

SECURITY REFERENCE

This document was last updated on January 1st, 2025.

1. DATA CENTER SECURITY

Services run on infrastructure from Google, a trusted cloud provider with broad coverage in terms of security certifications and compliance verifications. For further information, please consult the compliance documentation located at <https://cloud.google.com/security/compliance>.

2. SYSTEM SECURITY

Services are operated on servers with hardened Linux distributions (currently Container-Optimized OS). Servers exchange information with each other through a dedicated virtual network.

3. APPLICATION SECURITY

3.1. User authentication

Users authenticate to the Services through the use of single sign-on authentication logic, available for around 175 strategies, such as Google, Microsoft, SAML 2.0 and LDAP. The full list of available strategies is maintained at <https://github.com/intridea/omniauth/wiki/List-of-Strategies>.

Services also feature a built-in authentication mechanism with email validation. Passwords of the built-in authentication mechanism are hashed using BCrypt.

3.2. User authorization

Services implement a role-based access control approach.

3.3. Code releases

Manual and automated testing is conducted for each code release of the Services. Automated testing includes unit tests, integration tests, vulnerability tests, and code quality tests.

4. DATA TRANSFER SECURITY

All client-server communication is encrypted using TLS 1.2. A securely configured SSH setup is in place for all system administration access.

5. LOGGING AND MONITORING

Google actively monitors its data center environment (power access, temperature, access), network and servers, and notifies Supplier as soon as any issues are identified.

Supplier uses robust monitoring solutions (New Relic, StatusCake, Sentry) to proactively monitor the Services around the clock in order to maintain uptime and proactively resolve issues. Automated notifications are in place to notify Supplier of issues or outages.

6. BACKUPS AND DISASTER RECOVERY

Customer Data are backed up to file storage services at our cloud provider. Backup files are encrypted at rest. Only authorized users can access backup files.

Supplier performs disaster recovery exercises on at least quarterly basis. They include a variety of tests to validate adequate recovery times.

7. INCIDENT MANAGEMENT AND NOTIFICATION

Supplier has implemented and maintains security incident management policies and procedures. Supplier will promptly notify any impacted customer of verified or believed security incidents, such as any unauthorized disclosure of Customer Data, to the extent not prohibited by law, regulation or the order of any court or legal authority.