OMNILERT SECURITY FACTSHEET

PHYSICAL SECURITY	
Facilities	Omnilert servers and databases are hosted at SOC 1 Type II and ISO 27001 compliant facilities. Access to datacenters is highly restricted and monitored 24/7 by on-site staff. All power systems are fully redundant and protected against temperature, fire, and other environmental hazards. Omnilert's colocation data centers are located across at least two separate availability zones in the United States.
Security Monitoring	Omnilert maintains a Security Board which stays in constant contact with all partners, including datacenter security personnel. Any suspected or confirmed incidents are reported to the Security Board, who can initiate the Omnilert Incident Response Plan.
Monitoring	Automated and human monitoring is in place across all Omnilert systems, physical and virtual. Omnilert's Security Board provides 24/7/365 response coverage. Logging is enabled on all systems and user access to sensitive information is reviewed monthly.
DATA PROTECTION	
Network Security	Omnilert monitors its network security both internally and with its service providers. The Omnilert network sits behind a firewall and cannot be accessed without authorization to the company's virtual private network (VPN).
Authentication	Omnilert uses multi-factor authentication on all systems where it can be implemented.
Information Classification	All information stored, processed, or otherwise used by Omnilert is evaluated and labeled according to one of three internal data classifications. Each data classification carries a minimum level of required protections outlined in the Omnilert Information Security Policy.

ONGOING ASSESSMENTS	
Security Assessments	We conduct internal and external security assessments of our entire organization and infrastructure on a regular basis. Assessments help inform our current security posture and future improvements.
Vulnerability Scanning	Regular security reviews are conducted of application code at multiple stages of the Software Development Lifecycle (SDLC). Development teams use OWASP secure development guidelines and OWASP Top 10 for ensuring secure coding practices for each application language and platform. Third-party scans and code vulnerability tests are also conducted on a regular basis.
Security Training	All employees, including our development team, go through security education once per year; when there are significant changes to our policies or procedures; and when there are important changes or security news related to any technologies we use.
INCIDENT RESPONSE	
Incident Response	Our Security Board has three dedicated branches to provide reliability and flexibility in response to security incidents. The Security Board is tasked with maintaining the integrity of all customer, client, partner, and company data. Any suspected or detected breaches are immediately reported to our Security Board, initiating formal incident response procedures.
Logical Access	Access to the Omnilert network is restricted to only those individuals who require it to perform their duties. Privileges and access to our network is reviewed at least once per month. User access is revoked immediately if there is a change in duties and revoked upon termination or resignation.
CRYPTOGRAPHY	
Encryption Overview	Technical security controls are based on NIST and FIPS-preferred algorithms and bit lengths for symmetric and asymmetric encryption, as well as for message authentication and digital signatures.
Encryption Evaluation	Our encryption standards have been assessed by third-party subject matter experts to ensure sensitive information is encrypted in transit and at rest, depending on the level of sensitivity.

Encryption in Transit	Our internal policies require that all customer, client, partner, and company data is encrypted in transit using only NIST or FIPS-approved cryptography.
Encryption at Rest	All highly sensitive information is encrypted at rest at a minimum, using only approved cryptographic methods. Other levels of data may also be encrypted at rest.
BUSINESS CONTINUITY	
Omnilert Reliability	Clients are given 24/7 access to our Support portal. The Support team is the primary communication channel for clients, providing assistance with using and configuring applications. Our Security Board maintains contact with clients with information regarding maintenance, security monitoring, and for incidence response.
Disaster Recovery Plan	Omnilert's Disaster Recovery and Business Continuity Plan outlines how our organization will continue to provide service in the event of a disaster. Overlapping roles, technologies, and physical assets provide a robust foundation making the complete loss of service highly unlikely. Both the Disaster Recovery and Incident Response Plans have been evaluated by security experts to ensure efficiency and effectiveness in real-world situations.
Project Planning and Development	Security controls and reviews are an integral part of our operational and secure development practices. Source code is tested, sanitized, and evaluated according to secure coding guidelines for each programming language used.
DEVELOPMENT	
Development Environment	Developers follow the Omnilert SDLC which integrates secure code reviews, vulnerability scans, and separate test and production environments.
Methodologies	Omnilert has a well-defined and documented set of Information Security policies and procedures based on ISO/IEC 27001. Additionally, Omnilert has developed an Incident Response, Disaster Recovery, and Business Continuity Plan. Our development team follows the Omnilert Software Development Lifecycle (SDLC).

PERSONNEL	
Background Check	All employees and contractors with access to Omnilert systems undergo a background check before hire. Omnilert will also run any additional checks required by clients to meet regulatory requirements. Upon hire, all employees and contractors must complete the Omnilert information security education program. All employees and contractors are required to sign non-disclosure and confidentiality agreements.
Ongoing Education	As part of continuing education, asset managers provide their team members with special interest contact lists regarding the technologies they will be using.
Employee Guidelines	All members of the Omnilert team are provided with an employee handbook, in addition to the Information Security Policy. The employee handbook outlines general conduct, security best practices, as well as organizational methodology.

For more information about Omnilert's services, security features and controls, please feel free to contact us.

Phone: 800.256.9264

Technical Support: support@omnilert.com

Other Inquiries: info@omnilert.com