[logo tvrtke]

[naziv tvrtke]

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

|  |  |
| --- | --- |
| 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](#_Toc158814624)

[2. Referentni dokumenti 3](#_Toc158814625)

[3. Projekt implementacije ISMS-a 3](#_Toc158814626)

[3.1. Cilj projekta 3](#_Toc158814627)

[3.2. Rezultati projekta 3](#_Toc158814628)

[3.3. Rokovi 4](#_Toc158814629)

[3.4. Organizacija projekta 4](#_Toc158814630)

[3.4.1. Sponzor projekta 4](#_Toc158814631)

[3.4.2. Upravitelj projekta 5](#_Toc158814632)

[3.4.3. Projektni tim 5](#_Toc158814633)

[3.5. Glavni rizici u projektu 5](#_Toc158814634)

[3.6. Alati za provedbu projekta, izvještavanje 5](#_Toc158814635)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 6](#_Toc158814636)

[5. Valjanost i upravljanje dokumentom 6](#_Toc158814637)

# 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 najviše razine uprave i članovi projektnog tima.

# Referentni dokumenti

* Norma ISO/IEC 27001
* [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 [ciljani datum].

## Rezultati projekta

Tijekom projekta implementacije ISMS-a, izradit će se sljedeći dokumenti (neki od dokumenata posjeduju i priloge koji ovdje nisu izričito 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 uprava 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 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
* **Plan obučavanja i osvješćivanja** – detaljan pregled načina na koje će se osoblje obučiti za provedbu planiranih zadataka te kako će im se podići svijest o važnosti informacijske sigurnosti
* **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** – sažima ciljeve ISMS-a, metodu mjerenja, učestalost mjerenja i rezultate te se koristi za zaključivanje koliko je informacijska sigurnost učinkovita u vašoj tvrtki
* **Zapisnik s pregleda od strane uprave** – obrazac koji se koristi za izradu zapisnika sa sastanka uprave 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.

## Rokovi

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

|  |  |
| --- | --- |
| ***Dokument*** | ***Rokovi za prihvaćanje dokumenta*** |
| Procedura za upravljanje dokumentima i zapisima |  |
| Procedura za identifikaciju zahtjeva |  |
| Odluka o opsegu ISMS-a |  |
| Politika informacijske sigurnosti |  |
| Metodologija za procjenu i obradu rizika |  |
| Tablica procjene rizika |  |
| Tablica obrade rizika |  |
| Izvješće o procjeni i obradi rizika |  |
| Izvješće o primjenjivosti |  |
| Plan obrade rizika |  |
| (razne politike i procedure o sigurnosti) |  |
| Plan obučavanja i osvješćivanja |  |
| Procedura za interni audit |  |
| Izvješće o mjerenju |  |
| Zapisnik s pregleda od strane uprave |  |

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

## Organizacija projekta

### Sponzor projekta

Svaki projekt ima dodijeljenog ''sponzora'' koji u projektu ne sudjeluje aktivno. Sponzor projekta mora biti redovito informiran od strane upravitelja projekta o statusu projekta, i prema potrebi, intervenirati ukoliko dođe do zastoja u projektu.

Za sponzora projekta imenovan je [naziv radnog mjesta rukovodeće osobe najviše razine za nadzor sigurnosti].

### Upravitelj projekta

Uloga upravitelja projekta je osigurati resurse potrebne za provedbu projekta, koordinirati projekt, informirati sponzora o napretku te obavljati administrativne poslove vezane za projekt. Ovlasti upravitelja projekta trebale bi biti takve da osiguraju nesmetanu implementaciju projekta u zadanim rokovima.

Za upravitelja projekta imenovan je [ime i naziv radnog mjesta upravitelja projekta].

### Projektni tim

Uloga projektnog tima je pomagati u različitim aspektima provedbe projekta, izvršavati zadatke određene projektom te donositi odluke o raznim pitanjima koja zahtijevaju multidisciplinarni pristup. Projektni tim sastaje se svaki put prije izrade konačne verzije dokumenta, kao i u svim drugim slučajevima kada upravitelj projekta procjeni da je to potrebno.

*Tablica osoba koje će sudjelovati u radu na projektu*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Ime i prezime* | *Organizacijska jedinica* | *Radno mjesto* | *Broj telefona* | *Adresa e-pošte* |
|  |  |  |  |  |

## Glavni rizici u projektu

Glavni rizici u provedbi projekta su sljedeći:

1. Produženje rokova tijekom faze procjene rizika
2. Produženje rokova tijekom izrade politika i procedura o sigurnosti
3. Provedba aktivnosti koje uzrokuju nepotrebne troškove i gubitak vremena
4. Odabir prevelikog broja i/ili preskupih sigurnosnih mjera

Mjere za ublažavanje navedenih rizika su sljedeće:

* Upravitelj projekta prati odvijaju li se sve aktivnosti na projektu u utvrđenim rokovima te pravovremeno traži intervenciju sponzora projekta.
* Angažiranje konzultanta kako bi se osiguralo da se vrijeme ili resursi ne troše na aktivnosti koje nisu važne za projekt te da pojedinačne aktivnosti ne idu u krivom smjeru
* Angažiranje konzultanta koji će predložiti najisplativije sigurnosne mjere

## Alati za provedbu projekta, izvještavanje

Na lokalnoj će mreži biti kreirana dijeljena mapa u kojoj će biti smješteni svi dokumenti izrađeni tijekom rada na projektu. Svi članovi projektnog tima imat će pristup tim dokumentima. Samo će upravitelj projekta i članovi projektnog tima biti ovlašteni da mijenjaju i brišu dokumente.

Upravitelj projekta jednom će mjesečno pripremiti izvješće o provedbi projekta i proslijediti ga sponzoru projekta.

# Upravljanje zapisima koji se vode temeljem ovog dokumenta

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Naziv zapisa*** | ***Mjesto pohrane*** | ***Osoba odgovorna za pohranu*** | ***Mjere za zaštitu zapisa*** | ***Trajanje pohrane*** |
| Izvješće o provedbi projekta | Dijeljena mapa za aktivnosti vezane uz projekt | Upravitelj projekta | Upravitelj projekta jedini je ovlašten za uređivanje podataka. | Izvješće se pohranjuje na razdoblje od 3 godine. |

# Valjanost i upravljanje dokumentom

Ovaj dokument vrijedi od [datum važenja].

Vlasnik ovog dokumenta je [naziv radnog mjesta za vlasnika dokumenta o upravljanju], koji ovaj dokument mora pregledati i, ako je potrebno, dopuniti najmanje jednom godišnje..

Prilikom ocjenjivanja učinkovitosti i primjerenosti ovog dokumenta, u obzir treba uzeti sljedeće kriterije:

* obavljaju li svi zaposlenici angažirani na projektu svoje aktivnosti u skladu s ovim dokumentom
* jesu li svi projektni rokovi ispunjeni

[ime odobravatelja]

[naziv radnog mjesta odobravatelja]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(potpis)