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

[logo tvrtke]

[naziv tvrtke]

**SIGURNOSNE PROCEDURE ZA IT ODJEL**

|  |  |
| --- | --- |
| 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 4](#_Toc160459089)

[2. Referentni dokumenti 4](#_Toc160459090)

[3. Operativne procedure za informacijsku i komunikacijsku tehnologiju 4](#_Toc160459091)

[3.1. Upravljanje promjenama 4](#_Toc160459092)

[3.2. Upravljanje konfiguracijom 5](#_Toc160459093)

[3.3. Upravljanje kapacitetima 5](#_Toc160459094)

[3.4. Antivirusna zaštita 5](#_Toc160459095)

[3.5. Sigurnosne kopije podataka 5](#_Toc160459096)

[3.5.1. Procedura izrade sigurnosnih kopija 5](#_Toc160459097)

[3.5.2. Testiranje sigurnosnih kopija 5](#_Toc160459098)

[3.6. Upravljanje sigurnošću mreža 6](#_Toc160459099)

[3.7. Mrežne usluge 6](#_Toc160459100)

[3.8. Brisanje podataka 6](#_Toc160459101)

[3.9. Odlaganje i uništavanje uređaja i medija 7](#_Toc160459102)

[3.9.1 Uređaji 7](#_Toc160459103)

[3.9.2 Mediji za pohranu 7](#_Toc160459104)

[3.9.3 Papirnati mediji 7](#_Toc160459105)

[3.9.4 Zapisi o uklanjanju i uništavanju; povjerenstvo za uništavanje 7](#_Toc160459106)

[3.10. Prijenos informacija 7](#_Toc160459107)

[3.10.1. Elektronički komunikacijski kanali 8](#_Toc160459108)

[3.10.2. Odnosi s vanjskim stranama 8](#_Toc160459109)

[3.11. Rukovanje izvornim kodom 8](#_Toc160459110)

[3.12. Uporaba uslužnih programa 8](#_Toc160459111)

[3.13. Izrada dnevnika i praćenje rada sustava 8](#_Toc160459112)

[3.14. Praćenje tehničkih ranjivosti 9](#_Toc160459113)

[3.15. Praćenje vanjskih prijetnji 9](#_Toc160459114)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 9](#_Toc160459115)

[5. Valjanost i upravljanje dokumentom 12](#_Toc160459116)

# 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 [odjeli vezani uz IT].

# 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. Promjene na IT sustavima može predložiti bilo tko iz tvrtke.
2. Za promjenu ovlaštenje mora dati [naziv radnog mjesta za odobravanje promjena] koji mora procijeniti je li promjena poslovno opravdana i postoje li negativni sigurnosni učinci te odrediti koje će osobe biti odgovorne za (a) implementaciju, (b) provjeru, (c) testiranje te (d) kome se podnosi izvješće kao i (e) osobu odgovornu za ažuriranje dokumentacije.
3. Promjenu mora implementirati osoba nadležna za implementaciju.
4. Osoba nadležna za provjeru mora provjeriti je li promjena implementirana u skladu sa zahtjevima.
5. Osoba nadležna za testiranje mora testirati i potvrditi stabilnost sustava – sustav se ne smije pustiti u produkciju prije nego je provedeno temeljito testiranje.
6. Osobe nadležne za implementaciju, provjeru i testiranje moraju svoj napredak prijaviti osobi koja je određena za primanje izvješća.
7. Osoba nadležna za ažuriranje dokumenata mora ažurirati sve politike, procedure, planove, itd. na koje je promjena imala utjecaj.

Zapisi o provedbi promjena vode se [metoda za zapisivanje promjena].

## Upravljanje konfiguracijom

[naziv radnog mjesta za konfiguracijske postavke] 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 kapacitetima

[naziv radnog mjesta za upravljanje kapacitetima] je odgovoran za praćenje uporabe ICT resursa i planiranje potrebnih kapaciteta.

## Antivirusna zaštita

[naziv radnog mjesta za programe za zaštitu] određuje koji program zaštite mora biti instaliran na kojem IT sustavu.

## Sigurnosne kopije podataka

### Procedura izrade sigurnosnih kopija

Sigurnosne kopije moraju se izrađivati za sve sustave određene u [dokument koji određuje učestalost izrade sigurnosnih kopija], učestalošću navedenom u tom dokumentu.

[naziv radnog mjesta za izvođenje izrade sigurnosnih kopija] je odgovoran za izradu sigurnosnih kopija informacija, softvera i slika sustava te za osiguravanje pravilnog odgovora na kvarove prilikom planirane izrade sigurnosnih kopija.

[opis tehnologije za izradu sigurnosnih kopija, lokacija izvedbe, zaštite].

Dnevnici izvršenja izrade sigurnosne kopije automatski se izrađuju na sustavima na kojima je stvorena sigurnosna kopija.

### Testiranje sigurnosnih kopija

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

[naziv radnog mjesta za testiranje sigurnosnih kopija] je odgovoran za testiranje sigurnosnih kopija. Zapisi o testiranju sigurnosnih kopija vode se [oblik zapisa o testiranju sigurnosnih kopija].

## Upravljanje sigurnošću mreža

[naziv radnog mjesta za sigurnost mreža] je odgovoran za upravljanje računalnim mrežama i nadzor nad njima, za sigurnost informacija na mrežama, sprječavanje curenja podataka te za zaštitu od neovlaštenog pristupa usluga povezanih s mrežama.

Kao dio upravljanja sigurnošću mreža, ova osoba mora:

* odvojiti operativnu odgovornost za mreže od odgovornosti za osjetljive aplikacije i druge sustave
* zaštititi osjetljive podatke koji se prenose preko javne mreže
* zaštititi osjetljive podatke koji se prenose preko bežičnih mreža
* zaštititi opremu kojom se vrši povezivanje na mrežu s udaljenih lokacija u skladu s Politikom mobilnih uređaja, rada na daljinu i rada od kuće
* odvojiti mrežu
* razdvojiti razvojna, testna i operativna okruženja sustava
* odvojiti promet koji dolazi s mobilnih uređaja, postaviti jedinstvene politike vatrozida, statičkih ruta, virtualnih lokalnih mreža, itd.
* osigurati dostupnost mrežnih usluga
* 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 međusobno usklađeno

## Mrežne usluge

…

**\* 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/>)