Gmelius Security White Paper

Standards and Practices

Version 1.1

Effective July 2, 2019

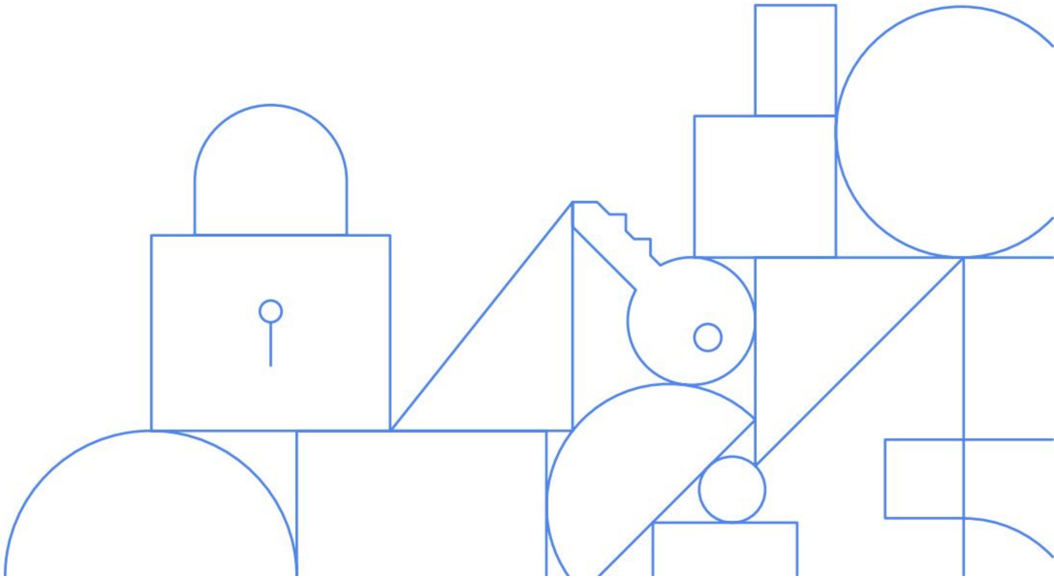

Table of Contents

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:

- ✓ Enforce a strict Privacy-By-Design framework, e.g., we never store the content of your emails.
- ✓ 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.

Governance Terms

The following terms are used throughout this document. Defining these terms establishes a common approach for their use and facilitates compliance.

Term	Definition
Governance	Corporate governance is a system of rules by which a company is governed. Governance includes policies, standards, and guidelines.

Policy

An information security policy is a high-level, mandatory statement that provides Gmelius' requirements with regard to security. A policy does not address the details of how something should be done. Rather, policies provide guidance for the creation of supporting standards, procedures, and guidelines.

Example: "Information Security (InfoSec henceforth) shall configure workstations to authenticate users."

Standard

A standard is a lower-level mandatory statement than a policy that also addresses what must be done, but not necessarily how it must be done. Standards are largely technology-specific, and often include the pseudo-code for configuration that will be translated into the actual code in the procedures. In many cases, standards are tiered.

A baseline standard provides the minimum requirements for a particular component or area. A specific standard may detail the requirements for a certain type of device or a device in a certain environment.

Example: "InfoSec shall configure workstations and require a 16 character, alphanumeric password that is different from the user account."

Guideline

Guidelines are recommendations from Gmelius's executive management that help support standards. Guidelines are not mandatory requirements.

Example: "Use a phrase to create a long, complex password, capitalizing the first letter of each word."

Procedure

Procedures are step-by-step instructions for how to implement what is required by the policies and standards. Procedures can be technical, as in the case of a configuration checklist for securing a particular piece of infrastructure, or process based, as in the case of a change management procedure.

Example: "To log in to your @gmelius.com account:

1. In the User account field, enter the user account you received from Corporate IT.
2. In the Password field, enter the temporary password you received from InfoSec.
3. Hit enter.

4. You will receive a prompt to change your password. Enter your new password at the prompt.”

Process

A process is a series of steps demonstrating how a goal is achieved.

These are generally illustrated by a diagram that shows responsibilities for each step, decision points, and alternatives, along with a description of what is happening at each step.

Example: “The request for a new user starts when HR enters a new employee or contractor in the HR system. The HR system generates a ticket to request the account.

- If the account is for an employee…
- If the account is for a contractor…”

Plan

A plan is an approach to get from one state to another, in alignment with the strategy. Whereas the strategy defines the goals, the plan describes how to get there. An annual plan helps Gmelius achieve its goals within that timeframe.

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:

1. 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.

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

3. 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, Google Cloud Build 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, Google Cloud Build will signal a green dot and identify the build process was successful. If there are issues, Google Cloud Build 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.

Information Classification & Handling Policy

We always protect information based on its sensitivity. At Gmelius, we classify information assets and the assets that store, process, transport, or otherwise handle or protect the asset based on legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. All Gmelius personnel with questions about the information classification of a specific data element or information asset is required to contact our Information Security team.

Scope

All Gmelius physical and electronic information.

Accountabilities

All personnel	Responsible
Legal	Responsible Consulted Accountable
Executives	Responsible Consulted Accountable
Security	Responsible Consulted
Technical Managers	Responsible

Requirements

The following table defines each of the classifications and provides illustrative examples of each.

Classification	**Definition**	**Examples**
Confidential	Information intended for use only by specific individuals on a need-to-know basis Information protected by law, contractual obligation, or policy Information with the potential for severe negative repercussions to Gmelius's reputation, resources, services, or individuals if disclosed	Sensitive personal information about users and customers, whether or not it is tied to identifying information Data "en masse," such as ALL user full names or ALL email addresses Passwords, PINs, access codes, security codes, tokens Employee records Corporate financial information Network diagrams and other system information
Internal	Information intended for Gmelius use only Non-public information that does not reach the sensitivity of Confidential Information with the potential for moderate negative repercussions to Gmelius' reputation, resources, services, or individuals if disclosed	Usage information about customer actions on the Gmelius site, such as viewing a page, trying to sign up, or accepting a credit card offer, in conjunction with identifiable information "In wallet" information, such as a user's address, phone number, email address, or name[1] Publicly posted content, such as customer reviews on an item Confluence Contracts

[1] Only applies to individual or small numbers of users. Large sets of user data, such as ALL email addresses in the database, are treated as "Confidential."

Public	Information intended to be publicly available Information that poses little or no risk to Gmelius' reputation, resources, services, or individuals if disclosed	Customer information that is publicly available or in an aggregate form that cannot be identified to a particular individual Job postings Blog Posts Corporate contact information Corporate address Public facing web pages Press releases

Confidential Information

The table below lists all data elements that Gmelius classifies as "Confidential," and under what circumstances the data element is Confidential.

- The "Isolated" column explains the classification of the data element if it is not listed with any other data elements.
- The "Aggregated" column lists data elements which, when combined with the listed data element, make the data element Confidential.

Data Element	**Isolated**	**Aggregated (Confidential)**
Address	Public	Name and email Name and phone number
Name	Public	Address and email Email and address Email and phone number Phone number and email
Employee records	Internal	Name

Information Handling

Gmelius shall handle information assets in accordance with their information classification, including how information is labeled, how removable media is managed, and how electronic storage media is destroyed.

InfoSec shall define requirements for the levels of protection for information assets based on the needs for confidentiality, integrity, and availability of those assets.

InfoSec and Legal shall define legal and contractual requirements.

All Gmelius personnel with questions about how to handle a specific information asset shall contact InfoSec.

Information Handling Chart

The chart below summarizes the requirements for handling information based on classification. Information comingled with multiple classifications must always be handled with the highest applicable classification (e.g. public information that is stored or transmitted along with Confidential information may be encrypted in order to simplify the use of encryption solutions).

Confidential	
Distribution	Not shared with third parties Customer information never included in reports, regardless of accompanying data
Labeling	Documents, spreadsheets, presentations and text files labeled “Confidential[2]”
Paper documents	Only printed when there is a legitimate business need and no reasonable alternative, with management approval Stored in a locked cabinet Placed in destruction bin for shredding immediately after use
Electronic files	Collected or stored when there is a legitimate business need and no

[2] See Labeling standard for labeling requirements.

	reasonable alternative, with management approval Stored and transmitted encrypted[3] Wiped from electronic media immediately after use[4]
Internal	
Distribution	Redistributed to anyone within Gmelius
Labeling	Not labeled
Paper documents	Only printed when there is a legitimate business need and no reasonable alternative Stored on Gmelius premesis or in locked cabinet Placed in destruction bin for shredding immediately after use
Electronic files	Stored and transmitted in clear text on Gmelius corporate systems Deleted or wiped from electronic media immediately after use
Public	
Distribution	Shared with anyone internal or external to Gmelius
Labeling	Not labeled
Paper documents	Recycled conventionally when no longer needed
Electronic files	Stored and transmitted in clear text Deleted or wiped from electronic media immediately after use

Verbal Communication

Personnel shall use caution when discussing Confidential or Internal information in public locations, and shall not leave Confidential or Internal Information in voice mails.

[3] See Encryption Management standard for encryption requirements.
[4] See Media Sanitation standard for wipe requirements.

Off-Site Assets

Personnel shall not leave Gmelius Internal or Confidential information assets unattended in public locations.

Removable Media

The transfer of Internal and Confidential information to removable media must be authorized by InfoSec. Management shall monitor the use of any authorized removable media to verify that it is handled according to the Asset Handling standard.

InfoSec shall provide removable media with an approved request. All removable media must be company-supplied; no personal removable media may be used on the Gmelius network.

All removable media that contains Internal or Confidential information must be stored in a locked cabinet or similarly restricted location when not in use.

The table below summarizes the required protection methods for each media type and classification.

Media Type	**Protection Method**		
	Confidential	**Internal**	**Public**
Backup tapes & drives	Encrypted	Encrypted	Encrypted
USB removable media[5]	Not stored	Not stored	Stored in clear text

Any physical media containing information needs to be protected against unauthorised access, misuse or corruption during transportation (unless already publicly available). Gmelius uses reliable transport or couriers part of the list of authorised couriers agreed with management, including sufficient packaging to protect the contents from any physical damage during transit, and logs to track and identify the content of the media and the protection applied.

Facsimile Machines

No facsimile machines are used or implemented on the Gmelius network, and Internal and Confidential information cannot be sent via facsimile (fax) machines.

[5] For example: thumb drives, pen drives, flash drives, USB hard drives, removable backup drives

Enforcement

Legal shall monitor compliance with this policy as an integrated part of routine assessments.

Standards

Labeling

Format	Requirement
Electronic files	Documents, spreadsheets, and presentations containing Confidential information must be labeled “Confidential” in the header or footer with a minimum font size of eight (8). Text files containing Confidential information must be labeled “Confidential” at the top of the first page. Documents, spreadsheets, presentations, and text files must have the word “Confidential” in the file name. Databases and applications do not require a label.
Paper documents	Documents that have the “Confidential” label must not be printed but transmitted via encrypted channels only. All other documents without the “Confidential” label can be printed.

Media Sanitation

Personnel shall turn in all end-of-life media to InfoSec. InfoSec shall destroy all end-of-life media as follows:

Media Type	Sanitation Method		
	Confidential	**Internal**	**Public**
Apple iPhone and iPad	Shred, incinerate, or pulverize	Select the full sanitize option[6]	Select the full sanitize option[7]
Backup tapes	Shred, incinerate, or pulverize	(See Confidential)	(See Confidential)
Google Android, Windows, and other mobile devices	Shred, incinerate, or pulverize	Varies by device manufacturer; contact InfoSec	Varies by device manufacturer; contact InfoSec
Hard Drives (ATA and SCSI)	Shred, incinerate, or pulverize	Shred, incinerate, or pulverize	Shred, incinerate, or pulverize
Network Devices	Shred, incinerate, or pulverize	Shred, incinerate, or pulverize	Shred, incinerate, or pulverize
USB removable media[8]	Shred, incinerate, or pulverize	Overwrite media using approved Sanitation Software	Overwrite media using approved Sanitation Software

InfoSec shall obtain destruction certificates or proofs for all destroyed media containing Confidential information. Legal shall retain these destruction certificates.

[6] The full sanitize option is typically located in “Settings > General > Reset > Erase All Content and Settings.”

[7] The full sanitize option is typically located in “Settings > General > Reset > Erase All Content and Settings.”

[8] For example: thumb drives, pen drives, flash drives, USB hard drives, removable backup drives

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

Privacy

Our privacy policy can be found at:
https://gmelius.com/legal/privacy

Data Processing Addendum and Standard Contractual Clauses

Our DPA and contractual clauses can be found at:
https://gmelius.com/extra/dpa

Appendices

Appendix A: Definitions

Term	Definition
Data Element	A data element is a unit, field, or range of values that conveys meaningful information. Examples of data elements are name, address, and account number.
Enterprise	The Gmelius enterprise refers to the entire organization.
Hardware	Hardware is physical equipment that is used to store, process, or transmit information.
Information Asset	An information asset is an electronic system that is used to store, process, or transmit information.
Information Asset Owner	An Information Asset Owner is an employee who has accountability and decision-making authority for an information asset.
Information Security (InfoSec)	Information security is the practice of protecting the confidentiality, integrity, and availability of information.
Management	Management refers to the heads of departments at the Director level and above.
Personnel	Personnel are individuals working at Gmelius, including all employees, vendors, and contractors.
Personally Identifiable Information (PII)	PII is information that can be used either on its own or with other information to identify, contact, or locate a single individual, or to identify an individual in context.
Procedure	Procedures are step-by-step instructions for how to implement what is required by the policies and standards. Procedures can be technical, as in the case of a configuration checklist for securing a particular piece of infrastructure, or process-based, as in the case of a change management procedure.
Process	A process is a series of steps demonstrating how a goal is achieved.

	These are generally illustrated by a diagram that shows responsibilities for each step, decision points, and alternatives, along with a description of what is happening at each step.
Risk	Risks are potential events with a negative impact on the integrity, availability or confidentiality of data and or to the reputation of Gmelius. Risks could also subject Gmelius to legal sanctions.
Security Weakness	A security weakness is a flaw that could potentially lead to a compromise of the confidentiality, integrity, or availability of a Gmelius information asset.
System	System is a category that includes all hardware, software, firmware, middleware, and electronic devices at Gmelius.

Appendix B: Revision History

This table lists each revision of Gmelius' security policies and standards, along with details about what was changed, who made the changes, and the date that those changes were effective.

Revision	Changes	Author	Effective Date
1.1	Information Classification and Handling Policy	Dr Florian Bersier	Dec 18, 2020
1.0	First version	Dr Florian Bersier	Jul 2, 2019

Appendix C: Framework Reference

Gmelius' security policies and standards are based on the International Standard Organization's (ISO) standard 27002:2013. References to ISO standards are marked throughout the document and are summarized below, followed by page numbers.

ISO Reference	**Page Number**
ISO 27002 11.2.6	18
ISO 27002 13.2.1	18
ISO 27002 8.2.1	13, 14
ISO 27002 8.2.2	16, 17, 19
ISO 27002 8.2.2, 8.3.1, 8.3.2, 8.3.3, 11.2.7	17
ISO 27002 8.2.3, 11.2.5	17
ISO 27002 8.3.1	18
ISO 27002 8.3.2, 11.2.7, NIST 800-88	19
ISO 27002 8.3.3	18