Saugumo politika

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

Safety Software (SaaS) aplikacijos saugumo politika

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

1. Tikslas ir taikymo sritis

Ši Saugumo politika nustato informacijos ir duomenų, tvarkomų naudojantis Safety Software taikomąja programa, teikiama Software as a Service (SaaS) modeliu, apsaugos taisykles.

Dokumentas taikomas naudotojų, besinaudojančių programa Safety Software paslaugoje, saugumui ir papildo Taisykles bei Privatumo politiką.

Politika yra informacinio pobūdžio ir aprašo pagrindines technines ir organizacines priemones, kurias taiko Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Krokuva, Lenkija (toliau – „Administratorius“).

2. Atsakomybės modelis

Sistema veikia bendros (pasidalytos) atsakomybės modeliu:

1. **Administratorius (Safety Software)** atsako už programos kodo saugumą, prisijungimo, autorizavimo ir sesijų mechanizmus, duomenų apsaugą programos sluoksnyje, atsarginių kopijų darymą bei reagavimą į saugumo incidentus.

2. **Infrastruktūros ir pagalbinių paslaugų teikėjai** atsako už elementų, patenkančių į jų teikiamų paslaugų apimtį, saugumą.

3. **Klientas** atsako už savo įrenginių, slaptažodžių, naudotojų tapatybių saugumą bei prieigų valdymą savo komandoje.

3. Programos saugumo taisyklės

1. Duomenų perdavimas vyksta tik naudojant TLS šifravimą.

2. Naudotojų sesijos apsaugomos naudojant slapukus su atributais **HttpOnly**, **Secure** (šifruotiems ryšiams) ir **SameSite**. Po autentifikavimo atliekama sesijos identifikatoriaus rotacija.

3. Sesijoms taikomi neaktyvumo ir maksimalaus galiojimo trukmės limitai.

4. Užklausos, keičiančios sistemos būseną, apsaugomos CSRF žetonais, kurie tikrinami serverio pusėje.

5. Programa taiko griežtą turinio saugumo politiką, įskaitant mechanizmus, ribojančius neautorizuotų scenarijų vykdymą, ir standartines naršyklės saugumo antraštes.

6. Taikomi mechanizmai, ribojantys piktnaudžiavimą, įskaitant rate limiting ir apsaugą nuo bruteforce prisijungimo bandymų.

7. Kiekviena operacija atliekama naudotojo ir organizacijos kontekste; neautorizuota prieiga blokuojama.

4. Šifravimas ir duomenų apsauga

1. Naudotojų slaptažodžiai saugomi naudojant **bcrypt** algoritmą.

2. Pasirinkti jautrūs duomenys, saugomi duomenų bazėje, apsaugomi naudojant duomenų šifravimo vokelio (envelope encryption) modelį. Kriptografiniai raktai valdomi atskirai išorinėje raktų valdymo sistemoje.

3. Ten, kur tai pagrįsta, taikomi mechanizmai, ribojantys duomenų atskleidimą, išlaikant paieškos ar identifikavimo funkcijas, be būtinybės saugoti pilnas reikšmes atviru pavidalu.

5. Atsarginės kopijos ir atkūrimas (BCP/DR)

1. Taikome sluoksninį atsarginių kopijų metodą: vietinės kopijos greitam atkūrimui ir kopijos, saugomos už pagrindinės aplinkos ribų.

2. Kopijos, saugomos už pagrindinės aplinkos ribų, apima aplinkos atvaizdus,

daromus inkrementiškai. Jos yra šifruojamos, reguliariai validuojamos ir joms taikomi atkūrimo testai.

3. Duomenų bazė apsaugoma taikant programos lygmeniu suderintas (aplikaciškai nuoseklias) kopijas. Papildomai palaikomi vietiniai duomenų bazės išklotiniai, padedantys greitam atkūrimui.

4. Kopijų vientisumas tikrinamas naudojant kontrolės mechanizmus, įskaitant kontrolines sumas.

5. Atsarginių kopijų darymo procesas automatizuotas, vykdomas kasdien ir stebimas pagal užduočių sėkmę bei nesėkmes.

6. Reguliariai atliekami duomenų atkūrimo testai, apimantys bent pasirinktų failų atkūrimą.

6. Stebėsena ir įspėjimai

1. Sistema registruoja pasirinktus saugumo įvykius ir administracines operacijas, ypač susijusias su autentifikavimu, prieigos bandymais ir kritinių procesų veikimu.

2. Taikomi stebėsenos mechanizmai ir automatiniai įspėjimai apie užduočių nesėkmes, kritines klaidas ir įvykius, galinčius rodyti piktnaudžiavimą ar saugumo incidentą.

3. Prieiga prie žurnalų (logų) ir operacinės informacijos apribota įgaliotiems asmenims.

7. Infrastruktūra ir saugumo palaikymas

1. Administracinė prieiga apribota įgaliotiems asmenims ir apsaugota stipraus autentifikavimo mechanizmais, įskaitant autentifikavimą raktais.

2. Tiesioginis prisijungimas prie privilegijuotos paskyros išjungtas arba apribotas pagal minimalių teisių principą.

3. Taikomi srauto filtravimo mechanizmai, apsauga nuo bruteforce prieigos bandymų

ir infrastruktūrinių įvykių stebėsena.

4. Saugumo atnaujinimai diegiami reguliariai.

5. Pašto paslaugos, naudojamos sistemos aptarnavimui, apsaugotos perdavimo šifravimu ir mechanizmais, ribojančiais piktnaudžiavimą.

8. Tiekėjai ir integracijos

1. Tiek, kiek sistema naudojasi išorinėmis paslaugomis ar pagalbinėmis integracijomis, sprendimų parinkimas atsižvelgia į duomenų saugumą, minimalizavimo principą ir perduodamos informacijos apimties kontrolę.

2. Komunikacija su išorinėmis paslaugomis vyksta naudojant šifruotą perdavimą.

9. Incidentų pranešimas

Pranešimus, susijusius su programos saugumu arba įtarimais dėl incidentų, prašome siųsti adresu:

office@safetysoftware.eu
Laiško tema: SECURITY

Pranešimai analizuojami pagal vidinę incidentų valdymo procedūrą.

10. Atitiktis ir jurisdikcija

1. Saugumo priemonės projektuojamos ir palaikomos atsižvelgiant į galiojančius teisės aktus, įskaitant **BDAR** reikalavimus, ir pripažintą informacijos saugumo praktiką.

2. Taikytina teisė yra Lenkijos teisė.

3. Esant neatitikimų tarp kalbinių versijų, lemiama yra lenkų kalbos versija.

11. Įsigaliojimas

Ši Saugumo politikos versija galioja nuo **2026-03-05**.

Aktuali dokumento versija skelbiama Safety Software paslaugoje.

Duomenų administratorius ir sistemos savininkas:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Krokuva, Lenkija
El. paštas: **office@safetysoftware.eu**

Pakeitimų žurnalas

Atnaujinimas: 2026-03-05

- patikslintos sluoksninės atsarginės kopijos ir duomenų atkūrimo procesas (BCP/DR)
- papildytas duomenų šifravimo aprašas vokinio modelio ir išorinio raktų valdymo informacija
- išplėstas taikomosios apsaugos aprašas, įtraukiant sesijas, CSRF, CSP ir anti-piktnaudžiavimo mechanizmus
- pridėta stebėsenos ir įspėjimų skiltis bei supaprastinta integracijos su išorinėmis paslaugomis skiltis