

Social Solutions Global, Inc. (“SSG”) takes comprehensive measures to ensure that data is kept safe, confidential and recoverable in the case of a disaster. Our software meets current HUD Domestic Violence, HMIS, and Social Security Administration data management and security protocols, as well as minimum required FERPA and HIPAA standards. Social Solutions’ office sits behind a ForcePoint™ firewall which extensively controls, tracks, and reports access to our internal infrastructure.

## Data Security

ETO® secures sessions with user names and passwords to prevent unauthorized access and to restrict user access within the application. Each unique user account is assigned access to programs and permission sets to restrict access to data and features in the system. Customer data is housed in two locations (U.S. and Canada) based on the location of the client. Data is stored using redundant AWS hardware technologies and SSG fault tolerant software and journaling file systems.

## Passwords

- ✓ can be set to have a minimum length
- ✓ can be set to contain non-alpha-numeric characters
- ✓ can be set to expire
- ✓ can be locked after a set # of invalid login attempts
- ✓ can be changed by a local administrator
- ✓ are not displayed upon entry and are encrypted

## Encryption

Social Solutions uses state-of-the-art equipment and technology to safeguard the confidential nature of your data. Your data is automatically encrypted while in transit between your computer and our servers through Transport Layer Security (TLS). The encryption protocols and the cipher suites used to access ETO software meet the Federal Information Processing Standard (FIPS) 140.2 requirements. ETO software’s data storage is secured by AES-256 while at rest.

## SOC2

Our SOC2 Type 2 (SSAE18) report is a comprehensive document that describes Social Solutions security controls in the domains of Administrative, Physical, and Technical security. Apricot is certified SOC 2 Type II compliant. SSG security controls are reviewed by independent external auditors during audits for our SOC compliance.

## Amazon Web Services (AWS) Server Security

Each of our servers is individually governed by a system that is designed to prevent unexpected Internet data from being processed by our server software. IDS, virus scanning, automated system checks, and remote logging guard against unauthorized access. AWS implements electronic surveillance and multi-factor access controls to secure its data centers. Data centers are staffed 24x7 by trained security guards, and access must be strictly authorized. The AWS database utilizes object-based storage in the form of backups to S3 in encrypted folders. Multiple availability zones allow ETO to remain resilient in the face of most failure modes, including natural disasters or system failures<sup>1</sup>. In case of a disaster at the AWS East region, Social Solutions will have ETO up and running between 24-48 hours at the AWS Oregon region. The disaster recovery process is tested annually.

## Redundant Infrastructure and Backups

- ✓ 24/7/365 monitoring of uptime across the infrastructure
- ✓ Redundant water, power, telecommunications, and internet connectivity to maintain continuous operations
- ✓ Fully redundant SAN access storage and daily AES-encrypted full backups

## Retention Policy

- Keep daily backups for 7 days
- Keep weekly backups for 6 weeks
- Keep monthly backups for 12 months
- Keep yearly backups for 1 year

## Compliance

The AWS cloud infrastructure has been designed and managed by Amazon.com. AWS adheres to: SOC 1/SSAE 16/ISAE 3402 (formerly SAS70) SOC 2 SOC 3 PCI DSS Level 1 ISO 27001<sup>2</sup>

<sup>1</sup> For additional information visit: <https://aws.amazon.com/whitepapers/overview-of-security-processes/>

<sup>2</sup> For additional information visit: <https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/>