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

[logo tvrtke]

[naziv tvrtke]

**METODOLOGIJA ZA PROCJENU I OBRADU RIZIKA**

|  |  |
| --- | --- |
| 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](#_Toc160451257)

[2. Referentni dokumenti 3](#_Toc160451258)

[3. Metodologija procjene i obrade rizika 3](#_Toc160451259)

[3.1. Procjena rizika 3](#_Toc160451260)

[3.1.1. Proces 3](#_Toc160451261)

[3.1.2. Resursi, ranjivosti i prijetnje 3](#_Toc160451262)

[3.1.3. Utvrđivanje vlasnika rizika 4](#_Toc160451263)

[3.1.4. Posljedice i vjerojatnost 4](#_Toc160451264)

[3.2. Kriteriji prihvatljivosti rizika 4](#_Toc160451265)

[3.3. Obrada rizika 4](#_Toc160451266)

[3.4. Redoviti pregledi procjene i obrade rizika 5](#_Toc160451267)

[3.5. Izvješće o primjenjivosti i Plan obrade rizika 5](#_Toc160451268)

[3.6. Izvješćivanje 5](#_Toc160451269)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 6](#_Toc160451270)

[5. Valjanost i upravljanje dokumentom 7](#_Toc160451271)

[6. Prilozi 8](#_Toc160451272)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta propisati metodologiju procjene i obrade informacijskih rizika u [naziv tvrtke] te propisati prihvatljivu razinu rizika.

Procjena i obrada rizika primjenjuju se na cjelokupni opseg Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*), odnosno na sve informacijske resurse koji se koriste unutar tvrtke ili koji mogu imati utjecaj na informacijsku sigurnost u ISMS-u.

Korisnici su ovog dokumenta svi zaposlenici [naziv tvrtke] koji sudjeluju u procjeni i obradi rizika.

# Referentni dokumenti

* Norma ISO/IEC 27001, točke 6.1.2, 6.1.3, 8.2 i 8.3
* Politika informacijske sigurnosti
* Popis pravnih, regulatornih , ugovornih i drugih zahtjeva
* Politika sigurnosti dobavljača
* Izvješće o primjenjivosti

# Metodologija procjene i obrade rizika

## Procjena rizika

### Proces

Procjena rizika provodi se kroz Tablicu procjene rizika. Proces procjene rizika koordinira [naziv radnog mjesta za koordinatora za upravljanje rizicima], utvrđivanje prijetnji i ranjivosti provode vlasnici resursa, a procjenu posljedica i vjerojatnosti provodi vlasnik rizika.

### Resursi, ranjivosti i prijetnje

Prvi je korak u procjeni rizika utvrditi sve informacijske resurse u opsegu ISMS-a od strane predstavnika svakog područja u opsegu ISMS-a – tj. utvrditi sve resurse koji mogu utjecati na povjerljivost, cjelovitost i dostupnost informacija u tvrtki. Resursi mogu uključivati dokumente u papirnatom i elektroničkom obliku, aplikacije i baze podataka, ljude, IT opremu, infrastrukturu, usluge u oblaku te vanjske usluge/vanjske procese. Prilikom utvrđivanja resursa potrebno je odrediti i njihove vlasnike – osobu ili organizacijsku jedinicu odgovornu za svaki od resursa.

Sljedeći je korak da vlasnici resursa utvrde sve prijetnje i ranjivosti vezane za pojedini resurs. Prijetnje i ranjivosti određuju se putem kataloga uključenih u Tablicu procjene rizika. Svaki resurs može biti povezan s nekoliko prijetnji, a svaka prijetnja može biti povezana s nekoliko ranjivosti.

### Utvrđivanje vlasnika rizika

Za svaki rizik potrebno je utvrditi i vlasnika rizika – osobu ili organizacijsku jedinicu odgovornu za pojedini rizik. Ta osoba može, ali ne mora, biti ista kao i vlasnik resursa.

### Posljedice i vjerojatnost

Nakon određivanja vlasnika rizika, potrebno je procijeniti posljedice za svaku kombinaciju prijetnji i ranjivosti za pojedini resurs, ukoliko se takav rizik ostvari:

|  |  |  |
| --- | --- | --- |
| Niske posljedice | 0 | Gubitak povjerljivosti, dostupnosti ili cjelovitosti ne utječe na financije tvrtke, pravne ili ugovorne obveze, ili njen ugled. |
| Srednje posljedice | 1 | Gubitak povjerljivosti, dostupnosti ili cjelovitosti uzrokuje troškove te ima manji ili srednji utjecaj na pravne ili ugovorne obveze, ili ugled tvrtke. |
| Velike posljedice | 2 | Gubitak povjerljivosti, dostupnosti ili cjelovitosti ima značajan i/ili trenutni utjecaj na financije tvrtke, poslovanje, pravne ili ugovorne obveze, ili ugled tvrtke. |

Nakon procjene posljedica, potrebno je procijeniti vjerojatnost nastanka takvog rizika, odnosno vjerojatnost da će prijetnja iskoristiti ranjivost predmetnog resursa:

…

**\* 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/>)