Stella CONNECT

Security and Data Protection Policies Overview

Version 1.1

Introduction & Purpose of this Document

Stella Connect employs a variety of policies, procedures, technical controls, and human resource initiatives to protect data, and this overview summarizes them for the purpose of explaining its security posture to its clients and other interested parties. This document is written so as not to reveal details that would otherwise weaken the security of StellaService's systems, including Stella Connect.

What is Stella Connect?

The service is designed to enable customer service representatives to request feedback from customers who have had a recent interaction. It gathers feedback and textual commentary. This information is organized for customer service representatives and their managers to identify opportunities to improve performance and to reward excellence.

Types of Data in Stella Connect

End customer information required by Stella Connect

The customer service representatives or Client Organization will supply the following data about their customers. This information is used to execute a feedback request via the Stella Connect web application or via an encrypted API request:

1. Customer email address
2. Customer name
3. Customer phone number
4. Customer custom identifier

As described in more detail below, all of the above data is encrypted in transit and encrypted at rest, and other additional layers of controls are in place to protect the privacy and security of this information.

Employee information collected by Stella Connect

In order to create accounts for customer service representatives/employees, the following information is needed about the employees using the system to request feedback:

1. Employee first name (required)
2. Employee last name or initial (required)
3. Hometown of the employee (optional)
4. Home state or country of the employee (required)
5. A description of the employee's interests (within 140 characters, optional)
6. A photo or avatar image of the employee (optional)

Employee accounts are created by a Company Administrator, who can either create the employee's entire profile or invite the employee to confirm his/her account and then complete a profile in the Connect system.

All employee account creations go through a validation process in which Manager accounts (previously created by the Company Administrator) receive an approval request after an employee creates an account. Only after the Manager has approved the employee account can the employee then have feedback request emails sent to customers from the Connect system.

Customer data storage and retention

All data is stored within Amazon Web Services - primarily in the US-East region.

Upon termination of the Connect service by a Client Organization, the data accumulated will be dealt with as follows:

- Upon client's request, all data will be removed that is not needed for contractual or legal reasons.
- In any case, within 7 days, customer name and email will be removed from the database and referenced solely via a system-generated anonymous identifier
- Within 30 days, email send logs referencing successful customer email deliveries will be purged
- Within 90 days, email send logs of any unsuccessful customer email deliveries will be purged

Security & Privacy Controls

Below is a list of security processes, technological controls and compliance details currently implemented in the StellaService Platform.

Data Center Security

The Stella Connect software platform is hosted on isolated cloud-based networks protected by firewalls and several layers of access control. The platform is hosted primarily by Amazon Web Services (AWS) in the northeastern United States. Details of physical and software security systems in place for AWS are here: https://aws.amazon.com/security.

Parts of StellaService are hosted on Google Cloud Platform (GCP) in its northeastern United States data center. Details of physical and software security systems at GCP are here: https://cloud.google.com/security.

Only authorized personnel have credentials to access the StellaService AWS and GCP accounts. Authorized personnel each have a separate account with different levels of permissions. We use Identity Access Management (IAM) services to manage roles at a granular level based on the position of the engineer, with minimal access granted in each case, and access levels are reviewed at least quarterly. Changes to permissions are audited by AWS Cloudtrail and GCP's Cloud Audit Logging. Multi-factor authentication is required to log into the accounts on AWS and GCP.

Database field encryption

Due to the sensitive nature of end customer information, PII of end customers is stored encrypted at rest with AES-256 symmetric encryption. The encryption keys are stored separately from the data and vary by client. This means exfiltration of the database will not allow a hacker to access end customer PII. Distinct client-based keys means that access controls force a logical separation of client data.

Security Patching Policy

Patching and updating of the underlying systems are performed and coordinated by our devops and security team. All changes to infrastructure assets are reviewed by qualified personnel before applied to systems. The StellaService tech team periodically applies OS patches to our EC2 servers. Critical security patches are applied promptly to all servers. Before applying OS patch releases to the live environment (accessed by customers), we first automate the process and run it in a testing environment to cover edge cases and prepare. Patching a server is considered a system upgrade, similar to the release of code. Patches are evaluated by the tech team and the appropriate level of testing is applied prior to releasing to production.
Once a patch is cleared for release, scheduling of the release follows the general StellaService Release Management Process. Each patch is classified based on severity of impact and potential for service disruption. Client notification on patches follows the risk classification of each patch, according the the StellaService Release Management Process. StellaService provides support for releases to ensure the platform is online to our clients after applying OS security patches to our servers in AWS and for other support needs.

Managed services such as S3, Lambda, databases and GKE are patched regularly by Amazon as part of the AWS SLA or by Google as part of the GCP SLA. Details of their patching policies can be found in their respective security policies.

Vulnerability Management and Web Application Security

StellaService runs a web application vulnerability scan of all of our applications on a quarterly basis and analyses the report in order to identify new vulnerabilities.

On an annual basis StellaService employs an outside penetration testing firm to do a deeper penetration test involving trained hackers who have access to the site’s source code. This test involves a wide range of attack vectors, from the network to the web application to the business logic and permissions systems.

Our software release process includes an automated scan of the codebase for vulnerabilities.

As part of the SDLC, an architecture review is initiated by a committee for infrastructure-changing features, and security impacts are considered. If there are material impacts to the security or handling of data, the change is accompanied by a Data Privacy Impact Assessment.

We have documented standard security configurations for each system type that are reviewed annually and as needed.

We have a tiered classification structure for vulnerabilities discovered through the above process, and there is a prioritization process for mitigation based on that structure. High risk vulnerabilities are addressed immediately without delay. Medium risk vulnerabilities are addressed within 1 month.

We review audit logs quarterly.

We have a formal plan in place for determining incident scope, building the correct response team, isolating the incident, gathering evidence, mitigation, and notification.

StellaService servers are virtualized and are managed via a container system. This means that our anti-malware activities are adjusted to the containerized architecture. All configuration is checked against our approved configuration. Source code changes are automatically scanned for malware. Libraries are analyzed for malware before being added to a container configuration. Container activity is monitored for malware signatures.

A combination of systematic safeguards and following security best practices as well as continuous monitoring of logfile output are used to guard against unauthorized access.

Intrusion Detection

StellaService servers are ephemeral containerized servers that run on top of a highly secured server subsystem that runs intrusion detection systems (IDSs). The IDSs use a range of signature-based detections that involve known malware signatures and heuristic processes for discovering new types of infiltration. We are alerted immediately if an intrusion is detected.

Separation of access levels for source code and non-privileged configuration information

Only named designated engineers and administrators authorized and responsible for making changes to the code and configuration of the Connect system are permitted write-access via source controls systems and configuration and deployment management systems.

Other designated engineers and administrators are provided with read-only access to source control systems and configuration management systems via specific read only roles within such systems.

Data Access Policy for StellaService employees

In order to maintain the confidentiality and security of customer and consumer data, StellaService has implemented a variety of access roles to balance the need to support and service customers and retain necessary security of information. The following levels of access exist for StellaService employees:

Designated Engineering and Infrastructure Personnel	Can access and maintain all data			
Designated Client Service Personnel	Access all Data	Destroy select data	Alter Client Configuration	grant similar access

All Client Service Personnel	Access all Data		Alter Client Configuration	
Client Account & Sales Personnel	Access all non-PII Data			

Exceptions to these access roles must be requested, granted and recorded in an internal management system.

Access to the production database store and backend systems is limited to the developers maintaining the system and our devops team.

Access to the Connect web interface is via https authentication, and is controlled via roles determined by the Connect administrators and Company administrators. Roles specifically restrict the ability to access and export sensitive data, to select accounts with specific business needs for it.

All personnel with access to the Connect platform have the following security measures enabled.

- Two factor authentication required for email and domain services
- Workstation hard drive secured using up-to-date industry standard encryption practice
- Workstations configured to require re-authentication if left unattended no more than 5 mins
- Inventory management system that includes the ability to remotely wipe the storage

For shared documents, any document or data containing raw or line item client data is shared via google drive shared folders, with explicit access granted only to authorized recipients.

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive information.
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
- We require the use of password managers with strong passwords as best practice internally, and we recommend them for our clients.
- We believe that enforced password expiration encourages easy-to-crack passwords and we do not require password rotation. Therefore, we do not have a policy around limiting password values based on originality.
- Within the application, passwords are never transmitted or stored in plain text, and are salted and hashed in our database, and once lost they can only be reset, not recovered.

Separation of Production and Staging (testing/development) environments

The Production infrastructure is kept separate from other infrastructures and access to each is distinct and uses unique credentials for each individually.

Additionally, only sanitized / anonymized data as opposed to full copies of production data is used in non-production environments.

Log management and Event Consolidation

Logging of all production systems is centralized, and access is restricted similarly via 2FA https account-based logins. Alerting of infrastructural problems and abnormal access patterns is provided via integrations with several hosted services which receive event and error logs that have been stripped of customer data.

For server access, security events are logged (e.g. logon, logoff, timeout, changes to privileges, etc). Security logs are also sent to ELK and follow the same backup procedures and retention policies as our server logs.

The system also logs to our database the audit log with changes to any entities in the system (users, roles, data changes, etc.).

Lastly, for Enterprise Service Management, we use AWS CloudTrail which records any access and changes to our AWS account, either via AWS console or API.

Acceptable Use Policies for Network and Equipment

StellaService employees are required to use the Internet in an effective, ethical, and lawful manner.

Outbound internet access is controlled via a network firewall that tracks all activity and blocks several types of malware and intrusion.

Unauthorized distribution of Information and data about clients or client's data is not permitted.

StellaService tracks devices using a centralized inventory management system that is synced with software on each device.

Data Backup Setup

Database backup is executed by AWS RDS every day with retention up to 30 days. The database is hosted in a replicated setup with point-in-time recovery enabled.

Source code is stored in a version control system that employs secure backups.

DDoS Protection

AWS provides protection against common, frequently occurring network and transport layer DDoS attacks that target our web applications through its AWS Shield service.

AWS Shield provides always-on network flow monitoring which inspects incoming traffic to AWS and uses a combination of traffic signatures, anomaly algorithms and other analysis techniques to detect malicious traffic in real-time.

Automated mitigation techniques are built-into AWS Shield, giving us protection against infrastructure (Layer 3 and 4) attacks. Automatic mitigations are applied inline to our applications so there is no latency impact. Always-on detection and inline mitigation minimize application downtime and does not require engagement with AWS Support to receive DDoS protection. AWS Shield uses several techniques including deterministic packet filtering, and priority based traffic shaping to mitigate attacks without impact to our applications.

Disaster Recovery and Business Continuity

StellaService has a written disaster recovery and business continuity program that is committed to by the leadership of the company. The plan includes:

1. Risk management and business impact analysis activities to identify recovery priorities
2. Processes for notification of stakeholders
3. Processes for disaster recovery

The plan is regularly tested and reviewed through the enactment of tabletop exercises and team reviews.

Compliance and Certification

StellaService reviews compliance with the StellaService Information Security policies as well as the Privacy Policy published on our website on a quarterly basis. After reviewing compliance, we provide a report to our executive board. Where applicable we highlight known compliance gaps and plans for addressing them in the future.

On an annual basis the internal information security and privacy policy is reviewed for consistency and accuracy with our practices and obligations, and it is reviewed for compliance with any updated privacy regulations globally.

Description of current compliance with existing standards:

OWASP

For OWASP, we follow security guidelines and implement the OWASP Top 10. We are continuously improving compliance to our policies to harden even more our web application security.

PCI Compliance

Because StellaService does not accept, process, or store credit card data, the PCI standard does not currently apply to our software.

GDPR Compliance

StellaService is on track to being GDPR compliant by May 25, 2018, when the GDPR goes into effect. This includes internal procedures to comply with data subject access requests, with a 20-day SLA to help our clients address their own customers' requests.

Security Awareness

We use third party alert services to keep up to date with the latest vulnerabilities, including: https://www.us-cert.gov/ncas/alerts

A combination of systematic safeguards and following security best practices as well as continuous monitoring of logfile output are used to guard against unauthorized access.

Employee Training

StellaService is committed to training and education on Information Security. The InfoSec team engages in the broader security ecosystem and brings insights and policies to the company as they are appropriate. The StellaService philosophy on security is that it is a continuously changing environment and requires ongoing engagement. Security training is provided to every employee as part of their onboarding process. Updates to any policy or procedure are disseminated to the team promptly. All employees are required to top up their security awareness through online or in-person security trainings every year, and to renew their commitment to the internal security and privacy policies. Additionally, security and compliance topics are covered in company-wide meetings as new vulnerabilities are discovered and new procedures are introduced. NDA and confidentiality agreements are reviewed at a minimum annually.

Revision History

Date of Change	Version	Responsible	Summary of Change
2017-05-01	1.0	CTO	Creation of the document
2018-05-14	1.1	CTO	Changed level of detail. GDPR changes.