Security and Data Protection Measures

Kami

May 2023

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

The information in this document is confidential and meant for use only by the intended recipient and only in connection with and subject to the terms of its contractual relationship with Kami. Acceptance and/or use of any of the information contained in this document indicates agreement not to disclose or otherwise make available to any person who is not an employee of the intended recipient, or to any other entity, any of the information contained herein. This documentation has the sole purpose of providing information regarding a Kami software product or service and shall be disclosed only to those individuals who have a need to know.

Any entity or person with access to this information shall be subject to this confidentiality Statement.

125 Saint Georges bay road, Auckland 1010, New Zealand

To protect the security and privacy of your data, Kami employs a well-designed infrastructure and adheres to industry best practices.

Kami Data Security Safeguards

Data encryption

- Encryption is used during transit for connections between users' browsers and our backend services. We employ industry best-standard cipher suites and protocols - currently TLS 1.2 with ECDHE_RSA key exchange and AES encryption.
- We use HSTS to ensure all HTTP requests through our domains shall always be encrypted and prevent MITM attacks.
- Data is protected at rest using encryption provided by our cloud services providers (Amazon Web Services and Google Cloud Platform).
- Kami is exposed to the same level of vulnerability of the AWS and Google Cloud platforms as other users of any technology stack; we ensure all latest security patches are promptly applied relating to our full technology stack.

Network protection

- We employ Google's "Beyondcorp" approach to enterprise security of zero-trust networks. Applications on said isolated networks employ best practices to ensure that they'd be considered secure even if they were accessible from the open web.
- Firewalls are used to segregate application tiers and provide strict controls on access to resources within our networks. Our services are also separated into separate networks using Amazon's Virtual Private Cloud technology and Google's Cloud Networking to provide an additional layer of protection.

Disaster recovery and backups

- Your data is protected using streaming replication to geographically distributed backup servers and log shipping to secure storage. We create daily backups using multiple independent systems and store them across multiple different providers. Our backups are encrypted on dm-crypt encrypted disks with strong passwords.
- We conduct disaster recovery drills quarterly to ensure we can quickly restore services without data loss in cases of emergency.

Secure networks and data centers

Staff require SSH keys and 2FA-login (via hardware tokens) to access our networks.

We implement best-practice protective measures against attacks including XSS, CSRF, and SQL injection.

Amazon Web Services (AWS) and Google Cloud Platform (GCP) power the server requirements for thousands of high-profile companies and government entities. We have chosen these providers because of their stringent security measures, which include compliance with the following certifications and third-party attestations:

- SAS70 Type II audits
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)
- ISO 27001 certification
- U.S. General Services Administration FISMA-Moderate level operation authorization

Read more about the security provided by AWS and Google Cloud Platform.

Password authentication

- We support both authentication with a username and password, and SSO through Google OAuth.
- Passwords are stored using bcrypt with a high stretching factor.

Data Stored

- Kami stores data in the secure data centers operated by our cloud hosting partners Amazon Web Services (AWS) and Google Cloud Platform (GCP).
- Kami only collects data that is used explicitly required to provide and maintain the service to you

Category	Elements
Application technology meta data	IP address, cookies
Application usage statistics	meta data on interaction with application
Authentication	Oauth key
User information	Mandatory information: email address, password
	Optional information: First name, last name (if entered by

	user), School/district/class information, indication if student or teacher, subjects taken.
User-generated data	Filenames, annotations, comments. A Document itself is only uploaded to Kami servers if shared by the user with other users for collaborative annotation. These uploaded Documents are fingerprinted and shared only, and are not stored persistently on Kami servers. (The sharing function may optionally be disabled for a given domain)

- Retention of data, unless specified in a MSA or requested formally for deletion, will be 90 days then a deletion of data will automatically happen using our cloud deletion processes.

People & Process

- Within Kami, user data access is limited to staff who need this access to carry out their role, in order to provide the service to the user: customer support, engineering.
- All Kami staff require SSH keys and 2FA-authentication (via hardware tokens) to access our secured networks.
- Policies, training and processes are in place to ensure user data is not downloaded to staff local machines or storage devices and not printed to hardcopy.
- Backup/archiving is carried out entirely within our partners' secure data center network.

Content Ownership and Data Privacy

- Kami claims no ownership over any content - information, documents or data - created or stored using our services. You retain copyright and any other rights, including all intellectual property rights, on created content and included content.

- Your content is only accessible to other Kami users you explicitly shared it with.

- We respect your privacy and will never share your content or personal data or make your content publicly available without your permission.

- Refer to our standard terms and conditions, and our privacy policy for further details.