Firsthand Platform

Security Procedures and Controls

2018-06-27

Version **1.1**

Revision History

Date	Version	Description	Author
2017-05-01	1.0	Initial revision.	Craig Leinoff
2018-06-27	1.1	Added policy for Red Flag handling	Craig Leinoff

Table of Contents

1 Definitions

The Application, see **Platform Software**.

Application Data is data that is stored in the Application’s database, containing mostly business data about Users, their availability within the Platform, the consultations they have or will hold on the Platform, and some non-technical customization data for clients, such as branding, terminology, and other discrete, non-technical data.

A **Branch** is a duplication of the Codebase under Version Control so that changes to code can exist in parallel to the changes committed to other Branches.

The Code, or **The Codebase** specifically refers only to the Platform Software written or introduced by Firsthand Staff as part of the primary server-side application logic, front-end logic transmitted from our platform to be executed client-side, associated libraries referenced by the Application.

A **Commit** is an atomic set of changes to files under Version Control in the Codebase to be stored and distributed to other Engineers.

Continuous Integration is the cycle espoused by Firsthand for the Application, wherein code is frequently committed and merged into the Codebase, and checked against a battery of predefined tests and expectations as specified by Firsthand Engineering Staff.

Engineering, or **Firsthand Engineering Staff** is any employee or authorized contractor working in development, deployment, maintenance, or any related capacity in service of the Firsthand Platform.

The **Firsthand Platform**, or **The Platform** is the software-as-a-service product made available to Firsthand clients under the designation “Alumni Mentorship Platform”, “Career Advisor Platform”, “Webinar-Only Platform”, and any future products utilizing the same codebase.

The Platform Software, is the resultant combination of the software side of the Firsthand Platform, composed of the primary server-side application logic, front-end logic transmitted from our platform to be executed client-side, associated libraries referenced by the Application, and any unrelated software executed in service of the application (search servers; regularly scheduled event scripts; deployment scripts) created or maintained by Firsthand Engineering Staff.

Procedures are the specific policies outlined in Section 5 of this document, outlined and followed in accordance with the goals stated in Section 2.

A **Pull Request** is a method of submitting contributions to the Codebase. It packages up a series of Commits on a single Branch, and allows them to be easily reviewed and merged into another branch by an Engineer.

Quality Assurance Team, or **QA Team** refers to, when possible, a set of authorized, third-party contractors specializing in providing professional testing of software applications as a service, specializing in functional testing, regression testing, and light security testing. In the event where a specializing third-party QA team is unavailable, other Firsthand staff may be deputized to provide light QA testing in a similar capacity. This term may refer to either the external or internal team participating in QA work.

A **Red Flag** is a warning sign indicating the possibility of or intention to commit identity theft.

Search Index refers to a normalized data store, separate from the Application's database, containing data that has been processed (via tokenization, stemming, filtering, etc.). Its primary purpose is to provide a search application with (a) a means of quickly finding relevant documents by term and (b) storing data to be returned when a matching document is found.

Staff, refers to **Firsthand Engineering Staff** specifically.

The **Version Control System** or **VCS** refers to a software-based system for tracking and coordinating changes in computer files in service of The Codebase by use of Engineering.

2 Introduction

This is the Security Procedures and Controls plan for the Firsthand Platform. It defines the steps and controls used by Firsthand's Engineering Staff to ensure the information security of data stored in and utilized by the Platform. It outlines the procedures required to be implemented and maintained by Engineering Staff to ensure the application of the controls outlined herein.

In general, this document is meant to address Protocols surrounding:

- Application Software Security
- Network Security
- Network Reliability and Performance
- Separation of concerns
- Application Monitoring

3 Scope and Applicability

These Procedures are applicable to all of Firsthand software and server/networking hardware that might impact the network performance, operations, and security of the Platform. Hardware and software used for specialty or business purposes that are disconnected from the Firsthand Platform do not fall under the scope of this Procedure.

4 Audience

The primary audience for the Configuration Management Procedure includes all Firsthand roles that are directly responsible for the configuration, management, oversight, documentation for, and successful day-to-day operations of Firsthand Platform hardware and software.

5 Policy

5.1 Engineering and Networking Staff

Firsthand will make every endeavor to ensure the security and reliability of the Platform by employing and contracting with only reputable and thoroughly vetted professionals in their field. All employees of Firsthand's Engineering Team will:

- Undergo a rigorous and consistent interview process containing relevant in-office and take-home tests, and culminating in background and reference checks prior to hire.
- Be required to have a degree from an accredited four-year institution.

Firsthand will ensure that the staff of its Engineering department, as a whole:

- Averages more than four years' experience in the field of Information and Network Security.

5.2 Application Infrastructure

5.2.1 Architecture

The Firsthand Application is architected to provide complete separation of (a) application logic, (b) application configuration, and (c) user data. The application has the following specifications:

- Application Logic (Code) is stored in a Version Control System, excepting all configuration, authentication, or other secure data (such as passwords and API keys)
- Application Code is deployed in the production environment identically to a set of web servers, accessible behind one or more load balancers, evenly distributing requests to each.
- Session Persistence information is stored on a separate server, accessible by each web server, such that session state need not be persistent to a single server.

- Application Data is stored in a managed Application Database instance separate from but accessible to the application web servers.
- The application maintains and queries a Search Index located on a separate Search Server. This server is also responsible for any processing required to index data for storage.
- Static user-submitted files such as profile image avatars and documents relating to user consultations, and long-term archives of Application Data being held on the platform are stored in an external, access-controlled cloud data store.
- Static user-submitted files may be replicated to different cloud servers automatically via a Content Delivery Network depending to ensure high-availability and a higher speed of access for users.

5.2.2 Network Infrastructure and Security Details

To accommodate the application architecture as defined in Section 4.2.1, Firsthand will ensure the aforementioned network infrastructure is provided as services by trusted Vendors in contract with our team.

Wherever possible, each Firsthand Staff member requiring access to any vendor should be equipped with his or her own personal, unique account data for authentication with each vendor. These accounts (and the credentials for accessing the accounts) should not be shared with other Staff members. Staff should not use the same credentials (username and password) across multiple accounts.

Wherever possible, Multi-Factor Authentication (MFA; sometimes known as 2-Factor Authentication or 2FA), are required to be activated for any Staff account with a vendor that provides MFA as an option.

Firsthand uses the following vendors:

Vendor	Details and Security Data
Rackspace	Self-Managed Web and Application Servers; Session/Logging Servers; Managed Database Instances; Search Server
	https://support.rackspace.com/white-paper/rackspace-private-cloud-security-white-paper/
Amazon Web Services (AWS)	Static file storage of User Profile Photos and User-Uploaded Consultation Files through Amazon S3 and delivered via Amazon CloudFront. Long-term database backus through a separate Amazon S3 bucket.
	https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
Postmark (hosted at	Transactional email delivery for the Application.

ServerCentral)	*Postmark:* http://support.postmarkapp.com/article/917-is-postmark-secure-and-redundant *ServerCentral:* https://www.servercentral.com/compliance
Hubspot (hosted at AWS and Akamai)	User “drip” onboarding engagement emails.
	AWS: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf *Akamai:* https://www.akamai.com/us/en/about/our-thinking/information-security/compliance/

5.2.3 Server Configuration, Controls, and Methodology

All self-managed Firsthand servers (e.g. servers managed by Firsthand staff, not those being offered as a service or managed instance) operate under the following standards:

- **Software**
    - *Methodology:* All self-managed servers are configured to use the same operating system and distribution. Servers should be configured to install patches and security updates provided by (and vetted by) the distribution. These patches and security updates are installed regularly via an automated process. Servers should be stripped-down and configured only with the software packages necessary for their function (and related dependencies).
    - *Operating System:* GNU/Linux
    - *Distribution:* Ubuntu 14.04 LTS
- **Application 3rd-Party Software Libraries**
    - *Methodology:* The Firsthand Application utilizes modern best-practices for including 3rd-party software libraries in the Application. Firsthand Engineers specify relevant major revisions of external libraries and these are automatically kept up-to-date by the deployment process. Firsthand Engineers otherwise are responsible for migrating software libraries to the latest version as it becomes relevant to their code.
- **Internal Accessibility**
    - *Firewall:* Servers should be firewalled to be accessible only by networks and devices that need access wherever possible.
    - *Encryption:* All server-to-server communication and all Engineer access occurs via Secure Shell (SSH) Protocol version 2.x using RSA cryptosystem pre-shared keys of at least 2048 bits.
- **Application Accessibility**
    - All HTTP traffic to Firsthand Platform websites Is routed over a secure connection, encrypted and authenticated using a strong protocol (such as TLS 1.2), a strong key exchange (such as ECDHE_RSA with P-256), and a strong cipher (such as AES_256_GCM).
    - Users should be able to log into the Firsthand Platform via unique email address/password combination and, optionally for each client, an external Single

Sign-On (SSO) service such as LinkedIn, Facebook, or a CAS-based authentication service provided by the Client organization.

  - Multi-Factor Authentication may be enabled for the platform at the user's or client's discretion by enabling one of these external SSO services.

5.3 Data Security

5.3.1 Policy

Firsthand provides a general Terms of Use and Privacy Policy on each Platform website. It may be viewed for Evisors, Firsthand's Generalized, Public Platform, here:

- Terms of Use: https://www.evisors.com/general/terms
- Privacy Policy: https://www.evisors.com/general/privacy

5.3.2 Password Security

User passwords are stored in the database as unique, salted hashes, using PHP's default hashing algorithm, currently *bcrypt*.

5.3.3 Database Security

Policy: Firsthand stores user data in managed, secure database instances accessible only via an internal network over encrypted connections.

Backups: Database instances are backed up automatically, daily, by Firsthand Engineering, to volatile local storage, and to a cloud-based data store for permanent archival. Backups are also triggered manually by Engineers immediately prior to the deployment of any new code to the Platform.

Encryption: Database backups at rest in permanent archives are encrypted using a modern algorithm such as AES-256. Active databases and data in temporary, volatile storage, are not currently encrypted.

5.3.4 Email Security

The Firsthand Platform may send automatically-triggered transactional emails to users at any time, as long as their account remains active (and until such time as they request it be deactivated) on the Platform. New users may be added into an automated "Drip" Email Campaign used for ensuring engagement, unless deactivated by Client administrators or by user opt-out. Users may opt-out of these emails at any time. Firsthand does not sell or share user information, including email address, with any individual or organization.

5.4 Logging

5.4.1 Server Logs

Self-managed servers all keep detailed authentication logs identifying user login attempts, IP address, and superuser login attempts for a period of at least 4 weeks. Software running on Firsthand servers (web server software, database software, search server software, etc.) follow similar logging procedures. All Firsthand Server software maintain detailed error logs wherever possible.

5.4.2 Application Logs

The Firsthand Application should track the last login date of all authenticated users. Endeavors are being made to extend user authentication logging to track all end-user login attempts and originating IP address by the end of Q2 2017.

The Firsthand Application also stores a permanent detailed recording of all errors and warnings occurring during use of the site indicating:

- Potential code logic issues (bugs)
- Unexpected user input
- Intentional malicious intent

5.5 Red Flag Rules

Because Firsthand Application Data may contain personally identifying information, Firsthand may be considered at risk as a target for potential identity-theft. When dealing with all Platform user accounts and data, Firsthand commits to preemptively address Red Flags through proper training of relevant Staff to spot the Red Flag; investigation into the suspicious activity; and the reporting of the occurrence to relevant client stakeholders, as-needed.

5.4.1 Handling of Red Flags

Firsthand commits that all relevant Staff will be instructed to exercise the following precautions in all dealings with user accounts and data:

1. Confirm that an individual requesting action on data (a) is who they purport to be and (b) has the right to receive or modify the requested data.
2. Check, confirm, and question all suspicious documents
3. Check, confirm, and question all suspicious personal identifying information
4. Investigate suspicious covered account activity or unusual use of account
5. Follow up on alerts from others

In the event that any Red Flag is presented, the Staff in question should report the occurrence, in writing, to a supervisor.

5.4.2 Investigation

Firsthand Staff and/oror supervisors should investigate, as-needed, any reported Red Flags to identify whether there is an obvious reason for the anomalous behavior and, in the event that a clear and satisfactory explanation does not exist, log and elevate the event further.

5.4.3 Notification

Upon investigation, any Red Flag event believed to be malicious will be reported to the affected clients or end-users no later than 5 business days after its occurrence, unless otherwise agreed-upon with the client.