(ЛОГО-ФИРМА)	ПРОЦЕДУРА-ПОЛИТКА	(НУМЕРАЦИЈА)
Класификација (инт….)		Верзија

ПРОЦЕДУРА УПРАВЉАЊА ИНЦИДЕНТИМА

	Назив/име	позиција	датум
Усвојио	…	…	…
Одобрио	…	…	…
Направио	…	…	…
Власник/одговоран	*(Одељење)*		
Важи од			…
Примењује се на	…		

ИСТОРИЈА ДОКУМЕНТА

ВЕРЗИЈА	ДАТУМ	АУТОР	ОПИС	

САДРЖАЈ

1 РЕЗИМЕ

Према регулаторним и захтевима Политике информационе безбедности < ИНСТИТУЦИЈЕ> неопходно је успоставити способност одговора на појаву инцидената. Сви запослени и уговорни спољни партнери морају одржати сталну пажњу на питања информационе безбедности и без одлагања пријавити потенцијалне инциденте како би се умањиле последице.

2 УВОДНЕ ОДРЕДБЕ

2.1 Сврха

Циљ систематичног приступа управљању инцидентима је поновно успостављање функционисања система и пословних сервиса што је то пре и (и боље) могуће уз очување форензички релевантних трагова за даљу анализу и унапређење процеса.

Овај документ дефинише процедуру одн. опште кораке које треба предузети у случају безбедносног инцидента.

2.2 Опис

Информациони систем <ИНСТИТУЦИЈЕ> има имплементиране различите контроле у циљу умањивања ризика по ИКТ системе и/или контролисане податке.

Документован и јасан процес пријаве инцидената унапређују опште стање информационе безбедности и основа су за брзи ефикасан поступак, систематску примену неопходних корака, и спречавање и/или умањивање последица угрожавања информационе безбедности заштићених информација.

Проблеми у ИКТ систему могу показати симптоме или последице безбедносног инцидента, али због природе ситуације (виша сила) сами по себи не могу бити третирани као безбедносни инцидент (нпр. губитак напајања и сл.). Овакви проблеми који потрају дуже и негативно утичу на пословне сервисе могу се третирати као потенцијални безбедносни инцидент. Исти захтевају иницирање ове процедуре како би се утврдио прави узрок.

2.3 Референце

- Политика управљања инцидентима;
- План за континуитет пословања;
- План за опоравак од катастрофа;
- Процедура управљања кризним ситуацијама.

3 ОПШТЕ ОДРЕДБЕ

3.1 Опсег

Процедура се примењује на све запослене у <ИНСТИТУЦИЈЕ>, као и уговорне спољне партнере који имају приступ ИКТ системима <ИНСТИТУЦИЈЕ>.

Сви наведени запослени су у обавези да се увек придржавају актуелне верзије процедуре.

3.2 Дефиниције

- **безбедносни инцидент** – било која активност која представља претњу по доступност, интегритет или поверљивост информационих добара, или био која активност која представља повреду политике информационе безбедности; покушај или успешни пробој имплементираних мера, неауторизовани приступ коришћење, откривање, модификација или уништење информација или уплитање у рад елемената одн. система у ИКТ систему;
- **безбедносни догађај** – опажена појава унутар ИКТ система (нпр. откривени покушај „инфекција“ малициозним кодом);
- **критични инцидент** – инцидент који као резултат може имати значајне последице по ресурсе <ИНСТИТУЦИЈЕ> уколико се не третира брзо или уколико је угрожени систем класификован као веома значајан или у посебну безбедносну категорију и инцидент је сразмерне категорије;
- **катастрофални догађај за ИКТ** – комплетан отказ примарних *data* центара, укљ. (али не само) и опасне околности из окружења, масивни отказ опреме, комплетан прекид комуникација итд.);
- **План за континуитет пословања** (*Business Continuity Plan*, *BCP*) – план направљен са циљем да обезбеди наставак (континуитет) пословних сервиса током критичних ситуација или катастрофалних догађаја (који се не појављују у уобичајеним околностима);
- **План за опоравак** (*Disaster Recovery Plan*, *DRP*) – план којим се описује како опоравити сервисе брзо и ефикасно; део је Плана за континуитет пословања и примењује се на аспекте институције који се ослањају на ИКТ сервисе/системе за своје функционисање;
- **критични сервиси** – сервиси означени првим приоритетом у Анализи утицаја на пословање (*Business Impact Analysis, BIA*);
- **тим за управљање кризним ситуацијама** (*Crisis Management Team*, *CMT*) – организациона структура надлежна и одговорна да прогласи и управља кризном ситуацијом;
- **CSIRT** (*Cybersecurity Incident Response Team*) – организациона целина одговорна за прикупљање, анализу и извештавање о безбедносним инцидентима и активностима, као и односе са националним ЦЕРТ-ом;
- **максимално прихватљиво време отказа** (*Maximum Tolerable Downtime, MTD*) – укупно време које је власник / надлежна особа за систем вољна да прихвати као (узрок) недоступности пословног процес/сервиса и укљ. сва разматрања потенцијалних последица.

4 ДЕТАЉНЕ ОДРЕДБЕ

4.1 CSIRT

1. У институцији је (обавезно) формиран засебни тим CSIRT који се бави управљањем, те развојем и унапређивањем управљања инцидентима. Ова тим прикупља, анализира и извештав о безбедносним инцидентима и активностима, и надлежан је за сарадњу са националним ЦЕРТ-ом.
2. Тим има своје сталне чланове, али може укључити и стручна лица из других организационих јединица у домену својих експертиза одн. области у којој неки инцидент утиче на њихову организациону јединицу.
    a. Стални чланови тима су из ових организационих јединица:
        - Безбедност
        - Усклађивање са регулаторним и захтевима стандардизације (*compliance*)
        - ИКТ
    b. Обавезни профили за оперативно функционисање CSIRT
        - Специјалиста за информациону безбедност > Координатор
        - Специјалиста за надзор догађаја > Аналитичар
        - Специјалиста за управљање рањивостима > други аналитичар
        - Специјалиста за администрацију (и безбедност) на мрежном нивоу
        - Специјалиста за администрацију (и безбедност) на системском нивоу (више ОС)
        - Специјалиста за системе за управљање базама података
        - Специјалиста за web сервисе и апликације
3. Тим се састаје „у пуном саставу“ у случају појаве инцидента, али одржава и редовне састанке мин. 1 годишње у циљу анализе, планирања и унапређивања активности.
4. (Номиновани) чланови тима су табели у/на …….

4.2 Период надзора

<ИНСТИТУЦИЈА> има успостављен *IT Service Desk* одељење које има улогу да пружа подршку корисницима и надзире функционисање ИКТ система 24x7x365.

Зависно од пријављеног инцидента *IT Service Desk* одлучује кога од доступних запослених контактира.

4.3 Процедура за посебне системе

За системе који су класификовани као веома значајни или спадају у посебну безбедносну категорију (сагласно Политици управљања инцидентима) потребно је припремити посебне процедуре за третман инцидената.

Ова процедура даје основне кораке који се морају спровести при појави безбедносних инцидената без обзира који систем је угрожен. У случају инцидената који су регулисани додатним посебним процедурама, CSIRT ће их применити.

4.4 Процедура декларације катастрофе

1. У случају појаве догађаја који се може квалификовати као катастрофални, CSIRT је одговоран за давање препоруке Тиму за управљање кризним ситуацијама о разматрању проглашавању Катастрофе, и то у случају да су задовољни седећи услови:
    a. Примарни *data* центри су изван нормалног функционисања због оштрих временски услова, масовног отказивања опреме, комплетног прекида комуникација, и сл. и без изгледа да се ситуација
    b. Отказивања критичних сервиса преко …… минута/сати без изгледа да ће бити опорављени на примарним локацијама унутар пред-дефинисаног Максимално прихватљивог времена отказа

    CSIRT треба да донесе одлуку о предлагању разматрања проглашавања катастрофе у року од 45 мин од пријаве оваквог инцидента.
2. Активирање / спровођење даљих корака у складу са Процедуром за управљање кризним ситуацијама. Тим за управљање кризним ситуацијама одговоран је за спровођење процедуре доношења одлуке о декларацији Катастрофе и активирања Плана за континуитет пословања / Плана за опоравак од катастрофе.

    У случају да се активира План за опоравка од катастрофа (DRP), руководилац ИКТ је одговоран да јави Тиму за управљање кризним ситуацијама стање и активности које се спроводе из Плана за опоравак од катастрофе.

    Декларација катастрофе је у домену и ради се у складу са Планом за континуитет пословања и Процедуром за управљање кризним ситуацијама; све даље активности, циљеви, одговорности, улоге су дефинисане кроз Плана за континуитет пословања.

4.5 Категорије инцидената и захтеви за пријављивањем

КАТЕГОРИЈЕ ИНЦИДЕНАТА			
Ознака	**Категорија (ЗИБРС)**	**Мапирање на пример ("тип") инцидента по ЦЕРТ таксономији**	**Опис/појашњење**
0	Тест	*Намењено за тестирање*	Користи се за договорена тестирања (пенетрациона тестирања, тест инт./екст. мера заштите, тестирања одзива и сл.)
1	проваљивање у ИКТ систем	*Компромитовање налога са посебним привилегијама*	напад на рачунарску мрежу и серверску инфраструктуру у оквиру кога је, кршењем мера заштите, остварен приступ који омогућава неовлашћен утицај на рад ИКТ система
		Компромитовање налога без посебних привилегија	
		Компромитовање апликације	
		Bot	

2	Отицање података	*Неовлашћени приступ информацијама*	доступност заштићених података ван круга лица овлашћених за приступ подацима;
3	неовлашћена измена података	*Безбедност (садржаја) информација - Неовлашћена измена информација*	Неовлашћена манипулација/измена података у датотеци, документу или бази података.
4	губитак података		
5	прекид у функционисању	*Саботажа*	...система или дела система
		Отказивање / квар (без зле намере)	
6	ограничавање доступности услуге	*Доступтност - DoS, DDoS*	
7	Малициозни код	*Вирус, Worm, Тројанац, Ransomware, Spyware, Rootkit*	инсталирање злонамерног софтвера у оквиру ИКТ система
8	неовлашћено прикупљање података путем неовлашћеног надзора над комуникацијом или социјалним инжењерингом	*Scanning* * *Скенирање*	*Напади којима се шаљу упити систему у циљу откривања слабих тачака; ово укључује и неку врсту тестирања у циљу прикупљања информација и системима, сервисима који се извршавају на њему, корисничким налозима (нпр. fingerd, DNS querying, ICMP, SMTP EXPN / RCPT, …).*
		Sniffing	*Праћење и снимање мрежног саобраћаја (wiretapping)*
		Social engineering * *Социјални инжењеринг*	*"Извлачење" информација из људи не-техничким методама (нпр. лагање, употреба трикова, подмићивање, претње)*
9	непрестани напад на одређене ресурсе	*Покушаји упада*	
10	злоупотреба овлашћења приступа ресурсима ИКТ система	*Неовлашћено коришћење ресурса*	*Коришћење ресурса за неодобрену намену укљ. и подухвате са циљем стицања профита (нпр. коришћење e-mail за учествовање у нелегалним ланчаним или пирамидалним схемама).*
		Повреда ауторских права	*Продаја или инсталирање нелиценцираних копија комерцијалног software-а или др. материјала под ауторско-правном заштитом (Warez)*
		Маскирање	*Типови напада у којима један ентитет преузима идентитет другог у циљу стицања неке користи од тога.*
		Phishing	*Маскирање/претварање да је у питању други ентитет како би се корисник убедио да открије своје креденцијале.*
11	Остало		Сви инциденти који не спадају у неку од претходних категорија.
12	Рањивост	*Отворено за напад и злоупотребу*	*Отворено доступни сервиси за разрешење Интернет адреса (Open resolver), отворено доступни штампачи, рањивости које су евидентне при скенирању неким алатом за проверу рањивости, неажурне базе "потписа" вируса, итд.*

Повреда Политике / Правила понашања и коришћења ресурса <ИНСТИТУЦИЈЕ> подводи се под наведене категорије, уз додатно обележје у пријави/извештајима.

ВРЕДНОВАЊЕ УТИЦАЈА ИНЦИДЕНАТА		
Утицај / Последица	**Опис**	
НЕМА	Нема утицаја на систем	
НИЗАК	Скоро занемарљив утицај на систем	
УМЕРЕН	Умерен утицај на системе који имају безбедносну категоризацију СТАНДАРДНИ	
ВИСОК	Значајан утицај на системе који имају Безбедносну категоризацију СТАНДАРДНИ или ЗНАЧАЈНИ	
КРИТИЧАН	Значајан утицај на системе који имају Безбедносну категоризацију ПОСЕБНИ	

ВРЕМЕНСКИ ОКВИР ЗА ПРИЈАВУ УНУТАР ИНСТИТУЦИЈЕ / ПРЕЛИМИНАРНИ ИЗВЕШТАЈ		
Категорија инцидента	**Време након откривања**	
1 2 3 4 5 6	1 час	Редовни статусни извештаји по усаглашеној динамици уколико нема адекватне мере
7	2 часа	Редовни статусни извештаји по усаглашеној динамици уколико нема адекватне мере
остало	1-2 дана	Извештај попуњава особа која води инцидент. Коначни извештај подноси се унутар 5 радних дана од разрешења. Уколико разрешење траје више од 2 седмице, подносе се редовни седмични извештаји одељењу за Информациону безбедност.

ИНЦИДЕНТИ КОЈИ СЕ ПРИЈАВЉУЈУ НАДЛЕЖНОМ ОРГАНУ	
Опис инцидента	**Рок за пријаву**
инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга	Први наредни радни дан
инциденти који утичу на велики број корисника услуга	Први наредни радни дан
инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга	Први наредни радни дан
који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност	Исти дан
инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије	Исти дан

инциденти који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе.	Исти дан

У случају хитности информација о инциденту се додатно пријављује телефонским путем, путем електронске поште или на други одговарајући начин.

4.6 Поступак пријаве и управљања инцидентом

4.6.1 Пријављивање

Идентификација потенцијалног безбедносног инцидента и пријављивање одељењу за Информациону безбедност .

У случају да је у питању ситуација за коју се сумња да може бити потенцијално инцидент (нпр. сумњиво понашање или константно „пуцање“ апликације) пријављује се *IT Service Desk* служби.

Пријављивање се спроводи тел. позивом на …… (Информациона безбеност), одн. …… (*IT Service Desk*) или електронском поштом на адресу incident@<ORGANIZACIJA>.rs

4.6.2 Тријажа

1. Увид у достављене информације у циљу процене да ли је у питању безбедносни инцидент.
2. У случају да јесте у питању безбедносни инцидент
   a) иницираће се наредна фаза (одзив), процес документовања активности које се предузимају.
   b) сазива се CSIRT у циљу детаљније истраге
      i) анализа логова и система;
      ii) идентификација логичких и физичких извора, процена мотивације, …;
      iii) прикупљање података и чињеница о нападнутим системима;
   c) Зависно од процене, Координатор предузима кораке окупљања тима са адекватном експертизом – како сталних чланова CSIRT тако и др. учесника (други запослени, спољни сарадници, …);
   d) Под вођством Координатора, а према прелиминарним закључцима чланова тима, спроводи се класификација инцидента и процена могућих последица.
   Инцидент се смешта у одговарајућу категорију.
3. У случају инцидената који се сматрају значајним, угрожени су веома значајни или посебни системи, или/и су потенцијалне последице процењене као значајне, извештава се у најкраћем року надлежни ниво управе.
4. По потреби, запослени се обавештавају о ситуацији, уз информацију која се може користити да се информишу спољни корисници у случају да их контактирају и додатна упутства како да се понашају.
5. По потреби ангажује се додатно људство за помоћ у Позивном центру.
6. У случају да је инцидент унутар датих параметара, пријављује се надлежном органу одн. ЦЕРТ-у. Ако је у питању криминална активност мора бити обавештено надлежно Тужилаштво.

4.6.3 Третирање инцидента

Спроводе се активности за ограничавање опсега и магнитуде инцидента. Разматрају се мере као што су backup/restore, промена лозинки, промене листа за контролу приступа компромитваним /

угроженим системима и /или подацима, имплементације додатних мера заштите, одређивање релевантних рањивости, те елиминације извора како би се избегло понављање након опоравка.

Координатор организује и олакшава извођење сесија размене информација и идеја.

По потреби, координатор предузима кораке за прелиминарне и периодичне извештаје о спроведеним активностима и тренутном стању.

4.6.4 Опоравак

Спроводе се акције успостављања нормалног функционисања система и пословних процеса / сервиса, као што су: *restore* или поновна инсталација и валидација система, надзор функционисања итд.

По потреби, координатор предузима кораке за прелиминарне и периодичне извештаје о спроведеним активностима и тренутном стању.

По потреби, запосленима се достављају ажуриране / нове информације о ситуацији, уз информацију која се може користити да се информишу спољни корисници у случају да их контактирају и додатна упутства како да се понашају.

4.6.5 Праћење

Припрема и достављање коначног извештаја Руководиоцу за информациону безбедност (према Политици управљања инцидентима). Извештај треба да садржи и поуку из процеса управљања инцидентом, спроведене успешне и неуспешне активности и препоруке CSIRT како би се спречиле овакве ситуације у будућности, одн. унапредила свеукупна имплементација система / процеса који спроводе мере информационе безбедности. Коначни извештај саставља Координатор у сарадњи са члановима тима који су пратили конкретни инцидент.

5 ЗАВРШНЕ ОДРЕДБЕ

Процедуре ступа на снагу на дан усвајања.

6 ПРИЛОЗИ

6.1 Образац за пријаву инцидента

6.2 Именовани чланови CSIRT