CAMP Infrastructure and Security Overview

Secure Data Centers

CAMP Systems uses two geographically dispersed state of the art data centers to run all applications and services. The Primary data center is located in Austin, Texas. And the DR data center is located in Ronkonkoma, New York. CAMP uses industry best practices to minimize disruption to CAMP's service and protect customer data, these practices are summarized below:

Austin, Texas

Ronkonkoma, New York

Access control and physical security

- 24-hour manned security, including foot patrols and perimeter inspections - Texas Facility.
- Biometric scanning for access – Texas Facility.
- Dedicated concrete-walled data center rooms.
- Computing equipment in access-controlled secure locations.
- Video surveillance throughout facility and perimeter.
- Building engineered for local seismic, storm, and flood risks – Texas Facility.
- SAE16 Type II Certified – Texas Facility.
- Tracking of asset removal.

Environmental controls

- Humidity and temperature control.
- Redundant (N+1) cooling system.

- Water leak detection system.

Power

- Underground utility power feed. –Texas Facility
- Redundant (N+1) UPS systems.
- Redundant power distribution units (PDUs).
- Redundant (N+1) diesel generators with on-site diesel fuel storage – Texas Facility. Single Generator in NY.

Network

- Concrete vaults for fiber entry – Texas Facility.
- Redundant internal networks.
- Network neutral; connects to all major carriers and located near major Internet hubs – Texas Facility.
- High bandwidth capacity.

Fire detection and suppression

- VESDA (very early smoke detection apparatus).
- FM-200 gas fire suppression system.
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe fire suppression – Texas Facility.

Network protection

- Perimeter firewalls and edge routers block unused protocols.
- Internal firewalls segregate traffic between the corporate and production tiers.
- A third-party service provider periodically scans the network externally and alerts changes in baseline configuration.

Disaster Recovery

- CAMP performs real-time replication to stand-by hardware at each data center, and near real-time data replication between the production data center and the disaster recovery data center.
- All data is transmitted across encrypted links.
- Disaster recovery tests verify our projected recovery times and the integrity of the customer data.

Backups

- Backups occur daily and data is retained according to weekly, monthly, and yearly schedules.
- Tapes are stored locally as well as at an off-site secure location.
- We have multiple backup layers incorporating data replication, disk to disk staging, and finally disk to tape backups.
- Retired tapes and hard disks are securely wiped and shredded.

System Security

- Our Information Security department monitors notifications from various sources and alerts from internal systems to identify and mange threats.
- Connection to the CAMP's Application environment is via TLS cryptographic protocols, using global step-up certificates, ensuring that our users have a secure connection from their browsers to our service individual user sessions are identified and re-verified with each transaction, using a unique token created at login.
- All production based systems are continually updated with the latest operating system security fixes and firmware updates to prevent system exploits.
- System access is given on a per-user basis and audited at random times.
- All front-end servers are behind firewalls and only accessible via https protocol. Database servers inside the perimeter firewalls are protected using proprietary non-routable IP addressing schemes, network address translation and more.
- No customer can see another customer's data. This is enforced on several layers of the architecture, including authenticated sessions, which are required for any page access.