Secured Communications, LLC.

SERVICE LEVEL AGREEMENT

1.0 SLA Overview

This Service Level Agreement ("SLA") addresses the provisioning of Mercury product services and related Information Technology services required to provide, support and sustain Mercury Subscriber services including Mobile Applications, and Subscriber Support (collectively as "Service" or "Services").

This SLA outlines the parameters of all Services covered as they are mutually understood by Subscriber and Service Provider. This SLA does not supersede current processes and procedures unless explicitly stated herein.

2.0 Description of Services

Mercury Service is a communication system for secure, end-to-end encrypted one-to- one and group messaging, voice, collaboration, audio, video, image and file sharing. Services consists of a hosted web portal "Dashboard" that automatically syncs with user mobile devices ("Mobile"). The Command Center is accessible through a secure Internet web browser connection. Service Mobile connectivity is provided through iOS and Android mobile applications, or through mobile web browser connections.

Service includes two account roles, each with a role-specific version of the Dashboard:

a) Administrator – Includes access to all groups and account users, and administrative control over group creation/management, on-boarding, user device and license management, group membership security and assignment.

b) Individual User – Include access to assigned groups, individual secured contacts and individual file shares, where applicable under the Individual User's license.

2.1 Encryption

Mercury uses Advanced Encryption Standard 256 ("AES 256-bit") technology to protect communications including one-to-one and group messaging, voice, audio, video, image and file share. All communication through the Dashboard and mobile application is encrypted.

2.2 System Requirements

a) Mobile Application - Users should have the most current device operating system for best performance.

b) Dashboard – Users are able to access the Dashboard through any approved web browsing platform, including Microsoft Edge, Safari, Firefox, and Chrome.

2.3 Basic Permissions

Subscriber account is established with a minimum of one account Administrator and the specified number of User Licenses. Onboarding occurs when Administrators invite Users, who are subsequently assigned a User License (becoming a "Licensed User").

a) Users specify their own username and password for mobile app and Dashboard access when registering.

b) Users can install the mobile app to multiple mobile devices.

c) Users can be assigned to multiple groups.

d) Only Administrators can Burn group messages and export group message documentation ("Archive").

e) Subscriber may specify to have the "Burn" feature removed/disabled in the account.

2.4 Support

Subscriber support is provided through a combination of online Support portal, self-help FAQs and articles, provided Administrator and User guides (PDF documents), online Support Ticket submit, and direct telephone and email support (see below for details). See also Support, below).

2.5 Compliance

a) Service integrates technology and features for Health Insurance Portability and Accountability Act (HIPAA) compliant use by Covered Entities (CEs) when communicating Protected Health Information (PHI).

b) Service uses only Federal Information Processing Standard (FIPS) Publication 140-2 approved encryption algorithms which have been validated in all relevant categories.

c) Service incorporates technology and features for compliance with EU General Data Protection Regulation 2016/679, and shall process client personal data in accordance with GDPR.

2.6 Account Restrictions

The maximum number of Users is limited to the number of Account Licenses assigned to the Account pursuant to the applicable Order. Subscriber may request changes to the number of licenses assigned to the account. There are no restrictions on account usage for number of groups, volume of messages sent or received (both group and one-to-one), or files shared. Account total file storage is limited to two (2) gigabytes of data per Individual User unless otherwise specified in Account Service Order.

SECURED COMMUNICATIONS RESERVES THE RIGHT TO DENY SERVICE TO ANY PERSON OR ENTITY.

2.7 Service Profile

Service Provider is a U.S. based corporation headquartered in San Francisco, CA. The company leadership, management and employees are U.S citizens. All company computer servers are located within the United States in Tier-III facilities. Multiple redundant servers are operated to ensure continuous service operations. All servers used to host/deliver Services are wholly owned and controlled by Service Provider (no sharing with any outside entities).

3.0 (Reserved)

4.0 Stakeholders

The following Service Provider(s) and Subscribers(s) will be used as the basis of the SLA and represent the primary stakeholders ("Stakeholders") associated with this SLA:

a) For Service Provider
Secured Communications, LLC
One East Liberty St., Suite 511
Reno, NV 89501
+1 (415) 773-2886

b) For Subscriber
Name
Address 1

Address 2
Phone

5.0 Periodic Review

This SLA is valid from _____ and remains in effect until Services are terminated by Subscriber, discontinued by Service Provider with 30 day advanced notification to Subscriber, or this SLA is superseded by a revised agreement mutually endorsed by Service Provider and Subscriber.

The parties will endeavor to review this SLA at least annually. The current SLA will remain in effect during this review. The purpose of each review is to determine what, if any, changes to the current SLA are mutually acceptable such that a new agreement may be mutually endorsed by Service Provider and Subscriber.

6.0 Cancellation

Termination of this SLA terminates Services. Once Services are terminated, the Subscriber Account, along with all current messaging, file shares and Administrator, and User information will be removed and deleted from Service Provider's computers and systems. Once removed, this information is not retrievable. In the event Subscriber chooses to terminate Services, Service Provider recommends that group messages be archived prior to giving notice of Termination.

6.1 Termination

a) Subscriber may terminate Services with 30 day advance written notice to Service Provider.

b) Service Provider may terminate Services to Subscriber with 30 day advance written notice to Subscriber. Subscriber may also immediately terminate the Services if Subscriber has been indicted or charged with any material violation of international, federal or state law during the period of use of the Services or a subsequent vetting of Subscriber indicates any such Subscriber material violation.

7.0 Representatives

a) Subscriber shall identify a primary Account Administrator ("Primary Administrator") to be the primary point of Subscriber contact for receipt and use of Services as provided by Service Provider. The Primary Administrator shall be responsible for managing the Services account ("Account") by and for Subscriber. Subscriber may designate one or more Secondary Administrators ("Secondary Administrators") to assist
the Primary Administrator.

b) The Subscriber shall designate an Account Business Representative to be the primary point of contact for all aspects of business, billing and account management for the Service account.

c) Service Provider shall identify a primary Account Relationship Manager ("Account Manager") to be the
primary point of Service Provider contact for delivery and performance of Services as provided to by Service Provider. The Account Manager shall be responsible for managing the Services account ("Account") by and for Service Provider. The Account Manager shall also be responsible for facilitating regular reviews of this document ("Document Owner"). Contents of this document may be amended in writing, as required, provided mutual agreement is obtained from Stakeholders to this Agreement, and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

8.0 Support

Account support ("Subscriber Support" or "Support") provided to Subscriber by Service Provider cover all aspects of Services as used/accessed by Subscriber, and include user self-help support, message and ticketing, and direct live-person first-level and second-level assistance (third-level programming support is internal to Service Provider).

8.1 General Help and Support Inquiries

a) Email: support@securedcommunications.com

b) Web: https://securedcommunications.freshdesk.com/support/home

8.2 For "How-To" Issues

a) Online "Help" page FAQ's and downloadable user guides. Help page link online at https://securedcommunications.freshdesk.com/support/home;

b) Online "Help" page downloadable User Guides. PDF user and "how-to" guides available;

c) Contact their Primary or Secondary Administrator for Subscriber;

d) Online "Help" page Submit a Support Ticket. Support tickets are logged for history and responded to within 24 hours, 7 days per week (usually same day); and

e) Email Support at support@securedcommunications.com. Support emails responded to within 24 hours, 7 days per week (usually same day)

8.3 For Other Non-Emergency Support

a) Online "Help" page FAQ's and downloadable user guides and help page link;

b) Online "Help" page downloadable User Guides. PDF user and "how-to" guides available;

c) Online "Help" page Submit a Support Ticket. Support tickets are logged for history and responded to within 24 hours, 7 days per week (usually same day); and

d) Email Support at support@securedcommunications.com. Support emails responded to within 24 hours, 7 days per week (usually same day).

8.4 For Subscriber Non-Emergency Support Escalation

a) Users should contact their Primary or secondary Administrator for Subscriber; then

b) Administrators should check the Service Providers Support Manager; then

c) Administrators to contact the Support Manager for Service Provider; then

d) Administrator to contact the IT Technical Support Manager for Service Provider; and then

e) Administrators should contact the Account Manager for Service Provider.

8.5 For emergency Support

a) Email Support at support@securedcommunications.com;

b) Call the Support Manager for Service Provider;

c) Call the Account Manager for the Service Provider; and

d) Call the IT Technical Support Manager for Service Provider.

8.6 For After-Hours Support

a) Call the Support Manager for Service Provider;

b) Call the Account Manager for the Service Provider; then

c) Call the IT Technical Support Manager for Service Provider.

9.0 Service Performance

9.1 Subscriber Responsibilities

a) Administrators to attend at least one full session of Service training (online live webinar) as conducted by Service Provider.

b) Administrators to read and review Administrator System Guides, User Guides, Mobile App Guides, and any other system documentation provided, including updates, as issued by Service Provider.

c) Administrators to issue a current copy of both the User and Mobile App Guides to all Users.

d) Administrators to advise Users of the how, and in order of preference, to access/request Service Support (see above).

e) Administrators to provide first line support to Users related to "how-to" questions.

f) Administrators and Users to, whenever possible, update registered mobile devices to the latest operating system (iOS or Android).

g) Administrators and Users to, whenever possible, update their Internet browser to the latest version available.

9.2 Service Provider Responsibilities/Commitments

9.2.1 Support Access

a) Email - Maintain a dedicated support email address for sending and receiving Support related communication. Email: support@securedcommunications.com. Monitor Support email from 8:00 AM to 5:00 PM (Pacific), Monday through Friday, 52 weeks per year. All Support email to be replied to within 24 hours.

b) Help Desk - Maintain a dedicated online help desk for current FAQ's, downloads (guides, etc.) and submission of online support tickets to Support. Online: https://securedcommunications.freshdesk.com/support/home

c) Support Tickets - Monitor Support online submitted tickets from 8:00 AM to 5:00 PM (Pacific), Monday through Friday, 52 weeks per year. All Support online tickets to be replied to within 24 hours.

d) Emergency Support - Calls received out of office hours to mobile phones for the Account Manager, Support Manager and/or IT Technology Manager, who will individually and/or collectively make best efforts to answer / reply and take action.

e) Onsite - Onsite assistance is available. Fees may apply and would be agreed to in advance by Subscriber.

9.2.2 Support Response Resolution

a) High Priority – Issues effecting immediate Service access and day-to-day usage. Resolution within 8 hours, during business hours, Monday through Friday.

b) Medium Priority – Issues effecting Service performance and improvements. Resolution within 48 hours, during business hours, Monday through Friday.

c) Low Priority – Issues related to Services updates and changes. Resolution within 5 working days.

9.2.3 Service Performance

a) Maintain all systems, software and hardware related to providing the service to ensure delivery of Services as herein described (se 3.0 Description of Services, above).

b) Maintaining a consistent Service uptime of at least 99.99% as measured by the Service Provider's system administrative logs. This includes scheduled maintenance. (Note: Current uptime is 99.9998%).

c) Maintain a separate, external system for monitoring system, software and hardware uptime, for monitoring redundancy and system administrative log validation.

d) Provide email notification to Subscriber at least 24 hours in advance of all scheduled maintenance, unless Subscriber and Service Provider both agree, verbally and/or in writing, on the need for a specific maintenance action to be initialed sooner than after a 24 hour notification window.

9.2.4 Changes to Services

a) Significant changes to Services as used/interfaced by Subscriber, including the delivery of significant new features, to be communicated in writing prior to Custom prior to implementation.

b) Significant changes to Service Provider maintenance practices or activities to be communicated in writing to Subscriber at least 24 hours in advance of implementation.

c) Significant changes to Services encryption or other core technologies to be communicated in writing to Subscriber at least 30 days prior to implementation.

d) Significant changes to Subscriber data storage methods/practices to be communicated in writing to the Subscriber at least 30 days prior to implementation.

9.2.5 Subscriber Data

a) Subscriber is the owner of all data, information and communication in their Account.

b) Service Provider permanently retains all Subscriber data in the account unless the Subscriber deletes and wipes message conversations (Burn feature).

c) Subscriber has the ability to delete and wipe all Group conversation from the Account (group message Burn feature). Only Administrators have the ability to Burn group message conversations.

d) Subscriber users have the ability to delete and wipe one-to-one message conversations from their perspective individual accounts (individual message Burn feature).

e) Subscriber has the ability to have Burn feature (both group and individual message conversation) disabled for the entire account.

f) Subscriber has the ability to archive and store outside of the account, all group message threads.

g) Service Provider will not sell, provide or allow access to Subscriber data to any third party.

h) In the event Subscriber terminates Agreement, Subscriber has full rights to all data, including export of all Group messaging data ("Archive"). Secured Communications will delete all Subscriber data after receiving approval from Subscriber to delete Subscriber data.

i) Service Provider to notify Subscriber within 72 hours in the event of known data breach.

9.2.6 Service Technology

a) Service Provider wholly owns its proprietary technology for its Services.

b) Service runs on Windows 2012 Servers using SQL Server Database platform and Dot Net Desktop application.

c) Interconnected mobile applications use Java (for Android) and xCode (for iOS)

d) Service Provider operates a redundant network with 100 percent dedicated servers located in Tier III data centers. All servers are dedicated to Service Provider. Servers are not shared.

e) Subscriber data is auto backed up daily with monthly backups maintained indefinitely.

f) Service Provider maintains redundant cold sites that can be operational in no more than four hours in a disaster recovery situation.

9.2.7 Encryption Validation

Service Provider uses only Federal Information Processing Standard (FIPS) Publication 140-2 approved encryption algorithms in all relevant categories for Services (industry standard AES encryption).

a) In transit, message and voice encryption uses AES -- NIST FIPS PUB 197.

b) System implements Perfect Forward Secrecy (PFS) by ensuring the encryption keys are unique, used only once and then forensically destroyed. The key exchange mechanism used is ECDH521 -- NIST FIPS 186-4

c) At rest (in database), messages are encrypted using TRIPLE DES algorithm with a 256 key bit length -- NIST FIPS PUB 46-3 DES

d) Passwords cannot be retrieved as they are one way hashed using SHA2 - NIST FIPS PUB 180-4 Secure Hash standard. [FIPS 140-2 - Annex A - National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015.]

e) All connections to server use TLS 1.2 (Obsolete cipher suite).

f) SQL Server runs in FIPS compliant mode (i.e. SQL Server configured and run such that it uses only the FIPS 140-2-certified algorithm instances that are called by using CryptoAPI for encryption or by hashing in every instance where FIPS 140-2 compliance is required).

g) SQL Server runs on an operating system (Windows Server 2012 R2 Datacenter) that is FIPS 140-2 certified.

h) Secured Communications uses BitLocker Drive Full-volume Encryption. BitLocker is set to run in FIPS- Compliant mode i.e. it uses FIPS 140-2 validated cryptographic modules.

i) File share uses Encrypting File System (EFS).

9.2.8 Internal Security

Service Provider warrants that the following apply to the internal security for server facilities associated with Services:

a) All Service Provider server facilities are Tier III compliant state-of -the-art facilities with complete power redundancy, fault-tolerant designs and dual access controlled with bio-metric and card key access control.

b) Server system includes complete multiple redundant connectivity, cooling and fire suppression.

c) Server facilities protected with 24/7 on-site security and NOC staff, alarm systems, dual authentication access controls, security cameras, access control systems log, full-perimeter fencing, reinforced concrete walls, and other physical/security protections.

d) All Service Provider personnel are subject to background checks.

e) All Service Provider employees are restricted to only areas of system access essential to their responsibilities.

f) All Service Provider employees are extensively trained on security as it relates to their access level and specific responsibilities.

g) Service Provider Management is specifically educated on Security Awareness, Sans Institute.

h) Service Provider employee actions are logged as they relate to the system. All data changes and program changes are logged with what was done, who did it and when.

9.2.9 Connectivity

Service Provider warrants that the following apply to connectivity systems for server facilities associated with Services:

a) 10 Gigabit/sec switches to the rack

b) Fully redundant network architecture

c) Connected to numerous telecommunications hubs

d) Multiple redundant bandwidth carriers

9.2.10 Power

Service Provider warrants that the following apply to power systems for server facilities associated with Services:

a) Dedicated, on-site 138 kV substation delivers dual-feed 12.47 kV utility power to the building

b) 480V generators as N+1 shared. Generators are 2500 kVA/2000 KW Cummins generators, and each one has a 4,000 gallon belly tank that provides a minimum of 24 hours of runtime at full load. Fuel is delivered locally and in case of an emergency, a national fuel provider will step in, with our data center's priority being second only to FEMA

c) Four 625 kVA UPS systems configured as 2N

d) Power room is a fully independent Electrical Distribution Matrix with dual ComEd source support

e) Redundant power infrastructure on all system levels

f) The Dedicated UPS is a 2N system and delivers 1125 kW of UPS capacity to the raised floor. The UPS system is comprised of four UPS modules 625 kVA with a pair of modules configured in parallel for capacity

g) Best-of-breed Switch Gear

h) Best-of-breed STS/PDU technology

i) Multiple generators

j) 72-hour on-site fuel capacity per generator

k) Multiple re-fueling vendors - Our data center's priority is second only to FEMA

9.2.11 Cooling

Service Provider warrants that the following apply to the cooling systems for server facilities associated with Services:

a) Sixteen 150 Ton RTU's configured as N+1

b) Air-side economization capable

c) N+1 cooling configuration utilizing CRAC units and RTUs

9.2.12 Fire Protection

Service Provider warrants that the following apply to the fire protection systems for server facilities associated with Services:

a) Overhead and under-floor smoke detection

b) State-of-the-art monitoring system provides real-time data on equipment operation, enabling easy system management and instant identification of problems

c) Monitoring includes power and cooling systems, as well as temperature, humidity, leak detection and fire protection

9.2.13 Network Security

Service Provider warrants that the following network security attributes apply to the technology and operations associated with Services:

a) Firewalled network

b) Virus protection

c) Redundant web and database servers

d) 10 GB - Internal information transferred on private network with no outside access

e) Information stored encrypted with AES 256 drive security

f) Written security procedures

g) 24/7 staff

9.2.14 Software and Procedures

Service Provider warrants that the following software and IT operating procedures apply to the technology and operations associated with Services:

a) Security upgrades for software and hardware

b) Internal password policies

c) Internal access policies and logs

d) Internal training and threat assessment

e) Backups are encrypted, stored in-house and remote.

f) White Hat Professional hacker on retainer to access any vulnerabilities

g) SAE 16 and SAS 70 Certified

h) PCI Compliant