Information Security

Table of contents

1. **Our Security Philosophy**
2. **Roles and Areas of Responsibility**
3. **Product Security**
4. **Google Cloud Platform Security Overview**
5. **Network Intrusion Prevention and Detection**
6. **Network and Server Access Policy**
7. **GCP SOC Compliance**
8. **Physical Security**
9. **Corporate Security**
10. **Secure Communication**
11. **Permissions for integrations**
    a. Slack
    b. GitHub
    c. Jira
12. **Customer Data Storage Location**
13. **Encryption**
    a. Encryption in transit
    b. Encryption at rest
14. **Data Retention, Backup, and Destruction**
15. **Personal Information**
16. **Customer Data Access**
17. **Security Awareness Training**
18. **Best Practices for Stepsize Employees**
19. **Incident Management Procedure**
20. **Fraud Policy**
21. **Contact**

1. Our Security Philosophy

At Stepsize, we hold ourselves to a set of principles that guide every engineering and operational decision.

WE TREAT YOUR DATA LIKE OUR DATA
We share our own internal business data with 3rd parties and expect them to adhere to a high level of security standards. We hold ourselves to this same level.

WE FOLLOW INDUSTRY BEST PRACTICES
The overwhelming majority of security issues can be avoided by following industry best practices: password policies, anti-virus software, encryption, access control. We adhere to them.

2. Roles and Areas of Responsibility

The CEO is the owner of the security policy (this document). The CEO delegates the responsibility for security-related documentation to the CTO. All policy changes must be approved and signed by the CTO.

The CTO holds the primary responsibility for ensuring the information security at Stepsize.

3. Product Security

Product security is of paramount importance at Stepsize. Stepsize uses a software development lifecycle in line with general Agile principles. When security effort is applied throughout the Agile release cycle, security oriented software defects are able to be discovered and addressed more rapidly than in longer release cycle development methodologies. Software patches are released as part of our continuous integration process.

Stepsize performs continuous deployment. In this way, we are able to respond rapidly to both functional and security issues. In this way, Stepsize is able to achieve extremely short mean time to resolution for security vulnerabilities and functional issues alike. Stepsize is always iterating to improve its DevOps practice.

4. Google Cloud Platform Security Overview

Google continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

Google Cloud Platform's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI DSS
- NIST 800-53
- Sarbanes-Oxley (SOX)

INFRASTRUCTURE SECURITY

Google Cloud Platform (GCP) provides several security capabilities and services to increase privacy and control network access. These include:

- Network firewalls built into GCP, the ability to create private networks, and control access to your instances and applications
- Encryption in transit with TLS across all services
- Connectivity options that enable private, or dedicated, connections from your office or on-premises environment

DATA ENCRYPTION

GCP offers the ability to add an additional layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. This includes:

- Data encryption capabilities available in GCP storage and database services, such as Compute Engine Persistent Disks, Cloud Storage, Cloud Storage Nearline, Cloud SQL, and BigQuery
- Flexible key management options, including GCP Encryption Key Management, allowing you to choose whether to have GCP manage the encryption keys or enable you to keep complete control over your keys
- In addition, GCP provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in a GCP environment

INVENTORY AND CONFIGURATION

Google Cloud Platform offers a range of tools to allow you to move fast while still ensuring that your cloud resources comply with organizational standards and best practices. This includes: A security assessment service, Cloud Security Scanner, that automatically assesses applications for vulnerabilities or deviations from best practices, including impacted networks, OS, and attached storage.

Deployment tools to manage the creation and decommissioning of GCP resources according to organization standards.

Inventory and configuration management tools, including GCP Config, that identify GCP resources and then track and manage changes to those resources over time.

Template definition and management tools, including GCP CloudFormation to create standard, preconfigured environments.

MONITORING AND LOGGING

Google Cloud Platform provides tools and features that enable you to see exactly what's happening in your GCP environment. This includes:

- Deep visibility into API calls, and data access through GCP Cloud Audit Logging, including who, what, when, and from where calls were made
- Log aggregation options, streamlining investigations and compliance reporting
- Alert notifications through Google Stackdriver when specific events occur or thresholds are exceeded
- These tools and features give you the visibility you need to spot issues before they impact the business and allow you to improve security posture, and reduce the risk profile, of your environment

IDENTITY AND ACCESS CONTROL

Google Cloud Platform offers you capabilities to define, enforce, and manage user access policies across GCP services. This includes:

- GCP Identity and Access Management lets you define individual user accounts with permissions across GCP resources
- GCP has options to activate multi-factor authentication for privileged accounts, including options for hardware-based authenticators
- GCP provides native identity and access management integration across many of its services plus API integration with any of your own applications or services.

5. Network Intrusion Prevention and Detection

NETWORK AND INTERNAL FIREWALL

Stepsize's web applications run on Google Cloud Platform (GCP) servers. Within the GCP network, firewalls are utilized to restrict access to systems from external networks and between systems internally. All access is denied and only explicitly allowed ports and protocols are allowed based on business need.

6. Network and Server Access Policy

OVERVIEW

- Access to Stepsize's web servers (hosted on GCP) is only available to select employees.
- Access within the Stepsize web server cluster on GCP network is controlled by Google's access policies (Google Cloud Identity and Access Management).
- Part-time or Full-time Consultants are not allowed access to Stepsize web servers.

USER PROVISIONING AND DEPROVISIONING PROCEDURES

All user provisioning and deprovisioning must be approved by the CTO by email or Slack. When access is no longer necessary, or following the departure of an employee from the company, users are systematically deprovisioned.

WEB SERVERS ACCESS

Stepsize's web servers are all inside a GCP Cluster, and access is strictly restricted through the Google Access Management to the employees that require access to the servers on a need-to-basis.

All web server security configurations changes must be approved by the CTO by email or Slack, and access is only granted to employees that require to do so to perform their duties. Accessing and modifying the web server security configurations can only be done after a 2-factor authentication.

7. GCP SOC Compliance

Google Cloud Platform (GCP) Service Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how GCP achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the GCP controls established to support operations and compliance. For more details or information: https://cloud.google.com/security/compliance/

8. Physical Security

GCP PHYSICAL SECURITY

The Stepsize production infrastructure is hosted in Google Cloud Platform (GCP). Physical and environmental security related controls for Stepsize production servers, which includes buildings, locks or keys used on doors are managed by GCP. "Google designs and builds its own data centers, which incorporate multiple layers of physical security protections. Access to these data centers is limited to only a very small fraction of Google employees. We use multiple physical security layers to protect our data center floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems."

PHYSICALLY SECURE LOCATION

Stepsize maintains a locked office at Brickfields (Unit 104), 37 Cremer Street, London E2 8HD. Stepsize's office is restricted access solely to employees, contractors and third parties who have a business need to gain access to the premise. The entrance to the building requires a security pass. Access to the private office of Stepsize requires a physical key.

9. Corporate Security

Stepsize recognizes the diminishing utility of perimeter as concerns modern network security. Once that perimeter is breached services reliant on network security guarantees quickly fall. As such Stepsize leverages internal services that require transport level security for network access and individually authenticate users, commonly by leveraging two factor authentication wherever possible.

10. Secure Communication

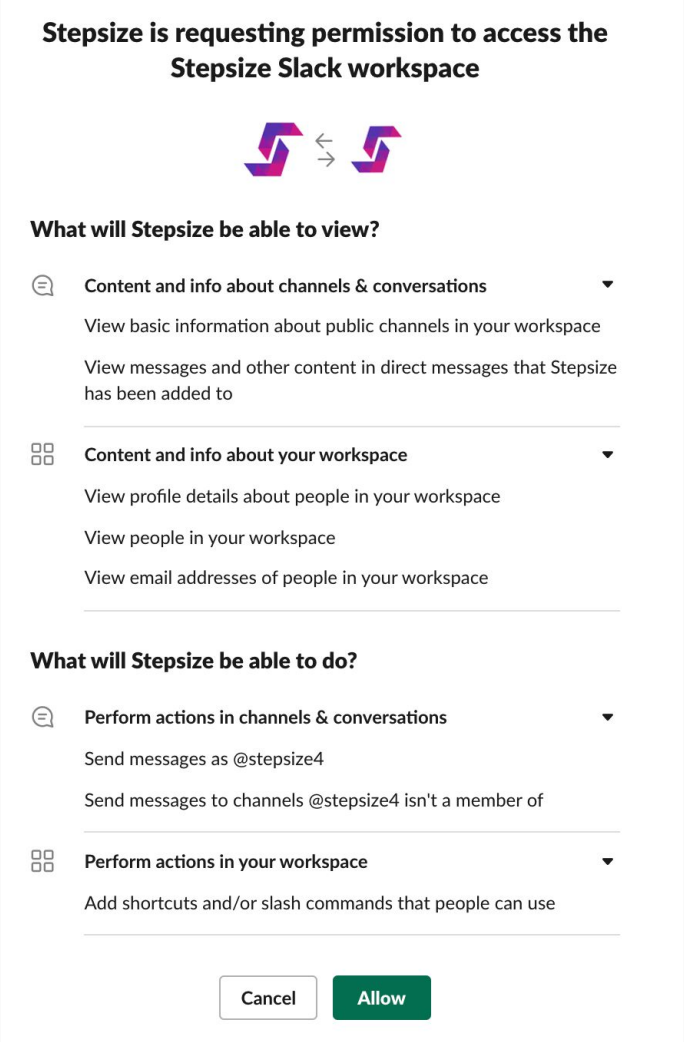
All data transmitted in between Stepsize's services, and in between Stepsize and Stepsize users is protected using Transport Layer Security (TLS) and HTTP Strict Transport Security (HSTS). If encrypted communication is interrupted the Stepsize applications are inaccessible. Stepsize does not "fail open."

11. Permissions for integrations

The permissions requested by the Slack integration, and GitHub integrations are described below, alongside comments regarding why we ask for each one of them.

SLACK

This is what the Stepsize Slack integration installation page looks like from the admin user installing the application on Slack:



View basic information about public channels in your workspace
We need it to list out the channels in our user's Slack workspace to allow allow users to select where to send Slack notifications.

View messages and other content ini direct messages that Stepsize has been added to
Required by Slack. We only have read access to the messages sent to the Stepsize bot. This enables us to respond with instructions on how to use Stepsize.

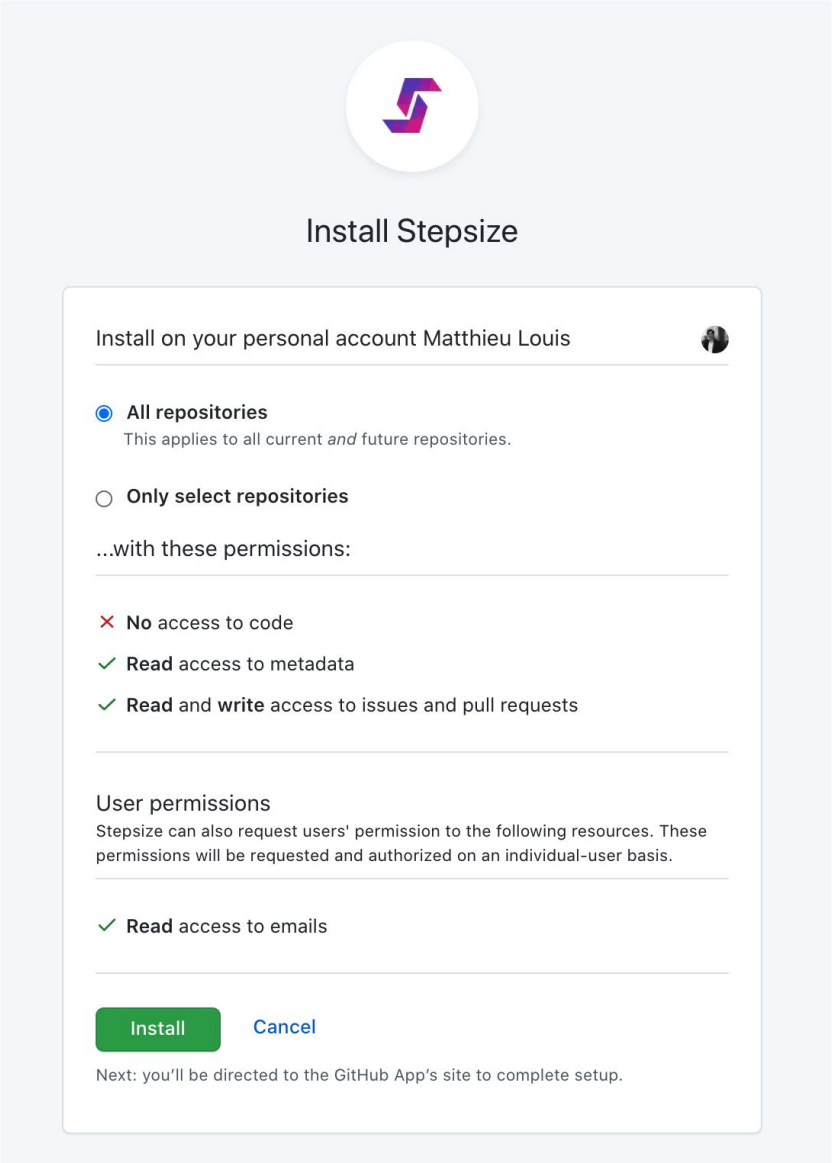
View people in your workspace
We use Slack as a method of authentication, and authorisation verification. As a result, we regularly check the list of users on your workspace to ensure that Stepsize's user permissions are in sync.

View Profile details about people in your workspace
We require Stepsize users to sign in with Slack, and we create the Stepsize users from their Slack profile.

View email addresses of people in your workspace
We require Stepsize users to sign in with Slack, and we create the Stepsize users from their Slack profile.

GITHUB

This is what the installation page looks like from the admin user installing the application on GitHub:



Read access to repository metadata
This is a default GitHub Applications permission scope. We use it to update the set of repositories on which Stepsize will be activated.

Read and write access to issues and pull requests
We need this to listen and report debt when users mention the Stepsize bot, to post success response comments on pull requests, and to inform users on how to use Stepsize when a pull request is opened.

JIRA

We don't store any Jira data on Stepsize, all the Jira data we display and use is fetched on-demand and never persisted on our servers and/or databases. We store some basic metadata as custom fields on Jira issues.

Read access to Jira instance data
We require read access to Jira issue data in order to display that data inside of the Stepsize webapp, and to recommend relevant technical debt for a given Jira issue

Write access to Jira instance data
We require write access to Jira issues in order to update Stepsize metadata that is stored on Jira issues (glance count, number of linked tech debt items, etc...).

12. Customer Data Storage Location

Stepsize service data currently resides in the United Kingdom.

13. Data Encryption

ENCRYPTION IN TRANSIT

All data transmitted between Stepsize's web servers, Stepsize's development machines, and Stepsize users is protected using Transport Layer Security (TLS) and HTTP Strict Transport Security (HSTS), or SSH protocol.

ENCRYPTION AT REST

All data held in Stepsize's databases, databases backups and development machines is encrypted at rest using a secure symmetric cipher AES with a key length of 256 bits.

14. Data Retention, Backup, and Destruction

DATA RETENTION

Stepsize retains customer data for the duration of their engagement with Stepsize. Should a customer terminate their relationship with Stepsize, all data shall be erased from Stepsize' databases ASAP. However that process can take up to 60 days, depending on operational difficulty. Stepsize and its cloud storage provider (Google Cloud) follow best practices recommended by NIST 800-88.

15. Personal Information

Stepsize is registered with the ICO and treats all personal information as per the ICO's recommendations.

Certain visitors to the Website and Service choose to interact with Stepsize in ways that require Stepsize to gather personal information. The amount and type of information that Stepsize gathers depends on the nature of the interaction. For example, when signing up for the private beta or a trial of the Service, we may ask a user to provide the user's name and the name of the user's company, as well as an email address and telephone number where we may contact the user and/or another representative of the user's company. For authentication purposes, each user will be expected to log in with their Slack account. This authentication gives Stepsize access to any information that is public on our users' profile. Stepsize collects such information only insofar as is necessary or appropriate to fulfill the purpose of the visitor's interaction with Stepsize.

Our processing and transfer of personal information is described in our Privacy Policy. In addition, visitors can always refuse to supply personal information.

16. Customer Data Access

A limited number of Stepsize employees have access to customer data via access controlled and logged mechanisms. Employees engaged in customer support access our logging tools and interact directly with customers to identify issues and fix them. Access to this system requires authenticating using two factor authentication. Access to our logging tools, development, staging and production servers is strictly logged. Technical operations employees have access to the raw service data storage. This access requires at least a two factor authentication. Access to the development, staging and production management infrastructure is strictly logged. All other employees are prohibited from accessing customer data.

17. Security Awareness Training

All Stepsize personnel undergo an annual security awareness training lead by our CTO that weaves security into technical and non-technical roles; all employees are encouraged to participate in helping secure our customer data and company assets.

18. Best Practices for Stepsize Employees & their Laptops

All employees are required to:

- Disable automatic login
- Enable full disk encryption
- Audit their security and privacy settings
- Check for software updates often

19. Incident Management Procedure

DATA-RELATED INCIDENT

In the event of a suspected data security or privacy incident, Stepsize will:

- Take immediate action to secure any information that has or may have been compromised.
- Stepsize will (1) convene our executive team including our CEO, CTO and Head of Product (2) as necessary, temporarily shut down all access to our systems, (3) document date and time and details surrounding the incident, (4) redirect and empower the technology team to assess, clean and protect our systems before bringing them back online, and (5) assess the reach of potential harm and our ability to mitigate the risk of harm, in consultation with legal counsel and law enforcement, if necessary.
- Notify, as appropriate, affected third-party data and technology partners;
- Review security procedures and programs to reveal how the incident occurred;
- Make commercially reasonable efforts to bring in security professionals to assess the incident, as necessary.

CUSTOMER DATA ENQUIRIES

In the event of a privacy complaint, Stepsize will:

- Investigate the matter in a commercially timely matter.
- Report findings of the investigation to the consumer within 96 hours.
- Provide remediation and support.

In the event of a subject access request and for data where the right applies, within 30 calendar days, Stepsize will:

- Ask for enough information to judge whether the person making the request is the individual to whom the personal data relates or the individual's legal representative. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception.
- Ask for information that you reasonably need to find the personal data covered by the request.
- Let the individual/individual's legal representative submitting the request know whether any personal data is being processed.
- Provide the individual/individual's legal representative with a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- Give the individual/individual's legal representative a copy of the information comprising the data; and details of the source of the data (where this is available).

BUSINESS CONTINUITY PLAN

Stepsize has implemented and approved the following business continuity plan.

- Our policy: Stepsize's policy is to respond to a significant business disruption by safeguarding employees' lives and firm property, making a financial and

operational assessment, quickly recovering and resuming operations, protecting all of the firm's records, and allowing our customers to transact business.

- Office space: Stepsize maintains office space at Brickfields (Unit 104), 37 Cremer Street, London E2 8HD.
- Emergency contacts: Alexandre Omeyer (CEO, 07463101091, alex@stepsize.com) and Matthieu Louis (CTO, 07875359773, matt@stepsize.com) are the two designated emergency contacts for Stepsize.
- Data back-up and mission critical systems: All of Stepsize's data and web services are operated in the cloud with always-on service providers (Google Cloud and Google Drive) who provide robust system redundancies and multiple geography replication. This ensures continuity of our service in the event of a localized disaster or systems outage. It also removes all dependence for system operation on the Stepsize office site and related infrastructure.
- Service, support and communications: All employees and consultants of Stepsize are enabled for remote access capabilities, allowing continuation of service and support in the event of an office disruption. Remote access will provide a necessary guarantee and restoration of support within 24 hours. Our corporate email service is provided by Google Apps for Work, ensuring always-on, remote access.
- Operational assessment and alternate communications: In the event of a business disruption, we will immediately identify what means will permit us to communicate with our customers, employees, and business constituents. Although the effects of a business disruption will determine the means of alternative communication, the communications options we will employ will include our website, telephone voice mail, and secure email.
- Updates to our business continuity plan: This plan will be updated within 90 days of a material change to our operations, structure, business or location.

20. Policy on Fraud and Responsibility

BACKGROUND

Like all companies, Stepsize is faced with risks from wrongdoing, misconduct, dishonesty and fraud. As with all business exposures, we must be prepared to manage these risks and their potential impact in a professional manner.

The impact of misconduct and dishonesty may include:

- The actual financial loss incurred
- Damage to Stepsize's reputation and our employees
- Negative publicity
- The cost of investigation
- Loss of employees
- Loss of customers
- Damaged relationships with our contractors and vendors
- Litigation
- Damaged employee morale

Our goal is to establish and maintain a business environment of fairness, ethics and honesty for our employees, our customers, our vendors and anyone else with whom we have a relationship. To maintain such an environment requires the active assistance of every employee and manager every day.

Stepsize is committed to the deterrence, detection and correction of misconduct and dishonesty. The discovery, reporting and documentation of such acts provides a sound foundation for the protection of innocent parties, the taking of disciplinary action against offenders up to and including dismissal where appropriate, the referral to law enforcement agencies when warranted by the facts, and the recovery of assets.

PURPOSE

The purpose of this document is to communicate Stepsize's policy regarding the deterrence and investigation of suspected misconduct and dishonesty by employees and others, and to provide specific instructions regarding appropriate action in case of suspected violations.

DEFINITION OF MISCONDUCT AND DISHONESTY

For purposes of this policy, misconduct and dishonesty include but are not limited to:

- Acts which violate an expected code of conduct
- Theft or other misappropriation of assets, including assets of the company, our customers, suppliers or others with whom we have a business relationship
- Misstatements and other irregularities in company records, including the intentional misstatement of the results of operations
- Profiteering as a result of insider knowledge of company activities
- Disclosing confidential and proprietary information to outside parties
- Forgery or other alteration of documents
- Accepting or seeking anything of value from contractors, vendors, or other persons providing services/materials to the company.
- Fraud and other unlawful acts
- Any similar acts.

Stepsize specifically prohibits these and any other illegal activities in the actions of its employees, managers, executives and others responsible for carrying out the organization's activities.

POLICY AND RESPONSIBILITIES

Reporting

It is the responsibility of every employee, supervisor, manager and executive to immediately report suspected misconduct or dishonesty to their supervisor. Supervisors, when made aware of such potential acts by subordinates, must immediately report such acts to the internal audit representative (the CTO). Any reprisal against any employee or

other reporting individual because that individual, in good faith, reported a violation is strictly forbidden.

Due to the important yet sensitive nature of the suspected violations, effective professional follow up is critical. Managers, while appropriately concerned about "getting to the bottom" of such issues, should not in any circumstances perform any investigative or other follow up steps on their own. Concerned but uninformed managers represent one of the greatest threats to proper incident handling. All relevant matters, including suspected but unproved matters, should be referred immediately to those with follow up responsibility.

Additional Responsibilities of Supervisors
All employees have a responsibility to report suspected violations.

However, employees with supervisory and review responsibilities at any level have additional
deterrence and detection duties. Specifically, personnel with supervisory or review authority have three additional responsibilities.

- First, you must become aware of what can go wrong in your area of authority.
- Second, you must put into place and maintain effective monitoring, review and control procedures that will prevent acts of wrongdoing.
- Third, you must put into place and maintain effective monitoring, review and control procedures that will detect acts of wrongdoing promptly should prevention efforts fail.

Authority to carry out these three additional responsibilities is often delegated to subordinates.
However, accountability for their effectiveness cannot be delegated and will remain with supervisors and managers.

Questions or Clarifications Related to This Policy
All questions or other clarifications of this policy and its related responsibilities should be addressed to the CEO, who shall be responsible for the administration, revision, interpretation, and application of this policy.

21. Contact

If you have any questions or believe you've found a vulnerability in Stepsize' security, please contact us at privacy@stepsize.com. We'll get back to you within 96 hours, usually earlier.