Omnilert Security

SECURITY CONTROLS

Omnilert provides emergency notification and management solutions to our customers. Since we need to be available at the most critical times, we take maintaining a reliable and robust security posture very seriously. All of our systems, as well as our staff, have redundancies in place to ensure there is a backup to every primary system and a backup to the backup as well.

Omnilert has a number of detailed policies that outline how we handle security at our organization. Our approach begins with the Omnilert Information Security Policy, which documents specific procedures, guidelines, and protections to be used based on data classification level.

With our 15+ years of industry experience, we're very familiar with the legal and regulatory requirements our customers face in sectors from education to finance. Our policies are aligned with industry standards for data protection, cryptography, and availability.

SECURING DATA FROM DEVELOPMENT TO DEPLOYMENT

Protecting customer, client, and partner information is critical to Omnilert, which is why it is given our highest level of data protection. These include U.S. Federal Government-approved cryptographic protections, regular internal and external security assessments, and a 24/7/365 Security Board.

Omnilert's security infrastructure from development to our own user accounts is evaluated at least once per year. All of our developers follow the Omnilert Software Development Lifecycle (SDLC), which integrates secure code reviews, vulnerability scans, and separate test and production environments.

Additionally, we maintain a current Incident Response Plan, as well as Business Continuity and Disaster Recovery Plans, in case of security events to detect issues, investigate, and remediate as soon and effectively as possible. Omnilert also maintains contacts with local and federal authorities as part of our security posture.

GOVERNMENT APPROVED CRYPTOGRAPHIC PROTECTIONS

INTERNAL & EXTERNAL SECURITY ASSESSMENTS

24/7/365 SECURITY BOARD

SECURITY

LOGGING, LEARNING, & LOGISTICS

The Omnilert SDLC incorporates security throughout the project lifecycle. Security considerations are part of each step, with a review phase we designed to not only meet our stringent requirements but also to evolve in response to changes in the technical architecture and the threat environment. Code does not move forward in our development process without meeting Omnilert's quality assurance testing and acceptance criteria.

Omnilert is committed to protecting our customer, client, and partner data, and to maintaining the robust infrastructure needed to provide reliable emergency notification and alert services.

CLOUD INFRASTRUCTURE

We leave physical security to the best in the industry by using the facilities of world class data centers, in collaboration with our Security Board, who continuously evaluate our virtual controls. Vulnerability scans are conducted regularly and we stay updated on security news with bulletins, industry contacts, and by attending the security-minded industry conferences.

SECURITY EDUCATED STAFF

Every member of the Omnilert team goes through a background check and our security training program annually. Developers not only need to know how to code, but also how to observe the security requirements for handling all levels of data classification. All customer and client information is considered highest sensitivity. We maintain a Security Board to coordinate our efforts, evaluate custom solutions, and develop Omnilert applications and services securely.

Access to our highest levels of data classification is evaluated monthly, to make sure it is only given on a need-to-know basis and revoked when no longer needed. We also evaluate all of our partners and service providers to make sure they meet our security requirements before engaging with them.

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