**\* OVO JE BESPLATNI OGLEDNI PREDLOŽAK DOKUMENTA \***

**Prilog 1 – Plan odziva na incident**

**Povijest promjena**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Verzija** | **Izradio** | **Opis promjena** |
|  | 0.1 | Advisera | Osnovni nacrt dokumenta |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sadržaj**

[1. Svrha, područje primjene i korisnici 2](#_Toc216370019)

[2. Ovlaštenja i odgovornosti prilikom odziva na incident 2](#_Toc216370020)

[3. Komunikacija 2](#_Toc216370021)

[4. Postupci prilikom incidenta koji remeti poslovanje 3](#_Toc216370022)

[4.1. Upravljanje incidentom koji remeti poslovanje 3](#_Toc216370023)

[4.1.1. Obveza svakog zaposlenika da prijavi incidente 3](#_Toc216370024)

[4.1.2. Postupanje s incidentom koji remeti poslovanje 4](#_Toc216370025)

[4.1.3. Upravitelj kriznim situacijama 4](#_Toc216370026)

[4.2. Ograničavanje i uklanjanje incidenta 4](#_Toc216370027)

[4.2.1. Evakuacija zgrade (neovisno o vrsti incidenta) 4](#_Toc216370028)

[4.2.2. Vatra 5](#_Toc216370029)

[4.2.3. Prekid napajanja električnom energijom 5](#_Toc216370030)

[4.2.4. Potres 5](#_Toc216370031)

[4.2.5. Prijeteće pismo 6](#_Toc216370032)

[4.2.6. Prijeteći poziv / prijetnja bombom 6](#_Toc216370033)

[4.2.7. Prekid telekomunikacijskih veza 7](#_Toc216370034)

[4.2.8. Prekid rada informacijskog sustava 7](#_Toc216370035)

[4.2.9. Napad zlonamjernim kodom 7](#_Toc216370036)

[4.2.10. Kršenje internih ili vanjskih pravila 8](#_Toc216370037)

[5. Upravljanje zapisima koji se vode temeljem ovog dokumenta 8](#_Toc216370038)

[6. Valjanost i upravljanje dokumentom 8](#_Toc216370039)

# Svrha, područje primjene i korisnici

Svrha je ovog Plana osigurati zaštitu zdravlja i sigurnosti ljudi u slučaju incidenta koji remeti poslovanje ili drugog incidenta, te ograničiti širenje incidenta. Cilj je smanjiti štetu za poslovanje na najmanju moguću mjeru.

Ovaj se Plan primjenjuje na sve velike incidente koji prijete da mogu poremetiti bilo koju kritičnu aktivnost unutar opsega Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*) [Sustava upravljanja kontinuitetom poslovanja (engl. *Business Continuity Management System – BCMS*)] na dulje vremensko razdoblje nego što je to ciljano vrijeme oporavka za svaku pojedinačnu aktivnost (u daljnjem tekstu: incident koji remeti poslovanje).

Korisnici su ovog dokumenta svi zaposlenici [naziv organizacije].

# Ovlaštenja i odgovornosti prilikom odziva na incident

|  |  |
| --- | --- |
| ***Uloga u oporavku / naziv radnog mjesta*** | ***Ovlaštenja i odgovornosti*** |
| Svi zaposlenici | Obavijestiti o incidentu odgovornu organizacijsku jedinicu. |
| [naziv radnog mjesta] ili tim u [naziv organizacijske jedinice] | Svi koraci nužni za aktivaciju rješenja za rješavanje incidenata vezanih uz IT i komunikacijsku tehnologiju. |
| [naziv radnog mjesta] ili tim u [naziv organizacijske jedinice] | Svi koraci nužni za aktivaciju rješenja za rješavanje svih drugih incidenata. |
| [naziv radnog mjesta] ili tim u [naziv organizacijske jedinice] | Aktivacija planova oporavka i rješenja za aktivnosti. |
| [naziv radnog mjesta] | Komunikacija s javnim medijima – ovo je jedina osoba ovlaštena za komunikaciju s javnim medijima. |
| [naziv radnog mjesta] | Psihološka pomoć zaposlenicima. |

# Komunikacija

Sljedeća tablica navodi odgovornosti za komunikaciju (slanje i zaprimanje informacija te odgovaranje na zahtjeve za informiranje) s različitim vrstama ciljanih grupa:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | ***[Telefon]*** | ***[Sastanci]*** | ***[Elektronička pošta]*** | ***[Konferencije za tisak]*** | ***[Mediji]*** |  |  |
| [Zaposlenici] |  |  |  |  |  |  |  |
| [Vlasnici / dioničari] |  |  |  |  |  |  |  |
| [Rodbina zaposlenika] |  |  |  |  |  |  |  |
| [Klijenti] |  |  |  |  |  |  |  |
| [Medijske kuće] |  |  |  |  |  |  |  |
| [Hitne službe] |  |  |  |  |  |  |  |
| [razna državna tijela] |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Komunikacijski postupak je kako slijedi:

1. Bilo koji zaposlenik koji zaprimi zahtjev za komunikacijom ili želi započeti komunikaciju prema zainteresiranim stranama mora takav zahtjev proslijediti odgovornoj osobi kako je navedeno u tablici iznad.
2. Odgovorna osoba mora se usuglasiti s [naziv radnog mjesta] oko sadržaja komunikacije. Kada je god moguće, trebali bi se koristiti predlošci sadržaja komunikacije kao način dovođenja u ravnotežu potreba zainteresiranih strana za informacijama te sprječavanja glasina i dezinformacija.
3. Ukoliko komunikacija s medijskim tijelima i drugim vanjskim stranama uključuje značajne rizike i utjecaje, [naziv radnog mjesta] mora odluku o takvoj komunikaciji dokumentirati i službeno odobriti, prije nego se takva informacija objavi.
4. Nakon dobivanja primjerenog odobrenja, odgovorna osoba prosljeđuje informacije zainteresiranoj strani.

Odgovorne osobe navedene u gornjoj tablici odgovorne su za dokumentiranje svake komunikacije sa bilo kojom zainteresiranom stranom.

# Postupci prilikom incidenta koji remeti poslovanje

## Upravljanje incidentom koji remeti poslovanje

### Obveza svakog zaposlenika da prijavi incidente

Svaki je zaposlenik obvezan prijaviti bilo koji incident na sljedeći način:

* svi incidenti vezani za IT i komunikacijsku tehnologiju telefonski se prijavljuju [naziv radnog mjesta ili tim u organizacijskoj jedinici]
* svi ostali incidenti telefonski se prijavljuju [naziv radnog mjesta] ili tim u organizacijskoj jedinici]

Na isti se način mora prijaviti i svaki događaj ili ranjivost sustava koji još nisu prerasli u incident koji remeti poslovanje.

Ako incident zahtjeva uključivanje policije, hitne pomoći ili vatrogasaca, prva dostupna osoba mora nazvati 112 te o tome obavijestiti odgovornu osobu u njegovoj/njezinoj organizacijskoj jedinici ili upravitelja kriznim situacijama.

U slučaju pojave incidenta, zaposlenici mogu slobodno komunicirati isključivo sa svojom rodbinom te policijom, hitnom pomoći ili vatrogascima, dok je sva ostala komunikacija prepuštena Timu za upravljanje krizama.

### Postupanje s incidentom koji remeti poslovanje

Osoba koja je zaprimila informaciju o incidentu mora procijeniti je li incident / mogući incident stvaran ili ne te, ako je zaključeno da je stvaran i da postoji mogućnost da će uzrokovati poremećaje u poslovanju, mora odmah aktivirati ovaj plan poduzimajući sljedeće korake:

* Početi s ograničavanjem i uklanjanjem incidenta na način opisan u slijedećim odjeljcima ovog dokumenta.
* Obavijestiti sve odgovorne osobe o pojavi incidenta u njihovom području odgovornosti.
* Obavijestiti [naziv radnog mjesta], koji mora razmotriti treba li neka od zainteresiranih strana biti upozorena.
* Pratiti status incidenta i, ako je potrebno, izvijestiti osobu koja je incident prijavila i ostale zaposlenike uključene u incident, o napretku postupanja s incidentom.

U slučaju da osoba ne može ograničiti i/ili ukloniti incident, on/ona mora obavijestiti upravitelja kriznim situacijama. Informacija koja se prosljeđuje upravitelju kriznim situacijama mora uključivati prirodu i veličinu incidenta koji remeti poslovanje te njegov potencijalni utjecaj.

Osoba odgovorna za uklanjanje incidenta mora, u Dnevnik incidenata, zapisati sve poduzete radnje.

### Upravitelj kriznim situacijama

…

**\* ZAVRŠETAK OGLEDNOG PREDLOŠKA \***

(Kako biste pristupili potpunoj verziji dokumenta molimo Vas da kupite ISO 27001 i ISO 22301 Premium paket dokumentacije   
<https://advisera.com/27001academy/hr/iso-27001-iso-22301-premium-paket-dokumentacije/>)