Procedura za upravljanje incidentima u informacijskom sustavu OBV

SADRŽAJ

POPIS PRILOGA	
Prilog 1	Klasifikacija incidenata
Prilog 2	Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga
Prilog 3	

NAPOMENA:

Gore navedeni vezani dokumenti kojih je vlasnik Opća bolnica Varaždin su iz razloga jednostavnosti korištenja izrađeni kao zasebni dokumenti a smatraju se sastavnim dijelom ovog dokumenta. Isti su dostupni osoblju u skladu sa distribucijom pojedinog dokumenta te putem Intranet portala na način da se nalaze u istoj radnoj mapi gdje i ovaj priručnik.

VEZANI DOKUMENTI	
1	Politika sigurnosti informacijskog sustava
2	Politika zaštite osobnih podataka
3	Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/18)
4	Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga
5	Uredba o mjerama informacijske sigurnosti (NN 46/08)
6	
7	

NAPOMENA:

Gore navedeni vezani dokumenti su izrađeni kao zasebni dokumenti nužni za pravilno razumijevanje sadržaja ovog dokumenta ali se ne smatraju njegovim sastavnim dijelom. Isti su dostupni osoblju putem Intranet portala.

Distribucija dokumenta

Broj kopije	Mjesto/lokacija/radno mjesto	Format	Količina	Datum	Potpis
	OPĆA BOLNICA VARAŽDIN				
1	Uprava	Tiskana kopija	1		
N/A	Svim radnicima – Intranet portal	Digitalna kopija	N/A		

Revizija dokumenta

Redni broj	Datum	Reviziju izradio	Reviziju odobrio	Naziv i broj poglavlja koje se mijenja/opis revizije
1	16.11.2022.	D. Uremović	D. Poljak	Cijelo izdanje

1. Namjena

Ovom Procedurom utvrđuje se proces upravljanja incidentima u informacijskom sustavu Opće bolnice Varaždin (dalje u tekstu: OBV) odnosno incidentima u procesu upravljanja informatičkom podrškom poslovnim procesima OBV-a.

Svaka organizacijska jedinica koja sudjeluje u procesu upravljanja incidentima u informacijskom sustavu u obvezi je sukladno svojoj poslovnoj domeni optimalno organizirati podršku navedenom procesu.

Ovim dokumentom definirana je procedura upravljanja incidentima i sve pripadne aktivnosti u informacijskom sustavu OBV.

Cilj procedure je osigurati mogućnost prijave incidenta svim korisnicima informacijskog sustava, definirati postupke prijave i vrste incidenata koje prijavljuju korisnici informacijskog sustava (uključujući i vanjske partnere) te osigurati ispravan i pravovremen odgovor na sigurnosne incidente.

Također je cilj procedure umanjiti utjecaje incidenata koji su se pojavili i to kroz jasno definirane procese upravljanja incidentima koji su prihvaćeni od strane OBV-ovih zaposlenika i pridruženih OBV-ovih trećih strana.

Efikasno rješavanje sigurnosnih incidenata osigurava se kroz pravovremenu prijavu i eskaliranje sigurnosnih incidenata te njihovu analizu.

Klasifikacija, aktivnosti i procedure navedene u ovom dokumentu potiču konzistentni pristup i efikasno rješavanje incidenata te osiguravaju:

- oporavak funkcionalnosti u definiranom vremenskom intervalu,
- uklanjanje uočenih sigurnosnih nedostataka,
- poboljšanje komunikacije između poslovnih subjekata te prikupljanje informacija tijekom cijelog incidenta,
- poduzimanje akcija u cilju izbjegavanja ponavljanja sličnih incidenata u budućnosti

Ovaj dokument definira sve potrebne korake koji se moraju poduzeti u slučaju da dođe do incidentne situacije.

2. Opseg

Procedura upravljanja incidentima u informacijskom sustavu obuhvaća cijeli informacijski sustav OBV i primjenjuje se na sve zaposlenike, ugovorne suradnike i korisnike treće strane.

3. Tijek procesa

3.1 Klasifikacija incidenata

U okviru upravljanja incidentima u informacijskom sustavu OBV-a definirane su 3 razine incidenata:

- incidenti niske razine,
- incidenti srednje razine,
- incidenti visoke razine,

Prema navedenoj klasifikaciji poduzimaju se aktivnosti za rješavanje incidenta, izvještavaju ključne osobe i prate definirana vremena rješavanja i eskalacije.

Detaljni opis razina incidenata s operativnim utjecajima te primjerima dan je tablici u prilogu Prilog 1 – Klasifikacija incidenata.

3.1.1 Incidenti niske razine (problemi)

Incidenti niske razine odnose se na razne korisničke probleme koje Odjel za informatiku, tj. organizacijska jedinica podrške korisnicima rješava u okviru svoje nadležnosti. Ovi problemi nemaju veći utjecaj na rad informacijskog sustava ili odvijanje poslovnih procesa.

3.1.2 Incidenti srednje razine

Incidenti srednje razine odnose se na zahtjeve i probleme korisnika koji utječu na rad informacijskog sustava OBV-a ili odvijanje poslovnih procesa, ali ne uzrokuju veće prekide u radu informacijskog sustava ili pri odvijanju poslovnog procesa. Nakon prijave incidenta, Odjel za informatiku proglašava incident srednje razine te pokreće potrebne aktivnosti za rješavanje incidenta.

3.1.3 Incidenti visoke razine

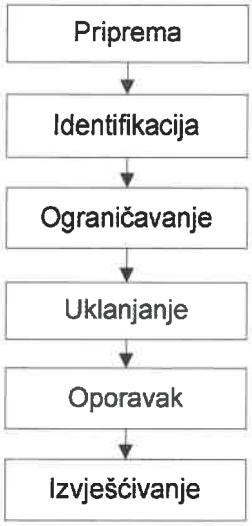
Incidenti visoke razine obuhvaćaju događaje i aktivnosti koje uzrokuju prekid jednog ili više kritičnih poslovnih procesa OBV-a. Ovi incidenti imaju veliki operativni utjecaj i znatno otežavaju poslovanje OBV-a.

3.2 Aktivnosti upravljanja incidentima u informacijskom sustavu

Procedura upravljanja incidentima temelji se na uspostavljenom postupku potpore korisnicima. Za potrebe tog postupka koristi se sustav Service Desk koji omogućava prijavu problema/incidenata te praćenje postupka rješavanja.

Budući da sustav sadrži bazu podataka svih prijava, komentara i pripadnih korektivnih akcija, predstavlja prikladan izvor informacija za naknadne analize nastalih incidenata.

Proces upravljanja incidentima odvija se u 6 faza koje su prikazane na sljedećoj slici:



Slika 1: Aktivnosti upravljanja incidentima

3.2.1 Priprema

Upravljanje incidentima počinje predradnjama koje se provode u svrhu zaštite informacijske imovine prije pojave incidenta. Navedene predradnje obuhvaćaju dokumentirane politike, pravilnike, procedure i ostale interne akte OBV-a, obuku krajnjih korisnika, te implementaciju dodatnih sigurnosnih kontrola u informacijski sustav OBV-a na sklopovskoj i programskoj razini (npr. nabava sigurnosnih uređaja ili programskih paketa).

Aktivnost pripreme ne odnosi se na pojedinačni incident, već predstavlja nužne preduvjete za ispravno i kontinuirano izvršavanje procedure upravljanja incidentima.

Aktivnost pripreme obuhvaća:

- određivanje osoba zaduženih za odgovor na incidente te definiranje njihovih ovlasti, odgovornosti i djelokruga rada,
- izradu komunikacijske liste za hitne slučajeve,
- edukaciju korisnika u vezi s prijavljivanjem događaja, osobito u kontekstu potencijalnih slabosti i ugrožavanja informacijske sigurnosti,
- edukaciju osoba zaduženih za odgovor na incidente,
- definiranje odgovornosti korisnika informacijskog sustava prilikom upravljanja incidentima,
- uspostavljanje odnosa s nadležnim institucijama.

3.2.2 Identifikacija

Postoje tri moguća izvora informacija o incidentima:

- prijave korisnika,
- prijave zaposlenika Odjela za informatiku,

- automatizirana prijava pomoću aplikacija i alata za nadzor i dijagnostiku IT sustava odnosno prijava zaposlenika Odjela za informatiku nakon uvida u navedene alate.

Prijava incidenta u informacijskom sustavu slijedi nakon uočavanja, a **sve incidente srednje i visoke razine potrebno je prijavljivati putem navedenih aplikativnih sustava**, osim incidente fizičke sigurnosti koji se mogu prijaviti telefonom, mailom ili osobno Službi zaštite na radu i zaštite od požara. Ta Služba vodi evidenciju incidenata fizičke sigurnosti.

Prijava zaprimljena u aplikativni sustav obrađuje se od strane zaposlenika Odjela za informatiku odnosno Voditelja sigurnosti informacijskog sustava (VSIS). Zaposlenici Odjela za informatiku odgovorni su za klasifikaciju incidenta i adekvatno označavanje te opis incidenta.

Za sve incidente visoke razine u informacijskom sustavu, uz regularnu obavijest višim razinama podrške, potrebno je obavijestiti Voditelja sigurnosti informacijskog sustava (VSIS). Svrha ovog mehanizma je mogućnost pravovremenog ukazivanja na mogući problem informacijske sigurnosti te mogućnost pravovremenog djelovanja VSIS-a zajedno s vlasnicima informacija u svrhu smanjivanja potencijalne štete za OBV.

Zaposlenici Odjela za informatiku donose odluku o klasifikaciji incidenta i pripadnoj eskalaciji na temelju osobnog iskustva, utemeljene prakse i potencijalne kritičnosti zaprimljene prijave. Ukoliko nije moguće jednoznačno odrediti klasifikaciju incidenata, incident je potrebno klasificirati prema najbližoj većoj razini klasifikacije. Ukoliko aplikativni sustav za prijavu incidenata nema predviđeno polje za unos klasifikacije, klasifikaciju treba unijeti ili u polje za naziv incidenta ili u polja predviđena za detaljniji opis incidenta.

U slučaju nemogućnosti prijave incidenta putem aplikativnog sustava, prijava se može podnijeti i telefonom ili na druge načine. Zaposlenici Odjela za informatiku dužni su naknadno u aplikativni sustav unijeti sve informacije o incidentima koji nisu bili prijavljeni putem aplikativnog sustava.

Tablica 1 pokazuje POKI (eng. *RACI - Responsibility assignment matrix*) matricu odgovornosti za fazu prijave i identifikacije incidenta.

Korak	Opis	Odgovornosti			
		Provodi	Odgovoran	Konzultira se	Informira se
Prijava	Korisnik informacijskog sustava prijavljuje uočeni problem pomoću aplikativnog sustava.	Korisnik	Korisnik	-	Odjel za informatiku
Označavanje i klasifikacija incidenta	Prijavljeni incident se klasificira u prikladan razred, te se označava na prikladan način putem indikatora prijave. Po potrebi se može konzultirati VSIS za precizniju identifikaciju i klasifikaciju incidenata. U slučaju incidenta visoke razine, šalje se obavijest VSIS-u.	Odjel za informatiku	Odjel za informatiku	VSIS	VSIS

Tablica 1 - Koraci prepoznavanja i obilježavanja sigurnosnih događaja

Prijava incidenta sadržava relevantne informacije o događaju:

- datum i vrijeme događaja,
- opis događaja (što se dogodilo i na koji način, na koje komponente informacijskog sustava događaj ima utjecaj, da li postoje i koje su posljedice za poslovanje, da li su identificirane eventualne ranjivosti i sl.),
- vezani događaji (ukoliko postoje),
- informacije o osobi koja prijavljuje događaj,
- trajanje događaja, ukoliko je događaj završio.

Ukoliko je incident klasificiran visokom razinom i ako incident predstavlja ekstremni rizik za kontinuitet poslovanja te zahtijeva hitnu reakciju, Rukovoditelj Odjela za informatiku može pokrenuti akciju za otklanjanje incidenta te paralelno obavijestiti VSIS-a.

Po obradi incidenta visoke razine, Rukovoditelj Odjela za informatiku ili VSIS o incidentu izvještavaju Odbor za ISMS ili Upravu OBV-a.

U slučaju potrebe za eskalacijom prilikom obrade incidenta, kontaktiraju se nadležne organizacijske jedinice ili nadležne službe u svrhu provođenja korektivnih akcija. Odgovarajuće nadležne organizacijske jedinice su unutar OBV-a (npr. Služba zaštite na radu i zaštite od požara), a nadležne službe izvan OBV-a (npr. policija), ovisno o vrsti i klasifikaciji incidenta. Ovu aktivnost provodi VSIS te izvješćuje Odbor za ISMS.

Ukoliko se obrada incidenta prepušta nadležnim organizacijskim jedinicama, nadležnim službama ili trećim stranama, za obradu incidenta i izradu izvještaja odgovorna je jedna ili više nadležnih organizacijskih jedinica i službi koje provode potrebne korektivne akcije. Po obradi incidenta nadležna organizacijska jedinica/služba mora izraditi izvještaj o provedenim aktivnostima koje prosljeđuje VSIS-u.

Povijest incidenata mora se čuvati najmanje godinu dana zbog kasnijih analiza i preporuka za unaprjeđenje sigurnosti i funkcionalnosti informacijskog sustava OBV-a.

3.2.3 Ograničavanje

Nakon što zaposlenici Odjela za informatiku (po potrebi zajedno s VSIS-om i ostalim nadležnim org. jedinicama) provedu preliminarnu analizu i identifikaciju/klasifikaciju incidenta, poduzimaju se sve potrebne mjere u ovisnosti o klasifikacijskoj razini incidenta, u svrhu ograničavanja utjecaja incidenta.

Incidenti niske razine obrađuju se na način predviđen uobičajenim procedurama podrške korisnicima.

U slučaju incidenta visoke razine, moguće je aktivirati plan kontinuiteta poslovanja (postupci aktivacije pojedinih planova su definirani u sklopu samih planova).

Faza ograničavanja obuhvaća odgovarajuće aktivnosti kojima se utvrđuje i nastoji ograničiti opseg i utjecaj incidenta te eventualnu izradu pričuvnih kopija kompromitiranih sustava i prikupljanje dokaza radi daljnje istrage o uzrocima incidenta, ukoliko je to potrebno. Faza ograničavanja odnosi se prije svega na sigurnosne incidente visoke razine čiji se utjecaj može ograničiti. Funkcionalni incidenti (poput prestanka rada sustava) ili incidenti koji se ne mogu ograničiti (potres, ispad napajanja električne energije i sl.) nisu u opsegu faze ograničavanja.

VSIS obavještava sve zainteresirane strane (rukovoditelje organizacijskih jedinica i sl.) na koje se visoki incident odnosi s ciljem koordinacije daljnjih aktivnosti na ograničavanju utjecaja incidenta.

Prije postupaka ograničavanja utjecaja, s ciljem prepoznavanja opsega i utjecaja incidenta, poželjno je utvrditi sljedeće:

- koliko računala, aplikacija, mrežnih resursa je obuhvaćeno incidentom?
- koliko lokacija je obuhvaćeno incidentom?
- jesu li kompromitirani kritični IT sustavi (u pogledu povjerljivosti, integriteta ili dostupnosti)?
- da li se na mrežnoj domeni gdje se nalazi kompromitirano računalo nalaze druga kritična računala?
- nalaze li se na kompromitiranom računalu osjetljivi podaci?
- koji je financijski i operativni utjecaj incidenta na odvijanje kritičnih poslovnih procesa?
- koga je sve potrebno kontaktirati (točke kontakta: rukovoditelji organizacijskih jedinica, dobavljači, policija, itd.)?
- koliko je procijenjeno vrijeme oporavka od incidenta i je li oporavak moguće izvesti u skladu s ciljanim vremenom oporavka?

Na temelju prikupljenih informacija, ukoliko se radi o sigurnosnim incidentima ili incidentima koji obuhvaćaju više sustava, potrebno je pokrenuti akcije s ciljem ograničavanja incidenta.

Neke od mogućih akcija su:

- potpuno gašenje sustava,
- uklanjanje sustava s računalne mreže,
- promjena pravila usmjeravanja ili pravila filtriranja mrežnog prometa na vatrozidima za uklanjanje vanjskog ili unutarnjeg pristupa kompromitiranom sustavu,
- onemogućavanje ili brisanje korisničkih računa koji su kompromitirani napadom,
- povećanje razine nadzora sistemskih odnosno mrežnih aktivnosti (npr. češći interval praćenja i sl.),
- onemogućavanje mrežnih servisa i funkcionalnosti, ukoliko napad iskorištava neku od ranjivosti takvog servisa,
- razne druge aktivnosti.

Neovisno o primijenjenom načinu ograničavanja utjecaja incidenta, potrebno je provjeriti jesu li kompromitirani i redundantni IT sustavi i podaci (na alternativnoj lokaciji ili u pričuvnoj pohrani).

3.2.4 Uklanjanje

Nakon primjene odgovarajućih mjera ograničavanja opsega i utjecaja incidenta, potrebno je utvrditi uzrok incidenta i provesti uklanjanje uzroka incidenta.

Na temelju utvrđenog uzroka incidenta, uklanjanje uzroka incidenta može obuhvaćati:

1) implementaciju dodatnih sigurnosnih kontrola na sklopovskoj i programskoj razini u informacijskom sustavu (nabava dodatnih sigurnosnih uređaja, poput IDS/IPS uređaja i vatrozida, nabava redundantnih sustava, filtriranje mrežnog prometa, povećavanje razine detaljnosti log zapisa, promjena pravila pristupa i sl.),
2) povratak sustava na stanje prije incidenta (korištenjem ugrađenih funkcionalnosti u slučaju virtualizacijskih poslužitelja ili korištenjem pričuvne kopije podataka),
3) analizu ranjivosti kako bi se onemogućili novi incidenti zbog istog uzroka.

U slučaju da nakon incidenta slijedi građanska ili kaznena akcija odnosno prijava protiv određene pravne ili fizičke osobe ili ako je riječ o potencijalnom kršenju ugovora odnosno regulatornog zahtjeva, potrebno je prikupiti, sačuvati i predstaviti sve dostupne dokaze. Prilikom prikupljanja dokaza o incidentima treba voditi računa o težini svih pribavljenih dokaza, pri čemu se treba držati sljedećih smjernica:

1) *za papirnatu dokumentaciju*: original je potrebno čuvati na sigurnom mjestu uz evidenciju osobe koja je pronašla dokument, mjesto pronalaska dokumenta te informaciju o svjedoku otkrića dokumenta; originali se ne smiju ni u kojem slučaju mijenjati.
2) *za informacije u elektroničkom obliku*: potrebno je napraviti preslike ili kopije („disk image" odnosno „memory dump") svih prijenosnih medija, informacija na tvrdim diskovima ili u memoriji; potrebno je napraviti zapis svih aktivnosti tijekom procesa kopiranja; proces kopiranja treba provesti uz prisutnost svjedoka; originalne medije i zapis treba čuvati na sigurnom mjestu bez mogućnosti promjene.

3.2.5 Oporavak

Nakon što je uzrok incidenta uklonjen, slijedi faza oporavka čiji je cilj vratiti sustave i ostalu informacijsku imovinu na koje je incident imao utjecaj u stanje prije incidenta.

Primjeri aktivnosti oporavka su slijedeći:

1) instalacija operativnog sustava iznova s provjerenog medija ili originalnog medija proizvođača,
2) povratak podataka korištenjem pričuvne kopije,
3) onemogućavanje nepotrebnih servisa i primjena zadnjih zakrpi i nadogradnji,
4) instalacija aplikacija i pripadnih zakrpi i nadogradnji,
5) izmjena lozinki,
6) ponovo uključenje sustava i sl.

Jednom kad je sustav oporavljen, potrebno je provjeriti konfiguracijske postavke kako bi se osiguralo da je funkcionalno stanje sustava jednako onome prije nego je nastupio sigurnosni incident. Prije puštanja u produkciju potrebno je provesti procedure testiranja.

Tablica 2 prikazuje POKI matricu za faze ograničavanja, uklanjanja i oporavka i incidente visoke razine.

Korak	Opis	Odgovornosti			
		Provodi	Odgovoran	Konzultira se	Informira se
Provjera i prikupljanje potrebnih podataka	Pregledavaju se zabilježeni podaci o prijavi. U slučaju nepotpunih ili neadekvatnih informacija za mjerodavnu procjenu o naravi prijave potrebno je Vlasnika informacije ili treću stranu kontaktirati za dodatne informacije.	VSIS	VSIS	Prema potrebi Vlasnika informacije ili treća strana	-
Brisanje oznake sigurnosnog događaja ukoliko nije incident	Ukoliko inicijalna oznaka /klasifikacija incidenta nije ispravno postavljena, VSIS briše oznaku, zapisuje komentar o napravljenoj procjeni i odluci te time dojavljuje svim uključenim stranama da ovo nije sigurnosni incident, odnosno incident visoke razine.	VSIS	VSIS	-	Odjel za informatiku
Odluka o prioritetnom djelovanju	VSIS odlučuje mora li se problem riješiti prioritetnim postupkom ili se problem može riješiti standardnim postupkom. U slučaju potrebe za prioritetnim djelovanjem, VSIS započinje aktivnosti ograničavanja incidenta, u suradnji sa Odjelom za informatiku	VSIS / Odjel za informatiku	VSIS / Rukovoditelj Odjela za informatiku	Po potrebi, vanjski stručnjak za informacijsku sigurnost	Odjel za informatiku
Odluka o eskalaciji	Vlasnik informacije i, prema potrebi, vanjski stručnjak za informacijsku sigurnost, se obavještava u svrhu provedbe analize utjecaja sigurnosnog incidenta na poslovanje. Svrha ove analize je ustanoviti ozbiljnost incidenta, na temelju čega se donosi odluka o eskalaciji.	VSIS	VSIS	Po potrebi, vanjski stručnjak za informacijsku sigurnost i Vlasnik informacije	Rukovoditelj Odjela za informatiku
Ograničavanje i uklanjanje	U slučaju kada ne postoji potreba za eskalacijom,	VSIS / Rukovoditelj	VSIS / Rukovoditelj	Po potrebi, vanjski	Vlasnik informacije /

Korak	Opis	Odgovornosti			
		Provodi	Odgovoran	Konzultira se	Informira se
uzroka incidenta te oporavak sustava	incident se interno obrađuje, te se u suradnji s Vlasnikom informacije identificira uzrok incidenta, posljedice na poslovanje i ostali rizici. U slučaju potrebe za eskalacijom, kontaktiraju se nadležne službe u svrhu obrade incidenta i provedbe korektivnih akcija, u skladu s klasifikacijom incidenata.	Odjela za informatiku	Odjela za informatiku	stručnjak za informacijsku sigurnost	procesa
Zatvaranje prijave	Na kraju postupka incident se zatvara, čime ulazi u izvor podataka za kasniju statističku analizu.	VSIS	VSSI		Prema potrebi uključene strane

Tablica 2 - Koraci faza ograničavanja, uklanjanja i oporavka incidenata visoke razine

3.2.6 Izvještavanje i naknadne aktivnosti

Faza izvještavanja i naknadnih aktivnosti uključuje:

- izvješćivanje o svim fazama upravljanja incidentom te izradu Izvještaja o incidentu,
- izradu preporuka radi bržeg prepoznavanja ili sprečavanja ponavljanja incidenta,
- učenje na incidentima.

Izvještaje za incidente niske razine nije potrebno raditi periodički izvještaj, ali Odjel za informatiku mora biti u mogućnosti pružanja izvještaja o zaprimljenim, riješenim, neriješenim incidentima, vremenima rješavanja i drugim relevantnim informacijama o incidentima na zahtjev Odbora za ISMS ili Uprave OBV-a.

Za incidente srednje razine Odjel za informatiku periodički (minimalno na godišnjoj razini) daje izvještaj o zaprimljenim, riješenim, neriješenim i eskaliranim incidentima, vremenima rješavanja i drugim relevantnim informacijama. Navedeni izvještaj se predaje Odboru za ISMS.

Za sve incidente visoke razine, po rješavanju incidenta, voditelj sigurnosti informacijskog sustava u suradnji s voditeljem Odjela za informatiku, izrađuju Izvješće o incidentu kojeg šalju na uvid Odboru za ISMS i/ili Upravi OBV-a (po potrebi).

Izvještaj o incidentu informacijske sigurnosti treba sadržavati sljedeće informacije:

- podaci o osobi koja podnosi izvještaj,
- vrsta i razina incidenta (klasifikacija incidenta),
- detaljan opis incidenta (može se preuzeti s prijave),
- vremena prijave/nastanka, trajanja i kraja incidenta,
- pogođena informacijska imovina,
- utjecaj/ posljedice incidenta,

- osobe uključene u incident,
- planirane akcije za rješavanje incidenta,
- izvršene akcije za rješavanje incidenta,
- neizvršene akcije,
- obaviješteni pojedinci/ entiteti.

Izvještaj se šalje Odboru za ISMS i svim odgovornim osobama u OBV-a na temelju prethodne suglasnosti Odbora (Vlasnik informacije, rukovoditelji organizacijskih jedinica, Uprava i dr.).

Izvještaj o incidentu treba poslužiti kao temelj za poboljšanje postojećih sigurnosnih kontrola i procedura ili uvođenje novih sigurnosnih kontrola u vidu planova implementacije s opisom kontrola, definiranim zaduženjima i rokovima za implementaciju sigurnosnih kontrola.

3.2.7 Incidenti vezani za osobne podatke ispitanika

U slučaju narušavanja sigurnosti osobnih podataka, OBV će bez odlaganja, a najkasnije u roku od 72 sata po otkrivanju incidenta, o tome izvijestiti nadležno tijelo (Agenciju za zaštitu osobnih podataka). U slučaju curenja osobnih podataka, OBV će o tome obavijestiti i ispitanike čiji su podaci kompromitirani ukoliko to bude provedivo na razuman način.

U ovakvim tipovima incidenata, pored Odjela za informatiku, voditelja sigurnosti informacijskog sustava i voditelja organizacijskih jedinica u čijem je području djelovanja došlo do povrede (incidenta), u aktivnostima rješavanja incidenta sudjeluje i službenik za zaštitu osobnih podataka (DPO).

3.2.8 Izvješćivanje CSIRT-a o visokim incidentima

Za sve incidente visoke razine (s visokim učinkom), po rješavanju incidenta, Rukovoditelj Odjela za informatiku odgovoran je za izradu Izvještaja o incidentu kojeg šalje na uvid Odboru za ISMS i/ili Upravi OBV-a (po potrebi). Također, o incidentima visoke razine koji imaju znatan učinak na kontinuitet usluga, potrebno je bez neopravdane odgode, obavješćivati nadležni CSIRT.

Nadležni CSIRT-ovi će informacije o incidentima te pripadajuća izvješća zaprimati na sljedeći način:

- Nacionalni CERT
  - Informacije o incidentu prijavljuju se na telefonski broj 01 6661 650 prema uputama opisanim na www.cert.hr/zks-incident
  - Inicijalne obavijesti, prijelazna i završna izvješća na e-mail adresu zks-incident@cert.hr
- Zavod za sigurnost informacijskih sustava
  - Informacije o incidentu na telefonski broj 01 4694 144 prema uputama opisanim na www.zsis.hr
  - Inicijalne obavijesti, prijelazna i završna izvješća na e-mail adresu cert@zsis.hr.

Vrste obavijesti koje se šalju CSIRTU te rok u kojem je obavijest potrebno poslati CSIRT-u su:

- inicijalna obavijest o incidentu sa znatnim učinkom (odmah, a najkasnije u roku od **četiri sata** od trenutka otkrivanja incidenta sa znatnim učinkom),
- prijelazno izvješće o incidentu sa znatnim učinkom (**tri radna dana** od podnošenja inicijalne obavijesti o incidentu),
- završno izvješće o incidentu sa znatnim učinkom (**15 dana** od dana procijene da je redovito pružanje usluge ponovno uspostavljeno).

Detaljne smjernice o postupanju i izvješćivanju o visokim incidentima koje se dostavljaju CSIRT-u te predlošci za pojedina izvješća navedeni su u Uredbi o kibernetičkoj sigurnosti, Poglavlje II, Odjeljak A i Smjernicama za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga (Prilozi 1, 2, 3 i 4).

3.2.9 Posebne odredbe o postupanju s incidentima koji se odnose na nacionalno klasificirane podatke

Za sve incidente koji se odnose na nacionalno klasificirane podatke stupnjeva „Vrlo tajno", „Tajno" i „Povjerljivo", potrebno je obaviti i sljedeće aktivnosti:

- Obavijestiti o incidentu Ured vijeća za nacionalnu sigurnost. Ured Vijeća za nacionalnu sigurnost, na temelju saznanja o uništenju, otuđenju ili dostupnosti klasificiranog podatka neovlaštenoj osobi, izvijestit će nadležnu sigurnosno-obavještajnu agenciju i druga nadležna tijela.
- U slučaju incidenta koja bi dovela do ugroze neovlaštenog pristupa nacionalno klasificiranim podacima, poduzeti sve korake za zaštitu pristupa takvim podacima što u krajnjoj mjeri može značiti i uništenje takvih podataka do neraspoznatljivosti. Prije poduzimanja ovakvih koraka potrebno je uzeti u obzir razinu štete takvih koraka u odnosu na štetu prouzročenu neovlaštenim pristupom takvim podacima.

4. Završne i prijelazne odredbe

Procedura stupa na snagu i primjenjuje se danom njezinog donošenja.

KLASA: 011-02/23-01/5

URBROJ: 2186-192-30-23-1

U Varaždinu, 28.03.2023.

RAVNATELJ

Dr. sc. Damir Poljak, mag.soc.geront.

Prilog 1 – Klasifikacija incidenata

U sljedećoj tablici naveden je detaljni opis razina incidenata s pripadnim operativnim utjecajima, ciljanim vremenom rješavanja problema te nizom primjera događaja s njihovom klasifikacijom.

Klasifikacija učinaka incidenata prema Smjernicama za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga dana je u prilogu ove procedure: Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga (Prilog 1).

Razina incidenta	Opis incidenta	Operativni utjecaj	Ciljano vrijeme rješavanja (za problem raspoloživosti)	Primjer
Niska	Svi zahtjevi i problemi korisnika koji nemaju utjecaja na rad informacijskog sustava ili odvijanje poslovnih procesa	Minimalan operativni utjecaj, incidentom su obuhvaćeni individualni korisnici	3 radna dana	• Individualni korisnik ne može pristupati sustavu • Korisnik je zaboravio zaporku, potrebna promjena • Korisnik zahtjeva poboljšanje funkcionalnosti ili informaciju o sustavu • Problemi s radom aplikacija na računalu korisnika (npr. MS Office aplikacija) • Problemi u radu testnih sustava • Teškoće u pružanju pojedinih nekritičnih usluga (npr. printer ne radi u određenoj organizacijskoj jedinici) • Incident koji uzrokuje manju nesukladnost prema regulatornim propisima
Srednja	Svi zahtjevi i problemi koji utječu na rad informacijskog sustava ili odvijanje poslovnih procesa ali ih ne prekidaju	Malen operativni utjecaj, incidentom je obuhvaćen veći broj korisnika	8 sati	• Problemi s funkcionalnošću računalne mreže s ograničenim utjecajem • Incident uzrokovan nedovoljnim kapacitetom informacijskog sustava (npr. otežan rad sustava elektroničke pošte) • Kvar (prestanak rada) kritičnih produkcijskih poslužitelja Incident koji izaziva kratkotrajan prekid odvijanja kritičnog poslovnog procesa • Incident koji duže sprječava zaposlenike organizacijske jedinice u radu • Neovlašteni pristup/izmjena/otkrivanje podataka klasificiranih kao **Ograničeni ili Povjerljivi** (prema Zakonu o tajnosti podataka) odnosno **Interni** (prema Pravilniku

Razina incidenta	Opis incidenta	Operativni utjecaj	Ciljano vrijeme rješavanja (za problem raspoloživosti)	Primjer
				o klasifikaciji informacija) • Incident koji je uzrokovan lakšom povredom ugovornih obveza s ključnim poslovnim partnerima
Visoka	Prekid u odvijanju ključnog poslovnog procesa ili značajno narušavanje povjerljivosti ili integriteta u informacijskom sustavu	Vrlo veliki operativni utjecaj, utjecaj na više kritičnih poslovnih procesa – otežano poslovanje (po potrebi pokreće se BC plan)	1 sat	• Incident koji izaziva potpun prekid više kritičnih poslovnih procesa (npr. dugotrajan zastoj središnje aplikacije/sustava) • Izravno štete na infrastrukturi (npr. gubitak sistem sale) • Incident koji sprječava veći broj organizacijskih jedinica u radu • Neovlašteni pristup/izmjena/otkrivanje podataka klasificiranih kao **Tajni ili Vrlo tajni** (prema Zakonu o tajnosti podataka) odnosno **Osjetljivi** (prema Pravilniku o klasifikaciji informacija) • Incident koji uzrokuje težu povredu regulatornih propisa • Incident uzrokovan kršenjem ugovornih obveza s ključnim poslovnim partnerima • Incidenti koji zadovoljavaju kriterije Uredbe o kibernetičkoj sigurnosti i Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga (Prilog 1)

Tablica 3: Klasifikacija incidenata