Politica di Sicurezza

Politica di Sicurezza dell’Applicazione Safety Software (SaaS)

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

1. Scopo e ambito

La presente Politica di Sicurezza definisce le regole di protezione delle informazioni e dei dati trattati nell’ambito dell’applicazione Safety Software resa disponibile nel modello Software as a Service (SaaS).

Il documento riguarda la sicurezza degli utenti che utilizzano l’applicazione nel servizio Safety Software e costituisce un’integrazione del Regolamento e della Politica sulla Privacy.

La Politica ha carattere informativo e descrive le misure tecniche e organizzative di base applicate da Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Cracovia, Polonia (di seguito: “Amministratore”).

2. Modello di responsabilità

Il sistema opera secondo un modello di responsabilità condivisa:

1. **Amministratore (Safety Software)** è responsabile della sicurezza del codice dell’applicazione, dei meccanismi di accesso, autorizzazione e sessione, della protezione dei dati a livello applicativo, dell’esecuzione dei backup e della risposta agli incidenti di sicurezza.

2. **Fornitori di infrastruttura e servizi ausiliari** sono responsabili della sicurezza degli elementi che rientrano nell’ambito dei servizi da essi forniti.

3. **Cliente** è responsabile della sicurezza dei propri dispositivi, delle password, delle identità degli utenti e della gestione degli accessi all’interno del proprio team.

3. Principi di sicurezza dell’applicazione

1. La trasmissione dei dati avviene esclusivamente con l’uso della crittografia TLS.

2. Le sessioni degli utenti sono protette mediante cookie con gli attributi **HttpOnly**, **Secure** (per le connessioni cifrate) e **SameSite**. Dopo l’autenticazione avviene la rotazione dell’identificatore di sessione.

3. Per le sessioni sono applicati limiti di inattività e di durata massima.

4. Le richieste che modificano lo stato del sistema sono protette da token CSRF verificati lato server.

5. L’applicazione applica una rigorosa policy di sicurezza dei contenuti, incluse misure che limitano l’esecuzione di script non autorizzati e le intestazioni di sicurezza standard del browser.

6. Sono applicati meccanismi che limitano gli abusi, inclusi rate limiting e protezione contro tentativi di accesso a forza bruta.

7. Ogni operazione è eseguita nel contesto dell’utente e dell’organizzazione; l’accesso non autorizzato è bloccato.

4. Crittografia e protezione dei dati

1. Le password degli utenti sono memorizzate utilizzando l’algoritmo **bcrypt**.

2. Determinati dati sensibili memorizzati nel database sono protetti mediante un modello di crittografia dei dati a busta (envelope encryption). Le chiavi crittografiche sono gestite separatamente in un sistema esterno di gestione delle chiavi.

3. Laddove giustificato, sono applicati meccanismi che limitano l’esposizione dei dati mantenendo le funzionalità di ricerca o identificazione, senza la necessità di memorizzare i valori completi in chiaro.

5. Backup e ripristino (BCP/DR)

1. Applichiamo un approccio stratificato ai backup: copie locali per un ripristino rapido e copie conservate al di fuori dell’ambiente principale.

2. Le copie conservate al di fuori dell’ambiente principale includono immagini dell’ambiente eseguite in modo incrementale. Sono cifrate, validate regolarmente e sottoposte a test di ripristino.

3. Il database è protetto mediante copie coerenti a livello applicativo. Inoltre, sono mantenuti dump locali del database a supporto di un ripristino rapido.

4. L’integrità delle copie è verificata mediante meccanismi di controllo, inclusi checksum.

5. Il processo di esecuzione dei backup è automatizzato, eseguito quotidianamente e sottoposto a monitoraggio dell’esito positivo e negativo delle attività.

6. Vengono effettuati regolarmente test di ripristino dei dati, includendo almeno il ripristino di file selezionati.

6. Monitoraggio e avvisi

1. Il sistema registra eventi di sicurezza selezionati e operazioni amministrative, in particolare quelle relative all’autenticazione, ai tentativi di accesso e al funzionamento dei processi critici.

2. Sono applicati meccanismi di monitoraggio e avvisi automatici in caso di esito negativo delle attività, errori critici ed eventi che possono indicare un abuso o un incidente di sicurezza.

3. L’accesso ai log e alle informazioni operative è limitato alle persone autorizzate.

7. Infrastruttura e mantenimento della sicurezza

1. L’accesso amministrativo è limitato alle persone autorizzate ed è protetto da meccanismi di autenticazione forte, inclusa l’autenticazione tramite chiavi.

2. L’accesso diretto a un account privilegiato è disabilitato o limitato in conformità al principio del minimo privilegio.

3. Sono applicati meccanismi di filtraggio del traffico, protezione contro tentativi di accesso a forza bruta e monitoraggio degli eventi infrastrutturali.

4. Gli aggiornamenti di sicurezza sono implementati regolarmente.

5. I servizi di posta elettronica utilizzati per la gestione del sistema sono protetti tramite crittografia della trasmissione e meccanismi che limitano gli abusi.

8. Fornitori e integrazioni

1. Nella misura in cui il sistema utilizza servizi esterni o integrazioni ausiliarie, la selezione delle soluzioni tiene conto della sicurezza dei dati, del principio di minimizzazione e del controllo dell’ambito delle informazioni trasmesse.

2. La comunicazione con i servizi esterni avviene mediante trasmissione cifrata.

9. Segnalazione degli incidenti

Le segnalazioni relative alla sicurezza dell’applicazione o al sospetto di incidenti devono essere inviate all’indirizzo:

office@safetysoftware.eu
Oggetto del messaggio: SECURITY

Le segnalazioni sono analizzate secondo la procedura interna di gestione degli incidenti.

10. Conformità e giurisdizione

1. Le misure di sicurezza sono progettate e mantenute tenendo conto delle disposizioni di legge applicabili, inclusi i requisiti del **GDPR**, nonché delle pratiche riconosciute di sicurezza delle informazioni.

2. La legge applicabile è la legge polacca.

3. In caso di discrepanze tra le versioni linguistiche, prevale la versione polacca.

11. Entrata in vigore

La presente versione della Politica di Sicurezza è in vigore dal **2026-03-05**.

La versione corrente del documento è pubblicata nel servizio Safety Software.

Amministratore dei dati e proprietario del sistema:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Cracovia, Polonia
E-mail: **office@safetysoftware.eu**

Registro delle modifiche

Aggiornamento: 2026-03-05

- sono state precisate le copie di backup a livelli e il processo di ripristino dei dati (BCP/DR)
- è stata integrata la descrizione della cifratura dei dati con il modello a busta (envelope) e la gestione esterna delle chiavi
- è stata ampliata la descrizione della protezione applicativa includendo sessioni, CSRF, CSP e meccanismi anti-abuso
- è stata aggiunta una sezione su monitoraggio e avvisi e semplificata la sezione sull’integrazione con servizi esterni