VST Security
All client data is encrypted in transit using TLS with 2048-bit RSA certificates, and at rest using FIPS 140-validated AES-256 encryption managed by AWS. Encryption keys for data at rest are generated, stored, and managed by AWS under the controls described in the security Org Documents listed below. All client data is stored and processed on VST's systems in AWS GovCloud (US), within the United States, and access is limited to accredited users only.

Definitions
Keyword – Definition

VST - Victim Services Tracking
VST-services - Cloud based software applications
Login-credentials - A unique username and password assigned to a VST-user
VST-user - An individual that has login-credentials and is authorized to use VST-services
VST-client - The individual and/or organization responsible for the VST membership and administration
VST-client-data - All information/data submitted by the VST-client to VST-services

Frameworks and Guidance Referenced (Org Documents)
VST's security practices are informed by the following frameworks and guidance. Listing a framework does not mean VST is certified or audited against it.

NIST - https://www.nist.gov/
CJIS - https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
HIPAA - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
FIPS 140-2 - https://csrc.nist.gov/publications/detail/fips/140/2/final
FIPS 200 - https://csrc.nist.gov/publications/detail/fips/200/final

What are VST-services and the cloud?
VST-services are cloud-based applications that assist the VST-client in managing case work and government grants. The only system requirement is a modern browser; such as Google Chrome, Microsoft Edge, Mozilla Firefox, or Safari. In this context, the cloud is Amazon Web Services GovCloud (US), a U.S.-only cloud environment designed for regulated government workloads, where VST-client-data is processed and stored.

How does the login/authentication work?
Access to VST-services is done by using a standard user login and password across the https protocol. Simply go to agencyservicestracking.com and provide your login-credentials; normally an email and password. Passwords must meet minimum complexity requirements, and VST-client Administrators can enable additional protections, including required password rotation, prevention of password reuse, and account lockout after repeated failed login attempts.

www.advocateadvantage.com (970) 425-6393 info@advocateadvantage.com

Multi-factor authentication (MFA) is available using any standard authenticator app (TOTP). VST-client Administrators can require MFA for all users; if it is not required, individual users can enable it for their own logins. Single sign-on (SSO) is supported through SAML, including Microsoft Azure Active Directory (Entra ID) and other SAML identity providers.

VST-services uses the RBAC (role-based access control) model to allow VST-clients the ability to control who has access to what. VST-client Administrators can set the permission levels for each advocate granting or revoking access to the various VST-services. After a successful login, a time sensitive access key is granted to the browser and used to make authenticated requests to a VST-service.

Your data is your data!

- All VST-client-data belongs to the VST-client.
- VST does not share VST-client-data with third parties, other than the service providers needed to operate VST-services (such as AWS hosting). Only aggregate, non-identifiable data may be used to improve VST-services.
- Only specific VST employees and contractors are authorized to access and maintain VST-client-servers.
- The VST-client has full authority over the VST-client-data and can decide what happens to it in terms of removal, storage and transmission at any time for any reason, subject to the Data Retention and Deletion section below.

Who has access?

- Only specific VST employees and contractors are authorized to access VST-client-data, and only to perform maintenance and upgrades or to resolve a support request. All VST support access to a VST-client account is recorded in an audit log.
- VST-client administrators are authorized to access the data at any time and the VST-client advocates can access the data according to their respective roles assigned by the administrator.

Personnel Security

- All VST employees and contractors with access to VST-client-data complete a background check and annual CJIS Security Awareness Training (CJIS Online certification).
- Upon request, VST will execute the FBI CJIS Security Addendum, or an equivalent addendum required by the VST-client's CJIS Systems Agency, and the applicable personnel will sign the corresponding certification.

Where is your data and data backups?

- All VST-client-data is stored in AWS GovCloud (US), in the United States, and protected with FIPS 140-validated AES-256 encryption managed by AWS.

www.advocateadvantage.com (970) 425-6393 info@advocateadvantage.com

- The data is encrypted in transit and at rest and backups are made daily and encrypted, and are also stored in AWS GovCloud (US).
- Each VST-client's data is isolated from other VST-clients.
- Each VST-client's data is stored in its own separate database. Standard memberships host these databases on a shared database server; VST-clients that require additional isolation can have their database hosted on a dedicated database server. Application code is shared across all VST-clients.
- Databases are not publicly accessible. They run on a private network, protected by firewalls that block all traffic by default and allow only explicitly approved connections.

Data Retention and Deletion
When a VST-client's subscription ends, VST-client-data is permanently deleted from VST's production systems between 90 and 97 days after the end of the subscription term (or after any grace period VST grants while awaiting payment). VST can reactivate the account on request during that period. Backup copies containing VST-client-data are permanently deleted no later than 95 days after that production deletion. Until deleted, backup copies remain encrypted, are not accessible to the VST-client, and are used solely for disaster recovery.

A full MySQL database backup, with documentation of the database structure, is provided free of charge to VST-clients who leave VST.

Personally Identifiable Information (PII)
The information stored in VST databases consists of, and is not limited to, victim contact information and the nature of their victimization. Identification numbers can be associated to victims as opposed to names and/or addresses to meet compliance requirements. Grant reports contain only aggregate statistics and do not include PII or location data.

Support Requests
VST-services is the secure environment for VST-client-data. Support requests are handled in VST's support system, which is separate from VST-services. To keep sensitive information within VST-services, please identify records in support requests by case or record number, and do not include client details, screenshots, or attachments containing client information.

Infrastructure Certifications
VST-services are hosted in AWS GovCloud (US). AWS maintains ISO/IEC 27001 certification, SOC 2 reports, and FedRAMP High authorization for AWS GovCloud (US), and supports customers hosting criminal justice information under the FBI CJIS Security Policy. These certifications apply to AWS's infrastructure; VST itself is not separately ISO 27001 certified and does not currently have a SOC 2 report.

www.advocateadvantage.com (970) 425-6393 info@advocateadvantage.com

What happens if a breach occurs, a vulnerability is found, or if a natural disaster occurs?
These are the steps VST will take once a breach or vulnerability has been discovered. The execution of these steps depends on the severity of the issue and will be performed in a timely manner from the date of discovery.

1 Disable and reset all login-credentials of affected accounts
2 Develop a plan-of-action based on the severity of the issue, this includes fixing the vulnerability and enabling data recovery if necessary
3 Notifying the affected VST-clients
4 Notifying law enforcement if necessary
5 Implementing the plan-of-action

In the event of a natural disaster or infrastructure outage, VST-client databases are replicated across multiple AWS availability zones, and encrypted daily backups are retained for 90 days so that VST-client-data can be restored if needed. VST-users are notified through the in-application Notifications area and by email of any significant service interruption.

VST Training and Service Schedule
VST performs recurring scheduled maintenance and employee training. The table below shows each procedure and its frequency. Maintenance routines generally run after the close of business (Mountain Time) to minimize client downtime; server updates may occur during business hours when safe.

Procedure	Daily	Annually
Data Backups	X	
CJIS Security Awareness Training		X

Server security updates are applied with each deployment.

Security Contact
Questions about VST security, or reports of a suspected vulnerability or security incident, can be sent to support@vstracking.com.