University of Adelaide BOX Enterprise Acceptable Use and Security Guideline

Version	Author	Remarks
1.0	SS	Initial Release

Overview

Box (https://adelaide.edu.au/technology/yourservices/storage-printing/storage/box/) is an enterprise file sharing and synchronisation (EFSS) tool supported by the University of Adelaide for use by all staff and students. Box is a great tool for storing and accessing files from multiple devices, and facilitates sharing and collaboration between people both within and external to the University. On the other hand, improper use of Box may lead to data loss and security breaches.

This guideline explains how to use (or not to use) Box safely for storage, collaboration, linking and synchronisation.

Acceptable and Unacceptable Use

- The IT Acceptable Use and Security Policy (ITAUSP) and associated IT Acceptable Use Procedures apply to the use of UofA Box.
- Also, refer to Do's and Don'ts (http://www.adelaide.edu.au/technology/policies/do/) for what is deemed acceptable and unacceptable when using University IT resources.
- The use of Box service must also abide by the Box Terms of Use: https://www.box.com/legal/termsofservice

Secure use of Box Features

Box has many useful features, including collaboration, linking, and synchronisation. These must be used judiciously to ensure that the security of files will be maintained.

Refer to **Appendix A** for details of which features to use based on file sensitivity.

1. Collaboration

The collaboration feature in Box allows you to invite both internal and external users to view, edit, and comment on files. To ensure only authorised parties have access to University documents, please take the following precautions:

- Always double-check the email address of the collaborator before sending an invitation.
- Periodically check the list of collaborators to ensure they are valid and still required.
- For external collaborators, configure automatic expiration of maximum of 1 year, and renew the access rights as required.
- Only grant minimum permission required (choose from: “Editor”, “Co-Owner”, “Viewer Uploader”, “Previewer Uploader”, “Viewer”, “Previewer” and “Uploader”).
- Enable “watermarking” on folders containing sensitive data.

2. Linking

Linking is a quick and simple way to share files with recipients both within and outside of the University. Depending on the sensitivity of files being shared via a link, the following precautions should be taken:

- Configure automatic "link expiration" after a fixed number of days
- Configure a link password for particularly sensitive files
- Untick [**Allow Download**] to prevent downloading of files, and restrict to just viewing online
- Apply [**Watermark**] to folders containing particularly sensitive files.

3. Synchronisation

Synchronisation allows you to have multiple copies of your files on various devices, and seamlessly uploads/downloads changes to and from Box. While this is a very power feature, it can pose a security risk if you synchronise files to "insecure" devices, or portable devices that can be lost, stolen, or "hacked".

You should only synchronise files to **trusted, secure devices**. What is meant by "secure devices"? Please refer to Secure IT website for what constitutes a "secure device" and how to secure your devices. You can also choose NOT to allow synchronisation for folders, which would be the recommendation for sensitive files.

4. Litigation Hold

To prevent permanent deletion of critical files, you can request Service Desk to apply a "litigation hold" on specific folders to disallow purging of deleted files for a specified period.

Reporting Incidents

Please immediately report any security incidents including the following to Service Desk at 8313 3000 or by emailing servicedesk@adelaide.edu.au:

- Suspected and actual unauthorised access to files and folders
- Loss or theft of devices containing (synchronised) sensitive file
- Suspected compromise of your UofA account password

Appendix A: Box Acceptable Use Matrix

Refer to the University of Adelaide Information Classification and Protection Guideline for definition of Class 1, 2 and 3

Data	Storage	Collaboration	Linking	Synchronisation
Class 1 • Publicly available information	• No restrictions	• No restrictions	• No restrictions	• No restrictions
Class 2 • Non-sensitive business data • De-identified, non-sensitive research data	• No restrictions	• Only with trusted and authorised collaborators within and outside of the University • *Use automatic expiration (max 1 year) for external collaborators*	• With trusted and authorised internal and external users. • *Use automatic expiration (max 30 days)* • *Use password (communicated via SMS) as appropriate*	• Only synchronise to trusted, secure devices.
Class 2 • University official records	• Ensure final copy is also stored in HPRM.	• With trusted and authorised collaborators within the University only. • *Apply retention policies where required* • *Use “No Download” and “Watermarking” as appropriate*	• With trusted and authorised internal and external users. • *Use automatic expiration (max 30 days)* • *Use password (communicated via SMS) as appropriate* • *Use “No Download” and “Watermarking” as appropriate*	• Only synchronise to trusted, secure devices.
Class 3 • Personally-identifiable data • Sensitive business data • Sensitive or restricted research data	• Use with caution (avoid unless collaboration is required) • *Consult Technology Services* • *Use file-based encryption requiring additional password as appropriate*	• Use with caution (avoid unless collaboration is required) • With trusted and authorised collaborators within and outside of the University • *Use “No Download” and “Watermarking”*	• Use with caution (avoid unless collaboration is required) • With trusted internal and external users. • *Use automatic expiration (max 7 days)* • *Use password (communicated via SMS)* • *Use “No Download” and “Watermarking”*	• Disable synchronisation to devices
Class 3 • Credit card data • Passwords	• Not allowed	• Not allowed	• Not allowed	• Not allowed
Non-commercial personal data • Photos, personal videos, etc.	• Within reasonable limits	• Within reasonable limits	• Within reasonable limits	• Within reasonable limits