Security Controls Overview

At Sitetracker, our solution may involve the processing of our customers' technical data, personal data, and other information (collectively, "Data"). We recognize that safeguarding the confidentiality, integrity, and availability of this Data is essential to protect our customers. We have implemented industry-standard security controls to ensure the safety of our customers' data. This overview outlines a summary of our security program, the security measures we have implemented, and the privacy and security certifications we have obtained.

Category	Description
Annual Evidence of Compliance	- Sitetracker undergoes annual SOC 1 and 2 Type II audits. - Sitetracker undergoes annual audits to maintain ISO 27001 and ISO 27701 certifications.
Web Application Penetration Test	- Independent third-party tests conducted annually for web, external network, and mobile applications. - Vulnerabilities remediated in accordance with industry-standard best practice timeframe based on severity of vulnerabilities.
Security Awareness Training	- Annual security awareness training covering data protection, phishing, and password management for all personnel.
Vulnerability Scans	- Annual scans of cloud systems using industry-standard tools, as approved by the cloud service provider.
General Controls	- Equipment access control, data media control, user control, and recovery mechanisms are implemented.
Personnel Controls	- Personnel are vetted, authorized, and trained in security processes relevant to their tasks.
Copy Control	- Personal data copies are limited to backup and archive purposes.
Security Controls	- Unique user IDs, session termination, password complexity, IP restriction, and SAML-based authentication.
Logging & Monitoring	- User passwords are stored using a one-way hashing

	algorithm (SHA-256) and are never transmitted unencrypted. - Logs maintained for a minimum of 90 days, including user access and security changes.
Intrusion Detection	- Network-based intrusion detection mechanisms continuously monitor services for unauthorized access.
User Authentication	- Access requires valid User ID and password, secured via TLSv1.2 encryption, with random session IDs for tracking.
Incident Management	- Detailed policies and procedures to manage and respond to security incidents.
Physical Security	- Data centers secured with biometric access, 24/7 guards, escort-controlled access, and backup generators.
Reliability	- Redundant configurations for all networking and database systems.
Disaster Recovery	- Geographically remote disaster recovery facility with necessary hardware and software for continuity.
Virus Protection	- Attachments or other Data uploaded by customers into Sitetracker platform will not be executed in Sitetracker Platform, thus will not damage or compromise Sitetracker platform if they carry viruses. Sitetracker does not offer virus scanning services.
Data Encryption	- 128-bit TLS certificates, 2048-bit RSA public keys, and AES 256-bit encryption for data at rest and during transmission.
System Changes & Enhancements	- Ongoing updates and enhancements to security controls and policies to maintain high protection standards.
Certifications & Compliance	- SOC 1, SOC 2, ISO 27001, and ISO 27701 certifications held and maintained.