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

[logo tvrtke]

[naziv tvrtke]

**POLITIKA SIGURNOSTI INFORMACIJSKOG SUSTAVA**

|  |  |
| --- | --- |
| 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

2. Referentni dokumenti 4

3. Prihvatljiva uporaba informacijskih resursa 4

3.1. Definicije 4

3.2. Prihvatljiva uporaba 4

3.3. Odgovornost za resurse 4

3.4. Brisanje informacija 5

3.5. Zabranjeni postupci 5

3.6. Iznošenje resursa izvan tvrtke 5

3.7. Povrat resursa prilikom prestanka ugovora 5

3.8. Procedura izrade sigurnosnih kopija 5

3.9. Antivirusna zaštita i zaštita od zlonamjernog softvera 5

3.10. Ovlaštenja za korištenje informacijskog sustava 6

3.11. Odgovornosti za korisnički račun 6

3.12. Odgovornosti za lozinke 6

3.13. Politika čistog stola i čistog ekrana 7

3.13.1. Politika čistog stola 7

3.13.2. Politika čistog ekrana 7

3.13.3. Zaštita zajedničkih prostorija i opreme 7

3.14. Korištenje Interneta 7

3.15. Elektronička pošta i ostale metode za razmjenu poruka 8

3.16. Zaštita autorskih prava 8

3.17. Uporaba mobilnih uređaja izvan poslovnih prostora 8

3.17.1. Uvod 8

3.17.2. Osnovna sigurnosna pravila za mobilne uređaje 9

3.18. Rad na daljinu i rad od kuće 9

3.18.1. Uvod 9

3.18.2. Dodatna pravila za rad na daljinu 10

3.19. Praćenje uporabe informacijskih i komunikacijskih sustava 10

3.20. Incidenti 10

4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 11

5. Valjanost i upravljanje dokumentom 12

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta odrediti pravila za prihvatljivu uporabu informacijskih sustava i ostalih informacijskih resursa u tvrtki [naziv tvrtke].

Ovaj se dokument primjenjuje na cijeli opseg Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*), tj. na sve informacijske sustave i ostale informacijske resurse koji se koristi unutar opsega ISMS-a.

Korisnici su ovog dokumenta svi zaposlenici tvrtke [naziv tvrtke].

# Referentni dokumenti

* Norma ISO/IEC 27001, mjere A.5.9, A.5.10, A.5.11, A.5.14, A.5.17, A.5.32, A.6.7, A.7.7, A.7.9, A.7.10, A.8.1, A.8.7, A.8.10, A.8.12, A.8.13, A.8.19 i A.8.23
* Politika informacijske sigurnosti
* Politika klasifikacije informacija
* Procedura za upravljanje incidentima
* Popis resursa
* Sigurnosne procedure za IT odjel
* Politika prijenosa informacija

# Prihvatljiva uporaba informacijskih resursa

## Definicije

Informacijski sustav – uključuje sve poslužitelje i klijente, mrežnu infrastrukturu, sistemski i aplikacijski softver, podatke te druge računalne podsustave i komponente, koje tvrtka posjeduje, koristi ili su pod njezinom odgovornošću. Korištenje informacijskog sustava podrazumijeva i korištenje svih unutarnjih servisa ili vanjskih servisa u oblaku kao što su pristup Internetu, elektroničkoj pošti i sl.

Informacijski resursi – u kontekstu ove Politike, pojam informacijskog resursa primjenjuje se na informacijske sustave i ostale informacije/opremu uključujući papirnate dokumente, mobilne telefone, prijenosna računala, medije za pohranu podataka, itd.

## Prihvatljiva uporaba

Informacijski resurs može se koristiti samo za poslovne potrebe, u svrhu izvršavanja zadataka vezanih uz tvrtku.

## Odgovornost za resurse

Svaki informacijski resurs ima vlasnika određenog u Popisu resursa. Vlasnik resursa odgovoran je za povjerljivost, cjelovitost i dostupnost informacija o predmetnom resursu.

## Brisanje informacija

Kada više nisu potrebne, vlasnik resursa mora izbrisati osjetljive informacije pohranjene na njegovom/njezinom računalu ili prenosivom uređaju.

## Zabranjeni postupci

Zabranjeno je koristiti informacijske resurse na način koji nepotrebno zauzima kapacitet, slabi performanse informacijskog sustava ili predstavlja sigurnosnu prijetnju. Također je zabranjeno:

* preuzimati slikovne ili video datoteke koje nemaju poslovnu svrhu, slati lančane poruka e-pošte i sl.
* instalirati softver na lokalno računalo bez izričitog dopuštenja od strane [naziv radnog mjesta za prihvatljivu uporabu]
* preuzimati izvršne (.exe) datoteke s uklonjivih medija
* instalirati ili korititi periferne uređaje kao što su modemi, memorijske kartice ili drugi uređaji za pohranu i čitanje podataka (kao npr. USB uređaji), bez izričitog dopuštenja od strane [naziv radnog mjesta za prihvatljivu uporabu]

## Iznošenje resursa izvan tvrtke

Za iznošenje opreme, informacija ili softvera, bez obzira u kojem obliku ili na kojem se mediju za pohranu nalaze, potrebna je prethodna pisana dozvola od strane [naziv radnog mjesta za prihvatljivu uporabu].

Sve dok su navedeni resursi izvan tvrtke, mora ih nadzirati osoba koja je dobila dozvolu za njihovo korištenje izvan tvrtke.

## Povrat resursa prilikom prestanka ugovora

Nakon prestanka ugovora o radu ili drugog ugovora na temelju kojeg se koristi različita oprema, programska oprema ili podaci u digitalnom ili papirnatom obliku, korisnik je dužan sve informacijske resurse vratiti koja mu/joj je direktno nadređena.

## Procedura izrade sigurnosnih kopija

Korisnici moraju izrađivati sigurnosne kopije svih podataka pohranjenih na njihovim računalima najmanje jednom dnevno [metoda izrade sigurnosnih kopija].

## Antivirusna zaštita i zaštita od zlonamjernog softvera

[naziv programa za zaštitu] mora biti instaliran na svakom računalu, s aktiviranim automatskim ažuriranjem.

## Ovlaštenja za korištenje informacijskog sustava

Korisnici informacijskog sustava mogu pristupiti samo onim resursima informacijskog sustava za koje su izričito ovlašteni od strane vlasnika resursa.

Korisnici smiju koristiti informacijski sustav samo u svrhe za koje su ovlašteni, odnosno za koje su im dodijeljena prava pristupa.

Korisnici ne smiju sudjelovati u aktivnostima koje se mogu koristiti za zaobilaženje sigurnosnih mjera informacijskog sustava.

## Odgovornosti za korisnički račun

…

**\* 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/>)