Safety Policy

Safety Software | Aktualizacja: 17.12.2025 | https://safetysoftware.eu

Safety Software Application Security Policy (SaaS)

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

1. Purpose and scope

This Security Policy sets out the principles for protecting information and data processed within the Safety Software application provided under the Software as a Service (SaaS) model.

This document concerns the security of users using the application within the Safety Software service and constitutes a supplement to the Terms and Conditions and the Privacy Policy.

The Policy is for informational purposes and describes the basic technical and organisational measures applied by Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Poland (hereinafter: the “Controller”).

2. Responsibility model

The system operates under a shared responsibility model:

1. **Controller (Safety Software)** is responsible for the security of the application code, login, authorisation and session mechanisms, data protection at the application layer, performing backups, and responding to security incidents.

2. **Infrastructure and ancillary service providers** are responsible for the security of elements remaining within the scope of the services they provide.

3. **Customer** is responsible for the security of their devices, passwords, user identities, and access management within their team.

3. Application security principles

1. Data transmission takes place exclusively using TLS encryption.

2. User sessions are secured using cookies with the **HttpOnly**, **Secure** (for encrypted connections) and **SameSite** attributes. After authentication, the session identifier is rotated.

3. Idle timeouts and maximum session duration limits are applied to sessions.

4. Requests that change the system state are protected with CSRF tokens verified on the server side.

5. The application applies a restrictive content security policy, including mechanisms limiting the execution of unauthorised scripts and standard browser security headers.

6. Mechanisms limiting abuse are used, including rate limiting and protection against brute-force login attempts.

7. Each operation is performed in the context of a user and organisation; unauthorised access is blocked.

4. Encryption and data protection

1. User passwords are stored using the **bcrypt** algorithm.

2. Selected sensitive data stored in the database is protected using the envelope encryption data model. Cryptographic keys are managed separately in an external key management system.

3. Where justified, mechanisms are used to limit data exposure while preserving search or identification functions, without the need to store full values in plaintext.

5. Backup and recovery (BCP/DR)

1. We use a layered approach to backups: local copies for rapid recovery and copies

stored outside the primary environment.

2. Copies stored outside the primary environment include incrementally created environment images. They are encrypted, regularly validated, and covered by recovery tests.

3. The database is protected with application-consistent backups. In addition, local database dumps supporting rapid recovery are maintained.

4. Backup integrity is verified using control mechanisms, including checksums.

5. The backup process is automated, performed daily, and monitored for job success and failure.

6. Data recovery tests are performed regularly, including at least the restoration of selected files.

6. Monitoring and alerts

1. The system records selected security events and administrative operations, in particular those related to authentication, access attempts, and the operation of critical processes.

2. Monitoring mechanisms and automatic alerts are used for job failures, critical errors, and events that may indicate abuse or a security incident.

3. Access to logs and operational information is restricted to authorised persons.

7. Infrastructure and security maintenance

1. Administrative access is restricted to authorised persons and secured with strong authentication mechanisms, including key-based authentication.

2. Direct login to a privileged account is disabled or limited in accordance with the principle of least privilege.

3. Mechanisms are used for traffic filtering, protection against brute-force access

attempts, and monitoring of infrastructure events.

4. Security updates are deployed regularly.

5. Email services used to operate the system are secured with transmission encryption and mechanisms limiting abuse.

8. Suppliers and integrations

1. To the extent that the system uses external services or ancillary integrations, the selection of solutions takes into account data security, the principle of minimisation, and control of the scope of information transferred.

2. Communication with external services takes place using encrypted transmission.

9. Incident reporting

Reports concerning application security or suspected incidents should be sent to:

office@safetysoftware.eu
Subject line: SECURITY

Reports are analysed in accordance with the internal incident handling procedure.

10. Compliance and jurisdiction

1. Security measures are designed and maintained taking into account applicable legal provisions, including the requirements of the **GDPR**, and recognised information security practices.

2. The governing law is Polish law.

3. In the event of discrepancies between language versions, the Polish version shall prevail.

11. Entry into force

This version of the Security Policy is effective as of **2026-03-05**.

The current version of the document is published on the Safety Software service.

Data controller and system owner:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Poland
E-mail: **office@safetysoftware.eu**

Changelog

Update: 2026-03-05

- clarified layered backups and the data restoration process (BCP/DR)
- supplemented the description of data encryption with the envelope model and external key management
- expanded the description of application protection to include sessions, CSRF, CSP, and anti-abuse mechanisms
- added a monitoring and alerts section and simplified the integration with external services section