

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS

Information Technology Services

Process Number: BP-03-011

Approved By: James August

AVP for Information Technology Services

Effective Date: 03/23/2017

Page 1 of 7

Business Practice for Public Cloud Storage, Enterprise File Sync, Share, and Storage.

PURPOSE:

Describe the usage of CSUCI-provided public cloud storage and enterprise file synchronization and sharing utilities (i.e. OneDrive, Dropbox, Google Drive, etc.) for university business.

BACKGROUND:

In support of collaborative data sharing practices ITS supports the use of public cloud storage and enterprise file synchronization and sharing (EFSS) practices at Cal State University Channel Islands (CI), provided that the university manages the risk of any loss or misuse of the data being shared.

BUSINESS PRACTICE: Accountability:

Associate Vice President for Information Technology Services:

Applicability:

All CI domain account holders. **Definitions:**

1. **Public Cloud Storage** - a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.
2. **Enterprise File Synchronization and Sharing (EFSS)** – EFSS refers to a range of on-premises or cloud-based capabilities that enable individuals to synchronize, store, and share documents, photos, videos, and files across multiple devices, such as smartphones, tablets, and PCs. File sharing can be within the organization, as well as externally (e.g., with partners and customers) or on a mobile device as data sharing among apps. Security and collaboration support are critical capabilities of EFSS to address enterprise priorities.
3. **OneDrive** - EFSS application offered by Microsoft (Official university cloud storage solution).
4. **Dropbox for Business** - EFSS utility offered by Dropbox.com.
5. **CI Docs/Google Drive** - EFSS utility offered by Google.
6. **Box** - EFSS utility offered by Box.net.

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS

Information Technology Services

Process Number: BP-03-011

Approved By: James August

AVP for Information Technology Services

Effective Date: 03/23/2017

Page 2 of 7

-
7. **Network File Share** – Enterprise network local storage for files administered by CI (H:\ Drive)

Business Practice for Public Cloud Storage, and Enterprise File Sync and Share

8. **Personal Cloud Storage** – File storage via a cloud service (such as Dropbox, Box, Microsoft, Google or Apple) using an account provided as a personal/individual account and not a university-issued account.
9. **University Cloud Storage** – File storage used in the context to conduct or transact academic or administrative business on behalf of CI or for purposes of academic knowledge, administration, University projects, or other academic activity to support the education of CI's students, support the professional and academic growth of CI's faculty, and the general advancement of CI as an institution. Data for university use must not be stored in Personal Cloud Storage. Please refer to the storage matrix for further instructions on storage
<https://www.csuci.edu/its/security/data-storage-matrix.htm>
10. **Storage Quota** – The maximum amount of file storage space university users can have.

Text:

General information on Microsoft OneDrive and Dropbox

OneDrive and Dropbox are used for Business products at our campus. Proper usage and disposal of CI data are required to comply with federal and state law and CSU policy. As such, using public cloud storage and sharing solutions for CI data requires data classification practices to be enforced before these technologies may be used.

Dropbox@CI shall be used only as a tool of convenience for sharing and storing files that do not contain high-risk / level 1 data (see chart below). All high-risk/level 1 data shall be maintained on CI's secure campus network file share (currently your campus assigned H:\ drive).

Storage quota for cloud storage will vary by solution due to differing cost structures with each provider.

OneDrive cloud storage:

- Students/Alumni 25GB
- Staff 100GB

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS
Information Technology Services**Process Number:** BP-03-011**Approved By:** James August

AVP for Information Technology Services

Effective Date: 03/23/2017**Page 3 of 7**

-
- Faculty/Emeritus: 1TB

Google Drive:

-
- Students/Alumni 5GB
 - Staff 0GB
 - Faculty/Emeritus: 500GB

The grid below describes allowable levels of usage for CI's designated cloud storage and sharing provider(s) listed in this document. Additional information regarding CI's data classification standard found at <https://www.csuci.edu/its/security/data-storage-matrix.htm>

Personal cloud storage should be used for storing and sharing personal data and not university-related data.

Google Drive is approved for collaborative purposes only and should not be used for storing and/or sharing university data, particularly high-risk/Level 1 data.

Business Practice for Public Cloud Storage, Enterprise File Sync, Share and Storage

Low Risk		Moderate Risk		High Risk	
Level 3 – General Information		Level 2 – Internal Use		Level 1 - Confidential	
Permitted to Store YES	Permitted to Share YES	Permitted to Store YES	Permitted to Share MAYBE	Permitted to Store NO	Permitted to Share NO

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS

Information Technology Services

Process Number: BP-03-011

Approved By: James August

AVP for Information Technology Services

Effective Date: 03/23/2017

Page 4 of 7

<ol style="list-style-type: none"> 1. Information at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of the campus in order to mitigate potential risks. 2. Disclosure of this information does Not expose the CSU to financial loss or jeopardize the security of the CSU's information assets. 	<p>Information may be classified as "internal use" based on criteria including but not limited to:</p> <ol style="list-style-type: none"> 1. Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations. 2. Moderate risk - Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights, or make legal action necessary. 	<p>Information may be classified as "confidential" based on criteria including but not limited to:</p> <ol style="list-style-type: none"> 1. Disclosure exemptions - Information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. 2. Severe risk - Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CSU's reputation, and legal action could occur. 3. Limited use - Information intended solely for use within the CSU and limited to those with a "business need-to know." 4. Legal Obligations - Information for which disclosure to persons outside of the University is governed by specific standards and controls designed to protect the information.
--	---	--

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS

Information Technology Services

Process Number: BP-03-011

Approved By: James August

AVP for Information Technology Services

Effective Date: 03/23/2017

Page 5 of 7

Business Practice for Public Cloud Storage, and Enterprise File Sync and Share

Additional information regarding access, storage and transmission of Level 1 Confidential information restrictions are described in [CSU Asset Management Standards](#).

Level 1 – Confidential Data Storage Alternatives

Confidential data shall be stored using the campus secure network file share. This solution allows for a more secure and controlled environment to protect the data entrusted to CI.

Level 2 – Internal Use Data Storage and Sharing

Special care should always be taken when sharing Level 2 internal use data. In cases where Level 2 data needs to be shared, utilization of the campus secure network file share may be the correct course of action to take for storing this data before sharing in an alternative, more secured manner. If you have any questions regarding storage of Level 2 internal use data, please contact the Information Security Officer at infosec@csuci.edu before storing your data.

Level 3 – General Information

Level 3 data may always utilize the designated EFSS solutions used at CI.

Any questions regarding this business practice should be directed to the Information Security Officer at infosec@csuci.edu.

NOTE: Email is not a suitable medium for storing, sharing, or transporting Level 1 Confidential or Level 2 Internal Use data.

Exhibits:

These documents are incorporated by reference. Please consult the ITS Policy website for the latest versions:

[IT.01.002 – Policy on Data Classification Standard](#)

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS
Information Technology Services

Process Number: BP-03-011

Approved By: James August

AVP for Information Technology Services

Effective Date: 03/23/2017

Page 6 of 7

[ICSUAM 8065.S001 – Information Security Asset Management Standard](#)

[ICSUAM 8065.S02 – Information Security Data Classification Standard](#)

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS
Information Technology Services**Process Number:** BP-03-011**Approved By:** James August

AVP for Information Technology Services

Effective Date: 03/23/2017**Page 7 of 7**

Business Practice for Public Cloud Storage, Enterprise File Sync, Share and Storage

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned	Date Completed
General review of this business practice	Annual – July	ITS Leadership	10/14/2024

Revision History

BP Nbr:	BP-03-011	Enacted Date:	03/23/2017		
Revision Nbr:	000	Revision Date:	99/99/9999	Revised By:	Neal Fisch
	001		10/14/2024		C Miranda