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

[logo organizacije]

[naziv organizacije]

**PROJEKTNI PLAN**  
**za implementaciju Sustava upravljanja informacijskom sigurnošću**

|  |  |
| --- | --- |
| Oznaka: |  |
| Verzija: |  |
| Datum verzije: |  |
| Izradio/la: |  |
| Odobrio/la: |  |
| Stupanj povjerljivosti: |  |

**Povijest promjena**

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

**Sadržaj**

[1. Svrha, područje primjene i korisnici 3](#_Toc216112109)

[2. Referentni dokumenti 3](#_Toc216112110)

[3. Projekt implementacije ISMS-a 3](#_Toc216112111)

[3.1. Cilj projekta 3](#_Toc216112112)

[3.2. Rezultati projekta 3](#_Toc216112113)

[3.3. Rokovi 4](#_Toc216112114)

[3.4. Organizacija projekta 5](#_Toc216112115)

[3.4.1. Sponzor projekta 5](#_Toc216112116)

[3.4.2. Voditelj projekta 5](#_Toc216112117)

[3.4.3. Projektni tim 6](#_Toc216112118)

[3.5. Glavni rizici u projektu 6](#_Toc216112119)

[3.6. Alati za provedbu projekta, izvještavanje 6](#_Toc216112120)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 6](#_Toc216112121)

[5. Valjanost i upravljanje dokumentom 7](#_Toc216112122)

# Svrha, područje primjene i korisnici

Svrha je ovog Projektnog plana jasno odrediti cilj projekta implementacije Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*), dokumente koji se izrađuju, rokove te uloge i odgovornosti u projektu.

Projektni se plan primjenjuje na sve aktivnosti koje se provode tijekom projekta implementacije ISMS-a.

Korisnici su ovog dokumenta [članovi top menadžmenta] i članovi projektnog tima.

# Referentni dokumenti

* Norma ISO/IEC 27001
* Norma ISO 22301
* [odluka ili sličan dokument koji propisuje pokretanje projekta]
* [metodologija za upravljanje projektima]

# Projekt implementacije ISMS-a

## Cilj projekta

Cilj je projekta implementirati Sustav upravljanja informacijskom sigurnošću sukladno normi ISO 27001 najkasnije do [datum].

## Rezultati projekta

Tijekom projekta implementacije ISMS-a, izradit će se sljedeći dokumenti (neki od dokumenata posjeduju i priloge koji ovdje nisu posebno navedeni):

* **Procedura za upravljanje dokumentima i zapisima** – procedura koja propisuje osnovna pravila izrade, odobravanja, distribucije i ažuriranja dokumenata i zapisa
* **Procedura za identifikaciju zahtjeva** – procedura koja identificira statutarne, regulatorne, ugovorne i ostale obveze
* **Odluka o opsegu ISMS-a** – dokument koji precizno propisuje resurse, lokacije, tehnologiju, itd. koji su dio opsega
* **Politika informacijske sigurnosti** – ovo je ključni dokument kojim menadžment nadzire upravljanje informacijskom sigurnošću
* **Metodologija za procjenu i obradu rizika** – opisuje metodologiju za upravljanje informacijskim rizicima
* **Tablica procjene rizika** – tablica koja je rezultat procjene vrijednosti resursa, prijetnji i ranjivosti
* **Tablica obrade rizika** – tablica u kojoj se određuju odgovarajuće sigurnosne mjere za svaki neprihvatljivi rizik
* **Izvješće o procjeni i obradi rizika** – dokument koji sadržava sve ključne dokumente izrađene tijekom procesa procjene i obrade rizika
* **Izvješće o primjenjivosti** – dokument koji određuje ciljeve i primjenjivost svake sigurnosne mjere (kontrole) prema Aneksu A norme ISO 27001
* **Plan obrade rizika** – implementacijski dokument koji određuje koje se sigurnosne mjere moraju implementirati, tko je odgovoran za implementaciju, rokove i sredstva
* **Procedura za interni audit** – određuje kako se biraju auditori, kako se pišu programi audita, kako se provode auditi i kako se izvješćuje o rezultatima
* **Procedura za popravnu radnju** – procedura koja opisuje proces provedbe popravnih i preventivnih radnji
* **Izvješće o mjerenju** – rezimira ciljeve ISMS-a, metodu mjerenja, učestalost mjerenja i rezultate te se koristi za zaključivanje koliko je informacijska sigurnost učinkovita u organizaciji
* **Zapisnik s pregleda od strane menadžmenta** – obrazac koji se koristi za izradu zapisnika sa sastanka menadžmenta održanog radi pregleda primjerenosti ISMS-a

Rokovi za politike i procedure koje opisuju detaljna sigurnosna pravila bit će opisani u Planu obrade rizika, jer se u trenutku pisanja ovog Projektnog plana ne zna koji će od ovih dokumenata biti potrebni.

Tijekom projekta implementacije BCMS-a, izradit će se sljedeći dokumenti (neki od dokumenata posjeduju i priloge koji ovdje nisu posebno navedeni):

* **Politika kontinuiteta poslovanja** – određuje osnovne okvire za BCMS, opseg i odgovornosti
* **Upitnik analize utjecaja na poslovanje** (engl. *Business Impact Analysis – BIA*)– analiza kvalitativnih i kvantitativnih utjecaja na poslovanje, potrebnih resursa i sl.
* **Strategija kontinuiteta poslovanja** – određuje kritične aktivnosti, međusobne zavisnosti, ciljana vremena oporavka, strategiju upravljanja i osiguravanja kontinuiteta poslovanja, strategiju oporavka resursa, strategiju pojedinih kritičnih aktivnosti
* **Plan kontinuiteta poslovanja** – detaljan opis na koji način će se provesti odziv u slučaju havarije ili drugog prekida u poslovanju te na koji način će se provesti oporavak svih kritičnih aktivnosti
* **Plan obučavanja i osvješćivanja** – detaljni pregled na koji način će se osoblje obučiti za provedbu planiranih zadataka te kako će im se podići svijest o važnosti kontinuiteta poslovanja
* **Plan vježbanja i testiranja** – na koji način će se provesti vježbanje odnosno testiranje planova sa svrhom utvrđivanja potrebnih korektivnih mjera i unaprjeđenja samog plana
* **Plan održavanja i pregledavanja BCMS-a** – detaljni pregled na koji način je potrebno održavati sve planove i ostale dokumente unutar BCMS-a kako bi bili upotrebljivi u slučaju prekida u poslovanju
* **Obrazac pregleda nakon incidenta** – obrazac koji se koristi za pregled učinkovitosti planova nakon što je došlo do incidenta
* **\***

## Rokovi

Rokovi za prihvaćanje pojedinačnih dokumenata tijekom implementacije ISMS-a su sljedeći:

|  |  |
| --- | --- |
| ***Dokument*** | ***Rokovi za prihvaćanje dokumenta*** |
| Procedura za upravljanje dokumentima i zapisima | 30. lipnja, 20XX |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Rokovi za prihvaćanje pojedinačnih dokumenata tijekom implementacije BCMS-a su sljedeći:

|  |  |
| --- | --- |
| ***Dokument*** | ***Rokovi za prihvaćanje dokumenta*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Završna prezentacija rezultata ovog projekta planirana je za [datum].

## Organizacija projekta

### Sponzor projekta

…

**\* 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/>)