

FAQ for IT People

Locatingus.com. understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security. Visit www.locatingus.com

Web-Based Solution and Secure Connection

Our Visitor Management and Event Management application services are provided across the web in the Software-as-a-Service model. All the user needs is a web browser (IE 6, 7, 8, Firefox)

We provide our service through a secure connection using HTTPS; which is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems.

Trust Locatingus.com

We provide our application service to many government departments as well as some of the world's largest multi-nationals including; Mining companies, Security Companies, Retail, Finance, Education, Energy, and Construction organizations.

Secure Data Centres

Our service is located in dedicated spaces at top-tier data centres. Servers are protected behind a dedicated Firewall. This firewall comprises the industry-leading [Checkpoint Firewall 1](#) software running on dedicated hardware and is monitored 24x7. These facilities provide carrier-level support, including:

Access control and physical security

- Fully-integrated building management system for smoke, fire and water detection.
- 24-hour manned security, including foot patrols and perimeter inspections
- Biometric scanning for access
- Dedicated concrete-walled Data Centre rooms
- Video surveillance throughout facility and perimeter

Environmental controls

- Humidity and temperature control
- Redundant (N+1) cooling system
- Anti-static false floors

Power

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems



- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

Network

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

Secure transmission and sessions

- Connection to the Locatingus.com environment is via SSL 3.0/TLS 1.0, using global step-up certificates from GEOTrust, (RSA 1024-bit) ensuring that our users have a secure connection from their browsers to our service

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
- A third-party service provider continuously scans the network externally and alerts changes in baseline configuration

Backups

- All data are backed up to tape at each data centre, on a rotating schedule of incremental and full backups

Internal and Third-party testing and assessments

Locatingus.com tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities. Third-party assessments are also conducted regularly:

- Application vulnerability threat assessments
- Network vulnerability threat assessments
- Selected penetration testing and code review
- Security control framework review and testing

Security Monitoring

We monitor notification from various sources and alerts from internal systems to identify and manage threats.

