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

[logo organizacije]

[naziv organizacije]

**POLITIKA KLASIFIKACIJE INFORMACIJA**

|  |  |
| --- | --- |
| 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](#_Toc216169173)

[2. Referentni dokumenti 3](#_Toc216169174)

[3. Klasificirane informacije 3](#_Toc216169175)

[3.1. Koraci i odgovornosti 3](#_Toc216169176)

[3.2. Klasifikacija informacija 3](#_Toc216169177)

[3.2.1. Kriteriji klasifikacije 4](#_Toc216169178)

[3.2.2. Stupnjevi povjerljivosti 4](#_Toc216169179)

[3.2.3. Popis ovlaštenih osoba 4](#_Toc216169180)

[3.2.4. Reklasifikacija 4](#_Toc216169181)

[3.3. Označavanje informacija 5](#_Toc216169182)

[3.4. Rukovanje povjerljivim informacijama 5](#_Toc216169183)

[3.5. Maskiranje podataka 8](#_Toc216169184)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 8](#_Toc216169185)

[5. Valjanost i upravljanje dokumentom 8](#_Toc216169186)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta osigurati da informacije dobiju primjerenu razinu zaštite.

Ovaj dokument obuhvaća cjelokupni opseg Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*), odnosno sve vrste informacija, bez obzira u kojem se obliku nalaze – papirnati ili elektronički dokumenti, aplikacije i baze podataka, znanje ljudi i sl.

Korisnici su ovog dokumenta svi zaposlenici [naziv organizacije].

# Referentni dokumenti

* Norma ISO/IEC 27001, mjere A.5.9, A.5.10, A.5.12, A.5.13, A.5.14, A.7.10, A.8.3, A.8.5, A.8.11 i A.8.12
* Politika informacijske sigurnosti
* Izvješće o procjeni i obradi rizika
* Izvješće o primjenjivosti
* Popis resursa
* Popis pravnih, regulatornih, ugovornih i ostalih zahtjeva
* Procedura za upravljanje incidentima
* [Sigurnosne procedure za IT odjel] / [Politika odlaganja i uništavanja]
* Politika sigurnosti informacijskog sustava

# Klasificirane informacije

## Koraci i odgovornosti

Koraci i odgovornosti za upravljanje informacijama su sljedeće:

|  |  |
| --- | --- |
| ***Naziv koraka*** | ***Odgovornost*** |
| 1. Upis informacijskog resursa u Popis resursa | [naziv radnog mjesta] |
| 1. Klasifikacija informacija | Vlasnik resursa |
| 1. Označavanje informacija | Vlasnik resursa |
| 1. Rukovanje informacijama | Osobe s pravima pristupa u skladu s ovom Politikom |

Ako su klasificirani podaci zaprimljeni izvan organizacije, [naziv radnog mjesta] je odgovoran za njihovu klasifikaciju u skladu s pravilima propisanim ovom Politikom te ta osoba postaje vlasnik takvog informacijskog resursa.

## Klasifikacija informacija

### Kriteriji klasifikacije

Stupanj povjerljivosti informacija klasificira se prema slijedećim kriterijima:

* vrijednost informacija – na temelju posljedica koje su procijenjene u procjeni rizika
* osjetljivost i kritičnost informacija – na temelju najvećeg izračunatog rizika za pojedinu informaciju u procjeni rizika
* zakonske i ugovorne obveze – na temelju [Popisa pravnih, regulatornih, ugovornih i ostalih zahtjeva]

### Stupnjevi povjerljivosti

Sve informacije moraju biti klasificirane po stupnjevima povjerljivosti.

|  |  |  |  |
| --- | --- | --- | --- |
| ***Stupanj povjerljivosti*** | ***Označavanje*** | ***Kriteriji za klasifikaciju*** | ***Ograničavanje pristupa*** |
| Javno | (bez oznake) | Objava informacija u javnosti ni na koji način ne može štetiti organizaciji. | Informacije su dostupne javnosti. |
| Interna uporaba | INTERNA UPORABA | Neovlašteni pristup informacijama prouzročio bi manju štetu i/ili neugodnosti organizaciji. | Informacije su dostupne svim djelatnicima i odabranim trećim stranama. |
| Ograničen pristup | OGRANIČEN PRISTUP | Neovlašteni pristup informacijama prouzročio bi veću štetu za poslovanje i/ili ugled organizaciji | Informacije su dostupne samo određenoj grupi djelatnika i ovlaštenim osobama trećih strana. |
| Povjerljivo | POVJERLJIVO | Neovlašteni pristup informacijama prouzročio bi katastrofalnu (nepopravljivu) štetu za poslovanje i /ili ugled organizacije. | Informacije su dostupne samo pojedincima u organizaciji. |

Osnovno je pravilo da se određuje minimum stupnja povjerljivosti koji osigurava dovoljnu razinu zaštite, kako se ne bi nepotrebno povećavali troškovi zaštite.

### Popis ovlaštenih osoba

Svaka informacija klasificirana stupnjem povjerljivosti „Ograničen pristup“ i „Povjerljivo“ mora uz sebe imati Popis ovlaštenih osoba kojom vlasnik informacije određuje imena i prezimena ili nazive radnih mjesta osoba koje imaju pravo pristupa toj informaciji.

Isto pravilo vrijedi i za stupanj povjerljivosti „Interna uporaba“ ukoliko takvom dokumentu pristup trebaju imati i osobe izvan organizacije.

### Reklasifikacija

Vlasnici resursa moraju pregledavati stupanj povjerljivosti svog informacijskog resursa svake [dvije godine] i procijeniti može li se stupanj povjerljivosti promijeniti. Ukoliko je moguće, stupanj povjerljivosti potrebno je sniziti.

## Označavanje informacija

Informacije se označavaju stupnjevima povjerljivosti na sljedeći način:

* **papirnati dokumenti** – stupanj povjerljivosti piše se u gornjem desnom kutu dokumenta, na svaku stranicu; piše se i na prednjoj strani omotnice ili kuverte kojom se takav dokument prenosi, kao i na registratoru u kojem se takav dokument nalazi
* **elektronički dokumenti** – stupanj povjerljivosti piše se u gornjem desnom kutu dokumenta, na svaku stranicu
* **…**

…

**\* 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/>)