HEALTH TECH

Platform Security

From large corporations and federal government agencies to local businesses and regional chains, our customers expect reliability and ease of use, but that is only part of what makes LST Health Tech the #1 rated SMS marketing platform.

When businesses entrust LST Health Tech to send messages on their behalf, they are relying on us to manage not only the business's privacy and data security but also that of their customers and clients.

We take that responsibility very seriously. To that end, we have developed an extensive set of industry-standard security policies and procedures that we dutifully carry out across our organization. Here is an overview of our platform, information, and infrastructure security protocols.

Platform Security Personnel & Policies

Our Operations Engineering team dedicates significant resources to the development and maintenance of our platform security.

This team administers LST Health Tech' Corporate Security Policies, which are informed by compliance and information security standards and detail protocols including infrastructure management, asset management, user data, data encryption, incident response, network security, and physical security.

Plus, we protect our customers by offering including support for consumer-driven consent, opt-out capabilities, and phishing monitoring.

Infrastructure & Network Security

LST Health Tech' infrastructure was designed with security in mind. We utilize both AWS and GCP cloud storage, and we have longstanding relationships with well-known industry security companies that perform third-party checks on our platform and infrastructure.

AWS complies with leading security policies, including SSAE 16, SOC framework, ISO 27001, and PCI DSS. GCP complies with similar policies, including SOC 1, ISO 27001, 27017, 27018, FedRAMP, and others.

Among the built-in cloud storage protections, we have zone redundancy and are working towards regional redundancy. We have a handful of tools at the system access level for DDoS protection.

We have a documented natural disaster and nuclear attack infrastructure continuity plan and DDoS plans in place.

We employ central logging in order to proactively catch malicious activity. If one of our triggers fires off, we immediately lock affected accounts, and our Account Management team begins to work with Account Owners to resolve the matter.

Additionally, an incident response protocol initiates a downtime report and informs all stakeholders.

Product Security

Throughout our software development process, our continuous integration, automated code review, and human code review ensure the highest levels of product security on the full SDLC.

To comply with our change management program, our Change Advisory Board (CAB) meets before every code release and involves each department lead and the entire Product and QA teams.

If a security vulnerability or bug is identified, we have a patch management process in place. We have an integrated system of identification, triage, and ticketing to address self-reported and customer-reported bugs.

On a routine basis, we apply brand-new images to our production stack and continually protect our infrastructure by re-provisioning our staging environments multiple times each week.

Data & Account Security

Data in transit is encrypted with the latest industry-recommended TLS standards (1.2). Our data backup policy complies with state, federal, and telecom compliance regulations

To prevent unauthorized account access, we combine robust security algorithms with oversight from human reviewers. Repeated attempts to login via the LST Health Tech app have brute force protection.

User accounts are segregated by multiple levels of logic, and we rely on a "soft delete" to ensure that data is never truly lost.

We automatically notify Account Owners when passwords are changed. Additionally, LST Health Tech passwords are hashed and irretrievable, meaning that if a password is lost, it can be reset, but not retrieved.

Our customers own their data. Their contacts are kept in strict confidentiality. We do not share, rent, or sell the contacts belonging to our clients with any third parties. Data (including contacts) belongs to the customer and the customer alone.

We maintain PCI Compliance for payment gateways as well as Phase 1 CCPA Compliance, which is on par with the GDPR data security requirements.

Physical & People Security

LST Health Tech employees utilize only company owned equipment and laptops to access client data. Employee equipment is secured via passwords and other security policies implemented by IT.

We continuously train employees on best security practices, including the importance of protecting internal customer data as well as how to identify any threats to our network.

All employees undergo criminal history and credit background checks prior to employment.

To obtain more information about our platform security program and security compliance measures, contact colton.scott@lstmarketing.com