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

[logo tvrtke]

[naziv tvrtke]

**IZVJEŠĆE O PRIMJENJIVOSTI**

|  |  |
| --- | --- |
| 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](#_Toc158898496)

[2. Referentni dokumenti 3](#_Toc158898497)

[3. Primjenjivost sigurnosnih mjera 3](#_Toc158898498)

[4. Prihvaćanje preostalih rizika 21](#_Toc158898499)

[5. Valjanost i upravljanje dokumentom 21](#_Toc158898500)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta odrediti koje su sigurnosne mjere primjerene za uvođenje u [naziv tvrtke], ciljeve tih mjera i kako se uvode, 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 tvrtke] 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 iz Aneksa A norme ISO 27001:

| ID | Sigurnosne mjere (kontrole) prema ISO/IEC 27001 | Primjenjivost (DA/NE) | Opravdanje za odabir/ izostavljanje | Ciljevi sigurnosne mjere | Metoda implementacije | 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 za upravitelja za sigurnost] 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 uprave |  |  |  | Uprava aktivno zahtijeva da sva pravila ISMS-a budu uvedena od strane svih zaposlenika, dobavljača i vanjskih partnera. |  |
| A.5.5 | Kontakt s vlastima |  |  |  | [naziv radnog mjesta za kontakt s vlastima] je odgovoran za kontakt s nadležnim tijelima (npr. policija, vatrogasci, itd.). |  |
| A.5.6 | Kontakt s posebnim interesnim skupinama |  |  |  | [naziv radnog mjesta za kontakt s posebnim interesnim skupinama] je odgovoran za praćenje interesnih skupina i foruma na temu sigurnosti. |  |
| 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 |  |  |  | Upravitelj projekta dužan je uključiti primjenjiva pravila informacijske sigurnosti u svaki projekt. |  |
| 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, Specifikacija zahtjeva za informacijski sustav |  |
| 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 |  |
| A.5.27 | Učenje iz incidenata informacijske sigurnosti |  |  |  | Procedura za upravljanje incidentima, Procedura za popravnu radnju |  |
| A.5.28 | Prikupljanje dokaza |  |  |  | Procedura za upravljanje incidentima |  |
| A.5.29 | Sigurnost informacija tijekom prekida poslovanja |  |  |  | Popis pravnih, regulatornih, ugovornih i drugih zahtjeva, Plan oporavka od katastrofe |  |
| 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 za zaštitu privatnosti] 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 akreditiranog certifikacijskog tijela |  |
| A.5.36 | Usklađenost s politikama, pravilima i normama informacijske sigurnosti |  |  |  | Svi vlasnici informacijskih resursa, kao i uprava, redovito provjeravaju provedbu sigurnosnih mjera. |  |
| A.5.37 | Dokumentirane operativne procedure |  |  |  | Sigurnosne procedure za IT odjel |  |
| A.6.1 | Provjera u pozadini |  |  |  | [naziv radnog mjesta za određivanje postupka provjere] određuje postupak provjere kandidata za posao, 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 paket dokumentacije <https://advisera.com/27001academy/hr/iso-27001-paket-dokumentacije/>)