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

[logo organizacije]

[naziv organizacije]

**POLITIKA SIGURNOSTI INFORMACIJSKOG SUSTAVA**

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

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 organizacije 5

3.7. Povrat resursa prilikom prestanka ugovora 5

3.8. Procedura izrade sigurnosnih kopija 5

3.9. Antivirusna 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 9

3.17. Mobilno računalstvo 9

3.17.1. Uvod 9

3.17.2. Osnovna pravila 9

3.18. Rad na daljinu i rad od kuće 10

3.18.1. Uvod 10

3.18.2. Dodatna pravila za rad na daljinu 10

3.19. Nadzor nad uporabom informacijskih i komunikacijskih sustava 10

3.20. Incidenti 11

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 jasna pravila za prihvatljivo korištenje informacijskog sustava i ostalih informacijskih resursa u [naziv organizacije].

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 [naziv organizacije].

# 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 organizacija posjeduje, koristi ili su pod njezinom odgovornošću. Korištenje informacijskog sustava podrazumijeva i korištenje svih unutarnjih ili vanjskih servisa 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 organizacijskih zadataka.

## 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

Nakon što više nisu potrebne, vlasnik resursa mora izbrisati osjetljive informacije pohranjene na njegovom/njezinom računalu ili mobilnom 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:

* preuzimanje slikovnih ili video datoteka koje nemaju poslovnu svrhu, slanje lančanih poruka e-pošte, igranje igrica i sl.
* instalacija softvera na lokalno računalo bez izričitog dopuštenja od strane [naziv radnog mjesta]
* korištenje Java aplikacija, Active X kontrola i drugog mobilnog koda, osim u slučaju da je odobreno od strane [naziv radnog mjesta]
* korištenje kriptografskih alata (enkripcije) na lokalnom računalu, osim u slučajevima propisanima Politikom klasifikacije informacija
* preuzimanje programskog koda s vanjskih medija
* instaliranje ili korištenje perifernih uređaja 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]; dopušteno je korištenje u skladu s Politikom klasifikacije informacija

## Iznošenje resursa izvan organizacije

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].

Sve dok su navedena sredstva izvan organizacije, mora ih nadzirati osoba koja je dobila dozvolu za njihovo iznošenje.

## 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 elektroničkom ili papirnatom obliku, korisnik je dužan sve informacijske resurse vratiti [naziv radnog mjesta].

## Procedura izrade sigurnosnih kopija

…

**\* 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/>)