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

[logo tvrtke]

[naziv tvrtke]

**PROCEDURA ZA UPRAVLJANJE INCIDENTIMA**

|  |  |
| --- | --- |
| Oznaka: | [oznaka dokumenta] |
| Verzija dokumenta: | [brojčana oznaka verzije dokumenta] |
| Datum verzije: | [datum verzije] |
| Autor: | [ime autora] |
| Odobravatelj: | [ime odobravatelja] |
| Stupanj povjerljivosti: | [oznaka povjerljivosti] |

**Povijest promjena**

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

**Sadržaj**

[1. Svrha, područje primjene i korisnici 3](#_Toc160468715)

[2. Referentni dokumenti 3](#_Toc160468716)

[3. Upravljanje incidentima 3](#_Toc160468717)

[3.1. Primitak i klasifikacija prijetnji, slabosti, događaja i incidenata 3](#_Toc160468718)

[3.2. Postupak obrade sigurnosnih prijetnji, slabosti ili događaja 4](#_Toc160468719)

[3.3. Postupak za obradu manjih incidenata 4](#_Toc160468720)

[3.4. Postupak za obradu većih incidenata 4](#_Toc160468721)

[3.5. Učenje iz incidenata 4](#_Toc160468722)

[3.6. Disciplinske mjere 4](#_Toc160468723)

[3.7. Prikupljanje dokaza 5](#_Toc160468724)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 5](#_Toc160468725)

[5. Valjanost i upravljanje dokumentom 5](#_Toc160468726)

[6. Prilozi 5](#_Toc160468727)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta osigurati brzo prepoznavanje sigurnosnih prijetnji, slabosti i događaja te brzi odgovor na sigurnosne incidente.

Ovaj se dokument primjenjuje na cijeli opseg sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*), tj. na sve zaposlenike i druge resurse koji se koriste unutar opsega ISMS-a, kao i na dobavljače i druge osobe izvan tvrtke koje dolaze u kontakt sa sustavima i informacijama unutar opsega ISMS-a.

Korisnici su ovog dokumenta svi zaposlenici tvrtke [naziv tvrtke], kao i sve gore navedene osobe.

# Referentni dokumenti

* Norma ISO/IEC 27001, točka 7.4 i mjere A.5.7, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.4 i A.6.8
* Politika informacijske sigurnosti
* Popis pravnih, regulatornih, ugovornih i ostalih zahtjeva

# Upravljanje incidentima

Incident informacijske sigurnosti je "pojedinačni događaj ili serija neželjenih ili neočekivanih događaja informacijske sigurnosti, koji će vrlo vjerojatno ugroziti poslovanje i informacijsku sigurnost" (ISO/IEC 27000: 2018).

## Primitak i klasifikacija prijetnji, slabosti, događaja i incidenata

Svaki zaposlenik, dobavljač ili treća strana koja je u kontaktu s informacijama, sustavima ili osjetljivim područjima tvrtke [naziv tvrtke] mora prijaviti svaku prijetnju, slabost sustava, incident ili događaj koji bi mogao dovesti do mogućeg incidenta [pozicija za primanje sigurnosnih incidenata i slabosti].

Incidente, prijetnje, slabosti i događaje potrebno je prijaviti što je prije moguće, telefonom ili osobno.

Osoba koja je informacije primila mora ih klasificirati na sljedeći način:

1. prijetnja, sigurnosna slabost ili događaj – nije došlo do incidenta, ali to može uzrokovati pojavu incidenta u budućnosti
2. manji incident – incident koji, samo u manjem obimu, može utjecati na povjerljivost, cjelovitost ili dostupnost informacija
3. veći incident – incident koji može prouzročiti značajnu štetu radi gubitka povjerljivosti ili cjelovitosti informacija, ili može prouzročiti prekid dostupnosti informacija i/ili procesa na neprihvatljivo vremensko razdoblje

Informacija o sigurnosnim prijetnjama, slabostima, događajima i incidentima mora se proslijediti [naziv radnog mjesta za upravljanje sigurnosnim incidentima].

## Postupak obrade sigurnosnih prijetnji, slabosti ili događaja

[naziv radnog mjesta za upravljanje sigurnosnim incidentima] proučava informaciju o sigurnosnoj prijetnji, slabosti ili događaju, utvrđuje uzrok te, ako je potrebno, predlaže preventivne i popravne radnje.

## Postupak za obradu manjih incidenata

…

**\* ZAVRŠETAK OGLEDNOG PREDLOŠKA \***

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