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

[logo organizacije]

[naziv organizacije]

**SIGURNOSNE PROCEDURE ZA IT ODJEL**

|  |  |
| --- | --- |
| 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 4](#_Toc216173805)

[2. Referentni dokumenti 4](#_Toc216173806)

[3. Operativne procedure za informacijsku i komunikacijsku tehnologiju 4](#_Toc216173807)

[3.1. Upravljanje promjenama 4](#_Toc216173808)

[3.2. Upravljanje konfiguracijom 5](#_Toc216173809)

[3.3. Upravljanje kapacitetom 5](#_Toc216173810)

[3.4. Antivirusna zaštita 5](#_Toc216173811)

[3.5. Sigurnosne kopije 5](#_Toc216173812)

[3.5.1. Izrada sigurnosnih kopija 5](#_Toc216173813)

[3.5.2. Testiranje sigurnosnih kopija 5](#_Toc216173814)

[3.6. Upravljanje mrežnom sigurnošću 5](#_Toc216173815)

[3.7. Mrežne usluge 6](#_Toc216173816)

[3.8. Brisanje podataka 6](#_Toc216173817)

[3.9. Odlaganje i uništavanje opreme i medija 6](#_Toc216173818)

[3.9.1 Oprema 7](#_Toc216173819)

[3.9.2 Prijenosni mediji za pohranu 7](#_Toc216173820)

[3.9.3 Papirnati mediji 7](#_Toc216173821)

[3.9.4 Zapisi o brisanju i uništavanju; povjerenstvo za uništavanje informacija 7](#_Toc216173822)

[3.10. Prijenos informacija 7](#_Toc216173823)

[3.10.1. Elektronički komunikacijski kanali 7](#_Toc216173824)

[3.10.2. Odnosi s vanjskim stranama 7](#_Toc216173825)

[3.11. Rukovanje izvornim kodom 8](#_Toc216173826)

[3.12. Korištenje uslužnih programa 8](#_Toc216173827)

[3.13. Nadzor nad sustavom 8](#_Toc216173828)

[3.14. Praćenje vanjskih prijetnji 9](#_Toc216173829)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 9](#_Toc216173830)

[5. Valjanost i upravljanje dokumentom 10](#_Toc216173831)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta osigurati ispravan i siguran rad informacijske i komunikacijske tehnologije (engl. *Information and communication technologies – ICT*).

Ovaj se dokument primjenjuje na cijeli opseg Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*), odnosno na svu informacijsku i komunikacijsku tehnologiju kao i s time povezanu dokumentaciju unutar opsega.

Korisnici su ovog dokumenta zaposlenici [organizacijske jedinice za informacijsku i komunikacijsku tehnologiju].

# Referentni dokumenti

* Norma ISO/IEC 27001, mjere A.5.7, A.5.14, A.5.37, A.7.10, A.7.14, A.8.4, A.8.6, A.8.7, A.8.8, A.8.9, A.8.10, A.8.12, A.8.13, A.8.15, A.8.16, A.8.17, A.8.18, A.8.20, A.8.21, A.8.22, A.8.23, A.8.31 i A.8.32
* Politika informacijske sigurnosti
* [Plan oporavka od katastrofe]
* [Politika mobilnih uređaja, rada na daljinu i rada od kuće]
* [Politika klasifikacije informacija]
* [Popis resursa]
* [Politika sigurnosti dobavljača]
* [Politika sigurnog razvoja]
* [Politika kontrole pristupa]

# Operativne procedure za informacijsku i komunikacijsku tehnologiju

## Upravljanje promjenama

Svaka promjena na operacijskim ili produkcijskim sustavima mora se izvršiti na sljedeći način:

1. promjenu može predložiti [navedite radna mjesta]
2. promjenu mora odobriti [naziv radnog mjesta], tako da procijeni je li poslovno opravdana i postoje li negativni sigurnosni učinci
3. promjene mora provesti [naziv radnog mjesta]
4. [naziv radnog mjesta] je zadužen za provjeru je li promjena provedena u skladu sa zahtjevom
5. [naziv radnog mjesta] je zadužen za testiranje i provjeru stabilnosti sustava – sustav se ne smije pustiti u produkciju prije nego se temeljito testira
6. provedba promjene mora se prijaviti slijedećim osobama: [navesti sve potrebne nazive radnih mjesta]
7. [naziv radnog mjesta] je odgovoran za ažuriranje dokumenata (politika, procedura, planova itd.) na koje je promjena utjecala.

Zapisi o provedbi promjena vode se [navedite naziv obrasca, ili opišite neku drugu metodu za bilježenje promjena].

## Upravljanje konfiguracijom

[Naziv radnog mjesta] je odgovoran za dokumentiranje konfiguracijskih postavki hardvera, softvera, usluga i mreža koje se moraju provoditi kako bi se osigurao ispravan i siguran rad te odredile osnove smjernice za izbjegavanje grešaka prilikom promjena.

## Upravljanje kapacitetom

[Naziv radnog mjesta] je odgovoran za praćenje korištenja ICT sredstava i planiranje potrebnih kapaciteta.

## Antivirusna zaštita

[Naziv antivirusnog softvera] mora biti instaliran na svakoj platformi (npr. fizički, virtualni ili poslužitelji u oblaku) na kojoj se nalaze IT sustavi kojima upravlja IT odjel, s aktiviranim automatskim ažuriranjima.

## Sigurnosne kopije

### Izrada sigurnosnih kopija

Sigurnosne kopije moraju se izrađivati za sve sustave određene u [Strategiji kontinuiteta poslovanja], učestalošću navedenom u tom dokumentu.

[Naziv radnog mjesta] je odgovoran za izradu sigurnosnih kopija informacija, softvera i slika sustava te za osiguravanje pravilnog odgovora na kvarove prilikom planirane izrade sigurnosnih kopija. [Ako je potrebno, opišite tehnologiju izrade sigurnosnih kopija, navedite odgovornosti za pojedine aktivnosti, lokacije za pohranu sigurnosnih kopija, fizičku zaštitu sigurnosnih kopija, enkripciju, lozinke, itd.]

Dnevnici (logovi) procesa izrade sigurnosne kopije automatski se kreiraju na sustavima na kojima se izrađuje sigurnosna kopija.

### Testiranje sigurnosnih kopija

Sigurnosne kopije i postupak njihovog oporavka moraju se testirati najmanje [jednom svaka tri mjeseca] provedbom procesa povrata podataka na [navedite poslužitelj na kojem se vrši oporavak podataka] i provjerom jesu li svi podaci uspješno oporavljeni.

[Naziv radnog mjesta] je odgovoran za testiranje sigurnosnih kopija. Zapisi o testiranju sigurnosnih kopija vode se [opišite obrazac zapisa – na papiru ili u elektroničkom obliku, postoji li propisani obrazac i sl.].

## Upravljanje mrežnom sigurnošću

[Naziv radnog mjesta] je odgovoran za upravljanje i nadzor računalnih mreža, za sigurnost informacija u mrežama, sprječavanje curenja podataka te za zaštitu usluga povezanih s mrežama od neovlaštenog pristupa. U tu svrhu potrebno je:

* odvojiti operativnu odgovornost za mreže od odgovornosti za osjetljive aplikacije i druge sustave
* zaštititi osjetljive podatke koji prolaze preko javne mreže [opišite tehnologiju koja se koristi za zaštitu i navedite odgovornosti i odgovorne osobe]
* zaštititi osjetljive podatke koji prolaze preko bežičnih mreža [opišite tehnologiju koja se koristi za zaštitu i navedite odgovornosti i odgovorne osobe]
* zaštititi opremu koja se povezuje na mrežu s udaljenih lokacija [opišite tehnologiju koja se koristi za zaštitu i navedite odgovornosti i odgovorne osobe]
* razdvojiti mrežu s obzirom na [opišite koji su segmenti mreže odvojeni; opišite je li odvajanje fizičko ili logičko]
* razdvojiti razvojna, testna i operativna okruženja sustava
* razdvojiti promet koji dolazi s mobilnih uređaja, postaviti jedinstvene politike vatrozida, statičkih ruta, virtualnih lokalnih mreža, itd.
* osigurati dostupnost mrežnih usluga [opišite mjere koje će osigurati dostupnost]
* filtrirati pristup web stranicama s potencijalno zlonamjernim ili nezakonitim sadržajem, ili stranicama koje se mogu koristiti za curenje podataka
* osigurati da je sistemsko vrijeme na svim računalima usklađeno [opišite kako se usklađuju i s kojim točnim izvorom vremena]
* [naziv radnog mjesta] mora redovito pratiti i testirati implementirane sigurnosne mjere

## Mrežne usluge

…

**\* 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/>)