ALVIN COMMUNITY COLLEGE	Information Technology Services	
Section Title: : Cloud Storage Standard - Microsoft OneDrive for Business - Employee	Number: cr-02	Page: 1 of 2
Policy Title: TECHNOLOGY RESOURCES	Policy Number: CR	
Local	Date Adopted by ELT: 12/12/17	

Purpose

The purpose of this procedure is to define the acceptable use of third party Cloud Storage, specifically Microsoft OneDrive for Business. This standard applies to all ACC employees, and to all third party organizations and individuals that require access to non-public electronic resources maintained by ACC.

1. Background

Cloud storage refers to any program owned by a third party that allows one to upload their data using the Internet. An advantage of cloud storage is that files can be easily accessed and synchronized from multiple devices anywhere in the world, and shared with anyone. Another benefit is increased resiliency and redundancy for business continuity planning and disaster recovery. This type of online storage can increase productivity, but it also comes with significant security risks. These risks may include:

- Potential loss of security, lessened security, or inability to comply with various regulations and data protection laws.
- Dependency on a third party for critical infrastructure and data handling processes.
- Potential security and technological defects in the infrastructure provided by a cloud vendor.
- Limited service level agreements for a vendor's services and the third parties that a cloud vendor might contract with.

Therefore, Cloud Storage should never be utilized to store sensitive or confidential data.

2. Standard – Microsoft OneDrive for Business

The College provides all employees access to Microsoft Office 365 suite of productivity tools. As part of this suite, employees have access with their ACC login ID to Microsoft "OneDrive for Business" cloud storage platform. The Information Technology Department only supports the use of enterprise OneDrive for Business for the cloud storage and collaboration needs of the campus. Please note that "OneDrive for Consumer" is a separate

service offered by Microsoft to the general public is not supported by ACC Information Technology Services. Information Technology Services also does not support the use other cloud storage providers.

3. Acceptable Use for Microsoft Office 365 and OneDrive for Business

The responsibility for storing College documents and files resides with the person who stores the data. Judgment is required about how and where College data will be stored.

Confidential data should NEVER be uploaded, shared, or stored on Microsoft OneDrive or any other cloud service. Data meeting these criteria should be stored on college-controlled servers and networked drives.

Confidential data includes data which is classified confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. Examples of confidential data include but are not limited to:

- Student education records protected by FERPA.
- Social security numbers
- Credit/debit card numbers covered by PCI-DSS
- Bank account numbers
- Personal financial information
- Classified National Security information under Executive Order 13526.
- Intellectual property such as copyrights, patents, and trade secrets
- Login/password credentials
- Patient billing information and protected health information as protected by HIPAA

OneDrive for Business accounts should only be used for data classified as Protected or Public. Refer to the College Data Classification Standard for more information.

4. Best Practices for Microsoft OneDrive for Business

Pay special attention to access levels when sharing files and folders with other collaborators to ensure that data is not inappropriately shared. Only share folders and files with specific individuals; never everyone, or 'public'.

Use caution when sending links to shared folders. Links, like an attachment, can be forwarded.

Do not store the only copy of a file in OneDrive. Always keep a backup of any files that are stored in OneDrive. Recovery of files in OneDrive is not supported.

Do not use One Drive for long-term retention of College documents or files. Alternatives such as department specific shared network drives (S: drive) or a document storage solution (e.g. DocuWare) should be utilized for long term retention.

5. Violations

An employee's computer use privileges may be suspended immediately upon the discovery of a possible violation of this Standard. Suspected violations will be confidentially reported to the appropriate system administrator, employee's supervisor, and Office of Human Resources.

Violations of this Standard will be dealt with in the same manner as violations of other College policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, termination from the College, and legal action. Violations of some of the above standards may constitute a criminal offense.