Sicherheitspolitik

Sicherheitsrichtlinie der Anwendung Safety Software (SaaS)

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

1. Zweck und Geltungsbereich

Diese Sicherheitsrichtlinie legt die Grundsätze zum Schutz von Informationen und Daten fest, die im Rahmen der Anwendung Safety Software verarbeitet werden, die im Modell Software as a Service (SaaS) bereitgestellt wird.

Das Dokument betrifft die Sicherheit der Nutzer, die die Anwendung im Dienst Safety Software verwenden, und stellt eine Ergänzung zu den Nutzungsbedingungen sowie zur Datenschutzrichtlinie dar.

Die Richtlinie hat informativen Charakter und beschreibt die grundlegenden technischen und organisatorischen Maßnahmen, die von Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polen (im Folgenden: „Administrator“) angewendet werden.

2. Verantwortungsmodell

Das System arbeitet im Modell der geteilten Verantwortung:

1. **Administrator (Safety Software)** ist verantwortlich für die Sicherheit des Anwendungscodes, Anmelde-, Autorisierungs- und Sitzungsmechanismen, den Schutz der Daten auf Anwendungsebene, die Erstellung von Backups sowie die Reaktion auf Sicherheitsvorfälle.

2. **Anbieter der Infrastruktur und unterstützender Dienste** sind verantwortlich für die Sicherheit der Elemente, die im Umfang der von ihnen erbrachten Dienstleistungen verbleiben.

3. **Kunde** ist verantwortlich für die Sicherheit seiner Geräte, Passwörter, Benutzeridentitäten sowie für die Verwaltung der Zugriffe in seinem Team.

3. Grundsätze der Anwendungssicherheit

1. Die Datenübertragung erfolgt ausschließlich unter Verwendung von TLS-Verschlüsselung.

2. Benutzersitzungen werden mithilfe von Cookies mit den Attributen **HttpOnly**, **Secure** (für verschlüsselte Verbindungen) sowie **SameSite** abgesichert. Nach der Authentifizierung erfolgt eine Rotation der Sitzungskennung.

3. Für Sitzungen werden Inaktivitätslimits sowie eine maximale Dauer angewendet.

4. Anfragen, die den Systemzustand ändern, sind durch CSRF-Token abgesichert, die serverseitig verifiziert werden.

5. Die Anwendung verwendet eine restriktive Content-Security-Policy, einschließlich Mechanismen zur Einschränkung der Ausführung nicht autorisierter Skripte sowie standardmäßiger Browser-Sicherheits-Header.

6. Es werden Mechanismen zur Begrenzung von Missbrauch eingesetzt, einschließlich Rate Limiting sowie Schutz vor Brute-Force-Anmeldeversuchen.

7. Jede Operation wird im Kontext des Benutzers und der Organisation ausgeführt; nicht autorisierter Zugriff wird blockiert.

4. Verschlüsselung und Datenschutz

1. Benutzerpasswörter werden unter Verwendung des Algorithmus **bcrypt** gespeichert.

2. Ausgewählte sensible Daten, die in der Datenbank gespeichert werden, sind durch ein Umschlagverschlüsselungsmodell (Envelope Encryption) geschützt. Kryptografische Schlüssel werden separat in einem externen Schlüsselverwaltungssystem verwaltet.

3. Wo dies begründet ist, werden Mechanismen eingesetzt, die die Datenexposition bei gleichzeitiger Aufrechterhaltung von Such- oder Identifikationsfunktionen begrenzen, ohne dass vollständige Werte im Klartext gespeichert werden müssen.

5. Backup und Wiederherstellung (BCP/DR)

1. Wir verwenden einen mehrschichtigen Ansatz für Backups: lokale Kopien zur schnellen Wiederherstellung sowie Kopien, die außerhalb der primären Umgebung gespeichert werden.

2. Kopien, die außerhalb der primären Umgebung gespeichert werden, umfassen inkrementell erstellte Umgebungsabbilder. Sie sind verschlüsselt, werden regelmäßig validiert und unterliegen Wiederherstellungstests.

3. Die Datenbank wird durch anwendungskonsistente Kopien abgesichert. Zusätzlich werden lokale Datenbank-Dumps vorgehalten, die eine schnelle Wiederherstellung unterstützen.

4. Die Integrität der Kopien wird mithilfe von Kontrollmechanismen, einschließlich Prüfsummen, verifiziert.

5. Der Backup-Prozess ist automatisiert, wird täglich durchgeführt und unterliegt einem Monitoring von erfolgreichen sowie fehlgeschlagenen Aufgaben.

6. Es werden regelmäßig Tests zur Datenwiederherstellung durchgeführt, die mindestens die Wiederherstellung ausgewählter Dateien umfassen.

6. Überwachung und Alerts

1. Das System protokolliert ausgewählte Sicherheitsereignisse sowie administrative Operationen, insbesondere im Zusammenhang mit Authentifizierung, Zugriffsversuchen und dem Betrieb kritischer Prozesse.

2. Es werden Überwachungsmechanismen sowie automatische Alerts bei Aufgabenfehlschlägen, kritischen Fehlern und Ereignissen eingesetzt, die auf Missbrauch oder einen Sicherheitsvorfall hindeuten können.

3. Der Zugriff auf Logs und Betriebsinformationen ist auf autorisierte Personen beschränkt.

7. Infrastruktur und Aufrechterhaltung der Sicherheit

1. Der administrative Zugriff ist auf autorisierte Personen beschränkt und durch Mechanismen starker Authentifizierung abgesichert, einschließlich Authentifizierung mittels Schlüsseln.

2. Direktes Einloggen in ein privilegiertes Konto ist deaktiviert oder gemäß dem Prinzip der geringsten Privilegien eingeschränkt.

3. Es werden Mechanismen zur Verkehrsfilterung, zum Schutz vor Brute-Force-Zugriffsversuchen sowie zur Überwachung von Infrastrukturereignissen eingesetzt.

4. Sicherheitsupdates werden regelmäßig eingespielt.

5. E-Mail-Dienste, die zur Bedienung des Systems verwendet werden, sind durch Verschlüsselung der Übertragung sowie durch Mechanismen zur Begrenzung von Missbrauch abgesichert.

8. Anbieter und Integrationen

1. Soweit das System externe Dienste oder unterstützende Integrationen nutzt, berücksichtigt die Auswahl der Lösungen die Datensicherheit, das Prinzip der Datenminimierung sowie die Kontrolle des Umfangs der übermittelten Informationen.

2. Die Kommunikation mit externen Diensten erfolgt unter Verwendung einer verschlüsselten Übertragung.

9. Meldung von Vorfällen

Meldungen zur Sicherheit der Anwendung oder Verdachtsfälle von Vorfällen sind an folgende Adresse zu richten:

office@safetysoftware.eu
Betreff der Nachricht: SECURITY

Meldungen werden gemäß dem internen Verfahren zur Bearbeitung von Vorfällen analysiert.

10. Konformität und Gerichtsstand

1. Sicherheitsmaßnahmen werden unter Berücksichtigung der geltenden Rechtsvorschriften, einschließlich der Anforderungen der **DSGVO**, sowie anerkannter Praktiken der Informationssicherheit konzipiert und aufrechterhalten.

2. Anwendbares Recht ist polnisches Recht.

3. Im Falle von Abweichungen zwischen Sprachversionen ist die polnische Version maßgebend.

11. Inkrafttreten

Diese Version der Sicherheitsrichtlinie gilt ab dem **2026-03-05**.

Die aktuelle Version des Dokuments wird im Dienst Safety Software veröffentlicht.

Datenverantwortlicher und Systeminhaber:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polen
E-Mail: **office@safetysoftware.eu**

Änderungsprotokoll

Aktualisierung: 2026-03-05

- schichtweise Backups sowie den Prozess zur Datenwiederherstellung (BCP/DR) präzisiert

- die Beschreibung der Datenverschlüsselung um ein Umschlagmodell und externe Schlüsselverwaltung ergänzt

- die Beschreibung des Anwendungsschutzes um Sessions, CSRF, CSP und Anti-Missbrauchs-Mechanismen erweitert

- einen Abschnitt zu Monitoring und Alarmierungen hinzugefügt sowie den Abschnitt zur Integration mit externen Diensten vereinfacht