Ohutuspoliitika

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

Safety Software (SaaS) rakenduse turvapoliitika

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

1. Eesmärk ja ulatus

Käesolev turvapoliitika määratleb teabe ja andmete kaitse põhimõtted, mida töödeldakse Safety Software rakenduse raames, mida pakutakse Software as a Service (SaaS) mudelis.

Dokument käsitleb Safety Software teenuses rakendust kasutavate kasutajate turvalisust ning on täienduseks kasutustingimustele ja privaatsuspoliitikale.

Põhimõtted on informatiivse iseloomuga ja kirjeldavad põhilisi tehnilisi ja organisatsioonilisi meetmeid, mida rakendab Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Poola (edaspidi „Administraator”).

2. Vastutusmudel

Süsteem toimib jagatud vastutuse mudelis:

1. **Administraator (Safety Software)** vastutab rakenduse koodi turvalisuse, sisselogimise, autoriseerimise ja seansimehhanismide, andmekaitse rakenduskihis, varukoopiate tegemise ning turbeintsidentidele reageerimise eest.

2. **Taristu ja abiteenuste pakkujad** vastutavad nende teenuste ulatusse jäävate komponentide turvalisuse eest.

3. **Klient** vastutab oma seadmete, paroolide, kasutajate identiteetide turvalisuse ning oma meeskonnas juurdepääsude haldamise eest.

3. Rakenduse turvapõhimõtted

1. Andmeedastus toimub üksnes TLS-krüptimise abil.

2. Kasutajaseansid on kaitstud küpsiste abil, millel on atribuudid **HttpOnly**, **Secure** (krüptitud ühenduste jaoks) ning **SameSite**. Pärast autentimist toimub seansiidentifikaatori rotatsioon.

3. Seanssidele rakendatakse tegevusetuse piiranguid ning maksimaalset kestust.

4. Süsteemi olekut muutvad päringud on kaitstud CSRF-tokenitega, mida kontrollitakse serveripoolel.

5. Rakendus kasutab ranget sisuturbe poliitikat, sh mehhanisme, mis piiravad volitamata skriptide käivitamist, ning standardseid brauseri turvapäringupäiseid.

6. Kasutatakse väärkasutuse piiramise mehhanisme, sh rate limiting ning kaitse jõurünnakute (brute force) teel sisselogimiskatsete vastu.

7. Iga toiming sooritatakse kasutaja ja organisatsiooni kontekstis; volitamata juurdepääs blokeeritakse.

4. Krüptimine ja andmekaitse

1. Kasutajate paroolid talletatakse algoritmi **bcrypt** abil.

2. Valitud andmebaasis talletatavad tundlikud andmed on kaitstud ümbrikkrüptimise (envelope encryption) mudeli abil. Krüptovõtmeid hallatakse eraldi välises võtmehaldussüsteemis.

3. Seal, kus see on põhjendatud, kasutatakse mehhanisme, mis piiravad andmete eksponeerimist, säilitades otsingu- või identifitseerimisfunktsioonid, ilma et oleks vaja hoida täielikke väärtusi avatekstina.

5. Varundus ja taastamine (BCP/DR)

1. Kasutame varukoopiate kihilist lähenemist: lokaalsed koopiad kiireks taastamiseks ning koopiad, mida hoitakse põhikeskkonnast väljaspool.

2. Põhikeskkonnast väljaspool hoitavad koopiad hõlmavad keskkonna pilte, mida tehakse inkrementaalselt. Need on krüptitud, regulaarselt valideeritud ja hõlmatud

taastamistestidega.

3. Andmebaasi kaitstakse rakendusetasandil koherentsete koopiatega. Lisaks hoitakse lokaalseid andmebaasi tõmmiseid (dump), mis toetavad kiiret taastamist.

4. Koopiate terviklust kontrollitakse kontrollmehhanismide abil, sh kontrollsummadega.

5. Varundusprotsess on automatiseeritud, toimub igapäevaselt ning on kaetud õnnestumise ja ebaõnnestumise monitooringuga.

6. Regulaarselt viiakse läbi andmete taastamisteste, mis hõlmavad vähemalt valitud failide taastamist.

6. Monitooring ja teavitused

1. Süsteem registreerib valitud turbesündmusi ning administratiivseid toiminguid, eelkõige autentimise, juurdepääsukatsete ja kriitiliste protsesside toimimisega seotud sündmusi.

2. Kasutatakse monitooringumehhanisme ning automaatseid teavitusi ülesannete ebaõnnestumise, kriitiliste vigade ja sündmuste kohta, mis võivad viidata väärkasutusele või turbeintsidendile.

3. Juurdepääs logidele ja operatiivinfole on piiratud volitatud isikutega.

7. Taristu ja turbehaldused

1. Administraatori juurdepääs on piiratud volitatud isikutega ja kaitstud tugeva autentimise mehhanismidega, sh võtmetega autentimisega.

2. Otsene sisselogimine privileegitud kontole on välja lülitatud või piiratud vastavalt minimaalse õiguse põhimõttele.

3. Kasutatakse liikluse filtreerimise mehhanisme, kaitset jõurünnakute (brute force) juurdepääsukatsete vastu ning taristutaseme sündmuste monitooringut.

4. Turvauuendusi rakendatakse regulaarselt.

5. Süsteemi teenindamiseks kasutatavad e-posti teenused on kaitstud edastuse krüptimise ning väärkasutust piiravate mehhanismidega.

8. Tarnijad ja integratsioonid

1. Ulatuses, milles süsteem kasutab väliseid teenuseid või abiintegratsioone, arvestab lahenduste valik andmeturvet, minimaliseerimise põhimõtet ning edastatava teabe ulatuse kontrolli.

2. Suhtlus väliste teenustega toimub krüptitud andmeedastuse abil.

9. Intsidentidest teatamine

Rakenduse turvalisusega seotud teated või intsidentide kahtlused tuleb saata aadressile:

office@safetysoftware.eu
Sõnumi teema: SECURITY

Teated analüüsitakse vastavalt sisemisele intsidentide käsitlemise protseduurile.

10. Vastavus ja jurisdiktsioon

1. Turvameetmed on kavandatud ja hallatud, arvestades kehtivaid õigusakte, sh **GDPR** nõudeid, ning tunnustatud infoturbe praktikaid.

2. Kohaldatav õigus on Poola õigus.

3. Keelteversioonide vaheliste vastuolude korral on määrav poolakeelne versioon.

11. Jõustumine

Käesolev Turbepoliitika versioon kehtib alates **2026-03-05**.

Dokumendi kehtiv versioon avaldatakse Safety Software teenuses.

Andmete vastutav töötleja ja süsteemi omanik:
Safety Software Sp. z o.o.

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

Muutuste logi

Uuendus: 2026-03-05

- täpsustati kihilised varukoopiad ning andmete taastamise protsess (BCP/DR)
- täiendati andmete krüpteerimise kirjeldust ümbrikumudeliga ja välise võtmehaldusega
- laiendati rakendusekaitse kirjeldust seansside, CSRF-i, CSP ja kuritarvitusvastaste mehhanismidega
- lisati seire ja häirete sektsioon ning lihtsustati väliste teenustega integreerimise sektsiooni