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

[logo organizacije]

[naziv organizacije]

**IZVJEŠĆE O PRIMJENJIVOSTI**

|  |  |
| --- | --- |
| 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](#_Toc216134482)

[2. Referentni dokumenti 3](#_Toc216134483)

[3. Primjenjivost sigurnosnih mjera 3](#_Toc216134484)

[4. Prihvaćanje preostalih rizika 17](#_Toc216134485)

[5. Valjanost i upravljanje dokumentom 17](#_Toc216134486)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta odrediti koje su sigurnosne mjere primjerene za uvođenje u [naziv organizacije], ciljeve tih mjera i kako se provode, kao i odobriti preostale rizike te službeno odobriti provedbu navedenih sigurnosnih mjera.

Ovaj dokument uključuje sve sigurnosne mjere navedene u Aneksu A norme ISO 27001. Mjere su primjenjive na cijeli opseg Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*).

Korisnici su ovog dokumenta svi zaposlenici [naziv organizacije] koji imaju ulogu u ISMS-u.

# Referentni dokumenti

* Norma ISO/IEC 27001, točka 6.1.3 d)
* Politika informacijske sigurnosti
* Metodologija za procjenu i obradu rizika
* Izvješće o procjeni i obradi rizika

# Primjenjivost sigurnosnih mjera

Primjenjive su sljedeće sigurnosne mjere (kontrole) iz Aneksa A norme ISO 27001:

| ID | Sigurnosna mjera prema normi ISO/IEC 27001 | Mjera je primjenjiva (DA/NE) | Obrazloženje za odabir/ izostavljanje | Ciljevi sigurnosne mjere | Način provedbe | Status |
| --- | --- | --- | --- | --- | --- | --- |
| A.5.1 | Politike informacijske sigurnosti |  |  |  | Sve politike navedene u nastavku ovog stupca; svaka politika ima određenog vlasnika koji mora pregledavati dokument u planiranim intervalima |  |
| A.5.2 | Uloge i odgovornosti u informacijskoj sigurnosti |  |  |  | Uloge i odgovornosti za informacijsku sigurnost navedene su u raznim dokumentima ISMS-a, [naziv radnog mjesta] određuje dodatne uloge i odgovornosti |  |
| A.5.3 | Podjela dužnosti |  |  |  | Svaku aktivnost koja uključuje osjetljive informacije odobrava jedna osoba, a provodi je druga |  |
| A.5.4 | Odgovornosti menadžmenta |  |  |  | Menadžment aktivno zahtijeva da svi zaposlenici, dobavljači i vanjski partneri provode sva pravila ISMS-a |  |
| A.5.5 | Kontakt s vlastima |  |  |  | [naziv radnog mjesta] je odgovoran za kontakt s nadležnim tijelima (npr. policija, vatrogasci, itd.)  [Strategija kontinuiteta poslovanja], [Plan odziva na incidente] |  |
| A.5.6 | Kontakt s posebnim interesnim skupinama |  |  |  | [naziv radnog mjesta] je odgovoran za praćenje [navedite imena interesnih skupina i sigurnosnih foruma] |  |
| A.5.7 | Obavještajni podaci o prijetnjama |  |  |  | [Politika sigurnosti dobavljača], [Procedura za upravljanje incidentima], [Sigurnosne procedure za IT odjel] |  |
| A.5.8 | Informacijska sigurnost u upravljanju projektima |  |  |  | Voditelj projekta dužan je uključiti primjenjiva pravila informacijske sigurnosti u svaki projekt; prilikom nabave novih informacijskih sustava ili promjene postojećih, [naziv radnog mjesta] mora dokumentirati sigurnosne zahtjeve u [Specifikaciji sigurnosnih zahtjeva] |  |
| A.5.9 | Popis informacijskih i drugih povezanih resursa |  |  |  | [Popis resursa], [Politika klasifikacije informacija], [Politika sigurnosti informacijskog sustava] |  |
| A.5.10 | Prihvatljivo korištenje informacijskih i drugih povezanih resursa |  |  |  | [Politika sigurnosti informacijskog sustava], [Politika klasifikacije informacija] |  |
| A.5.11 | Povrat resursa |  |  |  | [Politika sigurnosti informacijskog sustava], [Politika sigurnosti dobavljača] |  |
| A.5.12 | Klasifikacija informacija |  |  |  | [Politika klasifikacije informacija] |  |
| A.5.13 | Označavanje informacija |  |  |  | [Politika klasifikacije informacija] |  |
| A.5.14 | Prijenos informacija |  |  |  | [Sigurnosne procedure za IT odjel] / [Politika prijenosa informacija], [Politika korištenja vlastitih uređaja (BYOD)], [Politika klasifikacije informacija], [Politika sigurnosti informacijskog sustava] |  |
| A.5.15 | Kontrola pristupa |  |  |  | [Politika kontrole pristupa] |  |
| A.5.16 | Upravljanje identitetom |  |  |  | [Politika kontrole pristupa] / [Politika uporabe lozinki] |  |
| A.5.17 | Podaci o provjeri autentičnosti |  |  |  | [Politika kontrole pristupa] / [Politika uporabe lozinki], [Politika sigurnosti informacijskog sustava] |  |
| A.5.18 | Prava pristupa |  |  |  | [Politika kontrole pristupa], [Politika uporabe lozinki] |  |
| A.5.19 | Informacijska sigurnost u odnosima s dobavljačima |  |  |  | [Politika sigurnosti dobavljača] |  |
| A.5.20 | Rješavanje informacijske sigurnosti unutar ugovora s dobavljačima |  |  |  | [Politika sigurnosti dobavljača], odabrane sigurnosne klauzule iz dokumenta [Sigurnosne klauzule za dobavljače i partnere] |  |
| A.5.21 | Upravljanje informacijskom sigurnošću u opskrbnom lancu ICT-a (informacijske i komunikacijske tehnologije) |  |  |  | [Politika sigurnosti dobavljača] |  |
| A.5.22 | Praćenje, pregled i upravljanje promjenama usluga dobavljača |  |  |  | [Politika sigurnosti dobavljača] |  |
| A.5.23 | Informacijska sigurnost prilikom korištenja usluga u oblaku |  |  |  | [Politika sigurnosti dobavljača] |  |
| A.5.24 | Planiranje i priprema upravljanja incidentima informacijske sigurnosti |  |  |  | [Procedura za upravljanje incidentima] |  |
| A.5.25 | Procjena i odluka o događajima informacijske sigurnosti |  |  |  | [Procedura za upravljanje incidentima] |  |
| A.5.26 | Odgovor na incidente informacijske sigurnosti |  |  |  | [Procedura za upravljanje incidentima], [Plan odziva na incidente] |  |
| A.5.27 | Učenje iz incidenata informacijske sigurnosti |  |  |  | [Procedura za upravljanje incidentima], [Procedura za popravnu radnju], [Obrazac pregleda nakon incidenta] |  |
| A.5.28 | Prikupljanje dokaza |  |  |  | [Procedura za upravljanje incidentima] |  |
| A.5.29 | Sigurnost informacija tijekom poremećaja u poslovanju |  |  |  | [Popis pravnih, regulatornih, ugovornih i drugih zahtjeva], [Plan oporavka od katastrofe], [Politika kontinuiteta poslovanja], [Metodologija analize utjecaja na poslovanje], [Strategija kontinuiteta poslovanja], [Plan kontinuiteta poslovanja], [Plan održavanja i pregledavanja BCMS-a], [Plan vježbanja i testiranja], [Obrazac pregleda nakon incidenta] |  |
| A.5.30 | Spremnost ICT-a za kontinuitet poslovanja |  |  |  | [Plan oporavka od katastrofe], [Procedura za interni audit] |  |
| A.5.31 | Pravni, statutarni, regulatorni i ugovorni zahtjevi |  |  |  | [Procedura za identifikaciju zahtjeva], [Popis pravnih, regulatornih, ugovornih i drugih zahtjeva], [Politika o uporabi enkripcije] |  |
| A.5.32 | Prava intelektualnog vlasništva |  |  |  | [Politika sigurnosti informacijskog sustava] |  |
| A.5.33 | Zaštita zapisa |  |  |  | [Procedura za upravljanje dokumentacijom i zapisima], [Politika sigurnog razvoja] |  |
| A.5.34 | Privatnost i zaštita osobnih podataka |  |  |  | [naziv radnog mjesta] je odgovoran za provedbu zakonskih zahtjeva vezanih uz zaštitu osobnih podataka |  |
| A.5.35 | Neovisni pregled informacijske sigurnosti |  |  |  | [Procedura za interni audit], certifikacijski audit od strane [naziv certifikacijskog tijela] |  |
| A.5.36 | Usklađenost s politikama, pravilima i normama informacijske sigurnosti |  |  |  | Svi vlasnici informacijskih resursa, kao i menadžment, redovito provjeravaju provedbu sigurnosnih mjera; [naziv radnog mjesta] je zadužen za provjeru tehničke usklađenosti informacijskih sustava sa sigurnosnim zahtjevima |  |
| A.5.37 | Dokumentirane operativne procedure |  |  |  | [Sigurnosne procedure za IT odjel] |  |
| A.6.1 | Provjera u pozadini |  |  |  | [naziv radnog mjesta] provjerava kandidate za posao [opišite metode provjere], [Politika sigurnosti dobavljača] |  |
| ***(ostatak redaka ne prikazuje se u ovom oglednom predlošku)*** | | | | | | |
| … | … |  |  |  | … |  |

…

**\* ZAVRŠETAK OGLEDNOG PREDLOŠKA \***

(Kako biste pristupili potpunoj verziji dokumenta molimo Vas da kupite ISO 27001/ISO 22301 Paket dokumentacije za procjenu rizika   
<https://advisera.com/27001academy/hr/iso-27001-iso-22301-paket-dokumentacije-za-procjenu-rizika/>)