Varnostna politika

Safety Software | Aktualizacja: 03.09.2026 | https://safetysoftware.eu

Politika varnosti aplikacije Safety Software (SaaS)

ID: SE-2026-V2
Posodobitev: 2026-03-05

1. Namen in področje uporabe

Ta Politika varnosti določa pravila za zaščito informacij in podatkov, ki se obdelujejo v okviru aplikacije Safety Software, ki je na voljo v modelu Software as a Service (SaaS).

Dokument se nanaša na varnost uporabnikov, ki uporabljajo aplikacijo v storitvi Safety Software, in predstavlja dopolnitev Pravilnika ter Politike zasebnosti.

Politika je informativne narave in opisuje osnovne tehnične in organizacijske ukrepe, ki jih uporablja Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Poljska (v nadaljevanju: »Upravljavec«).

2. Model odgovornosti

Sistem deluje po modelu deljene odgovornosti:

1. **Upravljavec (Safety Software)** je odgovoren za varnost kode aplikacije, mehanizme prijave, avtorizacije in seje, zaščito podatkov na aplikacijski plasti, izdelavo varnostnih kopij ter odzivanje na varnostne incidente.

2. **Ponudniki infrastrukture in pomožnih storitev** so odgovorni za varnost elementov, ki so v okviru storitev, ki jih zagotavljajo.

3. **Stranka** je odgovorna za varnost svojih naprav, gesel, identitet uporabnikov ter upravljanje dostopov v svoji ekipi.

3. Načela varnosti aplikacije

1. Prenos podatkov poteka izključno z uporabo šifriranja TLS.

2. Uporabniške seje so zavarovane z uporabo piškotkov z atributi **HttpOnly**, **Secure** (za šifrirane povezave) ter **SameSite**. Po avtentikaciji se izvede rotacija identifikatorja seje.

3. Za seje se uporabljajo omejitve nedejavnosti in največjega trajanja.

4. Zahteve, ki spreminjajo stanje sistema, so zaščitene s CSRF žetoni, preverjenimi na strani strežnika.

5. Aplikacija uporablja restriktivno politiko varnosti vsebine, vključno z mehanizmi, ki omejujejo izvajanje nepooblaščenih skriptov, ter standardnimi varnostnimi glavami brskalnika.

6. Uporabljajo se mehanizmi za omejevanje zlorab, vključno z omejevanjem hitrosti (rate limiting) ter zaščito pred poskusi prijave z grobo silo.

7. Vsaka operacija se izvaja v kontekstu uporabnika in organizacije; nepooblaščen dostop je blokiran.

4. Šifriranje in zaščita podatkov

1. Uporabniška gesla se shranjujejo z uporabo algoritma **bcrypt**.

2. Izbrani občutljivi podatki, shranjeni v bazi, so zaščiteni z uporabo modela ovojnicnega šifriranja podatkov. Kriptografski ključi se upravljajo ločeno v zunanjem sistemu za upravljanje ključev.

3. Kjer je to utemeljeno, se uporabljajo mehanizmi, ki omejujejo izpostavljenost podatkov ob ohranjanju funkcij iskanja ali identifikacije, brez potrebe po shranjevanju celotnih vrednosti v nešifrirani obliki.

5. Varnostno kopiranje in obnova (BCP/DR)

1. Uporabljamo večplastni pristop k varnostnim kopijam: lokalne kopije za hitro obnovitev ter kopije, shranjene zunaj primarnega okolja.

2. Kopije, shranjene zunaj primarnega okolja, vključujejo slike okolja, izdelane

inkrementalno. Te so šifrirane, redno validirane in vključene v teste obnove.

3. Baza podatkov je zaščitena z aplikacijsko konsistentnimi kopijami. Poleg tega se vzdržujejo lokalni izvozi baze, ki podpirajo hitro obnovitev.

4. Celovitost kopij se preverja z uporabo kontrolnih mehanizmov, vključno s kontrolnimi vsotami.

5. Postopek izdelave kopij je avtomatiziran, izvaja se dnevno in je zajet v spremljanje uspešnosti ter neuspešnosti opravil.

6. Redno se izvajajo testi obnove podatkov, ki vključujejo najmanj obnovitev izbranih datotek.

6. Spremljanje in opozorila

1. Sistem beleži izbrane varnostne dogodke ter administrativne operacije, zlasti tiste, povezane z avtentikacijo, poskusi dostopa in delovanjem kritičnih procesov.

2. Uporabljajo se mehanizmi spremljanja ter samodejna opozorila ob neuspehu opravil, kritičnih napakah in dogodkih, ki lahko kažejo na zlorabo ali varnostni incident.

3. Dostop do dnevnikov in operativnih informacij je omejen na pooblaščene osebe.

7. Infrastruktura in vzdrževanje varnosti

1. Administrativni dostop je omejen na pooblaščene osebe in zavarovan z mehanizmi močne avtentikacije, vključno z avtentikacijo s ključi.

2. Neposredna prijava v privilegirani račun je onemogočena ali omejena v skladu z načelom najmanjših privilegijev.

3. Uporabljajo se mehanizmi filtriranja prometa, zaščite pred poskusi dostopa z grobo silo ter spremljanja infrastrukturnih dogodkov.

4. Varnostne posodobitve se uvajajo redno.

5. Poštne storitve, uporabljene za delovanje sistema, so zavarovane s šifriranjem prenosa ter mehanizmi za omejevanje zlorab.

8. Dobavitelji in integracije

1. V obsegu, v katerem sistem uporablja zunanje storitve ali pomožne integracije, izbor rešitev upošteva varnost podatkov, načelo minimizacije ter nadzor obsega posredovanih informacij.

2. Komunikacija z zunanjimi storitvami poteka z uporabo šifriranega prenosa.

9. Prijava incidentov

Prijave v zvezi z varnostjo aplikacije ali sumom incidentov je treba poslati na naslov:

office@safetysoftware.eu
Zadeva sporočila: SECURITY

Prijave se analizirajo v skladu z internim postopkom obravnave incidentov.

10. Skladnost in jurisdikcija

1. Varnostni ukrepi so načrtovani in vzdrževani ob upoštevanju veljavnih pravnih predpisov, vključno z zahtevami **GDPR**, ter priznanih praks informacijske varnosti.

2. Uporablja se poljsko pravo.

3. V primeru neskladij med jezikovnimi različicami je odločilna poljska različica.

11. Začetek veljavnosti

Ta različica Varnostne politike velja od **2026-03-05**.

Aktualna različica dokumenta je objavljena v storitvi Safety Software.

Upravljavec podatkov in lastnik sistema:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polska
E-pošta: **office@safetysoftware.eu**

Dnevnik sprememb

Posodobitev: 2026-03-05

- dodatno pojasnjene večplastne varnostne kopije ter postopek obnovitve podatkov (BCP/DR)
- dopolnjen opis šifriranja podatkov z ovojnim modelom in zunanjim upravljanjem ključev
- razširjen opis aplikacijske zaščite o seje, CSRF, CSP in mehanizme proti zlorabam
- dodano poglavje o spremljanju in opozorilih ter poenostavljeno poglavje o integraciji z zunanjimi storitvami