

Information System Storage and Data Sharing Standard

Current Version	Compliance Date	Approved Date
1.2	12/31/2018	11/13/2018

1. Purpose

The purpose of the Information System Storage and Data Sharing Standard is to define the acceptable facilities and services for the storage of Information Systems and Data sharing.

2. Standard

All University Information Systems and/or Data must be stored in services or locations that have completed an Information Security Risk Assessment in accordance with the *OUHSC Information System Storage and Data Sharing Policy* and *OUHSC Information Security Risk Assessment Policy*.

2.1 Common Services

Table 1 provides a list of common Information System storage and Data sharing services, the types of Information Systems and Data that can use these services, as well as any additional requirements that must be met in order to use these services. This table is subject to change as the University assesses the acceptable use of common services.

Table 1 - Common Services

Service/Solution	Category A HIPAA/Protected Health Information (PHI)	Category A Family Educational Rights and Privacy Act (FERPA)	Category A Human Participant Research Information	Category A Payment Card Industries (PCI)	Category A Personally Identifiable Information (PII)	Category B	Category C	Category D	External Sharing <small>* See External Sharing</small>	Technical Support Provided by OUIT
Shared Services Network File Storage	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes
Shared Services SharePoint	No	Yes	Yes ¹	No	No	Yes	Yes	Yes	No	Yes
OneDrive for Business	No	No	No	No	No	No	No	No	No	No
Dropbox for Business	No	Yes ¹	Yes ¹	No	No	Yes ¹	Yes ¹	Yes	Yes ²	No
Google Drive	No	No	Yes ¹	No	No	Yes ¹	Yes ¹	Yes	No	No

¹ Requires an OUHSC Information Security Risk Assessment and Legal Counsel approval of the contract, prior to use.

² Files and folders containing student data require OUHSC Information Security Risk Assessment and Legal Counsel approval of the contract, prior to use.

Service/Solution	Category A HIPAA/Protected Health Information (PHI)	Category A Family Educational Rights and Privacy Act (FERPA)	Category A Human Participant Research Information	Category A Payment Card Industries (PCI)	Category A Personally Identifiable Information (PII)	Category B	Category C	Category D	External Sharing <small>* See External Sharing</small>	Technical Support Provided by OU IT
Amazon Web Services	Yes ¹	Yes ¹	Yes ¹	No	Yes ¹	Yes ¹	Yes ¹	Yes	Yes ¹	No
Azure Cloud Services	Yes ¹	Yes ¹	Yes ¹	No	Yes ¹	Yes ¹	Yes ¹	Yes ¹	Yes ¹	No
Basecamp	No	No	No	No	No	Yes ¹	Yes ¹	Yes ¹	No	No
Qualtrics	No	No	No	No	No	Yes	Yes	Yes	No	Yes
Secure Email	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
OU Sync & Share	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
OU Research Cloud	No	No	Yes	No	No	Yes	Yes	Yes	No	Yes
Cisco WebEx	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
GoToMeeting	No	No	No	No	No	Yes	Yes	Yes	Yes	No
AdobeConnect	No	No	No	No	No	No	No	No	Yes	No
Desire2Learn (D2L)	No	Yes	No	No	No	No	No	No	No	No
Bittorrent	No	No	Yes ¹	No	No	No	Yes ¹	Yes	No	No
Box	Yes ¹	Yes ¹	Yes ¹	No	Yes ¹	No	Yes ¹	Yes ¹	Yes ¹	No
Aries	No	No	No	No	No	No	Yes ¹	Yes	No	No
EMule	No	No	No	No	No	No	Yes ¹	Yes	No	No
Kazaa	No	No	No	No	No	No	Yes ¹	Yes	No	No
Facebook	No	No	No	No	No	No	Yes ¹	Yes	No	No
Twitter	No	No	No	No	No	No	Yes ¹	Yes	No	No
Blogs	No	No	No	No	No	No	Yes ¹	Yes	Yes	No
Wiki	No	No	No	No	No	No	Yes ¹	Yes	Yes	No

2.2 OUHSC Information Security Risk Assessment

The mandatory OUHSC Information Security Risk Assessment process is intended to assist Business Units with understanding the technology risks associated with technology-related products and services.

All Information Systems receiving, storing, transmitting, and/or processing University data must have an Information Security Risk Assessment completed by OUHSC IT to identify risks and necessary regulatory or security controls to be implemented, as required by the *OUHSC Information Security Risk Assessment Policy*. Additional information is provided at <https://it.ouhsc.edu/forms/productreview.asp>.

Business Units looking to determine if the use of a service or solution has completed the OUHSC Information Security Risk Assessment Process may contact IT Security at 405-271-2644 or it-security@ouhsc.edu.

A completed Information Security Risk Assessment does not constitute an approval or authorization to purchase the requested service. State of Oklahoma and University purchasing rules still apply.

3. Related Documents

- Information System Storage and Data Sharing Policy
- Information Security Risk Assessment Policy

4. Scope

All Information Systems and Data are subject to this standard.

5. Revision, Approval and Review

5.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	07/25/2018	OUHSC IT	Baseline Version
1.1	09/10/2018	ITRC	Minor revisions
1.2	09/11/2018	Jill Raines	Removed "The use of non-OU IT Supported services establishes an obligation on the part of the requesting party to use the service responsibly and in compliance with OUHSC Policies and Standards." Updated footer to reflect Legal Counsel approval of contract. Added Section 2.2 with references to the IS Risk Assessment Policy, and disclaimer warning that the IS Risk Assessment does not constitute approval or authorization to purchase.

5.2 Approval History

Version	Date	Approved By
1.2	11/13/2018	Information Security Review Board

5.3 Review History

Date	Reviewed By
09/06/2018	ITRC