SECURITY & PRIVACY REFERENCE

This Security & Privacy reference was last updated on November 19th, 2018.

1 DATA CENTER SECURITY

Services run on infrastructure from trusted cloud providers with broad coverage in terms of security certifications and compliance verifications. For further information, please consult the compliance references from each individual provider:

- https://azure.microsoft.com/en-us/overview/trusted-cloud (Microsoft)
- https://cloud.google.com/security/compliance (Google)
- https://www.rackspace.com/compliance (Rackspace)

2 SYSTEM SECURITY

Services are operated on servers with hardened Linux distributions (currently Ubuntu and 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 third-party services, from Google to Microsoft to LDAP. The full list of available services 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 encrypted using BCrypt. Passwords can be set to automatically expire at a specified interval.

3.2. User authorization

Access control to models, controllers and views across the Services is defined in a single authorization logic file.

3.3. Code releases

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

Microsoft, Google and Rackspace actively monitor their data center environment (power access, temperature, access), network and servers, and notify Supplier as soon as any issues are identified. Automated tickets are immediately opened to address any issues.

Supplier uses robust monitoring solutions (New Relic, Pingdom, StatusCake, Sentry) to proactively monitor hardware and 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 Rackspace cloud files service which replicates three full copies on different storage nodes. Backup files are encrypted using AES-256-CBC. 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.