Infrastructure and Security FAQ

Actionstep

Document Revision History

Version	*Issue Date*	*Author*	*Comments*
2.0	19 July 2022	Steven Mayhew	Converted from version 1
2.1	20 July 2022	Steven Mayhew	Amendments to structure and content

Contents

Introduction

Actionstep is a “Cloud” based service meaning that the software and data are centrally hosted and accessed by clients using a web browser and Internet connection. This document is intended to answer questions around the infrastructure, security, and intellectual property rights associated with the software and the data. Actionstep takes data security very seriously and follows generally accepted best practices to ensure that clients’ data is backed-up and protected against unauthorized access.

Hosting Environments and Data Sovereignty

Actionstep uses the secure Amazon Web Services (AWS) infrastructure to provide a secure and scalable platform to clients around the world. Actionstep clients are hosted in one of our available AWS regions that meets their data sovereignty and performance requirements. Security specifications can be found on http://aws.amazon.com/security/ and locations at http://aws.amazon.com/about-aws/globalinfrastructure/

Actionstep hosts in the following regions.

North, Central and South America:

- US-West-2 (Oregon)
- US-East-1 (N. Virginia)
- CA-Central-1 (Canada)

United Kingdom, Middle East, Africa, and Europe

- EU-West-1 (Ireland)

New Zealand, Australia, and South Pacific

- AP-Southeast-2 (Sydney)

Asia

- AP-Southeast-1 (Singapore)

Password Policies

Actionstep allows clients to implement password policies by system role. The password policies include the following settings:

- Minimum length
- Inclusion of special characters
- Forced mixed case or numeric content
- Expiry time
- Password rotation minimum
- Time of day and day of week access windows
- Source IP address restrictions

Lockout for Unsuccessful Login Attempts

Users are locked out after unsuccessful attempts on a exponential delay finishing with a permanent lockout with CAPCHA response required after any failed login attempt.

User Permissions

Clients can control who has access to the system by adding and removing logins as required. Each login is associated with a specific system role which governs the access rights to all aspects of the application such as which pages or menu items they can see and whether they can create, view, edit or delete data.

Audit Trails

Audit trails and session logs record user activity and changes made to the data by each user.

Intrusion Detection & Independent Security Assessment

The servers run perimeter protection software and log unauthorized attempts to access the systems and add these to blacklists. Actionstep engages independent external security specialists to regularly monitor the service and software for security vulnerabilities

Transport Layer Security

All data is protected with TLS protocols. Each web server is accessed through a load balancer and those load balancers have valid certificates.

Network Layer Security

The networks are split into private (non-routable) and public subnets with a firewall between them. Access to the private subnets can only be achieved over encrypted network links. The public subnets restrict access to HTTP(S) ports only and other ports are restricted. Password access is disabled for all servers and the only access is via encrypted keys over SSH.

Application Layer Security

All data transmitted between Actionstep and the user is encrypted via HTTPS.

System Administration Procedures

Systems administrators monitor the systems in real-time for any errors or unusual activity and record the events and action taken in an electronic log.

Actionstep has a disaster recovery plan in place, which covers communication procedures, responsibilities, and technical procedures to be followed to recover from the disaster.

Our disaster recovery plan is reviewed at least annually in consultation with system operations teams and management.

FAQ’s

Is my data encrypted?

All data transmitted between you and Actionstep are encrypted using SSL. Data is encrypted at rest in both database and document level storage.

Can full backups of data be provided as an automatic download?

Yes. You can extract your data to vendor-neutral spreadsheet and HTML formats and documents are provided in their original formats (DOC, XLS, JPEG, etc). You can request a backup whenever you wish by following the instructions in the user guide.

Who owns the intellectual property?

Anything you enter in to Actionstep belongs to you. Actionstep owns the core system and any modules or extensions we develop. Data ownership rights are clearly set forth in the Terms of Use – See https://www.actionstep.com/terms/.The intellectual property with respect to workflow configurations and associated document templates are owned by the originator. If a client creates their own custom configurations, then these intellectual property rights belong to the client. Configurations can be distributed or sold by the copyright holder if they wish.

Who has access to your data and under what circumstances?

The client has exclusive access to the data via username and password. Actionstep support staff may access client’s data for support purposes with the client’s permission.

Can Actionstep staff see my password?

No. Passwords are encrypted. If you forget your password Actionstep can create a new password for you but are not able to see your current password.

If I terminate the service, how is my data returned to me?

You can request a backup of your data and documents upon termination of the agreement.

If I terminate the service, what happens to my data?

Actionstep will remove all data from the servers after termination in accordance with the terms of service. See https://www.actionstep.com/terms/.

Does Actionstep have a policy to ensure confidentiality?

Yes. Confidentiality is set forth in the Terms of Service between the client and Actionstep, see https://www.actionstep.com/terms/. Actionstep staff members are required to enter into a confidentiality agreement under the terms of their employment.

Where is my data hosted if I don’t specify my data sovereignty choice?

Actionstep will automatically select a region that is likely to give you the best performance based on your location. If you require your data to be hosted in a specific region we have available, please let us know.

What types of Data are collected and shared by Actionstep as part of products and services provided?

No data is shared with external products or services apart from services used to track usage through the system. Actionstep creates and collects collect session cookies. Beyond this, for each user Actionstep captures details required to verify that users. Similar details are captured about the organization. These details are also used for internal marketing demographic purposes

Does Actionstep have a policy to secure and cleanse client data on electronic and hard copy media that is to be disposed or re-used?

No client data is stored on physical devices.

What policies are in place to ensure that internal staff handle client data ethically and responsibly?

All prospective Actionstep staff are given full police and background checks prior to employment. All staff sign non-disclosure agreement as part of their employment contracts. Once hired, all new staff are trained on security awareness and policies during their onboarding training.

Does Actionstep have documented configuration management and hardening standards and a consistent build configuration for the operating systems and databases housing client data?

Actionstep has a documented configuration management system and we follow industry best practices

Is logging enabled for the systems housing client data?

Logging is enabled and will capture a large range of security events including logging on, logging off, creating, editing or deleting items, sending/receiving emails, calendar alerts, accounting functions, accessing matters, changes to admin functions and more.

Requests for Proposals/Information (RFP/RFI)

Some clients will send out a Request for Proposals (RFP) or Request for Information (RFI) before engaging with a supplier. The level of detail varies from client to client, and some can be very specific. However, providing too much detail on internal operations can be counter-productive to security. Consequently, Actionstep only provides the following additional information in relation to and RFPs or RFIs.

All questions relating to hosting infrastructure and security

Actionstep uses Amazon Web Services so please refer to http://aws.amazon.com/security/ for any related questions.

Scalability

Actionstep takes full advantage of the built-in scalability features offered by AWS, including auto-scaling and load balancing.

Certifications/Attestations, Laws, Regulatory, Privacy, Alignments/Frameworks

Actionstep hosted on Amazon Web Services inherits these assurance programs. For details please see https://aws.amazon.com/compliance/

Security assessments and penetration testing

Actionstep has an on-going engagement with an independent security firm which provides regular source code inspection and external penetration testing. If required, prospective clients can request to perform a penetration test at their cost.

Disaster Recovery Plan

Actionstep has a documented and tested disaster recovery and communications plan. The plan itself is hosted externally to the production infrastructure.

Incident Response Procedure

Actionstep has a documented incident response plan and a register of incident responses which includes a workflow for staff to follow.

Backups and Redundancy

Actionstep writes documents to redundant disk subsystems and uses database replication for real-time backups. Additionally, Actionstep backs up client databases at least once every 24 hours and utilizes multiple availability zones in each AWS region. In the event of an instance failure the disk subsystems can be attached to a new code instance. The disk subsystems consist of redundant disk arrays so any failure in an individual disk should not result in data loss.

Recovery Point Objective (RPO)

The RPO is 5 minutes.

Recovery Time Objective (RTO)

The RTO is 4 hours.