Politika sigurnosti

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

Politika sigurnosti aplikacije Safety Software (SaaS)

ID: SE-2026-V2
Ažuriranje: 2026-03-05

1. Svrha i opseg

Ova Politika sigurnosti utvrđuje pravila zaštite informacija i podataka koji se obrađuju u okviru aplikacije Safety Software dostupne u modelu Software as a Service (SaaS).

Dokument se odnosi na sigurnost korisnika koji koriste aplikaciju u servisu Safety Software te predstavlja dopunu Uvjeta korištenja i Politike privatnosti.

Politika je informativne naravi i opisuje osnovne tehničke i organizacijske mjere koje primjenjuje Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Poljska (dalje: „Administrator”).

2. Model odgovornosti

Sustav djeluje u modelu podijeljene odgovornosti:

1. **Administrator (Safety Software)** odgovoran je za sigurnost koda aplikacije, mehanizme prijave, autorizacije i sesije, zaštitu podataka na aplikacijskoj razini, izradu sigurnosnih kopija te odgovor na sigurnosne incidente.

2. **Pružatelji infrastrukture i pomoćnih usluga** odgovorni su za sigurnost elemenata koji su u okviru usluga koje pružaju.

3. **Klijent** odgovoran je za sigurnost svojih uređaja, lozinki, identiteta korisnika te upravljanje pristupima u svom timu.

3. Pravila sigurnosti aplikacije

1. Prijenos podataka odvija se isključivo uz upotrebu TLS enkripcije.

2. Korisničke sesije zaštićene su upotrebom kolačića s atributima **HttpOnly**, **Secure** (za šifrirane veze) te **SameSite**. Nakon autentikacije slijedi rotacija identifikatora sesije.

3. Za sesije se primjenjuju ograničenja neaktivnosti te maksimalnog trajanja.

4. Zahtjevi koji mijenjaju stanje sustava zaštićeni su CSRF tokenima koji se provjeravaju na strani poslužitelja.

5. Aplikacija primjenjuje restriktivnu politiku sigurnosti sadržaja, uključujući mehanizme koji ograničavaju izvršavanje neautoriziranih skripti te standardna sigurnosna zaglavlja preglednika.

6. Primjenjuju se mehanizmi ograničavanja zlouporaba, uključujući rate limiting te zaštitu od pokušaja prijave grubom silom.

7. Svaka se operacija izvršava u kontekstu korisnika i organizacije; neautorizirani pristup se blokira.

4. Šifriranje i zaštita podataka

1. Korisničke lozinke pohranjuju se uz upotrebu algoritma **bcrypt**.

2. Odabrani osjetljivi podaci pohranjeni u bazi zaštićeni su upotrebom modela omotničnog šifriranja podataka. Kriptografski ključevi upravljaju se odvojeno u vanjskom sustavu za upravljanje ključevima.

3. Tamo gdje je to opravdano, primjenjuju se mehanizmi koji ograničavaju izloženost podataka uz zadržavanje funkcije pretraživanja ili identifikacije, bez potrebe pohrane punih vrijednosti u otvorenom obliku.

5. Sigurnosne kopije i obnova (BCP/DR)

1. Primjenjujemo slojeviti pristup sigurnosnim kopijama: lokalne kopije za brzu obnovu te kopije pohranjene izvan primarnog okruženja.

2. Kopije pohranjene izvan primarnog okruženja uključuju slike okruženja izrađene

inkrementalno. One su šifrirane, redovito validirane i obuhvaćene testovima obnove.

3. Baza podataka osigurava se aplikacijski konzistentnim kopijama. Dodatno se održavaju lokalni dumpovi baze koji podržavaju brzu obnovu.

4. Integritet kopija provjerava se pomoću kontrolnih mehanizama, uključujući kontrolne zbrojeve.

5. Proces izrade kopija je automatiziran, provodi se svakodnevno i obuhvaćen je nadzorom uspješnosti i neuspješnosti zadataka.

6. Redovito se provode testovi obnove podataka, koji obuhvaćaju najmanje obnovu odabranih datoteka.

6. Nadzor i upozorenja

1. Sustav bilježi odabrane sigurnosne događaje te administrativne operacije, osobito povezane s autentikacijom, pokušajima pristupa i radom kritičnih procesa.

2. Primjenjuju se mehanizmi nadzora te automatska upozorenja o neuspjehu zadataka, kritičnim pogreškama i događajima koji mogu ukazivati na zlouporabu ili sigurnosni incident.

3. Pristup zapisnicima i operativnim informacijama ograničen je na ovlaštene osobe.

7. Infrastruktura i održavanje sigurnosti

1. Administrativni pristup ograničen je na ovlaštene osobe i zaštićen mehanizmima snažne autentikacije, uključujući autentikaciju ključevima.

2. Izravna prijava na privilegirani račun je onemogućena ili ograničena sukladno načelu minimalnih ovlasti.

3. Primjenjuju se mehanizmi filtriranja prometa, zaštite od pokušaja pristupa grubom silom te nadzora infrastrukturnih događaja.

4. Sigurnosna ažuriranja uvode se redovito.

5. Poštanske usluge koje se koriste za rad sustava zaštićene su šifriranjem prijenosa te mehanizmima ograničavanja zlouporaba.

8. Pružatelji i integracije

1. U mjeri u kojoj sustav koristi vanjske usluge ili pomoćne integracije, odabir rješenja uzima u obzir sigurnost podataka, načelo minimizacije te kontrolu opsega prenesenih informacija.

2. Komunikacija s vanjskim uslugama odvija se uz upotrebu šifriranog prijenosa.

9. Prijavljivanje incidenata

Prijave koje se odnose na sigurnost aplikacije ili sumnju na incidente potrebno je uputiti na adresu:

office@safetysoftware.eu
Predmet poruke: SECURITY

Prijave se analiziraju sukladno internom postupku obrade incidenata.

10. Usklađenost i jurisdikcija

1. Sigurnosne mjere projektiraju se i održavaju uzimajući u obzir važeće propise, uključujući zahtjeve **GDPR-a**, te priznate prakse sigurnosti informacija.

2. Mjerodavno pravo je poljsko pravo.

3. U slučaju odstupanja između jezičnih verzija, mjerodavna je poljska verzija.

11. Stupanje na snagu

Ova verzija Politike sigurnosti vrijedi od **2026-03-05**.

Važeća verzija dokumenta objavljuje se u servisu Safety Software.

Voditelj obrade podataka i vlasnik sustava:
Safety Software Sp. z o.o.

ul. Półłanki 80
30-740 Kraków, Poljska
E-mail: **office@safetysoftware.eu**

Dnevnik promjena

Ažuriranje: 2026-03-05

- precizirane su slojevite sigurnosne kopije te postupak obnove podataka (BCP/DR)
- dopunjen je opis šifriranja podataka o omotni model i vanjsko upravljanje ključevima
- proširen je opis aplikacijske zaštite o sesije, CSRF, CSP i mehanizme protiv zlouporabe
- dodana je sekcija nadzora i upozorenja te je pojednostavljena sekcija integracije s vanjskim uslugama