Clemson University
Box Storage Guidelines

Table of Contents

Introduction

This document provides recommendations on how to use Box in a departmental, workgroup, or research context. It's intended to assist data owners with using the Box storage solution in a way that complies with Clemson University policies and secures data against inadvertent loss.

Sensitive Data

Many of the recommendations within this document refer to "sensitive" or "protected" data. While medical records and social security numbers apply, other classes of data should also be treated carefully. Examples include documents and other materials under copyright, student information, and materials that may have an intrinsic value to the University (such as intellectual property).

Box makes it possible to share files and folders with internal and external collaborators. Box can also help a department retain control of sensitive data with features such as no-download previews, expiring links, and watermarks. When using Box in a group context, think broadly about the kinds of data used, and apply the recommendations in this document to implement the appropriate controls.

Considerations and Recommendations

Departmental/Workgroup Accounts

Individuals with owner, co-owner, or editor permissions of a Box folder determine who can view and update files. This ownership model works well for most folders. For sensitive data, however, a top-level folder owned by a Box service account needs to be created. The top-level folder will have security enabled that restricts collaboration invites and shared links.

(Note: There are BoxSecure and BoxPHI folder structures.)

Figure 1 illustrates this structure.

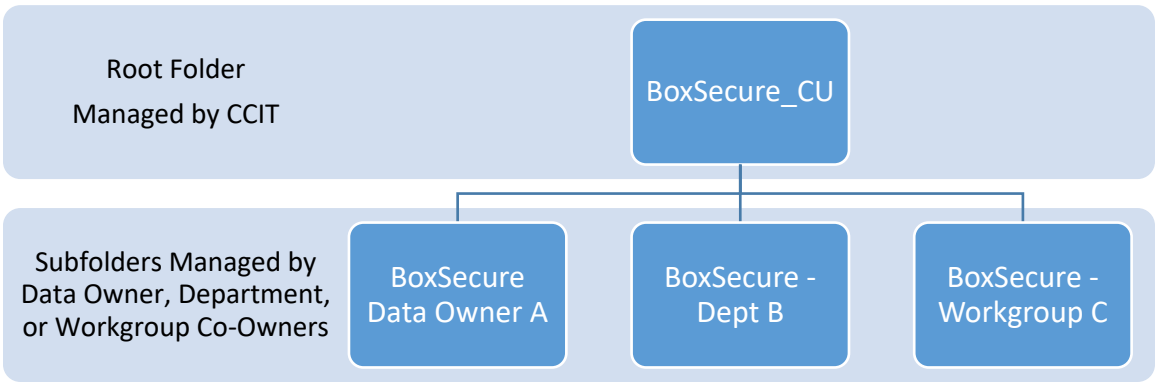

Figure 1: Unit/Department account structure

Collaborators vs. Shared Links

To share content, Box uses collaborators and shared links.

1. Collaborators are equivalent to folder permissions on a traditional file server. Collaborators can be Box users or groups. Each collaborator is assigned a permission level that dictates what they may do with the shared Box content. Typically, collaborators are used to share content among members of a department or workgroup.
2. Shared Links are unique URLs (web addresses) that grant read-only access to a specific file or folder within Box. There are options for shared links (e.g. having them expire on a certain date or allowing users to preview but not download content). Typically, shared links are used to share content with people external to the department or workgroup.

More information on the distinction between collaborators and shared links can be found here:

https://community.box.com/t5/Collaboration-and-Sharing/What-Is-The-Difference-Between-Collaboration-And-Shared-Links/ta-p/146

For content stored on Box that should not be shared outside of a workgroup, the ***best practice is to set folder settings to prevent the use of shared links with external users.*** It is also a best practice to grant the least level of access that allows the user to perform their job functions. The available access levels in Box are documented here:

https://community.box.com/t5/Collaboration-and-Sharing/What-Are-The-Different-Access-Levels-For-Collaborators/ta-p/144

Note that the Editor access level normally allows the user to invite other users as collaborators. For data that should not be shared outside of the workgroup, the ***best practice is to either limit most users to the Viewer Uploader access level or to use folder settings to explicitly restrict inviting collaborators to folder Owners and Co-Owners***, as described here:

https://community.box.com/t5/Collaboration-and-Sharing/How-Do-I-Disable-My-Collaborators-Ability-To-Invite-New/ta-p/164

Waterfall Permissions Model

Box has a "waterfall" permissions model, meaning that permissions set at one level in the folder tree are applied (inherited) by all sub-folders and cannot be revoked at a lower level. Permissions can be added at the sub-folder level, but not removed.

What this means in practice is that if a user is granted the Viewer access level on a root folder, the user will be able to see all content in all subfolders. This is in contrast to a traditional file server, where permissions can be changed at any level of the folder tree.

Given this waterfall permissions model, ***best practice is to grant permissions at the lowest level in the folder tree rather than at the root level***. This means that careful attention should be given to designing the folder structure up front, as changing it later will likely impact end users.

Figure 2 shows one possible permissions model that implements this best practice. Only the departmental Box administrator has the Co-Owner access level, meaning that this person will have Co-Owner permissions for all subfolders. Employees within each workgroup are given the lowest access level that allows them to efficiently do their jobs.

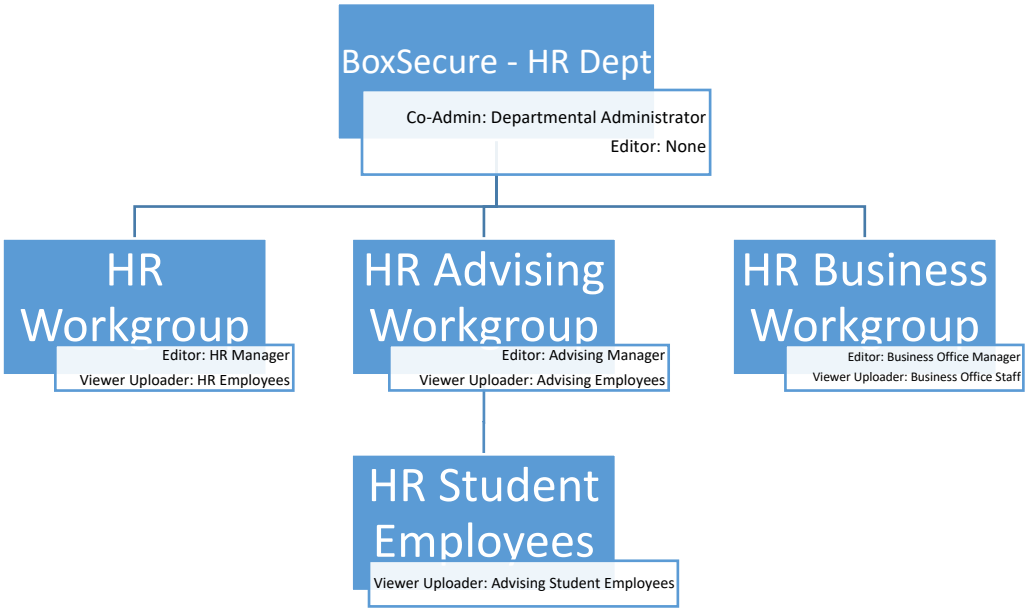

Figure 2: Example folder structure showing principle of lease privilege

Shared Folder Structure

With a traditional file server, users see shared folder structures starting at the share level (i.e. the top of the folder tree). With Box, users see folders starting with the top level at which they are granted access, and those folders appear in the root of the user's Box account.

For example (referring to Figure 2) the HR Manager and HR Employees will see the "HR Workgroup" folder in the root of their Box accounts. They will not see the "BoxSecure – HR Dept" folder. Similarly, the HR student employees will see the "HR Student Employees" folder in the root of their Box accounts and will NOT see the other folders.

Since sub-folders below the root of the departmental folder tree will appear as root-level folders to users, ***best practice is to institute a naming convention where all folders are prefixed with the root department name or abbreviation to distinguish them from user-created folders***.

Delineating Private and Public Spaces

Box makes it easy to share with external users. For this reason, it is a ***best practice to clearly delineate folders that are intended to be public from folders that are intended to remain private***. One strategy for this is to include it in the folder naming convention (e.g. "Department Public Documents" vs "Department Private Documents").

Folder Settings

For University business and other proprietary data, Box offers a number of security settings that may be useful for ensuring data is not inadvertently shared. Security settings can be found in the Box interface by browsing to the folder you wish to protect, hover over the folder name, click on "…" (ellipsis), then choose settings.

Security settings for a folder will automatically propagate to sub-folders when changed, and cannot be overridden on subfolders. Editor and other access levels cannot change folder security settings, so it is a ***best practice to grant Co-Owner rights only when there is a demonstrated business need; use Editor or lower access levels in most cases***.

- Collaborator invite controls

  If you wish to maintain control of sharing the content within your departmental Box space, use the "Only folder owners and co-owners can send collaborator invites" security setting to prevent Editors from inviting additional users to collaborate. Note that this impacts collaborators, but not shared links.

- Restrict collaboration to Clemson University

  By default, Box allows collaboration with anyone who has a Box account, including a free or paid Box account not affiliated with Clemson University. To ensure that data is restricted to only people who have University computing accounts, use the "Restrict collaboration to within Clemson University" security setting to prevent collaboration with external Box accounts. This will impact collaborators, but not shared links.

- Only collaborators can access this folder via shared links

  By default, Box allows collaborators to create and send shared links to files and folders. These links can be scoped to be completely public, available only to Clemson University Box users, or to only collaborators. If you wish to prevent users from creating and sharing links with other users outside of your department or outside of Clemson University**,** use the "Only collaborators can access this folder via shared links" security setting.

Version History, Backup, and Trash

Version History

As files are changed, Box maintains a minimum of 10 previous versions, along with metadata about which user changed the file and when the change was stored in Box.

Users can compare the current version with any previous version in the version history and restore any previous version. Version history serves as one form of backup and can provide a recovery mechanism from both accidental and intentional changes to files.

https://community.box.com/t5/Managing-Your-Content/How-To-Track-Your-Files-and-File-Versions-Version-History/ta-p/329

A common complaint about traditional file servers is the proliferation of separate files to track different versions of the same document (e.g., report.docx, report-v2.docx, report-v2-john-comments.docx, report-final.docx, report-REALLY-final.docx). Box can address this issue by allowing users to update (overwrite) the file while retaining access to previous versions through the Box version history feature. ***Best practice is to train users to avoid creating separate files for different versions and instead leverage Box version history***.

Note: In some cases it may be appropriate to store separate versions of files (e.g. when publishing official documents or forms where the version history should not be visible).

Data Backup (Disaster Recovery and Business Continuity)

The contract between Clemson University and Box provides strong assurances, supported by legal attestations, that data stored on Box is replicated to multiple, geographically diverse data centers, all within the continental United States. Based on the contract, most departmental uses of Box do not require separate backups for disaster recovery and business continuity.

Note: If departments are storing data under external contracts (e.g. data collected under federal or state grants or contracts with other entities), the terms of those contracts should be evaluated to determine if the level of data protection provided by Box meet the University's contractual obligations.

Trash

When files and folders are deleted from Box, they are stored in the Trash folder for 30 days. While in the Trash folder, both the owner of the folder/file and the user who deleted the folder/file can restore deleted folders/files. Users can permanently delete files by navigating to the Trash folder and marking files for deletion. This is similar to deleting email messages from Outlook.

Web Interface vs. Sync

Most desktop users are accustomed to working directly with files and folders stored on their computers (e.g. in the My Documents folder). Box offers the Box Sync utility that will selectively synchronize files and folders between the cloud and a user's computer, allowing users to work with content stored on Box in a familiar way.

Note: In a departmental context with sensitive data, the Box web interface is recommended. If the Sync option is to be used with sensitive data, full disk encryption must be configured on the users computer.

Box web interface advantages/disadvantages:

- The web interface includes features that are not available with locally synced files. For example, commenting, shared tags, version history, and access statistics. While a user can always access these features through the web interface for any content stored on Box, individuals who use Box Sync are less likely to incorporate these features.
- The web interface is the same across all platforms, which enables a consistent user experience on Mac, Windows and Linux. This can help with training and consistent workflow in bring-your-own-device (BYOD) or very heterogeneous computing environments.
- If multiple disconnected users are editing a file from their desktop (instead of in Box), this can lead to changes being overwritten.

Box sync advantages/disadvantages:

- Using the Box web interface requires a persistent network connection. If users need to work with data while disconnected from the network, Box Sync is a good option. A user can work with synced files normally, and changes will be uploaded back to Box when the user's device is next connected to the network.
- Users who are familiar with more traditional ways of interacting with files and folders will need training on the use of the web interface.

- Applications that access multiple files for a single project may not work well with sync. Examples include desktop publishing applications that store resources like images separately from the primary document (e.g. Adobe InDesign). One mitigation strategy is to store these kinds of application data files in a single folder in Box that can be selectively synced for users that work with these applications.
- Box Sync cannot be blocked on a folder-by-folder basis; therefore, administrative (vice technical) policies at the departmental level must be used to restrict Box Sync activities.

Box Utilities

Box offers convenience utilities that streamline interactions between desktop software and the Box web interface. The utilities include Box Edit and Box for Office.

Box Edit is available for Windows and Mac, and it integrates with all common browsers. With Box Edit installed, a user can open a file stored in Box directly in a desktop application without the extra step of first downloading it to the local computer. Box Edit handles the download automatically in the background and uploads changes to the file back to Box automatically. If users will be encouraged to use the Box web interface, best practice is to ensure that Box Edit is installed.

https://community.box.com/t5/Managing-Your-Content/Box-Edit-Overview-and-FAQs/ta-p/309

Box for Office is available for Windows only, and integrates with Microsoft Office 2010 and newer. The utility allows users to open and save files that are stored in Box directly from Microsoft Office desktop applications. It includes additional features for Microsoft Outlook to use Box and shared links rather than sending file attachments.

https://community.box.com/t5/Managing-Your-Content/Box-for-Office-Integrations/ta-p/324

Training Users

Box offers many online training resources to assist departments with transitions to Box. Leverage the training resources provided by Box to ensure that users are fluent in the use and features of Box.

Box offers a series of short online “Getting Started” videos to help users familiarize themselves with basic usage:

https://support.box.com/hc/en-us/sections/200144408-Getting-Started

Box Community offers how-to documentation covering basic and advanced features, along with forums (monitored by Box support personnel) where users can ask questions and get help:

https://community.box.com/

Summary of Recommendations

- For folders with sensitive content
    - Restrict the use of shared links to collaborators.
    - Limit most users to the viewer/uploader access level.
- Grant permissions at the lowest level in the folder tree rather than at the root level.
- Use a naming convention where all folders are prefixed with the root department name or an abbreviation to distinguish them from user-created folders.
- Clearly delineate folders that are intended to be public from folders that are intended to remain private via a naming convention.
- When appropriate, use the "Only folder owners and co-owners can send collaborator invites" security setting to prevent Editors from inviting additional users to collaborate. (Note: This is automatically enabled for the Secure and PHI folders.)
- Use the "Restrict collaboration to within Clemson University" security setting when storing sensitive data to prevent external collaboration. (Note: This is automatically enabled for the Secure folders.)
- If Box Sync is enabled for folders that may contain sensitive data, full-disk encryption needs to be setup on each collaborator's computer.
- Install Box edit if users will be encouraged to use the Box web interface.
- Establish administrative policies and expectations regarding what can be shared publicly and what must remain private.

Document History

Version	Date	Author	Revision Notes
1.0	2017-06-22	Office of Information Security & Privacy (OISP)	University of California (UC Davis) documentation used as a template.
1.1	2018-02-07	OISP	Added BoxPHI information.