Keemut

Data Security Public Overview

Disclaimer: The latest version of this document will be available at https://keemut.com /about/security

1. Version History

Version	Date	Editor	Changes	Approved By
1.0	June 15, 2020	HB	Initial Review	FG
1.1	June 20, 2020	HB	Additional content, removed private	FG
1.2	August 11, 2020	HB	New features added	HB
1.3	August 18, 2020	HB	Updated and finalized	FG

2. Disclaimer

This document can be updated without prior notice, to get the latest version, please visit www.keemut.com/about/security.

3. Introduction

This Keemut **Data Security Overview (DSO, aka Overview)** provides an overview of the technical and organizational data security measures Keemut Inc. ("Keemut" or "we") have implemented. By itself, this Overview shall not create any rights or entitlements for anyone. If Keemut and its customers incorporate this Overview by reference into a contract, then the parties' rights and obligations shall be determined based on such contract.

4. Intended Use

This document is intended to give our customers an overview of our security initiatives. As we take security measures continuously, it is likely that Keemut can make modifications based on the security needs, and if this document is saved, it could be out-of-date.

5. Network Policies

Keemut stores data with public cloud providers including Google, Microsoft Azure, and Amazon Web Services (AWS), along with other vendors that are located in USA, Europe and Asia. These providers data centers are Tier 4 level with multiple security features that we have implemented. In addition, we may add redundant tools from third party vendors as we see fit.

Depending on the customer size, we may include separate cloud solutions for certain customers to meet their cloud criteria.

5.1. Public Cloud Security

Keemut's use of public cloud is not limited to Google, AWS, or Azure, but here we will highlight these public cloud providers' security initiatives that we use.

With respect to Google, we use their Google Cloud Platform including Firebase, and some big data features. Google has extensive security measures in place which include but are not limited to:

- Data separation, encryption and management in an automated method to avoid single point of failure

- World class security personnel
- Tier 4 security at their data centers with multiple power sources, dedicated cooling strategies, and greater than 99.95% uptime.
- Six layers of security All Google data centers feature a layered security model, including safeguards like custom-designed electronic access cards, alarms, laser beam intrusion detection, and biometrics.

For more information on Google's Cloud Platform Security, please see here.

Similar to Google Cloud, Amazon Web Services (AWS) is one of the top three cloud providers and Keemut uses AWS for storage of some of your data. The data stored there is encrypted and protected in a manner that is similar to Google. Furthermore, Amazon builds their datacenters in remote areas with limited access for physical contact with the datacenters. AWS also has continuous physical and virtual monitoring of the location and the data to ensure the security of the data. We use some of the security functions that AWS offers within Keemut and use additional third-party tools that add another layer of security for your data.

Some of our clients require us to use Microsoft Azure and our solution and like Google and Amazon, they have world class security measures. Some highlights of Azure's security processes are:

- Azure uses encryption to protect communications and operational processes including your data in transit.
- Azure also offers encryption for your data at rest.
- Azure offers advanced tools to detect and defend against threats

From Microsoft's Security & Privacy Compliance paper,

> *Operational Security Assurance (OSA) makes Microsoft business cloud services more resilient to attack by decreasing the amount of time needed to prevent, detect, and respond to real and potential internet-based security threats*
> *Azure security a priority at every step, including code development that follows the Security Development Lifecycle (SDL), a company-wide, mandatory process based on a rigorous set of security controls that govern operations, as well as robust incident response strategies*

You can learn more about the Azure security overview here.

5.2. Physical Area Access Control

Our public cloud partner’s data centers are not accessible by outside, unauthorized persons, which includes Keemut personnel. These data centers employ state-of-the-art security access and prevention controls to ensure the data processing equipment (namely database and application servers and related hardware) from unauthorized access.

5.3. Access Control to Data Processing Systems

Keemut minimizes who can have access to the personnel data with multiple authorizations required for various different data sets. This is accomplished by:

- Identification of the user to the Keemut systems
- Automatic time-out of user terminal if left idle
- Identification, password and additional factor required to reopen terminal
- Automatic turn-off of the user ID when several erroneous passwords are entered
- log file of events, (monitoring of break-in-attempts);
- all access to data content is logged, monitored, and tracked

Keemut maintains a list of persons having access to the customer data and we grant access rights to a limited number of people only.

6. Employee Policies

Keemut implements measures and policies to ensure that all Keemut personnel are trained and fully aware of all security and privacy-related policies; and that only specific persons have access to specific areas within the network and systems. This is accomplished by:

- Keemut employees are granted limited credentials, and are only assigned additional credentials, when required, upon review and training
- Only authorized Keemut employees have the ability to gain access to secure areas within the backend systems
- Keemut uses multiple different cloud partners to align employees' access with their roles
- Any unused or inactive user credentials are automatically disabled after 90 days
- all employees undergo regular security awareness training
- all access rights follow the principle of need to know
- all access requests have to undergo a multi-factor authentication process, to ensure that the credentials have not been compromised;
- all access requests are logged
- for all employees that leave Keemut, a process to terminate their access is followed

6.1. Segregation of Duties

Keemut implements internal controls to minimize the risks associated with Keemut employees gathering excessive privileges within the network. Where possible, privileges are divided among multiple users in order to ensure that no single Keemut employee is capable of completely controlling a process from start to finish.

In addition, all server access requests require CTO approval and access is only granted for a limited period of time.

Disclaimer: The latest version of this document will be available at https://keemut.com /about/security

7. Data Transmission Control

Keemut implements suitable measures to prevent the Keemut from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- monitoring of the completeness and correctness of the transfer of data

8. Keemut System

8.1. Data Transmission

Keemut implements suitable measures to prevent any data from being read, copied, altered or deleted by unauthorized parties during the transmission or transport of any data to and from our backend. This is accomplished by:

- All TCP & UDP ports, and services (except specific ports & services required by the Keemut application) are disabled within the Keemut network
- All internet-facing servers are separated from Keemut internal systems by multiple firewalls

8.2. System Access

Keemut implements suitable measures to prevent unauthorized access into the Keemut backend. This is accomplished by:

- Keemut uses https (TLS) authentication (using a unique username and password) to authenticate users in the system
- The actual password a user uses can never be recovered as they undergo a 256-bit hash and the actual password is never stored or saved to disk
- Any third-party vehicle credentials are not stored
- All user accounts are monitored in real-time to check if they are being used by multiple Ips and blocked if it seems that accounts are being shared
- Customer personnel data is completely isolated from Keemut telematics and vehicle data, and is stored in a customer database is not accessible or available to other databases
- Only authorized Keemut employees are able to connect and log into all hosted databases for troubleshooting purposes, all of which is fully audited and logged within the audit log

8.3. Process Segmentation

Keemut implements suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished by:

- access to data is separated through application security for the appropriate users
- systems within Keemut are separated by function and in some cases by customer
- at the database level, data is stored in different tables, separated by function
- batch processes and reports are designed for only specific purposes and functions

8.4. General Concerns

Keemut customers should not share their passwords with others, and it is recommended that they do not reuse passwords that are common with other consumer web apps. It is important that customers take their password security seriously.

Keemut sets some initial requirements for customers' passwords but that should just be the start for customers in their password plan. If customers do share passwords with other sites, they should change their password in case of a security breach. Furthermore, they should report to Keemut's tech team any concerns they may have for a security breach.

9. Systems Monitoring

All Keemut cloud solutions are monitored 24 hours a day, 365 days a year by fully redundant monitoring systems.

All software updates and patches are tested within a contained staging environment, and then pushed to each server on a regular basis.

10. Penetration Testing / Vulnerability Scans

Keemut undergoes annual penetration testing on its system through trusted security partners, to ensure the systems remain secure and contained.

Keemut conducts systematic vulnerability testing on all our production servers to look for any potential security or privacy risks. Any vulnerabilities discovered during the process are mitigated and released immediately.

Disclaimer: The latest version of this document will be available at https://keemut.com /about/security

11. Audits

Keemut undergoes regular internal audits on its security policies and procedures. During the audit all Keemut employees are provided security and sensitivity awareness training; internal security policies, security update processes; and server monitoring processes are reviewed.

Information Security policies are reviewed annually. Employee awareness training and / or testing is conducted regularly throughout the year.

12. Data Removal

When you leave the Keemut service, your personal data is deleted. The process is as follows:

- User leaves Keemut
- User selects option to save data, default choice is to delete the data after 15 days
- If user keeps option to save the data, if a Keemut report is sold in the future, the Keemut owner will get a residual payment for their report
- Keemut may keep email on file for future marketing purposes
- If user wants to opt out, we will not send them further emails

13. Incident Response & Management

In the event of a security breach, Keemut engineering may cut off some or all access to Keemut services in order to mitigate any possible intrusion damage. Once the threat has been contained or neutralized, a thorough and immediate investigation by high-level Keemut staff will be conducted, specifically to determine names and / or location of attacker(s), method(s) of breach, what kind of data was exposed (if any), and customers who may be affected.

If Keemut determines that customer data has been accessed by unauthorized persons, Keemut will inform affected customers immediately.

Any information or knowledge of any suspected security weakness, security breach, attempted security breach or any other information that may be related to Keemut and its services can be forwarded to tech@keemut.com

14. Incident Response & Management

Incident response and management The Microsoft global incident response service works every day to mitigate the effects of attacks and malicious activity. The goal of security incident management is to identify and remediate threats quickly, investigate thoroughly, and notify affected parties. The incident response team follows an established set of procedures for incident management, communication, and recovery.

Keemut takes five steps to respond to and manage incidents:

- Detect. This is the first indication of an incident.
- Assess. An incident response team member assesses the impact and severity of the event.
- Diagnose. Security team will conduct a technical or forensic investigation to identify containment, mitigation, and workaround plan.
- Stabilize. The incident team creates a recovery plan to mitigate the issue.
- Close. The incident response team creates a post-mortem record that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence.

15. Data Aggregation and Enhancement

Keemut aggregates system usage information in the interest of its customers and to monitor and improve the service. Some examples of data aggregation include:

- Aggregate which kind of engine/battery information is available for each vehicle type
- AI data inputs for looking for dangerous locations based on driving behavior
- Calculate the average fuel consumption for each vehicle

16. Business Continuity

Members of Keemut senior management oversee business continuity planning to ensure that critical services can be continually delivered to clients.

Keemut conducts a regular business impact analysis to understand the relevant threat/risk landscape and prioritize planning. This includes cyber-attack, sabotage, utility/power outage, terrorism and random failure of mission-critical systems.