SUBJECT: Storage of Electronic Records	**Effective Date:** 9-24-24	**Policy Number:** 12.15	
	Supersedes: NEW	**Page:** 1	**Of**: 4
	Responsible Authority: Associate Provost and Chief Information Officer		

I. APPLICABILITY/ACCOUNTABILITY

This policy outlines the parameters for the storage of electronic records. This policy supplements University Policy 5.2, *Records Management*, which governs the retention and preservation of University Records, as defined therein.

II. DEFINITIONS

A. **Local Storage**: Storage on a physical device (e.g Desktop, Laptop, Mobile Phone, Tablet).

B. **Network Storage**: Storage hosted by the University and mapped as a drive, volume, or location on a desktop or laptop.

C. **Cloud Storage**: Storage provided through third-party services not hosted by the University.

D. **Individual Cloud Storage**: A form of cloud storage that is individually assigned to a specific user such as Microsoft Onedrive or Google Drive.

E. **Employee Data**: Information created by a University employee that is not a University Record.

F. **Group Cloud Storage**: A form of cloud storage shared with multiple users to support group or departmental needs such as Microsoft Teams, Microsoft SharePoint, or Google Shared Drive.

G. **Separation**: The end of an employee's formal employment with the University.

H. **Storage Platforms**: For purposes of this Policy, Storage Platforms shall include Local Storage, Network Storage Drives, and Individual Cloud Storage, and Group Cloud Storage.

I. **Student Data**: Information created by a University student that is not a University Record.

III. STUDENT DATA

A. Storage of Student Data: Students may store student data on University Storage Platforms; however, students are responsible for backing up such data, as they deem appropriate, outside of University Storage Systems. The Office of Information Technology (OIT) can provide reasonable assistance with the recovery of lost or damaged files, but recovery is not guaranteed.

B. Storage of Deleted Files or Emails: Office 365 Cloud Storage will be configured to retain files for a minimum period of one (1) year after deletion. Files stored on Google Cloud storage will be configured to retain files for a period of thirty (30) days or more after deletion. Files located on Network Storage Drives will be configured to retain data for one year after deletion. After such retention periods, files and emails may be purged and no longer accessible.

C. Storage of Files after Attendance: Student email and data will be configured to remain available for one (1) year after the last academic term of attendance or graduation. After one (1) year, the account and any associated data will be disabled and retained for one (1) additional year before being purged.

IV. UNIVERSITY RECORDS

A. Storage of University Records: University Records should not be stored on Local Storage unless the information is being saved temporarily to allow for offline or transactional use of data, which will be synced and stored in Cloud or Network Storage after use, for research or other applications requiring the use of Local Storage. University Records may only be stored in approved Cloud Storage as set forth in University Policy 12.9 and published on the OIT website. University provided Network Storage may be used when local or cloud storage cannot meet the department's needs. Records subject to the State of Florida Record Retention Schedule shall not be stored on Google Drive or Google Shared Drive.

B. Storage of Deleted Files or Emails: Email or files deleted from Office 365 Cloud Storage will be configured for seven (7) years of retention from the point of deletion. They may not be recovered after that time. Files located on Network Storage Drives will be configured for five (5) years of retention after deletion. Employees shall not delete files or emails that are subject to lifetime retention requirements as defined in the State of Florida Record Retention Schedule or litigation holds.

C. Storage of University Records upon Separation:

1. Email: Email accounts are disabled for a minimum of thirty (30) days after Separation. A supervisor may be granted access to a separated employees email if approved by Human Resources. Any emails that need to be retained should be removed from the user's account within thirty (30) days after Separation. After thirty (30) days, the account is deleted, and email will only be available in the archive. Email will be retained in the archive for seven (7) years.

2. Individual Cloud Storage: Individual Cloud Storage accounts are disabled for a minimum of thirty (30) days after Separation. Supervisors will receive an email notification within two weeks of the employee's Separation that they have access for thirty (30) days to retrieve any documents needed for operations or for compliance with record retention requirements. Individual Cloud Storage files will be retained in the archive for seven (7) years.

3. Group Cloud Storage: Upon Separation of an employee, supervisors will be sent a report of any Group Cloud Storage managed by that employee to determine if the storage needs to be retained. Managers of Group Cloud Storage that has not been accessed for two (2) years will be sent notifications indicating that the site will be archived if no further action is taken. If the manager has separated from the University, the supervisor of the department where the manager was previously employed will be notified. Group Cloud Storage that is cleared for deletion will be archived for a period of seven (7) years.

4. Network Storage. Supervisors will be given access to a former employee's individual Network Storage drive for (60) days after the date of separation. Sixty (60) days after an employee's separation, the employee's individual Network Storage drive is deleted and may not be recoverable. Backups of individual Network Storage drives will be maintained by OIT for five (5) years post deletion.

V. EMPLOYEE DATA

A. Storage of Employee Data: Employees may store incidental Employee Data on University Storage Platforms; however, employees are responsible for backing up such data, as they deem appropriate, outside of University Storage Systems. The Office of Information Technology (OIT) can provide reasonable assistance with the recovery of lost or damaged files, but recovery is not guaranteed.

B. Storage of Deleted Employee Data or Employee Data after Separation: Employees are solely responsible backing up or transferring any Employee Data off of University Storage Platforms prior to their separation date.

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: _12.15_

Initiating Authority
Signature: _____ Date: _____
Name: _____

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: _____

President
Signature: _____ Date: _____
Name: _____

Executed signature pages are available in the Office of Compliance