DATA PRIVACY AND SECURITY PLAN

In hosting Protected Data, Contractor and/or any of its subcontractors, affiliates or third parties that may receive, collect, store, record or display any Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

Hardware and infrastructure behind the service:

Application services provided are distributed between two data centers. The servers sit behind enterprise load-balancers that are connected to redundant, high-speed network connections.

The co-location data centers reside within the United States located in Denver, CO and Secaucus, NJ. Both co-location data centers provide Tier 3 level features including emergency backup environmental systems for continuous 24 x 7 operation.

Security utilized to protect customer data:

Customer Segregation:

Customers are logically segregated from one another ensuring only authorized personnel have access to data.

Encryption:

All end-user access to information stored in the Service is encrypted and transmitted via HTTPS. All authenticated access is protected by SSL certificate issued by a Certificate Authority

Firewalls and Intrusion Detection/Intrusion Prevention system is used to protect the Service network.

Diligent Employees with access to the underlying infrastructure is limited to authorized personnel only through VPN to create secure and encrypted connections.

Disaster Resilience and Recovery:

Geographical Redundancy

The Service's servers are housed at two geographically separated sites within the United States. one outside Denver, Colorado and one in a Secaucus, NJ co-location centers. Each site maintains copies of all production data. Each site functions in an active/warm standby environment and capable of providing the Service from either location. Administrative access is provided via VPN.

Staff is geographically dispersed, providing resilience in staff's ability to provide customer support.

Hardware Redundancy:

Each site has mirrored servers in an active/warm standby configuration. Production data is stored at both sites. The data centers have multiple internet backbones into both centers, ensuring resilience should there be a major internet backbone outage. The data centers also have backup power in the form of batteries for short-term problems and diesel generators for longer-term problems.

Monitoring:

Monitoring software is used within the production environment to monitor on a 24/7 basis and alert engineering and production operations staff.

Backups:

Full backups are stored and retained for 14 days. Access to the backups is limited to authorized and mission-critical staff only.

Disaster Recovery:

IT staff maintains a Business Continuity & Disaster Recovery plan and associated processes necessary to restore service.