thoughtexchange

Thoughtexchange and Security - Canada

We take Thoughtexchange Security extremely seriously

Security of any server-hosted product is the sum of 6 security concerns:

- physical access to the server machines and data storage hardware
- software security provided by operating system and web server settings and web communications protocols
- client-side security
- data redundancy (aka backups)
- data confidentiality for our customers and participants
- file sharing

We'll describe how Thoughtexchange handles each of these in turn.

Physical Security

Thoughtexchange is hosted on Cloud Servers (aka Virtual Private Servers) with RackForce Networks Inc. based in Kelowna, BC. Attached is their document describing how they handle physical security. Amongst the many benefits of using Cloud Servers, a big one is that expensive physical security systems can be implemented, as the cost of these is spread across thousands of customers.

Software Security

Thoughtexchange uses Ubuntu Linux as its Operating System (OS) and Apache as its Web Server. Both are mature and hardened products with many years of operational experience on hosting platforms. In addition, all recommended practices have been followed to secure our OS and Web Server. We can provide more details on these practices to interested customers.

All of our servers have mandatory SSL level encryption - that is, they use the https protocol. This is the standard internet communication encryption used by all e-commerce sites, banking and other high security web-based systems. We also monitor our systems regularly for possible vulnerabilities and attacks.

Client Security

Generally, the weakest link in any software product's security are the users' passwords as well as physical access to their work stations. Of course, these are the areas which we at Thoughtexchange have the least control over.

All access by facilitators to Thoughtexchange is controlled by a login with username and password. In order to reduce barriers to usage as much as possible, the participant applications do not require usernames and passwords.

Backups

All of the Thoughtexchange data is backed up nightly. We export the database and all other customer-specific data to a single file and then transfer this file to cloud storage not associated with the server. A redundant copy of the file is then transferred to cloud storage at another location. In the event of any data loss, we would be able to restore the database and other data from these backups.

Data Confidentiality

Our Subscription Agreement and End User Agreement require us to maintain confidentiality of all 'information' provided by our customers. This 'information' includes BOTH content stored in a Thoughtexchange database (i.e. managed by our software) and information provided to us by our customers in phone calls, meetings, email, etc.

Our agreements do allow for a customer to give us permission to share information publicly. Generally, we use an email to document this permission and the scope of the sharing allowed.

Our employees and contractors do have access to all customer information and are required by their employment agreement or contractor contract to maintain all such information within the company and not to share it publicly.

We do extract regular statistical summaries of our customers' usage and if shared publicly, all identifying information would be removed and only summary data would be shared (e.g. Count of Thoughtexchange Processes created across all our customers).

Ultimately, it is our customers themselves (especially when using the software as facilitators) who control data confidentiality. For example, our customers can do the following either directly as a software user or indirectly by instructing us, to:

- set report options (e.g. to show demographic information),
- share reports (via email within our product or outside of it),
- control data visibility (e.g. by approving or flagging thoughts)

amongst many other choices which may make content available publicly.

Participant Privacy and Terms of Use

Our participant Terms of Use, which includes our privacy policy for participants' information can be found here:
http://participants.thoughtexchange.com/tou/en.pdf

In summary, our privacy policy is that participants' Input (thoughts, stars or other data they provide) can be made public as part of our processes; their Identity (email address, name, other identifying information) is shared between our customer and us; the Association of Identity to Input (i.e. who said what thought) is kept private by us, except as required by legal considerations.

File Sharing

When sharing reports with our customers, our Stakeholder Engagement Facilitators use sync.com which provides secure and private data storage in Canada. Attached is their document describing how they handle privacy.

thoughtexchange

RACKFORCE

Security

The RackForce GigaCenter security strategy encompasses many facets, such as the location of the site, the structure of the building, the layout of the facility, security features & systems in the facility, and comprehensive processes and management systems. This includes:

Location

- Canada is a low risk country and city; stable geopolitical climate; virtually no risk of civil unrest or terrorist action
- Our building is located in a light industrial area away from public buildings and meeting places; not near government buildings, military installations, consulates, etc.
- Building is on a cul-d-sac with no through traffic.

Security Features & Systems

- Seven layers of physical security from the exterior to access a cabinet in a data hall
- Multiple man traps with a combination of card pass and biometrics
- Digital security cameras throughout the facility, both inside and out
- Multi-level alarm system monitored by NOC and outside security service
- All cameras are recorded and archived for a minimum of 90 days; archive is searchable
- Access level management ensures staff have access to authorized areas only
- Authorized maintenance personnel (ie UPS, generator, mechanical, etc) have access to utility corridor and electrical/mechanical areas only.

Building

- Single story concrete construction, on concrete slab
- No exterior signage
- Interior elevation is approximately 30" above street level
- Data halls are in the interior of the facility - no exterior walls; no windows
- Data hall walls are double 5/8" fire resistant drywall with diamond steel mesh barrier
- Raised floor has concrete tiles and all tiles are secured with screws.

Security Processes & Management

- All staff have criminal records checks
- All personnel entry and exit is recorded; pre-authorized staff are recorded electronically (pass card) and guests are recorded by a security concierge
- No unescorted visitor access
- No unannounced deliveries allowed; all deliveries and shipments are recorded
- Extensive SSAE16 SOC 1 and CSAE 3416 processes in place and audited
- PCI DSS SAQ Validation, questions 9.1 to 9.4 compliant

Cloud Security

A key element of Cloud security is the separation of client's data traffic at layer 2. Each client has their own private VLAN, and VLAN segments are not shared between clients.

Other key elements of our Cloud security include:

- Each Cloud VM has its own RAM
- Each Cloud VM has its own SAN space, allocated privately in a secure multi-tenant model
- Virtualization is delivered using industry leading VMware vSphere
- Cloud services are delivered from RackForce owned and managed high security vaults and racks, accessible by RackForce technicians only
- RackForce operations are audited under SSAE 16 SOC 1 and CSAE 3416 standards.

thoughtexchange

sync.com

Sync.com Your Privacy

Our Complete Privacy Guarantee

Sync.com guarantees that your data is completely private. Our unique secure storage environment ensures that only you have access to your data. We can't read your files — nor would we want to. Only you have the keys to access your data — nobody else.

The technology protecting your privacy

In case you're interested in just how we're doing all this, here are some technical details for you. There are three levels of encryption for each and every file.

For starters, all data transferred to and from Sync.com servers is encrypted using SSL (Secure Sockets Layer). Every file is encrypted with 256-bit AES encryption. Each AES encrypted file has a key which will unlock it. The key to unlock the encrypted file is encrypted with your private key (a 2048-bit RSA private key, that is).

Your private key is the secret to the encryption mechanism for file data. It is required to decipher any file. Keeping a safe copy of your private key is extremely important. With Sync.com, your private key is kept safe with AES 256-bit encryption. In order to unlock your private key, you have a password. At no time is your password stored on the server in clear text, or through any decipherable string.

For maximum security, user authentication passwords are maintained as a SHA256 string to ensure we can never see it in the clear. It is stored in our database as a salted, BCRYPT-hashed string in the database. The salt helps prevent a "rainbow table" lookup, and BCRYPT is a one-way hashing mechanism. Once hashed with BCRYPT, the password cannot be "unhashed" or deciphered.

Your password is only ever known to your browser. When you log in, a JavaScript function hashes your password with SHA1 before submitting the hash to the server. The server then salts and hashes that, again with Bcrypt before storing the salted hash on the server. Bcrypt is specifically designed to foil brute-force attempts at decoding hashed passwords.

Finally, once you're logged in using the web or mobile client, your file and folder names are stored encrypted on our servers (using 256-bit AES) and require your password to both view and decrypt. Thankfully, all this happens transparently after you've entered your password only once—the web app and mobile takes care of the rest.

We believe it's possible to enjoy the convenience of cloud storage without giving up the privacy of your data.

Server Location

Sync.com's servers are located in Canada.

www.sync.com/your-privacy

Sync.com Inc.
7030 Woodbine Avenue. Suite 900
Markham, ON L3R 6G2 Canada