљу пружања заштите од инцидента, као и да би се спровео план за непредвиђене догађаје.

Тамо где је потребно, Помоћник директора Сектора за информатичку подршку координира активност са другим организацијама или компанија да би обезбедио неометан рад УЗЗПРО-а.

Начелник одељења за системско-техничку подршку потврђује да су угрожени пословни системи поново оспособљени и да су примењене захтеване контроле пре повратка у нормалну радну активност.

Једном кад је инцидент под контролом, и све захтеване корективне акције завршене, Помоћник директора Сектора за информатичку подршку израђује комплетан извештај о инциденту, идентификујући разлог инцидента и анализирајући његов развој, настојећи да утврди:

- како је УЗЗПРО могао раније или ефикасније да одговори или предузме превентивну акцију пре догађаја,
- ефективност стављања инцидента под контролу и корективне акције

- план за непредвиђене догађаје
- како је инцидент затворен,

Овако израђен извештај Помоћник директора Сектора за информатичку подршку доставља Директору УЗЗПРО-а.

Помоћник директора Сектора за информатичку подршку и Начелник одељења за системско-техничку подршку су одговорни за затварање инцидента. Ово укључује све извештаје спољним органима (ако је потребно); планирање и спровођење корективне акције да се избегло будуће понављање инцидента, прикупљање и обезбеђивање података из провере и материјалних доказа (види одељак "Прикупљање доказа), извештавање Директора УЗЗПРО-а о инциденту, и комуникацију са онима који су погођени или су учествовали на било који начин у инциденту о повратку у нормалан рад.

Представник руководства за безбедност информација припрема ***Шестомесечни извештај*** (у слободној форми) Директору УЗЗПРО-а који садржи број, тип, категорију и озбиљност инцидената нарушавања безбедности информација у прошлом периоду, трошкове стављања инцидента под контролу и опорављања од инцидента, као и тоталне трошкове губитака проистеклих из сваког инцидента, као и препоручене (тамо где је то применљиво) додатне контроле које могу ограничити учесталост инцидената, нарушавања безбедности информација, побољшавајући способност УЗЗПРО да одговори и да смањи трошкове одговора на инциденте.

Сви извештаји о инцидентима који су настали у периоду између два преиспитивања од стране руководства, морају бити узети у разматрање током првог следећег преиспитивања, као што је и описано у процедури **ОДГОВОРНОСТ РУКОВОДСТВА**.

5.2.4 Прикупљање доказа

Где је утврђена могућност постојања прекршајне радње или кривичног дела у поступку одговора на инцидент, надлежне интерне и екстерне службе или одговорне особе се укључују што је пре могуће и њихова упутства се прате у погледу прикупљања и задржавања доказа. Ако догађај превазилази делокруг организације, Помоћник директора Сектора за информатичку подршку мора да консултује правну службу како би се осигурало да се докази прикупљају на правилан начин.

У свим другим случајевима, све папирне копије оригиналних докумената имају, прикачену на себи, потписану и датирану изјаву која описују прецизно где и под којим околностима је доказ пронађен, ко га је пронашао и ко је био очевидац догађаја.

Оригинални документ мора бити склоњен и чуван на сигурном месту. За чување докумената који представљају доказе о инциденту по безбедност информација одговоран је Помоћник директора Сектора за информатичку подршку односно надлежна служба, у зависности од врсте инцидента.

6. УПУТСТВА (која произилазе из ове процедуре)

- -

7. ЗАПИСИ (који произилазе из ове процедуре)

Назив записа	Број примерака	Период чувања	Одговорност за чување	Прилог број
Извештај о безбедносном инциденту	1	Трајно	Помоћник директора Сектора за информатичку подршку	1
Шестомесечни извештај	1	2 године	Представник руководства за безбедност информација	/

Прилог 1

ИЗВЕШТАЈ О БЕЗБЕДНОСНОМ ИНЦИДЕНТУ

Извештавање о настанку кризне ситуације / инцидента *Попуњава власник процеса*			
На дан:		У време:	
Дошло је до:			
Запослени су (евакуисани, , има повређених, ...)			
За насталу ситуацију извештени / алармирани су:			
ИТ системи су:			
Остале информације			
Оцена тежине оштећења и процена висине штете.			
Процењено потребно време за превазилажење несреће износи		_____ х/дана	
Увидом обима несреће, односно последица: ☐Предлажемо ☐Не предлажемо			
Проглашење кризне (ванредне) ситуације.			
Власник процеса:_____ (потпис)			
Проглашење кризне (ванредне) ситуације *Попуњава Помоћник Директора за ИКТ*			
Потребно / непотребно			
Категорија слабости система			

(догађај/инцидент/рањивост)					
Представник руководства од овог момента се налази на алтернативној локацији					
Контакт телефон:		Мобилни:		е-маил	
Остале информације и предлог мера:					
Помоћник Директора за ИКТ:_____ (потпис)					
Одлука о окончању кризне ситуације *Попуњава власник процеса*					
Функционисање је успостављено у следећем обиму:					
Активности које су предузете за санирање штете:					
Функционисање је успостављено према плану у предвиђеном обиму и процес се одвија без проблема, па се због тога проглашава прекид кризне ситуације: (да/не)					
Представник руководства: _____ (потпис) **Власник процеса: _____ (потпис)** **Помоћник Директора за ИКТ:_____ (потпис)**					

Достављено:

- **Власницима процеса**
- **Представнику руководства**
- **Директору**

Издање 01, од 15.10.2015.