How We Secure Your Data on Box Enterprise

AuditOne LLC

Protecting Your Data

Industry Standard Encryption:
Data-at-Rest Data stored on Box Enterprise is encrypted
Data-in-Motion Data is transported using end to end encryption between your computer and Box Enterprise

Least Privilege Access:
Our Primary Client Contact Access to all documents
Other Employees Access to specific audit folders

Access Monitoring:
Clients Full view of who has access to your folders

Data Retention Policy:
Documents Current and prior year
Client Accounts Revoked after one year of inactivity

Additional Material Available Upon Request: Redefining Content Security Box's Security Whitepaper Vendor Monitoring Performed by our IT Officer annually

Managing Our Employee Device Access

Not Permitted:
Box Sync for desktops and laptops
Box Mobile for iPhone, tablets, etc.
Third Party Applications

Complying with Regulatory Guidance

Initial Due Diligence and Ongoing Monitoring:
Initial Due Diligence We performed a risk assessment, reviewed Box's reputation and industry experience, and executed a GLBA-compliant contract
Ongoing Monitoring Annually, we review Box's financial condition, quality of service, insurance coverage, security controls audit report, and disaster recovery material

Audit Trails:
User Activities Login and security, and file access
Administrator Activities Login and security, user and group changes, file management, and external sharing activities

Callback:
Administrator Activities Review by an independent administrator

User ID:
Unique Attributed to a single user
Generic IDs Not allowed
Sharing IDs Not allowed
Internal Users Review Performed annually

Applying Security on Our Employees

Strong Password Policy Enforced:
Length Eight characters
Complexity Alphanumeric with upper case and special characters
Expiration 90 days
Passwords Reuse Last six cannot be reused
Common Passwords Not allowed by system
Multifactor Authentication Enforced with one-time password

Sharing with External Collaborators:
Invitation Can only be invited by our administrators
Public Access Disabled

Login Activities:
New Login Activities Alerts are sent to our users by e-mail
Suspicious Login Users are trained to alert our security staff

How To Secure Your Own Box Account

Whitelist the Following Domains on Your Web Filters:
- auditone.box.com
- *.app.box.com
- auditone.account.box.com

Whitelist the Following E-mail Address:
- noreply@box.com

Turn on Multifactor Authentication:
1. Click on your name on the top right of the screen
2. Click ⚙ Account Settings
3. Click on the **Security** tab
4. Check **Require 2-step verification for unrecognized logins**
5. Input your **mobile number**
6. Click Continue
7. Follow the instructions on screen

Use the principle of least privilege when requesting additional employee logins

Do not share user IDs

Use strong and unique passwords

Contact us when an authorized user is no longer with the Bank