Security Statement

Version	Release Date	Description
0.1	2023-10-31	Initial draft of the Security Statement
0.9	2024-12-03	QA and ready for signing
1.0	2024-12-05	Signing version

Table of contents.

Security at Keesing

Our objective is to enhance our clients' security when utilizing Keesing. To achieve this, the security and compliance framework of our company is certified on the following international standards, all of which have undergone independent audits.

Security organization

Keesing has an information security department specifically responsible and accountable for security administration. The Security department directly manages and oversees risk assessment, development of policies, standards, and procedures, testing, and security reporting processes. The objective is to maintain the confidentiality, integrity and availability of all computer and data communication systems.

Compliance

ISO 27001

ISO 27001 is an internationally recognized standard that governs the management of security for our organization's information. It outlines the prerequisites for establishing, implementing, sustaining, and continuously enhancing an information security management system. This system is designed to safeguard the confidentiality, availability, and integrity of both our clients' data and the essential systems required to deliver our services, shielding them from potential threats and vulnerabilities.

The following ISO-related documents are available upon request:

Keesing 27001 certificate

Keesing 27001 SOA

ISO 9001

ISO 9001 is an internationally recognized standard for quality management systems. It provides a framework for organizations to implement effective quality control, enhance customer satisfaction, and continually improve their processes. ISO 9001 certification is a testament to an organization's commitment to delivering high-quality products and services while ensuring compliance with established quality standards. It helps companies build trust with customers, reduce operational errors, and drive overall excellence in their operations.

OWASP and SANS (SWAT) Checklist

We adhere to OWASP guidelines for the secure development and testing of our applications. The policy is based on best practices according to the SANS instate as laid down in the Securing Web Application Technologies (SWAT) Checklist. A matrix has been drawn up for each application, which indicates the extent to which the application complies with the SWAT checklist.

GDPR

We have privacy controls to limit personal data collection. Such activities comply with global regulatory requirements, like the European Union's General Data Protection Regulation (GDPR), which governs data protection and privacy for EU and European Economic Area citizens.

Security policies and awareness

Keesing maintains a robust framework of information security policies, aligning with the ISO 27001 standard to ensure adherence and to provide clear guidance to employees and contractors for making informed security decisions. These policies encompass a wide range of areas, including but not limited to password management, data protection, information classification, secure communication practices, continuity and contingency planning, acceptable usage of workstations and mobile devices, and backup protocols. These policies receive periodic review and updates, which occur at least annually or when significant changes take place.

To reinforce security practices, Keesing enforces non-disclosure agreements with all employees and contractors and also conducts various security awareness training programs throughout the organization. Additionally, all service providers and contractors responsible for processing entrusted personal data are required to enter into data processing agreements that align with European data protection regulations, ensuring an adequate level of data protection. This collective effort underscores Keesing commitment to maintaining internal security standards.

Security monitoring and auditing

Keesing gathers application, infrastructure, and system logs within a centralized log repository, facilitating monitoring, troubleshooting, security assessments, and analysis by authorized personnel. These logs are retained in compliance with regulatory mandates to aid in responding to security incidents. These logs are necessary for monitoring anomalies and abusive patterns, inappropriate usage of resources, and overall operational status and health of the platform.

Physical security

Keesing's infrastructure is hosted by Microsoft Azure. Our main servers are located in West Europe. They are compliant with security and privacy standards. All physical security measures applying to Microsoft Azure premises are covered by the Microsoft Shared Responsibility Model.

Keesing's office is located in a multi-tenant building. Employees can enter the office by means of badges that are also registered by name and personnel number. All employees also have a physical key to the office space(s) they need to be able to access in order to perform their duties. Keesing's key plan includes who has access to secure rooms.

Network security

In Keesing's setup, each of the environments is hosted within separate Virtual Private Clouds (VPCs) on Microsoft Azure. These VPCs are configured to segregate production networks into public and internal services. Specifically, the private subnets within the network block inbound internet traffic, and the application servers exclusively exist within private subnets, devoid of public IP addresses. Ingress access to the application's internal servers is granted solely to Microsoft-managed and maintained load balancers, which are controlled by tight security groups managing inbound and outbound server access.

Azure VPC's used by Keesing are hosted in Europe.

Keesing's security measures extend to the perimeters, including firewalls, Intrusion Detection Systems, and Web Application Firewalls, fortify both internal and external network security. These edge locations provide an additional layer of protection. Technical controls for DDOS attacks are built into all Keesing products at multiple levels to mitigate a wide variety of attacks.

Segregation levels

Keesing segregates access to their data at various levels

Network level: We've established distinct Virtual Private Clouds (VPCs) tailored to different environments. For instance, we maintain a separate VPC for our production environment, isolating it from development and other environments.

Application level: Customers are logically segmented within the Application layer to enhance security and organization.

Asset management

Keesing adheres to a comprehensive asset management policy that encompasses the identification, classification, retention, and secure disposal of both information and assets.

Our Keesing devices are installed with complete disk encryption and regularly updated antivirus software.

Access control

Access to Keesing systems and applications will be password-protected. Passwords are only known be the account owner and should not be shared. In addition, alternative authentication requirements such as key-based authentication and two-factor authentication are utilized. The organization adheres to the principle of least privilege, systematically inspect and monitoring every access instance.

Consequently, employees are restricted to accessing Keesings systems exclusively via highly secure connections, such as VPN. In the event of an employee's departure from the company, their access privileges are promptly revoked.

Access to Keesing devices is fortified by a combination of Multi-Factor Authentication (MFA) adding an additional layer of security. This ensures that only Keesing -verified devices are granted access to our corporate networks.

Access to customer data by Keesing

Data obtained from our customers is categorized with the utmost criticality. We strictly prohibit any external providers from accessing respondent data, and access to this data is limited solely to authorized Keesing's personnel, with the minimum necessary privileges. Every instance of access to our data repositories is subject to auditing and stringent control measures. Keesing utilizes a defense-in-depth approach to implement layers of security controls throughout our organization.

Penetration tests

As a fundamental component of our security strategy, we engage respected security firms to conduct penetration tests on our platform. The results of these assessments are categorized based on their severity and subsequently prioritized.

This approach entails inviting security experts to evaluate the robustness of our security infrastructure, with the primary objective of identifying and addressing any vulnerabilities.

Vulnerability assessments and penetration tests are executed in accordance with our Cybersecurity Control policy and our Secure Software Development Life Cycle (SDLC) procedure.

Data protection measures

After your information is introduced into Keesing's systems, we implement several layers of security measures to ensure its protection. We employ robust encryption and access controls throughout the data lifecycle.

During data transmission, your information is safeguarded using secure TLS cryptographic protocols, including TLS 1.2 and TLS 1.3. This security extends within the virtual private cloud hosted on Azure.

Additionally, your data at rest, including backups, is fortified using the Advanced Encryption Standard (AES) with a 256-bit encryption key, adding an extra layer of protection.

To uphold the confidentiality of the data stored on all workstations and Keesing's devices, we maintain full encryption, providing a comprehensive security shield for the information contained within.

Data retention

Customer data is retained for a duration that aligns with the purposes for which it was initially collected and in accordance with relevant legal requirements.

Keesing has been engineered for both scalability and fault tolerance. In the event of a machine failure, a seamless transition to another machine is ensured, guaranteeing continuous service availability. This redundancy strategy is integrated at all levels of our platform.

Furthermore, following best practices recommended by Azure, our architecture employs a Multi-availability Zone configuration. In the event of a complete failure in one Availability Zone, the remaining machines in the operational zone have the capability to sustain the entire service, preventing disruptions.

To maintain the integrity of our data, Keesing implements a range of security controls on its services and servers. These controls are designed to uphold the quality, accuracy, and completeness of data throughout its entire lifecycle.

As an additional precaution, redundant backups of critical data are consistently created and securely stored in a separate location. This ensures business continuity in the event of a disaster, with a backup retention period of 15 days.

Information security incident management

Keesing maintains security incident response policies and procedures that align with the requirements outlined in articles 34 and 35 of the General Data Protection Regulation (GDPR). These policies outline the necessary steps for addressing security incidents, encompassing initial response, investigation, and notification in accordance with applicable laws. Additionally, the company has instituted a procedure for Personal Data Breach Notification, ensuring compliance with GDPR and other data protection regulations by promptly notifying the right authority, as well as the affected data subjects.

All instances of suspected or confirmed privacy or data security incidents must be promptly reported in accordance with our security policies. Keesing employees who identify potential incidents are responsible for initially classifying the severity of the incident based on their assessment. It is imperative that all incidents are reported as soon as they are identified, without any undue delay.

Our commitment extends to keeping our customers fully informed regarding matters related to the security of their accounts. We strive to provide customers with all the necessary information to assist them in meeting their own regulatory reporting obligations.

Continuity

Keesing has established robust contingency, and continuity plans that are crafted based on a comprehensive risk analysis. In the event of an emergency, these specific contingency plans are readily available to facilitate the uninterrupted operation of critical business processes. These plans are designed to safeguard data integrity while the organization operates under emergency conditions.

Development

Our development team make use of a Software Development Life Cycle (SDLC) framework based on industry standards including ISO 27001, OWASP Top 10, SANS Top 25, and CWE integrates secure design and engineering principles into the design and development process for all products built by Keesing. Developers follow regular training in secure practices as part of their onboarding process.

To ensure a secure and reliable environment, our test and production environments are kept separate and isolated. All modifications undergo thorough review, encompassing performance, audit, and security assessments, before they are fully deployed to the production environment. Multiple approvals are required before changes are implemented in production, serving as a precautionary measure to mitigate risks, including those originating from within the organization. It's important to note that Keesing never utilizes real data in non-production environments.

Shared responsibility

Ensuring the security of your data and responses is a collaborative effort involving both Keesing and our valued customers. Each party has a role to play in adhering to secure procedures and managing their respective responsibilities.

Product: DocumentChecker

- The platform maintains logs of various types and for all access and user activity. This includes application logs, OS logs, firewall logs. These logs are necessary for monitoring anomalies and abusive patterns, inappropriate usage of resources, and overall operational status and health of the platform. Log data is centralized to our security information and event management (SIEM) platform for analysis and alerting. Logs are reviewed regularly for anomalous activity.
- Our product offers role-based access control that allows administrators to provision control of billing and privacy information.
- Documentchecker is a SaaS solution that is hosted in the Netherlands

Product: AuthentiScan

- The platform maintains logs of various types and for all access and user activity. This includes application logs, OS logs, firewall logs. These logs are necessary for monitoring anomalies and abusive patterns, inappropriate usage of resources, and overall operational status and health of the platform. Log data is centralized to our security information and event management (SIEM) platform for analysis and alerting. Logs are reviewed regularly for anomalous activity.
- Our product offers role-based access control that allows administrators to provision control of billing and privacy information.
- Authentiscan is a SaaS solution that is hosted in the Netherlands