MIDDLE GEORGIA STATE UNIVERSITY

OFFICE OF TECHNOLOGY RESOURCES Effective Date: 03/01/2018

Title: Cloud Storage Policy

1.0 Overview

Cloud storage offers a number of advantages such as accessibility, low cost and increased collaboration. However, without adequate controls, it also exposes individuals and Middle Georgia State University to online threats such as data loss or theft and unauthorized access to sensitive and confidential data.

2.0 Purpose

This policy is meant to ensure that only approved cloud storage is used and proper precautions are taken to protect the integrity and confidentiality of Middle Georgia State University data stored "in the cloud."

3.0 Scope

This policy applies to all faculty, staff and students at Middle Georgia State University.

4.0 Policy

Middle Georgia State University has approved OneDrive for Business for use by faculty, staff and students as cloud storage. It is appropriate for most communication and collaboration; however, the sensitivity and nature of the information must be carefully considered before you choose to save information to cloud storage. Please note: One Drive for Business is different from the individual consumer version of OneDrive.

Confidential information is prohibited from being stored in the cloud. Examples include:

- Sensitive Personally Identifiable Information (PII)
- Regulated information, the disclosure of which is subject to regulatory compliance (including FERPA, GLBA, HIPAA, etc).
- Tax Return Information

Only approved cloud storage may be used to store Middle Georgia State University data in the cloud.

Approved cloud storage must be protected with multi-factor authentication (MFA).

Approved cloud storage must only allow sharing among Middle Georgia State University faculty, staff and students.

Approved cloud storage must only allow syncing of data to Middle Georgia State University owned computers.

The use of cloud storage must comply with Middle Georgia State University policies and all laws and regulations governing the handling of personally identifiable information, financial data or any other data owned or collected by Middle Georgia State University.

5.0 Enforcement

Middle Georgia State University will implement “Data Loss Prevention” (DLP) policies to detect and block sharing of confidential information placed on cloud storage. These policies use keyword matches, dictionary matches, the evaluation of regular expressions, internal functions, and other methods to detect content that matches DLP policies.

Middle Georgia State University will enable MFA on all cloud storage accounts.

Middle Georgia State University will permit sharing only among user accounts in the MGA.EDU Active Directory Domain.

Middle Georgia State University will block syncing to computers not joined to the MGA.EDU Active Directory Domain.

MGA.EDU accounts will deleted for users that are no longer current faculty, staff or students. Associated cloud data will be permanently deleted 30 days after the account is deleted.

The CIO must approve any waiver of these requirements.

6.0 Definitions

Confidential Information: information maintained by a Middle Georgia State University that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws and is legally protected from release.

Sensitive Personally Identifiable Information (Sensitive PII) - personally identifiable information that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples include social security numbers, driver’s license or state identification number, passport number, Alien Registration Number, or financial account number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation or lifestyle information and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII.

Cloud Storage – A model of networked online storage where data is stored in virtualized storage pools generally hosted by third parties and in locations not owned by the university. Examples include Dropbox, ICloud, OneDrive, etc.

Multi-factor Authentication - a method of authentication that requires more than one verification method and adds a critical second layer of security to user sign-ins and transactions. It works by requiring any two or more of the following verification methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)