Data Security Overview

COMET understands that the security of our Clients' data is one of our most important responsibilities. Our data security policy considers the confidentiality, availability and integrity of data. Data security ensures that data is accurate, reliable and available for those who are authorized to access the data. We implement practices and processes to ensure data is not being used or accessed by those who are not authorized.

A. COMET Security Overview

COMET security is a critical component of COMET services and considers both the protection of our clients' information that we have in our custody, as well as our continuity of service. The COMET system was designed to be secure and reliable, thus assuring our clients' records remain safe, confidential and available to those authorized to access them, leveraging stringent technologies, protocols and practices. COMET uses a multiple layered approach to protect client information. Our client Terms of Service outlines our obligations and responsibilities related to data security. We utilize proven methods and algorithms from best practices to prevent data breaches.

B. Site Protection

The physical location(s) of our COMET servers is confidential and known to only a few. They reside in unmarked, dedicated, secure, third-party professional data centers. Persons authorized to access the data are limited to only a few key staff. Unauthorized access is prevented by multiple layers of electronic and physical systems such as: full hand scans (with pulse detection required), IDs, passwords, cross-reference checks, closed-circuit television (CCTV) and more. Our data center facilities provide redundant operational systems for automated fire detection / extinguishing, flood protection, room environmental control, and automatic power backup (battery and generators). Redundant servers automatically back up data and are available when a primary host server crashes. The continuation of service to you has multiple layers of redundancy and backups to assure your data is available when you needed it.

C. Continuity of Service

- **High Availability:** Boasting up time higher than 99.83%, COMET offers a five-layer approach to data reliability and backup, allowing a continuity of service in case of page server and database server failure.
- **Disaster Recovery Rehearsals:** COMET engineering team rehearses disaster events and recovery protocols under the supervision of the Director of Systems.

D. Security Monitoring and Auditing

COMET performs regular security audits covering the protection of COMET clients' data and continuity of service. This audit extends its scope to the entire organization and also covers COMET personnel, facilities, assets and many other aspects of the COMET organization. The COMET security plan includes a full disclosure to COMET's clients in case of a detection of a security breach. In the unlikely event of a breach of security and/or unauthorized release of private data, COMET will contact the appropriate individuals as soon as possible to notify any clients who may have been impacted.

E. Electronic Protection

- **"Data in transit":** the https secure web protocol offers a high level of protection which is widely accepted for web-based confidential transactions.
- **"Data at rest":** COMET uses field-level encryption incorporating tested and approved algorithms
- **Secure architecture:** COMET is a web application and access to its databases and related web transmissions are protected through multiple layers of firewalls, filters, page servers, and other protective devices.

F. Client Data Security Practices

COMET also includes several levels of security within the COMET System, which are designed to allow clients to maintain control over their own data. It is the responsibility of each client to maintain its own data using COMET System features. The product includes a robust set of feature-specific permissions which can be tied to user accounts. It also allows clients to define their own access to various features. We encourage all clients to familiarize themselves with COMET System security features, as well as our recommendations and best practices for ensuring a secure environment for all COMET System implementations.