closingsite
real estate settlement solutions

LOOP INFORMATION SYSTEMS, INC.
P.O. Box 7096
The Woodlands, TX 77387
Phone: 888-590-0999

Security Policy

Loop Information Systems, Inc (Loop) is serious about protecting you and your client's privacy and recognizes that you care how information about your transactions is used and shared. Loop's ClosingSite (Service) provide our clients with secure data and transaction management service for conducting real estate transactions.

Loop Information Systems – Client Data Policy

- Contact information: including names, email addresses, street addresses, and direct, business and fax phone numbers are not redistributed, sold or used any manner by Loop outside of providing Loop services to clients.
- Transaction information: any information regarding transactions is not redistributed, sold or used any manner by Loop outside of providing Loop services to client.

Physical Security

- The Service is housed on servers owned by Loop Information Systems, Inc. and are only used for ClosingSite clients. Access is limited to Loop employees.
- The Service servers are located in a secured/locked cabinet(s) that are only accessible by Loop employees.
- The secure cabinet(s) are located in a Level3 (www.level3.com) datacenter in Houston Texas.
- Level3 manages a stringent multi-layered security control procedure including 24x7x365 security monitoring, 4 security check points and photo id access cards required to enter the facility.

Level3 Datacenter Connectivity/Power

- N+1 electrical design and distribution, including redundant UPS and battery backup.
- Automatic Transfer Switches ensure smooth transition to backup power.
- 24-hour backup generator with enough capacity to power more than 4,484 homes
- 99.999% power availability.
- At least 125 watts/sq. ft of primary breaker power (with ability to upgrade).

Backup Policy

- Daily Backups: Loop performs scheduled full backups of client data nightly. Nightly backups are retained for 1 week.
- Weekly Backups: Loop performs weekly scheduled full backups of client data every Saturday. Weekly backups are retained for up to 1 month.
- Off Site Backup: A secondary weekly backup is performed each Saturday which is stored on a external device and is taken off site (at least 20 miles from the server facility) and stored in a secure location. Weekly off site backups are retained for at least 1 month.

Disaster Plan

- In the event of a disaster, Loop will perform the steps necessary to reestablish client's website and data based on the level of recovery needed in the fastest manner possible. Loop's server infrastructure has been designed to have multiple servers which can perform the same functionality, website, data or email. In the event there is an incident where the data center is no longer able to provide Loop service; Loop will relocate/restore client services from another Level3 facility. Disaster recovery timelines are based on the level of disaster and can range from less than an hour (with a server outage) to 1-3 days with a natural disaster (such as a hurricane, fire, food, etc.).

Server Security

- Loop Servers reside behind a Sonic Firewall, which has been setup to block any internet traffic except on ports opened specifically by Loop in order to provide the ClosingSIte Service. The firewall is configured to detect and block abuse, including but not limited to IP Spoofing, DNS attacks, and Port Scanning.
- Service applications including Web Site Hosting (IIS) and Database (SQL Server) reside exclusively on Microsoft Servers.
- Microsoft Server user accounts are limited on only Loop employees and usernames and passwords are changed routinely. Loop's policy is to require strong usernames and passwords requirements.
- Servers run antivirus and perform weekly scans.

Email Security

- Loop utilizes a SmarterTools email server with real time Anti-Spam and Anti-Virus detection and protection.
- The email server is setup to both send and receive email via Transport Layer Security (TLS) if supported by the remote server.

How Do We Protect Transaction Information?

ClosingSite places a high value on protecting information transmitted via the client website.

- ClosingSite client web sites are secure with a minimum of 4096 bit encryption Secure Socket Layer (SSL), provided by either GoDaddy, Network solutions, or similar provider. SSLs are commonly identified by the https URL.
- ClosingSite does not provide a contact database field for storing contact Social Security Numbers; due to the fact this information is not necessary for the purposes of transaction management.
- ClosingSite provides a privacy flag for every contact profile, which can be defaulted on or off depending on the contact role (buyer, seller, realtor, lender, etc.). When the privacy flag is turned on, no external parties to transaction can see any information except the parties first and last names.
- Access to transactions is limited to authorized users. Each time an authorized user logs into the client website, a site log is created which contains all user activity which includes pages visited, the user's IP address, referring URL, access URL, user agent and date and time stamps.
- Document Access – External users cannot access any document for transactions that the user is not an assigned as a transaction party. Within a transaction external users cannot access any document for which they have not be given access. Each document access is recorded with the user account and access date and time.
- Secure Messages - Secure messages can be sent to authorized parties to a transaction. A secure message consists of 2 parts, the first is an email which party receives to inform them of a secure message. The second part is the secure message, when the user accesses your website they can view their secure messages, and reply securely. Since the secure messages are accessed via a web browser, security is provided through SSL which encrypts all data transferred from the web server to the web browser.
- Secure Email - Loop can enable TLS email validation prior to sending email communications from your website. When this feature is enabled, email communications will generate an error message if Loop's email server is unable to confirm the recipient's email servers cannot receive email securely via TLS.