sosafe

Security and Trust

SoSafe's approach to security

Index

Our Approach to Security

In this section, we discuss SoSafe's approach to security. It covers the key steps we take and controls we implement across a number of security domains, both in securing our own environments (including our cloud-based platform), and the processes we have in place to ensure we create products that are as secure as possible for our customers and users.

Our security motivation

Information security is of very high priority to us. We provide an information security product to our customers, so we aim to fulfill a high standard of info-rmation security on our own.

The more we grow, the more customers will use our product and, therefore, our need for strong and state-of-the-art information security will grow even further.

The success of SoSafe GmbH is particularly dependent on the fact that our business information, as well as customer information, is up-to-date and unaltered and handled with the required confidentiality.

Our team

We have hired professionals in a variety of fields relating to information security to fulfill our very ambitious security requirements – and we keep looking for qualified professionals to build, maintain, and improve a state-of-the-art security structure at SoSafe. We want to be "best-in-class" in the field of information security. Therefore, our information security team is built with the following roles:

- **CISO** - Head of the information security team, responsible for monitoring and maintaining the security of SoSafe by ensuring proper collaboration of all roles in the information security team.
- **Information Security Officer/Manager** - Responsible for compliance with ISO27001 requirements, certifications, and keeping our ISMS updated and properly operational.
- **Business Continuity Manager** - Responsible for ensuring that BCM objectives and requirements are met.
- **Application Security** - Responsible for the security of our products and platforms.
- **SOC Team** - Responsible for incident management and monitoring testing, predictive attack analysis and gathering threat intelligence.
- **Offensive Security** - Responsible for red team assessments, penetration testing, predictive attack analysis and gathering threat intelligence.

- **Legal** - Responsible for compliance with legal requirements and certifications.
- **Compliance Manager** - Responsible for ensuring that a business, its employees, and its projects comply with all relevant regulations and specifications.
- **Data Protection Officer** - Responsible for ensuring overall GDPR compliance for all SoSafe's personal data processing activities.

Besides our specialized team, all employees at SoSafe complete our e-learning on information security and are well trained to fulfill our information security requirements.

Certifications

As a company, we completed the ISO 27001 audit and are ISO 27001-certified as of December 20, 2022. We aim to be TISAX-certified by Q1 2023 and to maintain our regular audits from independent third parties. Additionally, our service providers undergo regular SOC1, SOC2, and/or ISO/IEC 27001 audits to verify their practices.

Securing Internal Operations

An effective approach to security starts with keeping our internal environments secure. Our internal security strategy includes the following security principles

Access management

In our context of application "Access" refers to the use of IT systems, system components, networks and the use of information.

General access management principles

- **Need-to-know principle**
  SoSafe's employees are only granted the rights or privileges that are absolutely necessary to fulfill their tasks. As an extent, administrative privileges are granted on a very limited extent.
- **Least-privilege principle**
  Users are only granted the rights and privileges that are absolutely necessary to fulfill their tasks.
- **Separation of duties and dual control principle**
  When granting user rights, the separation of duties and/or the control principle with regard to conflicting duties must be considered.

- **User administration**
  User, group, and permission management is centralized using techniques like SSO to minimize the number of user directories to be maintained.

- **Granting, adjustment, and withdrawal of rights**
  The modification of access rights is carried out following the four-eyes principle. If a user right is granted outside the permission baseline, it must be documented. Double approval for administrative access is being implemented, meaning that it will need to be approved by the asset owner and a supervisor.

  All access rights are also checked at least annually. Administrative access is checked at least every six months following our access management policy or in the event of a relevant change to an asset.

  As part of the need-to-know principle and least-privilege policies, inactive accounts are blocked or removed accordingly.

  Finally, all access rights are revoked within 24 hours after employee off-boarding.

- **Access to source code**
  Access to the source code or the code repository is restricted to prevent unauthorized persons from gaining access to it and to also avoid the possible disclosure of company secrets. The need-to-know and least-privilege principles must always be followed as much as possible. Particular attention is paid to temporary employees, such as working students, interns, or external developers.

- **Authentication requirements**
  An account is locked after six failed attempts.

  Remote access from public external network zones can only be achieved with the company VPN which encrypts the information in transit and is accessible via 2FA.

Security of our endpoint devices

All endpoints are secured with endpoint protection, as well as our file storage and file sharing platforms.

All SoSafe employees use company-managed mobile devices to ensure security while working with company assets, including an antivirus system. This is enforced by a mobile device management software and cannot be deactivated by users.

Freelancers that join SoSafe are equipped with mobile devices depending on their work responsibilities and access needs to ensure the same level of security with third parties. This equipment can include the provision of virtual machines or completely managed mobile devices.

All employees receive training on the acceptable use of mobile devices.

Security in Day-to-Day Operations

Log management

→ **Required logging activities**
All hosts and networking equipment perform security log generation for all system components.

All hosts and networking equipment issue alerts on security log processing failures, such as software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. All alerts must be as close to real-time as possible.

→ **Centralized logging**
Security events are transferred to a managed logging service in real-time or as quickly as technology allows. Log integrity for consolidated log infrastructure is preserved, such as storing logs in read-only.

→ **Required monitoring activities**
Processes are developed and implemented to review logs for all systems to identify anomalies or suspicious activity such as our SIEM system. Security baselines are developed, and automated monitoring tools used, to generate alerts when exceptions are detected.

→ **Authorized personnel**
Logs are secured by limiting access to individuals whose access is needed to perform their job and protect files from unauthorized modifications following the need-to-know principle. Access to log management systems is recorded.

→ **Compliance**
Data are logged securely, taking into consideration the log retention requirements, business requirements, as well as legal and regulatory requirements (e.g., GDPR, Federal Data Protection Act (Bundesdatenschutzgesetz)).

Any log containing personal identifiable information needs to be approved by our DPO.

→ **Retention**
Electronic logs that are created due to the monitoring outlined in this document are maintained and readily available for a minimum of 90 days.

Business continuity and disaster recovery management

We have a business continuity management plan in place. This is described in a business continuity management policy and is based on ISO 22301:2019 Business Continuity Management.

Backup management

We operate a comprehensive backup plan for all of our assets and have a backup policy with requirements for each of them.

We have implemented specific requirements for our databases containing customer data.

→ **Schedule**
The database is fully backed up every night, and afterwards continuously backed up by streaming WAL (write-ahead logging).

→ **Recovery time objectives**

- In case full recovery is needed (complete database crash), we will need between 1h and 1h 30m depending on the size of the WAL.
- In case of partial data loss we can spin a fully working replica of production in 1h and recover the required data.

Keeping Data Secure

Data centers

SoSafe hosts its own data and also its customers' data in multiple data centers from the same provider, namely an ISO27001-certified data center, which provides a very high physical security standard. There is no high threat to our physical security as we are a cloud-driven company. Furthermore, the data center offers multiple security measures to keep customer data protected with the highest security standards.

Encryption of data

Any customer data in our products are encrypted in transit over public networks using at least TLS 1.2 to protect them from unauthorized disclosure or modification. Our implementation of TLS enforces the use of strong ciphers and key lengths where supported by the browser. All our systems and data drives that hold customer information use full-disk, industry-standard AES encryption at rest and following BSI (German Federal Office for Information Security) guidelines whenever selecting cryptographic procedures, algorithms, and key length.

Key management

SoSafe uses state-of-the-art technologies for the secure generation, storage, archiving, retrieval, distribution, withdrawal, and deletion of the keys following the National Institute of Standards and Technology (NIST) recommendations.

Private keys are stored in a password manager which makes unauthorized access impossible.

Controlling access to customer data

We do not require the provision for special categories of personal data, although we treat all customer data as equally sensitive and have implemented strict controls governing this data. Within SoSafe, only authorized SoSafe em-

ployees have access to customer data stored within our systems. All access is restricted to privileged groups unless requested and reviewed for validity of the request, such as customer requests to access the data, with additional authentication requiring 2FA. Unauthorized or inappropriate access to customer data is treated as a security incident and managed through our incident management process. This process includes instructions to notify affected customers if a breach of policy is observed.

Retention and deletion of data

→ **Customer data**
Only customer master data (if they qualify as personal data) are stored for 10 years according to §§ 147 AO, 257 HGB.

Archiving of the customer takes place three months after the expiration of the licenses (to ensure data quality for any subsequent licenses). This period can be extended or shortened at the request of the customer.

A reminder is sent 4 weeks before archiving to the contact person of the customer to download the reports / certificates.

SoSafe maintains a proof of proper destruction, following ISO27001 standard for deletion and disposal of data, stating that any storage media shall be verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or reuse.

During client deletion from the SoSafe Management Software, a deletion report is generated documenting the time and scope of the deletion. This deletion report is retained and presented to the client upon request.

→ **Customer's employees' data**
The deletion of individual data or all a customer's employee data is possible for the customer at any time manually via the control panel.

User access to our e-learning will be deactivated at the end of the license period.

Personal data of participants of a phishing simulation or an e-learning campaign in the user database are automatically deleted when the client is archived (three months after license expiration).

Up to 28 days after deletion, the data could still be reconstructed from back-ups, if necessary.

→ **Active directory**
If users are deactivated in Active Directory (AD) by the customer or lose the right to use the SoSafe E-Learning application, they are also deactivated on the SoSafe platform, won't be able to log in, and are no longer part of the phishing campaigns.

If users are reactivated in AD or regain the right to use the SoSafe E-Learning application within 30 days, users will be reactivated and will be able to continue at their last status.

After 30 days, deactivated users are deleted, including progress data. If the user is then reactivated in AD, a new user is created on the SoSafe platform, which no longer has access to their old data.

Securing Our People

Security awareness training

We make sure all SoSafe employees undergo security awareness training during the onboarding process and then on an ongoing basis so that security remains part of their default thinking. The training is reinforced with the help of constant phishing simulation attacks that our employees go through to help them be prepared and aware of real attacks.

Topics addressed in our security awareness training program include current threats and scams, secure working practices, potentially risky behaviors that create security risks, and compliance and regulatory issues.

Security Champions Program

Through our Security Championship Program we are building a security culture among SoSafe that increases the cybersecurity awareness and accelerates and improves development and product releases in terms of security.

Our focus is mainly on the Product Development and Engineering departments where we have security champions that fill the gap between the Application Security and experience squads, and ensure that our security gates are fulfilled and the security controls are not bypassed in the software development lifecycle.

Protection against security threats

Security testing

Security testing is an important aspect of the development lifecycle and it is tackled in the implementation phase and as well in the testing phase of the Secure Development Life Cycle (SDLC).

The security testing is accomplished through our tools in the implementation phase, and it follows a shift-left approach and ensures that the developers are writing secure code. Moreover, all the open-source external libraries used in our product are continuously monitored.

In the testing phase, the security testing is ensured by the Application Security Engineers, and all the important features are dynamic security tested as well.

Vulnerability management

→ **Vulnerability scanning**
Our platform is continuously monitored by ensuring automatic vulnerability scanning and addressing vulnerabilities immediately for remediation after discovery.

→ **External open-source libraries scanning**
The external open-source libraries that we use are continuously scanned by our Software Composition Analysis and addressed to the right team for patching. The libraries are patched by taking into consideration the SLAs defined based on the severity of the vulnerabilities.

Incident response

→ **Security incident response testing**
To be able to respond properly to a real attack, it is necessary that all stakeholders know in advance how they should react and what they need to do. Having a frequent simulation of the security incident response is mandatory to achieve this.

Red Team Program

With the onboarding of the newly established Red Team/Offensive Security in the Security Team, we want to increase our mature security posture to do next-level testing of protections, procedures, and responses. With that, we ensure that we are on track with the development of the new adversary tactics and techniques and that we are protected against new threats.

The Red Team is supporting the Security Team with the following services: Penetration Testing, Red Team Exercises, and Advanced Adversary Simulation.

Purple Team Program

One of the Security Team's core values is collaboration. We want to ensure that we have the properly defined and configured security controls and that we are also able to detect and respond to the possible security incidents. We ensure this by having a continuous feedback loop between the SOC Team and Red Team and by organizing dedicated Purple Team assessments, which the right stakeholders are part of.