SmartSimple Security, Privacy & Architecture Documentation

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 the 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 encompass 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	Production Region	Backup Region
EU	Amazon Web Services (AWS) EU (Ireland)	AWS EU Frankfurt)
United Kingdom	Amazon Web Services (AWS) Europe (London Region)	AWS Europe (London Region)
United States	Amazon Web Services (AWS) US East (North Virginia)	AWS US West (Oregon)
Canada	Amazon Web Services (AWS) Canada (Central) – Montreal, Canada	AWS Canada (Central) – Montreal, Canada
Asia Pacific	Amazon Web Services (AWS) Asia Pacific – Sydney, Australia	AWS Asia Pacific – Sydney, Australia
US Federal	Amazon Web Services (AWS) GovCloud (US)	AWS GovCloud (US)

2. Audits, Certifications and Compliance

SmartSimple has engaged in a number of information security, quality management, and data protection-related audits, certifications and compliance activities. These provide a comprehensive framework for how client data is handled and how we deliver our services.

- Service Organization Controls (SOC) Compliance: SmartSimple Software engages in yearly third-party evaluation by our auditors, Deloitte, which produce SOC 1, SOC 2 Type II, SOC 2 + HITRUST mapping, and SOC 3 compliance reports. These reports are available upon request and under the Non-Disclosure Agreement (NDA), with the exception of the SOC 3 report, which is public and can be accessed and shared without an NDA.
- ISO/IEC 27001 Certification: SmartSimple is certified to the ISO/IEC 27001 standard, which specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). This certification is maintained through yearly third-party audits conducted by BSI (British Standards Institution).
- ISO 9001 Certification: SmartSimple is certified to ISO 9001, which sets out the criteria for a quality management system (QMS) and is based on a number of quality management principles, including a strong customer focus, the process approach, and continual improvement. The scope of this certification covers the provision of Project Management, Implementation, Deployment, and Training Services for the SmartSimple Software. This certification is maintained through yearly third-party audits conducted by BSI.
- Cyber Essentials Certification: Cyber Essentials is a UK government-backed scheme that sets out basic standards for cybersecurity to protect organizations against common online threats. SmartSimple holds the Cyber Essentials certification, which is renewed annually through a self-assessment questionnaire verified by an authorized third-party certification body. This certificate, issued by The IASME Consortium Ltd, assures that SmartSimple complies with the requirements of the Cyber Essentials framework, demonstrating our commitment to safeguarding our systems against common cyber threats.
- TX-RAMP Level 2 Certification: SmartSimple Software is certified at TX-RAMP Level 2, confirming compliance with Texas state requirements for cloud services handling sensitive data. This certification ensures that SmartSimple's services meet the security and privacy requirements mandated for Texas state agencies and institutions of higher education.
- Federal Information Security Management Act (FISMA): SmartSimple's ISO/IEC 27001 certified Information Security Management System (ISMS) is aligned with the Federal Information Security Management Act (FISMA) requirements. This includes categorizing information systems, selecting and implementing appropriate security controls, and continuously monitoring and assessing these controls. These processes are part of our ISO 27001 framework, which emphasizes comprehensive risk management and ongoing security audits to ensure compliance.
- 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.

3. Security Controls

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

4. Security Policies and Procedures

SmartSimple identifies potential threats that would impair system security, availability, processing integrity, and confidentiality commitments and requirements. SmartSimple analyzes the significance of risks associated with these threats and determines mitigation strategies, including controls, mitigation strategies, and other protective measures.

- 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 these ratings are reviewed by management.
- The Information Security Committee and ISMS teams evaluate the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation.
- The Information Security Committee and ISMS teams recommendations are reviewed and approved by senior management. Regarding the identification of potential threats, SmartSimple addresses security risks through various mitigation approaches. Below is a sample of risks and corresponding mitigation approaches:

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.

Risk	Mitigation Approach
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 Information Technology Information Sharing and Analysis Center (IT-ISAC). As such, we receive access to real-time threat intelligence, the opportunity to collaborate on defense strategies, and the ability to enhance our incident response. As a result, we significantly strengthen our risk mitigation efforts and ensure proactive protection against emerging threats. • Host-based security appliances are employed to secure and monitor servers. • Antivirus program employed on each environment at the OS level
Vulnerability discovered in existing Client Configuration	• Client System Security Summary Assessments, for System Administrators • Client specific pen testing (with an executed security testing agreement) • System Error Logs
Logical Breach of Hosting Security	• Continuous monitoring is provided by intrusion detection systems (IDS) and intrusion prevention systems (IPS), alongside anti-malware and logging solutions. • A Security Information and Event Management (SIEM) system is employed for real-time monitoring and alerting to potential security breaches. • Incident and Breach Response Policy and Procedures in place.
Physical Breach of Hosting Facility Security	• See Disaster Recovery plans

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 and/or access:**

SOC 1 Report – This report is an externally prepared independent service audit report conducted annually by Deloitte. It outlines our organization's controls relevant to financial reporting, as defined by the American Institute of Certified Public Accountants, Inc. (AICPA), and Chartered Professional Accountants of Canada (CPA Canada). SOC 1 reports are ideally suited for businesses that handle financial or non-financial information for their clients that impact the customer financial statements or internal controls over financial reporting, as it provides assurance that the necessary controls are in place to protect the integrity of financial transactions and reporting.

SOC 2 + HITRUST Report – This report is an externally prepared independent service audit report conducted annually by Deloitte, combining SOC 2 compliance with the HITRUST CSF (Common Security Framework). It outlines our compliance with both the Trust Services Principles and Criteria, as defined by the American Institute of Certified Public Accountants, Inc. (AICPA), and the stringent requirements of the HITRUST CSF. The HITRUST CSF is a widely adopted security framework in the healthcare industry, integrating various security, privacy, and regulatory requirements. This report provides assurance that our organization meets industry-leading standards for information security and privacy, particularly in contexts requiring rigorous healthcare-related data protection and regulatory compliance.

SOC 2 Type II Report – This is an independent service audit report prepared by Deloitte, an external firm, on an annual basis. The SOC 2 Type II report outlines our organization's compliance with Trust Services Principles and Criteria as defined by the American Institute of Certified Public Accountants, Inc. (AICPA), and Chartered Professional Accountants of Canada (CPA Canada). This report provides a detailed assessment of our organization's controls relevant to information security, and provides assurance that our systems are designed and operating effectively to meet rigorous industry standards. SmartSimple leverages the SOC frameworks to effectively manage security, availability, and processing integrity across our systems.

SmartSimple Software Policies and Procedures – SmartSimple maintains a comprehensive set of policies and procedures to ensure compliance with Trust Framework and ISO standards. These include our Information Security Management System (ISMS) policies, aligned with ISO 27001, Quality Management System (QMS) policies in accordance with ISO 9001, as well as our General Policies and Procedures (GPP) and Human Resources Policies and Procedures (HRP). Together, these policies guide our operations and governance to maintain the highest standards of security, availability, processing integrity, privacy, quality, and organizational effectiveness.

SmartSimple Trust Portal – To provide transparency and facilitate compliance reviews, SmartSimple offers clients access to our Trust Portal. This self-service portal is designed to help our communities and stakeholders understand our commitment to information security, data privacy, and corporate compliance. The Trust Portal provides real-time access to a comprehensive range of governance, risk, and compliance documentation, including certifications, audit reports, security policies, corporate code of conduct and ethical procedures, questionnaires, and other related resources. Access to the Trust Portal is granted under a Non-Disclosure Agreement (NDA) or an executed Master Services Agreement (MSA).

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.

5. GDPR Compliance Platform Features

SmartSimple is designed to empower clients in meeting their GDPR obligations through a flexible and comprehensive set of features. We provide tools and configurations that enable clients to manage personal data effectively and maintain compliance with GDPR requirements. Our platform supports GDPR compliance through two primary categories: Personal Data Management and Consent and Compliance. These features allow clients to customize their system configurations to align with GDPR principles, ensuring that personal data is handled with the utmost care and transparency. For more detailed information on how SmartSimple supports GDPR compliance, you can visit our GDPR Overview on SmartSimple's Wiki.

6. 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). Alongside IDS/IPS, SmartSimple uses a centralized monitoring solution for OS-level detection, ensuring comprehensive asset protection and streamlined security management.

Network firewalls are employed to restrict network traffic to the servers. Only specified ports are opened to the public.

7. Security Logs

The SmartSimple application logging contains 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. SmartSimple's system logging also tracks system performance, security threats, and resource utilization. Logs such as OS-level security activity, web server requests, and automation processes are retained indefinitely. System logs are aggregated and analyzed using a centralized security event management system, enabling rapid detection and response to incidents.

8. 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. SmartSimple's incident response process includes automated notifications, continuous monitoring, and a dedicated response team to ensure timely and appropriate action. Incidents are logged and tracked, with clear steps for investigation and resolution. Key events like system disruptions or security alerts trigger notifications that are promptly reviewed by authorized personnel. Where applicable, 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.

9. Physical Security

SmartSimple has partnered with Amazon Web Services (AWS) for our infrastructure hosting. AWS control points include secure design (site selection, redundancy, availability, capacity planning), business continuity & disaster recovery (BCP, pandemic response), and physical access controls (including employee data center access, third-party data center access, AWS GovCloud data center access). Access to sensitive areas is controlled and monitored through secure systems, with strict access protocols. Monitoring, logging, and surveillance (such as CCTV, Data Center Entry Points, intrusion detection) protect data centers, with operational systems (power, climate and temperature, fire detection and suppression, leakage detection) and infrastructure maintenance ensuring reliability, are all inherited by SmartSimple clients. SmartSimple conducts regular reviews of AWS physical security measures through vendor reviews, including audit reports to ensure compliance. More information on AWS compliance programs can be found here.

10. Reliability and Backup

All SmartSimple systems are backed-up on a nightly basis to a separate, secure data center in a different region or availability zone than the production environment.

A warm backup environment is maintained to ensure redundancy and uptime, utilizing automatic replication. Snapshots and backups are securely stored following industry best practices, including encryption and retention protocols for a period of up to 90 days. Additionally, monitoring processes ensure the integrity of backups, which are stored in geographically distinct locations to mitigate potential disaster risks. The security and recoverability of infrastructure assets is supported by comprehensive measures that ensure data is protected and easily recoverable in case of failures.

11. Disaster Recovery

SmartSimple maintains a comprehensive disaster recovery and business continuity plan based on SOC and ISO 27001 control points. Further redundancy is achieved through AWS-hosted infrastructure, with critical components backed up to a secondary, physically distinct environment to ensure high availability and reliability. In the event that a SmartSimple environment becomes unreachable and is deemed unrecoverable, the warm backup environment will be promoted to replace the production environment to restore availability.

12. Viruses

The SmartSimple platform accepts a large variety of file types for upload, but by default blocks the upload of select executable and binary types, and further configuration may be applied to further restrict allowable file types. Uploaded files are automatically scanned for viruses and malware once uploaded to the system. Any files flagged during scanning are quarantined. To ensure additional security, the system continuously monitors for virus threats and provides real-time alerts when issues are detected.

13. Data Encryption

All SmartSimple platform data is encrypted in transit and at rest using SSL and TLS protocols to prevent interception. Encrypted hard disk storage uses AES (256 Bit Key). Separate environments for production and non-production are logically and physically segregated to ensure security. Passwords are securely stored in the database using SHA-256 and are further protected with techniques like salting and key stretching.

14. Data Return and Deletion of Customer Data

SmartSimple provides a 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.

In the event of contract termination or expiration, the following steps will be taken to ensure the secure handling and deletion of customer data:

1. **Data Export:**
    - Within 30 days after the effective date of termination, SmartSimple will provide the Client with the ability to securely export their data. The data export will be made available through a secure method, typically via Secure File Transfer Protocol (SFTP), ensuring confidentiality and integrity during transit. The Client is responsible for retrieving the data within 90 days from the provisioning date. Any request for an extension must be communicated in a timely manner.
2. **Data Retention and Deletion:**
    - After the 90-day period, SmartSimple will permanently delete the Client's data from all active and archival storage systems. Data deletion will follow industry standards such as those outlined in the Department of Defense (DoD) 5220.22-M or NIST SP 800-88 guidelines for media sanitization, to ensure complete data destruction.
    - Upon completion of the deletion process, SmartSimple will issue a Certificate of Destruction, signed by a senior officer, confirming that all copies of the Client's data have been securely purged.

SmartSimple adheres to ISO 27001 and SOC 2 Type II compliance throughout the data export and deletion process, ensuring actions taken align with documented policies and procedures in our Information Security Management System (ISMS).

15. Sub-processor List

The current list of Sub-processors engaged in processing corporate and customer data for the performance of the Service, including a description of their processing activities and countries of location, is detailed in the "Infrastructure and Sub-Processor Documentation" (ISMS_44). This document can be provided directly to customers upon request, or can be accessed through SmartSimple's Trust Portal. Additionally, the Trust Portal contains a mechanism that allows customers to subscribe to notifications regarding any updates or new documentation, including new Sub-processor lists.