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

[logo tvrtke]

[naziv tvrtke]

**PROCEDURA ZA INTERNI AUDIT**

|  |  |
| --- | --- |
| 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](#_Toc160470043)

[2. Referentni dokumenti 3](#_Toc160470044)

[3. Interni audit 3](#_Toc160470045)

[3.1. Svrha internog audita 3](#_Toc160470046)

[3.2. Planiranje internih audita 3](#_Toc160470047)

[3.3. Imenovanje internih auditora 4](#_Toc160470048)

[3.4. Provedba pojedinačnih internih audita 4](#_Toc160470049)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 4](#_Toc160470050)

[5. Valjanost i upravljanje dokumentom 5](#_Toc160470051)

[6. Prilozi 6](#_Toc160470052)

# Svrha, područje primjene i korisnici

Svrha je ove Procedure opisati sve aktivnosti vezane uz audit – pisanje programa za interni audit, odabir auditora, provedba pojedinačnih audita te izvješćivanje.

Ova se Procedura primjenjuje na sve aktivnosti koje se provode u Sustavu upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*).

Korisnici su ovog dokumenta članovi najviše razine uprave tvrtke [naziv tvrtke], kao i interni auditori.

# Referentni dokumenti

* Norma ISO/IEC 27001, točka 9.2 i mjere A.5.30, A.5.35 i A.8.34
* Politika informacijske sigurnosti
* Procedura za popravnu radnju

# Interni audit

## Svrha internog audita

Svrha je internog audita utvrditi jesu li procedure, mjere, procesi i ostale aktivnosti unutar ISMS-a u skladu s normom ISO 27001, važećim propisima i internom dokumentacijom tvrtke, jesu li učinkovito implementirani i održavani te ispunjavaju li zahtjeve i postavljene ciljeve politika.

## Planiranje internih audita

[naziv radnog mjesta za upravitelja za sigurnost] odobrava godišnji program internih audita, napisan kako je navedeno u obrascu u Prilogu 1 – Godišnji program internog audita.

Tijekom godine dana mora se provesti jedan ili više internih audita koji će kumulativno pokriti cijeli opseg ISMS-a. Interni auditi planiraju se na temelju rezultata procjene rizika, kao i rezultata prethodnih audita; obično se provode neposredno prije pregleda od strane uprave.

Godišnji program internog audita mora sadržavati sljedeće podatke o svakom pojedinom internom auditu:

* razdoblje održavanja audita (precizirajući datume ili mjesece u kojima je audit planiran)
* opseg audita (odjeli, procesi, točke iz norme, itd.)
* kriteriji audita (norme, zakoni i propisi, interna dokumentacija, korporativni standardi i/ili ugovorne obveze)
* metode audita (pregled dokumentacije, razgovori sa zaposlenicima, pregled zapisa, pregled informacijskih sustava, itd.)
* tko će provoditi interni audit (ako je auditora više, precizirajte tko je voditelj audit tima)

Imenovani interni auditori dužni su obavljene audite zapisati u Godišnjem programu internog audita.

## Imenovanje internih auditora

…

**\* 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/>)