gmelius

WHITE PAPER

Gmelius Corporate Security White Paper

Standards and Practices

Table of Contents

Gmelius is a leading collaboration platform that offers integrated solutions for Google Workspace (formerly G Suite). We take our customers' privacy and security very seriously. This document provides an overview of our security policies and technology.

Our Security Policy takes each of our customers' security requirements into consideration and arrives at a set of requirements and initiatives unique to us and our environment.

We don't look at security as a destination to reach — it's an ongoing journey. We continually strive to improve our software development and internal operational processes with the aim of increasing the security of our software and services. The secure way should be the easy way, and that's why security is built into the fabric of our products and infrastructure. Here are a few ways we build security in as part of the way we work, day-to-day.

Website	https://gmelius.com
Legal	https://gmelius.com/legal
Email	security@gmelius.com
Tel	+1 (888) 978-1725

Gmelius SA (Gmelius AG / Gmelius Ltd)
Avenue Louis-Casaï 71
1216 Meyrin
SWITZERLAND

Security Management Program

We know that your mission is as important to you as our mission is to us, and information is at the heart of all our businesses and lives. This is why customer trust is at the center of what we do and why security is our top priority. We're transparent with our security program so you can feel informed and safe using our products and services.

Security Policy

We have developed a couple of foundational principles to our Policy Program:

- ✓ Be posted and available - we make it clear the bar our teams are expected to meet.
- ✓ Outline our security objectives - we like to have goals and be clear about them.
- ✓ Show commitment to meet our regulatory obligations - GDPR, anyone...
- ✓ Be focused on continual iteration and improvement - we continue to evaluate risks in our environment and our program, and reflect those in our policies.
- ✓ Believe in and understand the Values and Principles of the Data Manifesto.
- ✓ Review annually - including updating our policies as we observe new threats and risks.

Risk Assessment

In order to continuously evaluate risks to our environments and our products, we perform on-going risk assessments. In many cases, especially in the case of our products, these are performed as technical risk assessments or code reviews. Our approach to risk management includes:

i. Conduct risk assessment activities - including executing risk assessments, facilitating risk treatment decisions. This includes identifying the scope and the assets under that scope, identifying risks, assessing the impact and likelihood, review and report on the risks.

ii. Monitor and report on projects intended to manage security risks - continue to monitor and report on programs or projects designed to manage security risks.

iii. Support the SMP - through continued risk evaluation as a mechanism to improve the environment and to ensure that the implemented security controls effectively manage identified security risks.

Reliability

We run our business on our own solution, so we understand the importance of reliability and recoverability.

Gmelius cloud infrastructure is implemented with industry-leading services resulting in optimal performance with redundancy and failover options globally. Gmelius is an official Google Cloud partner and uses Google Cloud Platform ("GCP") to persistently store user data meaning we do not store data on our premises. All Gmelius applications include failover and backup instances and our infrastructure respects and maintains industry-standard security certifications, including ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, FedRAMP ATO and PCI DSS v3.2.

The latter architecture or infrastructure provides us sufficient assurance that aspects such as physical security, network and IP backbone access, customer provisioning and problem management are controlled at a level that we require and demand.

In addition to platform-wide resiliency, we also have a comprehensive backup program. Application database backups for Gmelius occur on a daily frequency and are automated. Those backups are retained for 30 days.

Product Security

One of today's challenges is to ship secure products while maintaining a healthy speed to market. Our goal is to achieve the right balance between speed and security.

Encryption and Key Management

All data sent between our customers and our applications is encrypted in transit. We protect your data throughout the data flows of the Gmelius product, from account creation and integration through Google's OAuth service, to encryption of data in transit to Gmelius servers (using browser-based TLS) and encryption of that data at rest, to a variety of administrative, physical, and technical safeguards designed to create a secure environment for our customers' data.

Data in Google Cloud Platform is broken into subfile chunks for storage, and each chunk is encrypted at the storage level with an individual encryption key. The key used to encrypt the data in a chunk is called a data encryption key (DEK). Because of the high volume of keys at Google, and the need for low latency and high availability, these keys are stored near the data that they encrypt. The DEKs are encrypted with (or “wrapped” by) a key encryption key (KEK). For more information, please see https://cloud.google.com/security/#dataencryption

All user data is tagged with a project-specific token, and a customer must have access to the corresponding API key and secret in order to retrieve that data via API. This provides logical separation between data belonging to multiple clients. Gmelius is the sole tenant on our infrastructure. A user's data may reside on database systems which house data belonging to other users, but our logical controls (token, key, and secret) separates one client from another client's data.

Product Security Testing

Our approach to vulnerability management for our products consists of internal and external security testing.

Internal Testing

This approach spans planning, development and testing phases, each test building on previous work and progressively getting tougher. We have an established approach to static and dynamic code analysis at both the development and testing phases. In the development phase, we focus on embedding code scanning to remove any functional and readily identifiable, non-functional security issues.

In the testing phase, our engineering team switches to an adversarial approach to attempt to break features using automated and manual testing techniques.

External Testing

Once a release moves to production, external testing takes over. This approach is built around the concept of "ongoing assurance."

When a vulnerability is identified by one of our users during standard use of a product, we welcome notifications and respond promptly to any vulnerabilities submitted. We keep the submitter updated as we investigate and respond to the issue thanks to a vulnerability program hosted on the HackerOne platform.

Besides, specialist security consultants are used to complete penetration tests on high-risk products and infrastructure, like a new infrastructure architecture (e.g., our cloud environment), a new product, or a fundamental re-architecture (e.g., the extensive use of micro-services).

We don't make these reports or extracts available externally due to the extensive information made available to the testers in conducting these assessments.

Operational Practices

As much as securing our products is a priority, we also understand the importance of being conscious of the way we conduct our internal day-to-day operations. The concept of “building security in” is the same philosophy we use with our internal processes and influences how our business is conducted.

Access to Customer Data

Access to customer data stored within applications is restricted on a 'need to access' basis. Within our SaaS platform, we treat all customer data as equally sensitive and have implemented stringent controls governing this data. Awareness training is provided to our employees during the on-boarding process which covers the importance of and best practices for handling customer data.

Within Gmelius, only authorized Gmelius employees have access to customer data stored within our applications via secure and encrypted channels. 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.

Support Access

Our support team will only access customer data when necessary to resolve an open ticket.
Our support team has access to our cloud-based systems and applications to facilitate maintenance and support processes. Hosted applications and data are only able to be accessed for the purpose of application health monitoring and performing system or application maintenance, and upon customer request via our support system.

Employee Hiring

We strive to hire the best. Just like any company, we want to attract and hire the best and the brightest to work for us. On acceptance of an offer, we ensure each new hire has a 90-day on-boarding plan and access to on-going training based on their role. **All new hires and contractors are required to sign a confidentiality agreement prior to starting with us.**

Change Management

We have embraced open source style change management. Specifically, each change, whether going into our code or infrastructure, has a requirement to be reviewed by one or more peers to identify any issues the change may cause. We increase the number of reviews based on the criticality of the change or product. We trust our development teams and engineers to identify security issues and performance issues, and to flag the change before we allow it to go through.

Relatedly, we use a continuous integration tool, TravisCI, to identify whether any of the changes, once merged into the main branch, will create issues through our integration, unit, functional or security tests. If there are no issues identified in the build and test phases, TravisCI will signal a green dot and identify the build process was successful. If there are issues, TravisCI will signal a red dot and the merge will then be re-evaluated to identify the changes that are causing it. Such a process helps control and monitor the hundreds of changes we make a week.

Security Processes

We acknowledge that there is always margin for error. We're proactive in detecting security issues, which allows us to address identified gaps as soon as possible to minimize the damage.

Security Incident Management

Incidents will happen, but we're confident our speed and efficiency in response will keep the impact as low as possible.

We monitor our systems 24/7/365 with a variety of performance measurement and error-checking tools. When problems are detected, our ops team is notified immediately, and the issues are investigated. We work closely with our hosting providers to ensure that underlying systems remain secure, and any security breaches are investigated, patched and remediated promptly. Our customers and the wider community are encouraged to report suspected security incidents through Gmelius Support.

Our system operations are logged, and the logs are stored for at least a 7-day period in the cloud. If needed, these logs may be mined to investigate incidents or to reconstruct a chain of events.

When a serious incident occurs, or a long interval of downtime is anticipated, we notify our users via our blog, Twitter, and/or email. **Should a security breach occur, we will promptly notify affected users of the nature and extent of the breach, and take steps to minimize any damage.**

Vulnerability Management

We have an extensive vulnerability management program to ensure that we are actively seeking out weaknesses that may be present in our environment. Internal processes are in place to review any reported vulnerabilities and act on them.

Compliance

We run our security program in compliance with a range of well-known industry standards. We're an official Google Cloud partner and our infrastructure respects and maintains industry-standard security certifications, including ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, FedRAMP ATO and PCI DSS v3.2.