Washtenaw
Community College

Cloud Storage Policy

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

PURPOSE

The purpose of this policy is to establish the rules regarding the use of "Cloud Storage" Services at Washtenaw Community College. The College is committed to ensuring its IT Systems and data stored externally in the cloud are secure and are only accessed by authorized users.

SCOPE

As new technologies are developed and adopted, and new compliance requirements covering Data security emerge, issues multiply around Data management and security. All College staff using "Cloud Storage" Services must therefore adhere to this Policy.

ROLES & RESPONSIBILITIES

Information Security Office: The Information Security Office is responsible to ensure compliance with this policy as a component of the College's information security program.

Users: All Cloud Storage users agree to comply with this policy and apply safeguards to protect Washtenaw Community College information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include protection of their access credentials and the use of discretion in choosing what and where College Data is stored.

REQUIREMENTS & PRACTICES

The purpose of this policy is to protect College data. Washtenaw Community College understands that public cloud storage provides a convenient method for accessing files and data from a number of different devices. If employed in a work context, however, such services can also introduce risks including security, compliance, privacy, copyright and retention of College data.

You are required to use only those supported solutions when storing sensitive college data. Only approved Cloud Storage services may be used to store confidential, restricted or internal data as defined by *Data Classification Policy*. Approved Cloud Storage services hosting sensitive data are required to satisfy all minimum compliance and regulatory safeguard requirements for access control, authentication (e.g. strong passwords, multi-factor), encryption (e.g. transmission, data-at-rest), data integrity, and audit controls (e.g. logging).

Before using cloud storage for work, users of the College computing environment must ensure the usage is appropriate and follow the policy requirements detailed in this document to limit their exposure and the risk imposed on College data. For example, using cloud storage client software to synchronize files between work and personal devices could result in sensitive information being held inappropriately on personal equipment. Users must therefore understand and adhere to the following requirements:

- All Washtenaw Community College Users have a responsibility to protect the College's data. Users must familiarize themselves with the security requirements of the data in their custody.
- The College has provided all staff access to Microsoft Office 365. As part of this, users have access to Microsoft "OneDrive for Business" using accounts based on their WCC netID. Using OneDrive via a user's logon ID is therefore the approved Cloud Storage solution for use.
- The College has also provided Google Drive for academic use via an individual's WCC netID. Google Drive use via the WCC netID is therefore an approved Cloud Storage solution for academic use only.
- All documents placed on Cloud storage services are subject to College data classification, protection and retention requirements. Users shall not use cloud or hosted storage for storage of any documents containing sensitive information with first ensuring they are in compliance with the requirements established within the *Data Classification Policy*, *Data Protection Policy* and *Records Retention and Disposal Policy*.

- All computers, both College-owned and personal, connecting to College-approved Cloud Storage services shall be configured to comply with the *Server and Computer Configuration Standards*. While ITS ensures that College-owned computers conform with these standards, individuals with personal computers are responsible for compliance and are expected to have taken precautions to avoid common security vulnerabilities, including:
  - Use of up-to-date anti-virus software
  - Ensure that client systems and applications are up-to-date on available patches, including security patches for installed operating systems (ideally with auto-update enabled), web browsers, and common applications shall be applied in a timely manner.
  - A personal firewall should be installed and enabled on each client system
  - Ensure that a screen lock is used whenever the remote session is unattended

- All mobile devices, including tablets and phones, accessing approved Cloud Storage services shall be configured in accordance with the College's *Mobile Device Policy*
- There may be circumstances when other Cloud Storage services and providers need to be considered for work-related use, for example when collaborating with other institutions which have a different service in place, such as Dropbox or Box.com. Approval for use of these services will be handled as Exceptions, defined later in this policy. Considerations for approval include:
  - Use of strong passwords for authentication, as defined within *Password Complexity & Management Policy*.
  - Cloud service providers may utilize data centers and network resources outside of the United States to transmit, store, or process data. Due diligence should be exercised to verify legal compliance or contractual requirements concerning possible geographical restrictions on data activities prior to engaging these services for College business.
  - College data stored with Cloud Service providers may be subject to Federal, State or compliance-related public records

retention and disposal provisions. Understand that such data may also be subject to subpoena during an E-discovery litigation request. Users of College approved cloud storage services to conduct college business must understand the requirements for responding to public record requests as well as discovery in the litigation process.

- Cloud provider risk mitigation controls in the event of a disaster or service interruption may impact accessibility of data in their care. Business continuity or data recovery procedures in place for data residing on Washtenaw Community College systems may not extend to cover data stored externally.
- Campus departments may lose access to College data stored with cloud services should an individual terminate their employment.
- Considerations and ramifications for situations where the only copy of a file may be placed within a Cloud Storage service.

COMPLIANCE

This policy is a component of Washtenaw Community College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA, HIPAA and other regulations.

EXCEPTIONS

The Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the *Request for Policy Exception* form and a copy maintained by the CIO.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Washtenaw Community College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

DEFINITIONS

Cloud Storage: Term cloud storage refers to third party online storage services such as Google Drive, Dropbox and OneDrive. Files stored on these services can usually be accessed via any web browser and often have the capability to be "synchronized" to multiple computers and mobile devices such as mobile phone and tablets. They may also have facilities for sharing files with other people.

Confidential Data: Specifically restricted data from open disclosure to the public by law is classified as Confidential Data. Confidential Data requires a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use.

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

User: Any Washtenaw Community College faculty, staff, students or partner who has been authorized to access any College electronic information resource.

REFERENCES

Data Classification Policy

Data Protection Policy

Password Complexity & Management Policy

Request for Policy Exception

Records Retention and Disposal Policy

Server and Computer Configuration Standards

Mobile Device Policy

REVISION HISTORY

Version	Description	Revision Date	Review Date	Approver
1.0	Initial version	10/11/18	-	WJO