thoughtexchange

Thoughtexchange and Security - USA

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 Rackspace Inc located in Dallas, Tx. 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

Thoughtexchange provides 2 levels of backup for each customer virtual server: server backups and data backups. Sever backups are nightly backup "snapshots" of the entire server. These are stored with the servers. In the event of a problem, we can restore the server to its state at the time of the backup.

For data backups 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. Attached is their document describing how they handle privacy.

RACKSPACE® SECURITY

Triple-strength Security Backed by Fanatical Support®

Rackspace Hosting Security is a powerful, fully integrated portfolio of services, managed devices and best practices — all designed to ensure the highest levels of security for customer data.

Our portfolio covers all three critical security areas: physical security; operational security; and system security. Physical security includes locking down and logging all physical access to servers at our data center. Operational security involves creating business processes that follow security best practices to limit access to confidential information and maintain tight security over time. System security involves locking down customer systems from the inside, starting with hardened operating systems and up-to-date patching. Rackspace offers a full range of options to take system security to the next level.

As with all Rackspace offerings, our promise of Fanatical Support stands behind our security solutions. We will do whatever it takes to ensure that all our customers are satisfied.

Rackspace Security supports all three areas of data security, ensuring maximum protection for customer data.

RACKSPACE SECURITY AT A GLANCE

Physical Security

- Data center access limited to Rackspace data center tech cians
- Biometric scanning for controlled data center access
- Security camera monitoring at all data center locations
- 24x7 onsite staff provides additional protection against unauthorized entry
- Unmarked facilities to help maintain low profile
- Physical security audited by an independent firm

System Security

- System installed on using hardened, patched OS
- System patching configured by Rackspace to provide ongoing protection from exploits
- Dedicated Firewall and VPN services to help block unauthorized system access
- Data protection with Rackspace managed backup solutions
- Optional, dedicated intrusion detection devices to provide an additional layer of protection against unauthorized system access
- Distributed Denial of Service (DDoS) mitigation services based on our proprietary Rackspace Prevent Ion™ system
- Risk assessment and security consultation by Rackspace professional services teams

Operational Security – *the Rackspace Infrastructure*

- ISO17799-based policies and procedures, regularly reviewed as part of our SAS70 Type II audit process
- All employees trained on documented information security and privacy procedures
- Access to confidential information restricted to authorized personnel only, according to documented processes
- Systems access logged and tracked for auditing purposes
- Secure document-destruction policies for all sensitive information
- Fully documented change-management procedures
- Independently audited disaster recovery and business continuity plans in place for Rackspace headquarters and support services

Operational Security – *Customer's Application Environment*

- Best practices used in the random generation of initial passwords
- All passwords encrypted during transmission and while in storage at Rackspace
- Secure media handling and destruction procedures for all customer data
- Support ticket history available for review via the MyRackspace® customer portal
- Help available from Rackspace in configuring system logging to create a system audit trail
- Rackspace Security Services can provide guidance in developing security processes for compliance programs

experience fanatical support®

Toll Free: 1.800.961.2888 | International: 1.210.312.4700 | www.rackspace.com

rackspace HOSTING

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.

www.sync.com/your-privacy

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