Säkerhetspolicy

Säkerhetspolicy för applikationen Safety Software (SaaS)

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

1. Syfte och omfattning

Denna säkerhetspolicy anger reglerna för skydd av information och data som behandlas inom ramen för applikationen Safety Software som tillhandahålls enligt modellen Software as a Service (SaaS).

Dokumentet avser säkerheten för användare som använder applikationen i tjänsten Safety Software och utgör ett komplement till Reglerna samt Integritetspolicyn.

Policyn är av informativ karaktär och beskriver grundläggande tekniska och organisatoriska åtgärder som tillämpas av Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polen (nedan: ”Administratören”).

2. Ansvarsmodell

Systemet fungerar enligt en modell för delat ansvar:

1. **Administratören (Safety Software)** ansvarar för säkerheten i applikationskoden, inloggnings-, behörighets- och sessionsmekanismer, skydd av data på applikationsnivå, genomförande av säkerhetskopior samt hantering av säkerhetsincidenter.

2. **Leverantörer av infrastruktur och stödtjänster** ansvarar för säkerheten för de komponenter som omfattas av de tjänster de tillhandahåller.

3. **Kunden** ansvarar för säkerheten för sina enheter, lösenord, användaridentiteter samt hantering av åtkomster inom sitt team.

3. Principer för applikationssäkerhet

1. Dataöverföring sker uteslutande med användning av TLS-kryptering.

2. Användarsessioner säkras med hjälp av cookies med attributen **HttpOnly**, **Secure** (för krypterade anslutningar) samt **SameSite**. Efter autentisering sker rotation av sessionsidentifieraren.

3. För sessioner tillämpas gränser för inaktivitet samt maximal varaktighet.

4. Begäranden som ändrar systemets tillstånd skyddas med CSRF-token som verifieras på serversidan.

5. Applikationen tillämpar en restriktiv policy för innehållssäkerhet, inklusive mekanismer som begränsar körning av obehöriga skript samt standardiserade säkerhetsheaders för webbläsare.

6. Mekanismer för att begränsa missbruk tillämpas, inklusive rate limiting samt skydd mot brute force-inloggningsförsök.

7. Varje åtgärd utförs i kontexten av användare och organisation; obehörig åtkomst blockeras.

4. Kryptering och dataskydd

1. Användarlösenord lagras med algoritmen **bcrypt**.

2. Utvalda känsliga data som lagras i databasen skyddas med hjälp av en envelope-krypteringsmodell. Kryptografiska nycklar hanteras separat i ett externt nyckelhanteringssystem.

3. Där det är motiverat tillämpas mekanismer som begränsar exponeringen av data samtidigt som funktioner för sökning eller identifiering bibehålls, utan behov av att lagra fullständiga värden i klartext.

5. Backup och återställning (BCP/DR)

1. Vi tillämpar en lagerbaserad strategi för säkerhetskopior: lokala kopior för snabb återställning samt kopior som lagras utanför den primära miljön.

2. Kopior som lagras utanför den primära miljön omfattar miljöavbildningar som tas inkrementellt. De är krypterade, valideras regelbundet och omfattas av återställningstester.

3. Databasen säkras med applikationskonsistenta kopior. Dessutom upprätthålls lokala databasutskrifter som stödjer snabb återställning.

4. Integriteten hos kopior verifieras med kontrollmekanismer, inklusive kontrollsummor.

5. Backup-processen är automatiserad, körs dagligen och övervakas avseende lyckade och misslyckade jobb.

6. Återställningstester av data genomförs regelbundet och omfattar minst återställning av utvalda filer.

6. Övervakning och larm

1. Systemet loggar utvalda säkerhetshändelser samt administrativa åtgärder, i synnerhet sådana som är kopplade till autentisering, åtkomstförsök och drift av kritiska processer.

2. Övervakningsmekanismer och automatiska larm vid misslyckade jobb, kritiska fel och händelser som kan indikera missbruk eller en säkerhetsincident tillämpas.

3. Åtkomst till loggar och driftinformation är begränsad till behöriga personer.

7. Infrastruktur och upprätthållande av säkerhet

1. Administrativ åtkomst är begränsad till behöriga personer och skyddas med mekanismer för stark autentisering, inklusive autentisering med nycklar.

2. Direkt inloggning på privilegierat konto är inaktiverad eller begränsad enligt principen om minsta privilegium.

3. Mekanismer för trafikfiltrering, skydd mot brute force-åtkomstförsök samt övervakning av infrastrukturella händelser tillämpas.

4. Säkerhetsuppdateringar implementeras regelbundet.

5. E-posttjänster som används för att driva systemet skyddas med krypterad överföring samt mekanismer som begränsar missbruk.

8. Leverantörer och integrationer

1. I den utsträckning systemet använder externa tjänster eller stödintegrationer beaktar valet av lösningar datasäkerhet, principen om minimering samt kontroll av omfattningen av den information som överförs.

2. Kommunikation med externa tjänster sker med användning av krypterad överföring.

9. Rapportering av incidenter

Anmälningar som rör applikationens säkerhet eller misstanke om incidenter ska skickas till adressen:

office@safetysoftware.eu
Ämne: SECURITY

Anmälningar analyseras i enlighet med den interna rutinen för incidenthantering.

10. Efterlevnad och jurisdiktion

1. Säkerhetsåtgärderna utformas och upprätthålls med beaktande av gällande lagstiftning, inklusive kraven i **GDPR**, samt erkända praxis för informationssäkerhet.

2. Tillämplig lag är polsk rätt.

3. Vid avvikelser mellan språkversioner är den polska versionen avgörande.

11. Ikraftträdande

Denna version av Säkerhetspolicyn gäller från och med **2026-03-05**.

Den aktuella versionen av dokumentet publiceras i tjänsten Safety Software.

Personuppgiftsansvarig och systemägare:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polen
E-post: **office@safetysoftware.eu**

Ändringslogg

Uppdatering: 2026-03-05

- förtydligade flerskiktade säkerhetskopior samt processen för återställning av data (BCP/DR)
- kompletterade beskrivningen av datakryptering med kuvertmodell och extern nyckelhantering
- utökade beskrivningen av applikationsskydd med sessioner, CSRF, CSP och mekanismer mot missbruk
- lade till ett avsnitt om övervakning och larm samt förenklade avsnittet om integration med externa tjänster