Turvallisuuspolitiikka

Safety Software -sovelluksen turvallisuuskäytäntö (SaaS)

ID: SE-2026-V2
Päivitys: 2026-03-05

1. Tarkoitus ja soveltamisala

Tässä turvallisuuskäytännössä määritellään periaatteet Safety Software -sovelluksessa käsiteltävien tietojen ja datan suojaamiseksi, kun sovellus tarjotaan Software as a Service (SaaS) -mallilla.

Dokumentti koskee Safety Software -palvelussa sovellusta käyttävien käyttäjien turvallisuutta ja toimii käyttöehtojen sekä tietosuojakäytännön täydennyksenä.

Käytännöllä on informatiivinen luonne ja siinä kuvataan Safety Software Sp. z o.o.:n, ul. Półłanki 80, 30-740 Kraków, Puola (jäljempänä ”Rekisterinpitäjä”), soveltamat keskeiset tekniset ja organisatoriset toimenpiteet.

2. Vastuumalli

Järjestelmä toimii jaetun vastuun mallilla:

1. **Rekisterinpitäjä (Safety Software)** vastaa sovelluskoodin turvallisuudesta, kirjautumis-, valtuutus- ja istuntomekanismeista, tietojen suojauksesta sovelluskerroksessa, varmuuskopioiden tekemisestä sekä tietoturvapoikkeamiin reagoinnista.

2. **Infrastruktuurin ja tukipalvelujen toimittajat** vastaavat niiden palvelujen piiriin kuuluvien elementtien turvallisuudesta.

3. **Asiakas** vastaa omien laitteidensa, salasanojensa, käyttäjien identiteettien turvallisuudesta sekä käyttöoikeuksien hallinnasta omassa tiimissään.

3. Sovelluksen turvallisuusperiaatteet

1. Tiedonsiirto tapahtuu yksinomaan TLS-salauksella.

2. Käyttäjäistunnot suojataan evästeillä, joilla on attribuutit **HttpOnly**, **Secure** (salattuja yhteyksiä varten) sekä **SameSite**. Tunnistautumisen jälkeen istunnon tunniste rotaatioidaan.

3. Istunnoille sovelletaan toimettomuusrajoja sekä enimmäiskestoa.

4. Järjestelmän tilaa muuttavat pyynnöt suojataan palvelinpuolella validoitavilla CSRF-tokeneilla.

5. Sovellus käyttää tiukkaa sisällön turvallisuuskäytäntöä, mukaan lukien mekanismit, jotka rajoittavat luvattomien skriptien suorittamista, sekä selaimen vakiomuotoiset tietoturvaotsakkeet.

6. Käytössä on väärinkäyttöä rajoittavia mekanismeja, mukaan lukien rate limiting sekä suojaus kirjautumisen brute force -yrityksiä vastaan.

7. Jokainen toiminto suoritetaan käyttäjän ja organisaation kontekstissa; luvaton pääsy estetään.

4. Salaus ja tietojen suojaus

1. Käyttäjien salasanat tallennetaan käyttäen **bcrypt**-algoritmia.

2. Valitut tietokantaan tallennetut arkaluonteiset tiedot suojataan käyttämällä envelope-salausmallia. Kryptografisia avaimia hallitaan erikseen ulkoisessa avaintenhallintajärjestelmässä.

3. Siellä missä se on perusteltua, käytetään mekanismeja, jotka rajoittavat tietojen altistumista säilyttäen haku- tai tunnistustoiminnot, ilman tarvetta tallentaa täydellisiä arvoja selväkielisinä.

5. Varmuuskopiointi ja palautus (BCP/DR)

1. Käytämme kerroksellista varmuuskopiointilähestymistapaa: paikalliset kopiot nopeaa palautusta varten sekä kopiot, jotka säilytetään ensisijaisen ympäristön ulkopuolella.

2. Ensisijaisen ympäristön ulkopuolella säilytettävät kopiot sisältävät ympäristökuvia, jotka tehdään inkrementaalisesti. Ne salataan, validoidaan säännöllisesti ja ne kuuluvat palautustestauksen piiriin.

3. Tietokanta suojataan sovellustasolla johdonmukaisilla varmuuskopioilla. Lisäksi ylläpidetään paikallisia tietokantadumppauksia nopean palautuksen tukemiseksi.

4. Varmuuskopioiden eheys varmistetaan valvontamekanismeilla, mukaan lukien tarkistussummat.

5. Varmuuskopiointiprosessi on automatisoitu, suoritetaan päivittäin ja sitä monitoroidaan tehtävien onnistumisten sekä epäonnistumisten osalta.

6. Tietojen palautustestauksia tehdään säännöllisesti, kattaen vähintään valittujen tiedostojen palautuksen.

6. Valvonta ja hälytykset

1. Järjestelmä kirjaa valittuja tietoturvatapahtumia sekä hallinnollisia toimintoja, erityisesti tunnistautumiseen, pääsyyrityksiin ja kriittisten prosessien toimintaan liittyen.

2. Käytössä ovat valvontamekanismit sekä automaattiset hälytykset tehtävien epäonnistumisista, kriittisistä virheistä ja tapahtumista, jotka voivat viitata väärinkäyttöön tai tietoturvapoikkeamaan.

3. Pääsy lokitietoihin ja operatiivisiin tietoihin on rajoitettu valtuutettuihin henkilöihin.

7. Infrastruktuuri ja turvallisuuden ylläpito

1. Ylläpitäjätason pääsy on rajoitettu valtuutettuihin henkilöihin ja suojattu vahvan

tunnistautumisen mekanismeilla, mukaan lukien avainpohjainen tunnistautuminen.

2. Suora kirjautuminen etuoikeutetulle tilille on poistettu käytöstä tai rajoitettu vähimpien oikeuksien periaatteen mukaisesti.

3. Käytössä ovat liikenteen suodatusmekanismit, suojaus brute force -pääsyyrityksiä vastaan sekä infrastruktuuritapahtumien valvonta.

4. Turvallisuuspäivityksiä otetaan käyttöön säännöllisesti.

5. Järjestelmän ylläpidossa käytettävät sähköpostipalvelut on suojattu tiedonsiirron salauksella sekä väärinkäyttöä rajoittavilla mekanismeilla.

8. Toimittajat ja integraatiot

1. Siltä osin kuin järjestelmä käyttää ulkoisia palveluja tai tukevia integraatioita, ratkaisujen valinnassa huomioidaan tietoturva, minimointiperiaate sekä siirrettävien tietojen laajuuden hallinta.

2. Viestintä ulkoisten palvelujen kanssa tapahtuu salatun tiedonsiirron avulla.

9. Poikkeamien ilmoittaminen

Sovelluksen turvallisuutta koskevat ilmoitukset tai poikkeamaepäilyt tulee lähettää osoitteeseen:

office@safetysoftware.eu
Viestin aihe: SECURITY

Ilmoitukset analysoidaan sisäisen poikkeamien käsittelymenettelyn mukaisesti.

10. Vaatimustenmukaisuus ja toimivalta

1. Turvatoimenpiteet suunnitellaan ja ylläpidetään sovellettavan lainsäädännön vaatimukset huomioiden, mukaan lukien **GDPR**-vaatimukset, sekä tunnustettujen tietoturvakäytäntöjen mukaisesti.

2. Sovellettava laki on Puolan laki.

3. Kieliversioiden välisissä ristiriitatilanteissa ratkaiseva on puolankielinen versio.

11. Voimaantulo

Tämä Tietoturvakäytännön versio on voimassa alkaen **2026-03-05**.

Asiakirjan ajantasainen versio julkaistaan Safety Software -palvelussa.

Rekisterinpitäjä ja järjestelmän omistaja:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Puola
Sähköposti: **office@safetysoftware.eu**

Muutosloki

Päivitys: 2026-03-05

- täsmennettiin kerrokselliset varmuuskopiot sekä tietojen palautusprosessi (BCP/DR)
- täydennettiin tietojen salauksen kuvausta kirjekuorimallilla ja ulkoisella avaintenhallinnalla
- laajennettiin sovellussuojauksen kuvausta sessioilla, CSRF:llä, CSP:llä ja väärinkäytön estomekanismeilla
- lisättiin seuranta- ja hälytysosio sekä yksinkertaistettiin ulkoisten palvelujen integraatio-osiota