

EAG DATA SECURITY POLICIES

EAG utilizes Amazon Web Services (AWS) scalable cloud computing platform to host the CaseTrack application. This highly-secure, state-of-the-art computing environment provides significant protection against physical and network security issues.

In order to keep your sensitive data confidential and secure, EAG has implemented the following security policies:

Certifications and Accreditations

AWS has successfully completed a Statement of Auditing Standards No. 70 (SAS 70) Type II Audit. SAS 70 is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). It represents that a service organization has successfully undergone an in-depth audit of its controls over information technology and other related processes. Further, it ensures that the service meets the requirements of Section 404 of the Sarbanes-Oxley Act.

Physical Security

The data centers are housed in non-descript facilities with physical access strictly controlled both at the perimeter and building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means.

Data Encryption/Network Security

The hosting infrastructure provides significant protection against traditional network security issues including redundant firewalls, network intrusion protection, and bi-directional data encryption using SSL 128-bit encryption.

Performance and Availability

CaseTrack is hosted on high-performance servers, eliminating any issues with respect to bottleneck performance and hardware failure. Data stored in the system is redundantly stored in multiple physical locations. System durability is ensured by storing snapshots of data objects multiple times across multiple datacenters on the initial write with continuous replication in the event of device unavailability or detected bit-rot.

In order to provide end-to-end security and ensure the integrity and availability of our customer's data, EAG employs a number of best practices including:

- SAS 70 Type II – Certified Environment
- 24 x 7 Network Monitoring
- SSL 128-bit Encryption
- 99% Service Availability
- Regular System Patching and Updates
- Technical Support Team Staffed Exclusively with EAG Employees