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

[logo tvrtke]

[naziv tvrtke]

**POLITIKA SIGURNOG RAZVOJA**

|  |  |
| --- | --- |
| 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 3](#_Toc133501235)

[2. Referentni dokumenti 3](#_Toc133501236)

[3. Sigurni razvoj i održavanje 3](#_Toc133501237)

[3.1. Procjena rizika za proces razvoja 3](#_Toc133501238)

[3.2. Osiguravanje razvojnog okruženja 3](#_Toc133501239)

[3.3. Načela izgradnje sigurnih sustava 3](#_Toc133501240)

[3.4. Sigurno kodiranje 4](#_Toc133501241)

[3.5. Sigurnosni zahtjevi 4](#_Toc133501242)

[3.6. Sigurnosni zahtjevi povezani s javnim mrežama 4](#_Toc133501243)

[3.7. Provjeravanje i testiranje implementacije sigurnosnih zahtjeva 4](#_Toc133501244)

[3.8. Spremište 4](#_Toc133501245)

[3.9. Upravljanje verzijama 4](#_Toc133501246)

[3.10. Upravljanje promjenama 5](#_Toc133501247)

[3.11. Zaštita testnih podataka 5](#_Toc133501248)

[3.12. Obvezna obuka o sigurnosti 5](#_Toc133501249)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 5](#_Toc133501250)

[5. Valjanost i upravljanje dokumentom 5](#_Toc133501251)

[6. Prilozi 6](#_Toc133501252)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta utvrditi osnovna 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 tvrtki [naziv tvrtke].

# 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 za sigurnost razvoja] mora redovito provoditi i procjenu sljedećeg:

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

## Osiguravanje razvojnog okruženja

Razvojno okruženje bit će osigurano na sljedeći način: [sigurnost razvojnog okruženja].

## Načela izgradnje sigurnih sustava

[naziv radnog mjesta za sigurnost razvoja] 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 i na razvoj od strane vanjskih suradnika i bit će propisana kroz sporazume na način koji je opisan u Politici sigurnosti dobavljača.

## Sigurno kodiranje

[naziv radnog mjesta za sigurnost razvoja] 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, vlasnik sustava mora dokumentirati sigurnosne zahtjeve u Specifikaciji zahtjeva za informacijski sustav.

## Sigurnosni zahtjevi povezani s javnim mrežama

…

**\* 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/>)