Original: https://www.livechatinc.com/kb/livechat-security-and-data-storage/

LiveChat security and data storage

by Jacob Firuta

Data transmission and storage security is imperative in the modern enterprise. That's why we have taken all measures to keep all information appropriately protected.
Our data centers, provided by Softlayer, are located in Texas, US. They are behind a number of security clearances, and there's always a security guard on duty.
Services provided to us by Softlayer are in compliance with the **SSAE16 standard**.
Our staff is granted access only in their respective fields and day to day work. They are also required to maintain confidentiality after departure from the company.
LiveChat developers treat stored data of customers with the highest level of security and care. Each piece of customer data is treated as personal and in need of standardized protection. We have employed security policies which ensure safety of the data storage and transmission.
All LiveChat connections are encrypted with **256bit SSL protocol**. There is no expiration date on the stored data. The data will remain on our servers even if a client does not extend his or her license.

Domain used by LiveChat

To make sure your firewall is not blocking any LiveChat requests, please add the following domain to your firewall's exception list.

*.livechatinc.com

Our CDN and anti-DDoS infrastructure is build on tens of thousands edge servers, so we cannot provide a list of all IP addresses on our Network.

Note that a firewall with an IP ACL policy has the additional disadvantage that access control based solely on IP addresses is prone to error due to attacks like spoofing, DNS cache poisoning, and BGP hijacking. We recommend that network administrators using IP ACLs for web traffic employ a simple proxy server that filters traffic based on domain name ***.livechatinc.com** in the HTTP request, rather than by the IP address of the remote server.

Security of information

LiveChat is in the compliance with the following information related security and monitoring procedures:

- Documented and defined security standards and procedures
- Employee confidentiality agreement
- Verification of employees who have access to customer data
- Access to information granted only to employees who need to work with customer data or hosting servers
- Access to customer data is limited within 24 hours of employee departure or relocation within LiveChat
- Training on internal security policies and raising of security awareness as a day-to-day process

- Physical security of the data center

Physical security ensured by data centers and hosting provided to and by LiveChat meets the following requirements:

- Secure rooms with at least two access mechanisms, i.e., key-cards, man traps, security guards, and computer room badge-in
- Authorized employees only are allowed physical access to the servers. 24/7 security at the location
- Backups of customer data are stored on-site with limited access and at a securely controlled or commercial off-site location
- The site guarantees additional protection such as uninterruptible power and fire suppression
- Flawed components in the data center undergo DoD-approved “erase” or “wipe” procedure (if functionally possible) prior to physical destruction

Technical controls

LiveChat supports technical controls to provide protection to its network, systems, and applications:

- LiveChat utilizes professional facilities via a top tier hosting provider that protect customer data from external threats
- LiveChat maintains individual accountability for employees that can access systems hosting customer data
- LiveChat has documented user account/password management systems for employees with access to systems that are hosting customer data
- LiveChat ensures that individual access to customer data is controlled, i.e., a diverse user name and password is required for each individual administrator
- Customer data is compartmentalized to prevent unauthorized access and separated from the data of other customers
- Access to customer data is protected by hardened passwords rotated on a 90 day basis
- Wireless connectivity to networks or servers hosting customer data is protected using security mechanisms such as EAP, TTLS, TLS, or PEAP
- LiveChat’s data center has formal security policies and procedures in place that deal with viruses, other malware and related threats

Usage

To ensure protection of confidentiality, integrity, and availability of customer data, LiveChat meets the following usage criteria:

- Each user is assigned a unique ID
- User IDs and passwords can be edited at any time
- Passwords must be at least 5 characters long
- The application and resulting access to data in the database has based-on-permission controls limiting access to only authorized customers
- Each change of user login status is logged within each application
- All logs are treated as confidential information and access to reports can be restricted using the permission system
- Reporting of this information is available within each instance of LiveChat
- If confidential data, personal data (i.e., names, addresses, phone numbers), or authentication information (i.e., passwords) is transmitted, LiveChat ensures

security by employing 256bit SSL encryption between each component of the communications path

- LiveChat’s security policy assumes customer data retention is permanent and is designed to that standard