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

[logo organizacije]

[naziv organizacije]

**POLITIKA SIGURNOG RAZVOJA**

|  |  |
| --- | --- |
| 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 3](#_Toc216177993)

[2. Referentni dokumenti 3](#_Toc216177994)

[3. Sigurni razvoj i održavanje 3](#_Toc216177995)

[3.1. Procjena rizika za proces razvoja 3](#_Toc216177996)

[3.2. Osiguravanje razvojnog okruženja 3](#_Toc216177997)

[3.3. Načela izgradnje sigurnih sustava 3](#_Toc216177998)

[3.4. Sigurno kodiranje 4](#_Toc216177999)

[3.5. Sigurnosni zahtjevi 4](#_Toc216178000)

[3.6. Sigurnosni zahtjevi povezani s javnim mrežama 4](#_Toc216178001)

[3.7. Provjeravanje i testiranje implementacije sigurnosnih zahtjeva 4](#_Toc216178002)

[3.8. Spremište 4](#_Toc216178003)

[3.9. Upravljanje verzijama 4](#_Toc216178004)

[3.10. Upravljanje promjenama 5](#_Toc216178005)

[3.11. Zaštita testnih podataka 5](#_Toc216178006)

[3.12. Obvezna obuka o sigurnosti 5](#_Toc216178007)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 5](#_Toc216178008)

[5. Valjanost i upravljanje dokumentom 5](#_Toc216178009)

[6. Prilozi 6](#_Toc216178010)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta propisivanje osnovnih pravila za siguran razvoj softvera i sustava.

Ovaj se dokument primjenjuje na razvoj i održavanje svih usluga, arhitektura, softvera i sustava koji su dio Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*).

Korisnici su ovog dokumenta svi zaposlenici koji rade na razvoju i održavanju u [naziv organizacije].

# Referentni dokumenti

* Norma ISO/IEC 27001, mjere A.5.33, A.8.11, A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31, A.8.32 i A.8.33
* Metodologija za procjenu i obradu rizika
* Politika sigurnosti dobavljača
* [Politika upravljanja promjenama] / [Sigurnosne procedure za IT odjel]
* Plan obučavanja i osvješćivanja

# Sigurni razvoj i održavanje

## Procjena rizika za proces razvoja

Osim procjene rizika koja se provodi prema Metodologiji za procjenu i obradu rizika, [naziv radnog mjesta] povremeno mora provoditi i procjenu:

* rizika povezanih s neovlaštenim pristupom razvojnom okruženju
* rizika povezanih s neovlaštenim promjenama razvojnog okruženja
* tehničkih ranjivosti IT sustava koji se koristi u organizaciji
* rizika koje može donijeti nova tehnologija ako se koristi u organizaciji
* rizika koje može donijeti nova razvojna metodologija i/ili programski jezik ako se koriste u organizaciji
* rizika povezanih sa zahtjevima licenciranja

## Osiguravanje razvojnog okruženja

[Navedite unutarnje kao i vanjske zahtjeve; ovdje opišite kako će pristup razvojnom okruženju biti ograničen samo na ovlaštene zaposlenike, kako će biti odvojen od okruženja za testiranje i proizvodnju, kako se izrađuju sigurnosne kopije.]

## Načela izgradnje sigurnih sustava

[Naziv radnog mjesta] će izdati procedure za izgradnju sigurnih informacijskih sustava, kako za razvoj novih sustava, tako i za održavanje postojećih sustava, kao i postaviti minimalne sigurnosne zahtjeve kojih se potrebno pridržavati.

Ista načela sigurne izgradnje primjenjivat će se na razvoj od strane vanjskih suradnika i bit će propisana kroz ugovore na način koji je opisan u [Politici sigurnosti dobavljača].

## Sigurno kodiranje

[Naziv radnog mjesta] će izdati procedure za sigurno kodiranje informacijskog sustava, kako za razvoj novih sustava tako i za održavanje postojećih sustava, kao i postaviti minimalne zahtjeve za sigurno kodiranje kojih se potrebno pridržavati.

Ista načela sigurnog kodiranja primjenjivat će se na razvoj od strane vanjskih suradnika i bit će propisana kroz ugovore na način koji je opisan u [Politici sigurnosti dobavljača].

## Sigurnosni zahtjevi

Prilikom nabave novih informacijskih sustava, ili razvoja ili izmjene postojećih, [naziv radnog mjesta] mora dokumentirati sigurnosne zahtjeve u Specifikaciji zahtjeva za informacijski sustav.

## Sigurnosni zahtjevi povezani s javnim mrežama

[Naziv radnog mjesta] je odgovoran za propisivanje sigurnosnih mjera vezanih uz informacije u aplikacijskim uslugama koje prolaze preko javnih mreža:

* …

…

**\* 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/>)