Elemica

Security Statement

Infrastructure Security Overview

Elemica employs a defense-in-depth approach to securing its systems (internal), production and non-production applications and customer data. Elemica understands that the confidentiality, integrity, and availability of our customers' data are vital to their business operations and our own success. We use a multi-layered approach to protect key information, monitoring and improving our application, systems and processes to meet the growing demand and challenges of security.

Secure Data Centers

Access Control and Physical Security

- 24-Hour manned security, including video monitoring
- Biometric scanning and Smartcard for access
- Computing equipment in access-controlled steel cages
- Building engineered for local seismic, storm and flood risks
- Access is restricted to authorized IT staff only

Environmental, Power, Fire Protection

- Humidity and temperature controlled
- Redundancy (N+1) coolingsystem
- Underground power feed; Redundant power distribution units
- Redundant diesel generators with on-site diesel storage
- Dual alarm, dual inter-lock, multi-zone, pre-action dry pipe water based fire suppression

Network

- Concrete vaults for fiber entry
- Redundant internal networks
- Network neutral, connects all major carriers
- High bandwidth capacity

Secure Transmissions And Sessions

- Connecting to Elemica production applications via VPN and secure access or secure authentication
- Applications are accessed via https and certificate authenticated allowing secure access to Elemica production applications
- Individual customer sessions are identified and re-verified with each transaction, using two step authentication

Network Protection

- Perimeter firewalls and edge routers block unused protocols
- Internal firewalls segregate traffic between the application and database tiers
- Intrusion detection sensors throughout the internal network report events to a security event management system for logging, alerts and reports
- Employ vulnerability management program framework to assess risk to servers and systems and remediates identified risks on a cyclical basis
- Employ the latest technologies to detect and deter unwanted intrusions or attempts to disrupt data flow

Disaster Recovery

- Real-time replication to disk at a data center and near real-time data replication between the production data center in the disaster recovery data center
- Data are transmitted across encrypted links

Backups

- All data are backed up via disk to disk replication on a rotating schedule of incremental and full backups
- Backups are replicated to an offsite disaster recovery facility over secure links to a disk backup device

Testing and Assessments

- All Elemica applications are protected using SSL (Secure Socket Layer) to protect data in transmission
- Elemica maintains a structured application development process and change management/change control framework with regard to the Elemica applications
- All code within Elemica applications is functionally tested and reviewed for adherence to applicable security standards
- All changes to the code in the Elemica applications are tracked across the lifecycle of such application and are tightly integrated with Elemica's software release management protocols.
- Third-party assessments are also conducted regularly:
  - Application vulnerability threat assessments
  - Network vulnerability threat assessments
  - Selected penetration testing
  - Security control framework review
- All data centers must be SOC II audited and certified.

Security Monitoring

Our information security department monitors notifications from various sources and alerts from internal systems to identify and manage threats.