| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ovdje unesite naziv registrirane pravne osobe | | | | | | | |
| Broj dokumenta:<br>P06 | | | | | Naziv dokumenta:<br>**Politika upravljanja rizicima** | | | | | | | |
| Verzija:<br>1.0 | | Datum stupanja na snagu:<br>01.01.2025 | | | Vlasnik dokumenta: | | | | | | | |
| X | Politika | | Standard | | Postupak | | Obrazac | | Registar | | Drugo | |

| **Povijest revizija** | | | | |
|---|---|---|---|---|
| **Broj revizije** | **Datum revizije** | **Promjene** | **Pregledao/la** | **Vlasnik procesa** |
| | | | | |
| | | | | |

| **Odobrenja** | | | |
|---|---|---|---|
| **Ime** | **Radno mjesto** | **Datum** | **Potpis** |
| | | | |
| | | | |

Usklađeno sa standardima i regulativom

| Standard/regulativa | Točka/članak | Napomena |
|---|---|---|
| ISO/IEC 27001:2022 | Točke 6.1, 8.32, 10 | Temelj upravljanja rizicima i njihove identifikacije, integracija u upravljanje promjenama, kontinuirano poboljšavanje |
| ISO/IEC 27005:2024 | Cjelokupna metodologija životnog ciklusa rizika | Cjelovit proces upravljanja rizicima u skladu sa standardom |
| ISO 31000:2018 | Načela i okvir za upravljanje rizicima | Načela upravljanja rizicima usvojena u okviru |
| NIST SP 800-30 Rev.1 | SP 800-30, SP 800-39 | Smjernice i struktura za procjene rizika, višerazinsko upravljanje rizicima |
| GDPR EU | Članci 24, 25, 32 | Procesi i kontrole rizika za zaštitu podataka |
| Direktiva EU NIS2 | Članak 21(2)(a–d) | Obveze procjene rizika i sigurnosne procjene |
| Uredba EU DORA | Članci 5, 6 | Upravljanje IKT rizicima i operativna otpornost |
| COBIT 2019 | APO12, MEA | Struktura upravljanja rizicima i nadzor |

## 1. Svrha

1.1 Ova politika uspostavlja jedinstven i formaliziran okvir za identifikaciju, analizu, vrednovanje, obradu, praćenje i pregled rizika informacijske sigurnosti u cijeloj organizaciji.

1.2 Njome se osigurava dosljedna primjena načela odlučivanja temeljenog na riziku radi zaštite povjerljivosti, cjelovitosti i dostupnosti informacijske imovine, u skladu s točkom 6.1 norme ISO/IEC 27001:2022 i normom ISO 31000:2018.

1.3 Ova politika ugrađuje upravljanje rizicima informacijske sigurnosti u procese odlučivanja organizacije radi ispunjenja internih strateških ciljeva i vanjskih regulatornih zahtjeva.

## 2. Opseg

2.1 Ova politika primjenjuje se na sve organizacijske jedinice, poslovne procese, sustave, osoblje i angažmane trećih strana koji sudjeluju u obradi informacijske imovine, njezinu razvoju, pohrani ili upravljanju njome.

2.2 Opseg obuhvaća fizičku, digitalnu i u oblaku hostiranu imovinu, uključujući strukturirane i nestrukturirane podatke, aplikacije, infrastrukturu, mreže i usluge.

2.3 Ova politika obuhvaća rizike informacijske sigurnosti na strateškoj, operativnoj, projektnoj i tehničkoj razini te je obvezna za sve zaposlenike, ugovorne izvođače i pružatelje usluga uključene u aktivnosti ISMS-a.

**2.4 Upravljanje rizicima mora se primjenjivati na sljedeće scenarije:**

**2.4.1 Uvođenje novog projekta ili sustava**

2.4.1.1 Značajne promjene (npr. arhitekture, vlasništva, procesa)

2.4.1.2 Uvođenje dobavljača i ugovori s trećim stranama

2.4.1.3 Odgovor na incidente i pregled nakon incidenta

2.4.1.4 Periodični organizacijski pregledi rizika ili revizije

**3. Ciljevi**

3.1 Uspostaviti i provoditi ponovljiv proces upravljanja rizicima na razini cijele organizacije, temeljen na metodologijama ISO/IEC 27005 i ISO 31000.

3.2 Osigurati da se rizici identificiraju, analiziraju, vrednuju i obrađuju strukturiranim metodama koje omogućuju sljedivost, uključujući dodjelu vlasništva nad rizikom i povezivanje s kontrolama.

3.3 Održavati centralizirani registar rizika i plan obrade rizika pod kontrolom verzija, koji odražavaju trenutačni status rizika, obuhvat kontrola i napredak mjera ublažavanja.

3.4 Uskladiti odluke o rizicima s dokumentiranim apetitom za rizik i razinama tolerancije na rizik te omogućiti informirano odlučivanje upravljačkih tijela o prihvaćanju, ublažavanju, prijenosu ili izbjegavanju rizika.

3.5 Kontinuirano pratiti trendove rizika i osiguravati djelotvornost obrade rizika, uz omogućavanje proaktivnih prilagodbi na temelju razvoja prijetnji ili promjena u poslovanju.

**4. Uloge i odgovornosti**

**4.1 Izvršno vodstvo / upravni odbor**

4.1.1 Odobrava okvir za upravljanje rizicima i definira prihvatljivi apetit za rizik i pragove prihvaćanja rizika.

4.1.2 Odobrava strategije obrade rizika za preostale rizike koji prelaze toleranciju.

4.1.3 Dodjeljuje resurse i osigurava nadzor za učinkovito funkcioniranje programa upravljanja rizicima.

**4.2 Voditelj ISMS-a / službenik za upravljanje rizicima**

4.2.1 Vlasnik je ove politike i održava njezinu usklađenost s normama ISO/IEC 27001 i 27005.

4.2.2 Vodi proces procjene rizika na razini organizacije te održava registar rizika i plan obrade rizika.

4.2.3 Osigurava periodične preglede i eskalaciju ključnih rizika prema izvršnom vodstvu ili Upravljačkom odboru ISMS-a.

[ ... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ... ]

**9. Zahtjevi za pregled i ažuriranje**

**9.1 Ova politika i pripadajući okvir moraju se pregledavati jednom godišnje ili:**

9.1.1 Nakon značajnog događaja povezanog s rizikom ili sigurnosnog incidenta

9.1.2 Nakon značajne organizacijske ili tehničke promjene

9.1.3 Kao odgovor na nalaze revizije ili nove regulatorne zahtjeve

**9.2 Voditelj ISMS-a, službenik za upravljanje rizicima i tim za usklađenost zajednički su odgovorni za:**

9.2.1 Pokretanje ciklusa pregleda

9.2.2 Prikupljanje ulaznih podataka od poslovnih jedinica

9.2.3 Reviziju postupaka i pragova prema potrebi

**9.3 Sve izmjene moraju biti:**

9.3.1 Pod kontrolom verzija i evidentirane

9.3.2 Odobrene od strane izvršnog vodstva

9.3.3 Komunicirane dionicima

9.3.4 Pohranjene u revizijskom repozitoriju najmanje 5 godina

## 10. Povezane politike i poveznice

### 10.1 Ova politika međuovisna je sa sljedećim politikama informacijske sigurnosti:

10.1.1 P1 – Politika informacijske sigurnosti: utvrđuje opći model upravljanja sigurnošću u okviru kojeg se ova politika upravljanja rizicima provodi.

10.1.2 P2 – Politika uloga i odgovornosti u upravljanju: definira odgovorne vlasnike i razine upravljanja navedene u matrici eskalacije rizika.

10.1.3 P5 – Politika upravljanja promjenama: pokreće ponovnu procjenu rizika za infrastrukturne i organizacijske promjene.

10.1.4 P13 – Politika klasifikacije i označavanja podataka: podupire procjenu utjecaja tijekom identifikacije rizika.

10.1.5 P33 – Politika praćenja revizije i usklađenosti: potvrđuje pridržavanje politici, uključujući potpunost registra rizika i dokaze o obradi rizika.

## 11. Referentni standardi i okviri

11.1 Ova politika izričito je usklađena sa sljedećim standardima i okvirima kako bi se osiguralo ispunjavanje međunarodno priznatih dobrih praksi i regulatornih očekivanja za upravljanje rizicima informacijske sigurnosti:

### 11.2 ISO/IEC 27001:

11.2.1 Točka 6.1: utvrđuje zahtjeve za identifikaciju rizika i prilika, uključujući cjelokupni životni ciklus procjena i obrade rizika informacijske sigurnosti. Ova politika provodi zahtjeve točaka 6.1 i 6.1.2 kroz strukturirani okvir koji propisuje dokumentiranu identifikaciju, analizu, vrednovanje, obradu i protokole za prihvaćanje preostalog rizika.

11.2.2 Točka 8.32: integracija pristupa temeljenog na riziku u procese upravljanja promjenama osigurava da sve značajne organizacijske promjene pokreću formalne ponovne procjene rizika.

11.2.3 Točka 10: kontinuirano poboljšavanje ugrađeno je kroz redovite preglede politike, analizu trendova rizika i ažuriranja SoA potaknuta spoznajama iz upravljanja rizicima.

### 11.3 ISO/IEC 27005:

11.3.1 Pruža specijalizirane i detaljne smjernice za upravljanje rizicima informacijske sigurnosti. Ova politika provodi cjelovit model procesa rizika prema ISO/IEC 27005: utvrđivanje konteksta, identifikacija rizika, analiza rizika, vrednovanje rizika, obrada rizika, prihvaćanje rizika, komunikacija rizika te praćenje i pregled rizika.

### 11.4 ISO 31000:

11.4.1 Ova politika integrira načela norme ISO 31000 kao što su predanost vodstva, integracija s odlučivanjem i kontinuirano poboljšavanje. Time se osigurava da je upravljanje rizicima ugrađeno u kulturu i operativno djelovanje organizacije.

### 11.5 NIST SP 800-30 Rev.1:

11.5.1 Usklađena je s NIST-ovim vodičem za provođenje procjena rizika, uključujući identifikaciju prijetnji, analizu ranjivosti, procjenu vjerojatnosti i utvrđivanje utjecaja. Struktura ove politike odražava korake procjene rizika koje definira NIST i prilagođava ih tehničkim i poslovnim procesima.

### 11.6 NIST SP 800-39:

11.6.1 Podupire upravljanje rizicima na razini organizacije, s naglaskom na višerazinsko upravljanje rizicima na razini organizacije, misije/poslovnog procesa i informacijskog sustava. Ova politika osigurava da je vlasništvo nad rizikom jasno definirano na svim razinama te uključuje strategije obrade na razini organizacije.

### 11.7 GDPR EU:

11.7.1 Članak 24: zahtijeva provedbu odgovarajućih tehničkih i organizacijskih mjera kako bi se rizicima zaštite podataka pravilno upravljalo, što se ostvaruje kroz strukturirani proces upravljanja rizicima propisan ovom politikom.

11.7.2 Članak 25: „Zaštita podataka već u fazi projektiranja i prema zadanim postavkama" usklađena je s ugrađivanjem obrade rizika u dizajn sustava i procesa.

11.7.3 Članak 32: propisuje pristup sigurnosnim mjerama temeljen na riziku, što se ispunjava kroz vrednovanje rizika temeljeno na utjecaju i odabir kontrola temeljen na riziku.

**11.8 Direktiva EU NIS2:**

11.8.1 Članak 21(2)(a–d): zahtijeva da subjekti provode procjene rizika, uspostave politike za analizu rizika i osiguraju razmjerne sigurnosne mjere. Ova politika ispunjava te obveze kroz kontinuiranu primjenu životnog ciklusa rizika i dokumentirano upravljanje.

**11.9 Uredba EU DORA:**

11.9.1 Članak 5: propisuje dokumentirani okvir za upravljanje IKT rizicima, koji je u cijelosti obuhvaćen arhitekturom ove politike, uključujući mapiranje na SoA i KRI-jeve.

11.9.2 Članak 6: zahtijeva integraciju upravljanja rizicima u strategije operativne otpornosti, što se uređuje kroz matrice eskalacije i praćenje kritične imovine.

**11.10 COBIT 2019:**

11.10.1 APO12 – Upravljanje rizicima: izravno se preslikava na uspostavu strukturiranog pristupa upravljanju rizicima u organizaciji, uz dodjelu uloga, praćenje obrada i osiguravanje odgovornosti na razini upravnog odbora.

11.10.2 MEA01 – Pratiti, vrednovati i ocjenjivati uspješnost i usklađenost: odražava se u usmjerenosti ove politike na analizu trendova, praćenje KRI-jeva i integraciju povratnih informacija iz revizije u cikluse kontinuiranog poboljšavanja.