SmartSimple Security, Privacy & Architecture

1. Architecture and Data Segregation

The service can be run in a multi-tenant, single tenant, or enterprise (on-premise) hosting environment.

SmartSimple has developed a logical abstraction layer in order to separate client-maintained data and system configuration from underlying core system functionality. This innovation represents one of the key components of the platform and has been the subject of our research and development activities since the start of the company. System security and access models meet the needs of different user groups. This approach provides an appropriate interface for each 'stakeholder' group such as applicants, staff reviewers, non-staff reviewers, board members, administrators and others. Attribute and Role Based Security & Permissions are a cornerstone of SmartSimple's security design. Attribute Based Access Control (ABAC) – in combination with standard Role Based Access Control (RBAC) - dictates everything from portal access to application access to the ability to view and modify the contents of a field. These controls extend past the user role, and encompasses the context (location within the corporate network, time of day, rank/classification, material to be accessed, and other attributes) at the field level.

Customer Location	Hosting Regions
Australia	Amazon Web Services (AWS) Asia Pacific – Sydney, Australia
Canada	Amazon Web Services (AWS) Canada (Central) – Montreal, Canada iWeb Canada – Montreal, Canada
EU	Amazon Web Services (AWS) EU (Ireland) Amazon Web Services (AWS) EU (Frankfurt)
United Kingdom	Amazon Web Services (AWS) Europe (London Region)
United States	Amazon Web Services (AWS) US East (N. Virginia) Amazon Web Services (AWS) US West (Oregon)
US Federal	Amazon Web Services (AWS) GovCloud (US)

2. Subprocessor List

Entity Name	Entity Type	Entity Country
Computer Services, Inc. (CSI Web)	Watchlist services related to terrorist and criminal organizations and individuals	United States

3. Audits and Certifications

SmartSimple has engaged in several security and privacy-related audits and certifications which provide the framework in which your data is handled.

- Service Organization Control (SOC) reports: SmartSimple Software engages in yearly third-party evaluation by our auditors, Deloitte, which produce SOC 1 and SOC 2 compliance reports. These reports are available upon request and under the Non-Disclosure Agreement (NDA).
- Federal Information Security Management Act (FISMA) Compliance: SmartSimple is compliant with the comprehensive framework created to protect government information, operations and assets against natural and man-made threats.
- Federal Information Processing Standard (FIPS 140-2) Compliance: SmartSimple is compliant with the computer security standard used to approve cryptographic modules.
- GSA IT Schedule 70 Contract Holder – SmartSimple is an approved United States Government General Service Agreement (GSA) Advantage Schedule 70 supplier.
- AWS GovCloud – SmartSimple is an Amazon AWS Partner and is authorized to connect with the AWS GovCloud dedicated server. GovCloud's isolated AWS region allows government agencies and customers to move sensitive workloads to the cloud.
- GOV.UK – SmartSimple is an authorized supplier to the United Kingdom, through the GOV.UK website managed by the Government Digital Service.

4. Code of Conduct

As of April, 2018, SmartSimple is pursuing certification from the EU Cloud Code of Conduct, a code of conduct drafted by the Cloud Select Industry Group (C-SIG). The Cloud Select Industry Group was convened by the European Commission.

5. Security Controls

SmartSimple provides a number of platform-level configurable security, privacy, and data retention controls that allows clients to setup and then manage their solution in a manner that is non-prescriptive. For additional security details visit our public Wiki.

6. Security Policies and Procedures

SmartSimple identifies potential threats that would impair system security, availability, processing integrity, and confidentiality commitments and requirements; analyzes the significance of risks associated with the identified threats; and determines mitigation strategies for those risks (including controls and other mitigation strategies).

- SmartSimple uses a configuration management database and related process to capture key system components, technical and installation specific implementation details, and to support ongoing asset and service management commitments and requirements.
- SmartSimple has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
- During the risk assessment and management process, risk management office personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.
- Identified risks are rated using a risk evaluation process and ratings, are reviewed by management.

- The Security Committee evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation.
- The Security Committee's recommendations are reviewed and approved by senior management. Regarding the identification of potential threats SmartSimple addresses the following security risks:

Risk	Mitigation Approach
Malicious code added by developer	● Source Code Security Testing ● Both automated and manual testing is performed.
Insecure code added by developer	● Source Code Security Testing ● Both automated and manual testing is performed.
Vulnerability in existing code	● Source Code Security Testing ● Both automated and manual testing is performed. ● Penetration Testing is performed by a third party security firm at least once a year.
Vulnerability discovered in existing operating components	● Servers are scanned weekly for new vulnerabilities. ● Penetration Testing is performed by a third party security firm at least once a year. ● SmartSimple is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC). As such we receive the earliest warning available related to potential vulnerabilities. ● Trend Micro's Deep Security tools are used to monitor servers.
Vulnerability discovered in existing Client Configuration	● Client specific pen testing ● System Error Logs
Logical Breach of Hosting Security	● The response is based on the extent of the breach
Physical Breach of Hosting Facility Security	● See Disaster Recovery plans

Penetration Testing is performed by a third-party security firm at least once a year. Internal and External network scanning is performed monthly with reports being received weekly. Results are integrated into security enhancements to the platform as part of the regularly scheduled upgrade cycle.

Your organization may require our platform to be reviewed and approved for use either by internal staff or a third party. To assist in this process, SmartSimple can provide, under a Non-Disclosure Agreement, the following

documents:

SOC 2 Report – This report is an externally prepared independent service audit report prepared annually by Deloitte. This report outlines our organization's compliance with the Trust Services Principles and Criteria as defined by the Assurance Services Executive Committee (ASEC) of the American Institute of Certified Public Accountants, Inc.(AICPA), and Chartered Professional Accountants of Canada (CPA Canada).

SmartSimple uses this framework to manage security, availability, processing integrity, confidentiality, and privacy.

SmartSimple Software Operational Policies – This document defines the policies enforced at SmartSimple to ensure day-to-day compliance with the Trust Framework.

Third Party Penetration Test – This report describes the results of a third-party security assessment that is carried out annually. The assessment provides details as to the security of the system based on industry standards.

7. Intrusion Detection

SmartSimple employs tools that monitor network traffic for network intrusion. Intrusion protection includes both Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

Software firewalls are employed to restrict network traffic to the servers. Only specified ports are opened to the public. Secure Shell (SSH) is restricted by source IP address, only allowing connections from the SmartSimple office or backup/non-production servers. All other ports are restricted and Internet Control Message Protocol (ICMP) disabled.

8. Security Logs

SmartSimple maintains the following logs: User login and logout, Including IP address; Change value logging (old/new values, date/time and user performing the change); Security logs can be enabled on a field-by-field basis throughout the system; All record deletion events are logged and the deleted records archived; Reader Log can be enabled to track all users that view and/or edit a record.

9. Incident Management

In the event that the monitoring tools and scheduled procedures (in each of the hardware, software and data security sections) identify an incident, SmartSimple will immediately assess the situation and determine the nature of the incident. All appropriate parties will be contacted within 24 hours (the client will always be notified of security breaches), and collectively these parties, under the direction of SmartSimple, will determine a resolution.

10. Physical Security

SmartSimple has partnered with Amazon Web Services (AWS) for our production data centers. Amazon's control points includes secure design (site selection, redundancy, availability, capacity planning), business continuity & disaster recovery (BCP, pandemic response), physical access (employee data center access, third-party data center access, AWS GovCloud data center access), monitoring & logging (data center access review, data center access logs, data center access monitoring), surveillance & detection (CCTV, Data Center Entry Points, intrusion detection), device management (asset management, media destruction), operational support systems (power, climate and temperature, fire detection and suppression, leakage detection), infrastructure maintenance (equipment maintenance, environment management), and governance & risk, are all inherited by SmartSimple clients.

11. Reliability and Backup

All SmartSimple systems are backed-up on a nightly basis at a separate but equally secure data center from where production data is hosted.

A hot backup server is used to save and mount the daily backups every night (the backup and mounting frequency can be determined by a client if they choose dedicated hosting). Acting as a hot backup, this server is always online and available. Physically, the server can either be hosted by the client, or using Amazon's EC2 cloud offering. Each daily incremental backup is archived to a separate location. Incremental backups are generally archived for a period of three (3) months and then removed.

12. Disaster Recovery

SmartSimple has a comprehensive disaster recovery and business continuity plan based on SOC control points. In the event that a SmartSimple server becomes unreachable, the hot backup server may be used in a read-only fashion for users wishing to view information entered into the system up to the previous date.

After triaging the situation there are two possible routes of action: In the event that the production server data is intact and is recoverable within a predetermined amount of time, then users will continue to use the hot backup server in a read-only fashion until the production server is restored online. In the event that the production server data is unrecoverable or the server is not recoverable within a predetermined amount of time, then the hot backup server will be promoted as the production server. A new server will be procured and a maintenance window scheduled to promote the new server as the production server, and demote the existing server back to the hot backup.

13. Viruses

The system can accept all file types (documents, spreadsheets, PDF files, PowerPoint presentations, jpg, png, gif, mp3, mp4, mpg, mov, qt, wav, zip...) except for exe and binary files. All files are scanned for viruses once uploaded to the system.

14. Data Encryption

All data is encrypted in motion (through Transport Layer Encryption - TLS) and at rest. Encrypted hard disk storage uses AES (256 Bit Key). Passwords are encrypted within the database using SHA256. Passwords are salted and stretched.

15. Return of Customer Data

SmartSimple also provides data export functionality from your system to National Archives Electronic Records Archives (ERA) standards. The significance of this functionality is that it provides self-serve access to exported data in a format that can be used beyond the confines of the SmartSimple application and platform.

16. Deletion of Customer Data

(a) Upon termination of an account, the Client's right to use such account and the Service immediately ceases.

(b) SmartSimple shall return to the Client all of its Participant Data, subject to fee for the time required to do so determined at the then current billing rates, in an agreed format such as CD-ROM or the Client supplies a USB Key or USB Hard Disk within thirty (30) days and shall retain the Data for ninety (90) days thereafter ("Retention Period").

(c) Within a reasonable time after the return of such Participant Data to the Client and the expiry of the Retention Period. SmartSimple shall deliver to the Client a certificate signed by a senior officer of SmartSimple stating that all of the Participant Data has been permanently deleted/purged from the database. As archive data is retained for the archive cycle (currently (6) six months), all residual copies of the data will be deleted.