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

[logo tvrtke]

[naziv tvrtke]

**POLITIKA O UPORABI ŠIFRIRANJA**

|  |  |
| --- | --- |
| 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](#_Toc160463285)

[2. Referentni dokumenti 3](#_Toc160463286)

[3. Uporaba kriptografije 3](#_Toc160463287)

[3.1. Kriptografske kontrole 3](#_Toc160463288)

[3.2. Kriptografski ključevi 3](#_Toc160463289)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 4](#_Toc160463290)

[5. Valjanost i upravljanje dokumentom 5](#_Toc160463291)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta odrediti pravila za uporabu kriptografskih mjera kao i pravila za uporabu kriptografskih ključeva, radi zaštite povjerljivosti, cjelovitosti, autentičnosti i neporecivosti informacija.

Ovaj se dokument primjenjuje na cijeli opseg Sustava upravljanja sigurnošću informacija (engl. *Information Security Management System – ISMS*), tj. na sve sustave i informacije koji se koriste unutar opsega ISMS-a.

Korisnici su ovog dokumenta [odjeli vezani uz IT].

# Referentni dokumenti

* Norma ISO/IEC 27001, mjere A.5.31 i A.8.24
* Politika informacijske sigurnosti
* Politika klasifikacije informacija
* Popis pravnih, regulatornih, ugovornih i ostalih zahtjeva

# Uporaba kriptografije

## Kriptografske kontrole

Sukladno Politici klasifikacije informacija, kao i zakonskim i ugovornim obvezama, tvrtka mora štititi sljedeće sustave ili informacije, koristeći sljedeće kriptografske mjere:

|  |  |  |  |
| --- | --- | --- | --- |
| ***Uređaji / informacijski sustavi*** | ***Naziv kriptografskog alata*** | ***Algoritam za šifriranje*** | ***Veličina ključa*** |
| *Sustav elektroničkog plaćanja* | *Sigurnosni token* | *AES algoritam* | *256 bita* |
| *Komunikacija između poslužitelja i mobilnih uređaja* | *Kriptografski softver XXXX* | *RSA algoritam* | *256 bita* |

…

**\* 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/>)