DropBox and University Data Guideline

Syracuse University – Information Technology and Services Information Security Guideline – G0100

(Based on the University of Melbourne's *DropBox and University Information* Policy)

(Used with the permission of the University of Melbourne)

1.0 Scope

- Any use of DropBox with University information to include use by or with
  - SU full time faculty and staff
  - SU part time faculty and staff
  - All data created, processed and stored on SU owned computing devices
  - All data owned by SU
- This guideline is to be used in conjunction with the *Cloud Based Storage and University Data Standard.*
- This guideline does not authorize any action which would infringe any other policy, rule, statute or legislation to which the University and users of its IT resources are subject.
- This guideline does not authorize the install or use of the DropBox application on any computing device. Installation of the DropBox application is approved on an individual basis by the unit IT departments.

2.0 Purpose

DropBox is a convenient and near seamless internet service for storing or synchronizing a consistent set of files on one or more computers and online storage. The files stored on DropBox can be used on any synchronized computer and can be accessed via any modern web browser. Online files can also be accessed from mobile devices like the iPhone, iPad, and Android devices, and there are facilities for sharing data with other users. This makes cloud storage a most attractive platform for collaboration and sharing amongst colleagues.

However, the use of the DropBox services does pose risk related to the security, privacy, copyright and retention of SU data, A University review of DropBox, its terms of use and its security, leads to the conclusion that subject to the guidelines set out in section 3.0 of this document , DropBox may be used for some University information.

3.0 Guidelines

3.1 Dropbox ***may not be used*** to store or transmit confidential information as defined in the *Syracuse University Information Security Standard*. Confidential information includes any

information that is governed by federal, state or local law, or regulated by industry. Examples include (but are not limited to):

- ***Personally Identifiable Information*** (SSN, account numbers, birth dates, driver's license numbers, etc..)
- ***HIPAA information*** (Any health related information including diagnosis, dates of service, doctor visit information, treatment information, EOBs, provider information, etc…)
- ***FERPA Information*** (Any Student Records, grades, class enrollment information, etc..)
- ***Payment Card Industry Information*** (Credit Card Numbers, PINs, verification codes etc.)

3.2 DropBox should not be used with enterprise information as defined in the *Syracuse University Information Security Standard* unless there is no alternative method, of comparable immediate availability and ease of use and with better security, to achieve the required functionality. Enterprise Information includes (but is not limited to):

- University Records
- SU Contract Data
- SU Financial Data
- SU Business Data
- SU Employee Information

3.3 Any enterprise information stored on DropBox must be in encrypted form. Several encryption products exist. Truecrypt is a free, open source, multiplatform encryption utility, but does not work on mobile devices. ***DropBox's "built in" encryption is NOT sufficient to meet this guideline!***

3.4 Any DropBox file sharing is limited to small groups of highly trusted colleagues, using shared folders not public folders.

3.5 Files should be left online for no longer than is necessary.

3.6 Owners of shared folders should frequently review DropBox events and shared folder membership, and promptly update shared folder membership to reflect changes in colleagues' roles.

3.7 Participants should not put anything on DropBox that they would not be comfortable having taped to their office door.

3.8 DropBox is not to be used as the sole storage for any University Record, or as a recordkeeping system.

3.9 All University users of DropBox should exercise self-discipline to ensure that passwords are reasonably strong and are changed at reasonable intervals.

3.10 You may not use the same NetID and password that you use at SU to access DropBox.

3.11 As with any use of personal computers, those who use and manage the computers should be vigilant against security threats including phishing, viruses, trojan horses and key-logging.

3.12 DropBox should not be used on mobile devices connected via unencrypted Wi-Fi networks.

4.0 Referred Documents, Web Pages and Contact Information

Item	Location/Info
Standard: *Cloud Based Storage and University Data Standard –S0102*	http://its.syr.edu/security/standards/CloudStorageStandard-S0102.pdf
Standard: *Syracuse University Information Security Standard*	http://its.syr.edu/security/standards/ITSecurity-standard.pdf
Contact: Director of Information Security	Christopher Croad ccroad@syr.edu

Document Info

Version:	1.0
Effective Date:	May 24, 2012
Date of Last Review	Sep 24, 2015
Date of Next Mandatory Review	Apr 24, 2017