Sikkerhedspolitik

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

Sikkerhedspolitik for Safety Software-applikationen (SaaS)

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

1. Formål og omfang

Denne sikkerhedspolitik fastsætter reglerne for beskyttelse af informationer og data, der behandles som led i Safety Software-applikationen, som stilles til rådighed i Software as a Service (SaaS)-modellen.

Dokumentet vedrører sikkerheden for brugere, der anvender applikationen i Safety Software-tjenesten, og udgør et supplement til Vilkår og betingelser samt Privatlivspolitikken.

Politikken er af informativ karakter og beskriver de grundlæggende tekniske og organisatoriske foranstaltninger, der anvendes af Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polen (herefter: „Administrator”).

2. Ansvarsmodel

Systemet fungerer efter en model med delt ansvar:

1. **Administrator (Safety Software)** er ansvarlig for sikkerheden i applikationskoden, login-, autorisations- og sessionsmekanismer, beskyttelse af data på applikationslaget, udførelse af sikkerhedskopier samt håndtering af sikkerhedshændelser.

2. **Leverandører af infrastruktur og hjælpeydelser** er ansvarlige for sikkerheden af de elementer, der ligger inden for rammerne af de ydelser, de leverer.

3. **Kunden** er ansvarlig for sikkerheden af sine enheder, adgangskoder, brugeridentiteter samt administration af adgange i sit team.

3. Principper for applikationssikkerhed

1. Datatransmission sker udelukkende ved brug af TLS-kryptering.

2. Brugersessioner er sikret ved brug af cookies med attributterne **HttpOnly**, **Secure** (for krypterede forbindelser) samt **SameSite**. Efter autentifikation sker der rotation af sessionsidentifikatoren.

3. For sessioner anvendes der grænser for inaktivitet samt maksimal varighed.

4. Anmodninger, der ændrer systemets tilstand, er sikret med CSRF-tokens, der verificeres på serversiden.

5. Applikationen anvender en restriktiv content security policy, herunder mekanismer, der begrænser udførelse af uautoriserede scripts, samt standardiserede sikkerhedsheaders i browseren.

6. Der anvendes mekanismer, der begrænser misbrug, herunder rate limiting samt beskyttelse mod brute-force-loginforsøg.

7. Hver operation udføres i konteksten af bruger og organisation; uautoriseret adgang blokeres.

4. Kryptering og databeskyttelse

1. Brugeres adgangskoder opbevares ved brug af algoritmen **bcrypt**.

2. Udvalgte følsomme data, der lagres i databasen, beskyttes ved brug af en envelope-krypteringsmodel. Kryptografiske nøgler forvaltes separat i et eksternt nøglehåndteringssystem.

3. Hvor det er begrundet, anvendes mekanismer, der begrænser dataeksponering, samtidig med at søge- eller identifikationsfunktioner bevares, uden nødvendigheden af at lagre fulde værdier i klartekst.

5. Backup og gendannelse (BCP/DR)

1. Vi anvender en lagdelt tilgang til sikkerhedskopier: lokale kopier til hurtig gendannelse samt kopier, der opbevares uden for primærmiljøet.

2. Kopier, der opbevares uden for primærmiljøet, omfatter miljøbilleder udført inkrementelt. De er krypterede, valideres regelmæssigt og er omfattet af gendannelsestests.

3. Databasen sikres med applikationskonsistente kopier. Derudover opretholdes lokale database-dumps, der understøtter hurtig gendannelse.

4. Kopiernes integritet verificeres ved brug af kontrolmekanismer, herunder checksums.

5. Backup-processen er automatiseret, udføres dagligt og er omfattet af overvågning af opgave-succes og -fejl.

6. Der gennemføres regelmæssigt tests af datagendannelse, som mindst omfatter gendannelse af udvalgte filer.

6. Overvågning og alarmer

1. Systemet registrerer udvalgte sikkerhedshændelser samt administrative operationer, særligt relateret til autentifikation, adgangsforsøg og drift af kritiske processer.

2. Der anvendes overvågningsmekanismer samt automatiske alarmer ved opgavefejl, kritiske fejl og hændelser, der kan indikere misbrug eller en sikkerhedshændelse.

3. Adgang til logs og driftsinformation er begrænset til autoriserede personer.

7. Infrastruktur og opretholdelse af sikkerhed

1. Administrativ adgang er begrænset til autoriserede personer og sikret med mekanismer til stærk autentifikation, herunder autentifikation med nøgler.

2. Direkte login på en privilegeret konto er deaktiveret eller begrænset i overensstemmelse med princippet om mindste privilegium.

3. Der anvendes mekanismer til trafikfiltrering, beskyttelse mod brute-force-adgangsforsøg samt overvågning af infrastrukturhændelser.

4. Sikkerhedsopdateringer implementeres regelmæssigt.

5. Mailtjenester, der anvendes til drift af systemet, er sikret med transmissionskryptering samt mekanismer, der begrænser misbrug.

8. Leverandører og integrationer

1. I det omfang systemet anvender eksterne tjenester eller hjælpeintegrationer, tager valg af løsninger hensyn til datasikkerhed, minimeringsprincippet samt kontrol af omfanget af de oplysninger, der videregives.

2. Kommunikation med eksterne tjenester sker ved brug af krypteret transmission.

9. Indberetning af hændelser

Indberetninger vedrørende applikationens sikkerhed eller mistanke om hændelser skal sendes til adressen:

office@safetysoftware.eu
Emne: SECURITY

Indberetninger analyseres i overensstemmelse med den interne procedure for hændelseshåndtering.

10. Overholdelse og jurisdiktion

1. Sikkerhedsforanstaltningerne designes og vedligeholdes under hensyntagen til gældende lovgivning, herunder kravene i **GDPR**, samt anerkendte praksisser for informationssikkerhed.

2. Gældende ret er polsk ret.

3. I tilfælde af uoverensstemmelser mellem sprogversioner er den polske version

afgørende.

11. Ikrafttræden

Denne version af Sikkerhedspolitikken gælder fra og med **2026-03-05**.

Den aktuelle version af dokumentet offentliggøres i tjenesten Safety Software.

Dataansvarlig og systemejer:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polska
E-mail: **office@safetysoftware.eu**

Ændringslog

Opdatering: 2026-03-05

- præciseret lagdelte sikkerhedskopier samt processen for gendannelse af data (BCP/DR)
- suppleret beskrivelsen af datakryptering med envelope-modellen og ekstern nøglestyring
- udvidet beskrivelsen af applikationsbeskyttelse med sessioner, CSRF, CSP og anti-misbrugs-mekanismer
- tilføjet en sektion om overvågning og alarmer samt forenklet sektionen om integration med eksterne tjenester