AWTTC Vault

onehub

SECURITY

Onehub's mission is to provide robust tools that allow you to confidently share files and collaborate online. Protecting your data is our top priority, so we take active measures to secure your content throughout each step of your collaboration.

Secure Connection

Any time you interact to Onehub, you are automatically connected to the encrypted version of our service via HTTPS. Non-HTTPS connection attempts are redirected to a secure protocol.

Secure Sharing

When you upload or download content through Onehub, all of your data is encrypted using Transport Layer Security. Onehub disables use of older cryptographic protocols and requires at least TLS 1.0 or later for added protection.

Secure Storage

The content you share through Onehub is securely stored across multiple, remote data centers and replicated to provide redundancies. The data centers have physical access controlled by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass multi-factor authentication a minimum of two times to access data center floors. All physical access to data centers is logged and audited routinely. Data center staff do not have access to the encrypted information stored in the Onehub service.

Onehub's data centers are compliant with various certifications and third-party attestations including:

- SSAE 16
- PCI DSS Level 1
- ISO 27001
- FISMA

This ensures that customers storing and sharing sensitive information with Onehub can comply with their own internal controls and regulatory requirements such as HIPAA.

SECURE COLLABORATION

Once your data is stored in Onehub, you can ensure that only the people you allow will access your files, and only in the way you want them to.

Sign Ins

For files you don't make publicly available, a user must establish a session before interacting with the Onehub system. Every sign in is done securely with 256 bit SSL encryption. On every subsequent operation, sessions are verified, and access checking is done with each request.

Passwords are private and managed by the user. Administrators do not assign passwords or manage them. This increases security and decreases management burden for administrators. Additionally, passwords are stored using a cryptographic one way hash and are salted for additional entropy, conforming with industry standard best practices.

Granular Permissions

You can determine how much access others have to the content you share through our role-based permission settings. Each level of permission grants increased interaction capabilities with your content and includes the abilities of the lower roles.

Administrator	Can edit the Workspace pages, modify the logo and colors, and modify the Workspace security settings.
Moderator	Can upload, edit, and delete any file or folder. Can invite other users to the Workspace, invite users to a file and folder, create secure links, and edit all comments in the Workspace.
Creator	Can view previews, print, and download files. Can upload files to a folder or Workspace and delete folders and files they created. Can view and add comments to files, folders, and messages. Can post Messages to a Workspace.
Downloader	Can view previews, print, and download files. Cannot view or add comments to items.
Printer	Can view previews and print but cannot download files. Cannot view or add comments to items.
Viewer	Can view previews of files but cannot print or download files. Cannot view or add comments to items.

ADDITIONAL SECURITY

To create an environment where you feel confident in sharing your content and collaborating online, Onehub provides extra precautions.

Activity Reports

Onehub tracks every interaction with your content and collects that into an activity report so you know precisely who accessed your data, when they accessed it, and what they did with it.

Automatic Watermarking

Help ward off unwanted sharing by enabling automatic watermarking on your documents. The user's email or IP address, along with the word "CONFIDENTIAL", will be overlaid across each page of your file.

24/7 Monitoring

Onehub's servers and availability are monitored 24 hours a day, 7 days a week, 365 days a year from multiple locations around the world. Operations staff are notified immediately of any issues. The Onehub service is also monitored and tracked to ensure quality and responsiveness.

For more information about Onehub security practices, feel free to contact us at (877) 644-7774