

4.2 Cloud, Network, and Local Storage Guidelines

Effective Date: January 28, 2025

Revised Date: February 14, 2025

Purpose

To ensure secure and reliable data management at Arkansas State University, this document outlines guidelines for using cloud storage, network storage (file share), and local storage—focusing primarily on Microsoft OneDrive as the approved platform for storing confidential and internal data.

Scope

These guidelines apply to all A-State employees, faculty, staff, and students who manage, store, or access data using local devices or cloud services.

Definitions

- **Cloud Storage:** Internet-based data storage through a third-party provider, offering flexibility and redundancy.
 - **Network Storage (File Share):** Centralized storage managed by ITS on the A-State network, suitable for department-level sharing and automated report delivery.
 - **Local Storage:** Files stored on personal computers or external devices without backup or redundancy.
-

Guidelines

1. Cloud Storage Overview

Cloud storage provides secure, accessible, and backed-up solutions for storing data.

Benefits of Approved Cloud Storage:

- **Accessibility:** Access files from any internet-connected device.
- **Collaboration:** Real-time sharing and co-editing with colleagues.
- **Security:** Meets A-State security standards.
- **Redundancy:** Protects against local device failure.

2. Storage Type Comparison

Storage Type	Key Characteristics	Recommended Use
Cloud Storage (OneDrive)	Secure, backed-up, accessible	Primary solution for confidential/internal data
Local Storage	Not backed up, at-risk of loss	Not recommended for critical data
Network Storage (File Share)	Centrally managed, backed up	For departmental/shared reports, not collaboration



3. Approved Storage Services

- **Microsoft OneDrive** (*Primary Cloud Solution*)
 - Meets A-State security standards.
 - Default quota provided; email security@astate.edu to request more.
- **Kaltura** (*Multimedia*)
 - Ideal for large media files (e.g., videos).
- **Canvas LMS**
 - Best for academic course content and storage.
- **Dropbox** (*Limited Support*)
 - Requires case-by-case approval. Migration to OneDrive is encouraged.

4. Usage Guidelines

Cloud Storage

- **File Sharing:** Grant access only to necessary individuals. Do not share confidential data externally without approval.
- **Device Sync:** Do not sync confidential data to non-A-State-owned devices.

Local Storage

- Avoid using local devices to store critical or sensitive data. Local data is not backed up and may be lost permanently.

Network Storage

- **Access Control:** Managed by ITS. Access is granted on a need-to-know basis.
- **Use Case:** Ideal for receiving automated reports from systems like Banner or Automic/UC4.
- **Backups:** Regularly backed up by ITS, but not intended for personal or collaborative files.

Roles and Responsibilities

- **ITS Department:** Maintains these guidelines and ensures the use of approved platforms.

- **All Users:** Must adhere to these guidelines to protect university data.
-

Compliance

Misuse of storage solutions or failure to follow these guidelines may result in violations of the **ASU System Appropriate Use Policy** or other applicable regulations. Compliance is monitored by ITS.

Review and Maintenance

These guidelines are reviewed and updated periodically to stay current with technological and legal developments.

Frequently Asked Questions (FAQ)

1. What is cloud storage?

Cloud storage allows you to store files on the internet using services like OneDrive, enabling secure and remote access.

2. Why is cloud storage important?

It ensures data is backed up, secure, and accessible from anywhere.

3. Can I use Google Drive or other unapproved platforms?

No. Storing confidential or internal data on unapproved platforms may result in data breaches.

4. What's the risk of local storage?

Local files are not backed up and can be lost due to hardware failure or theft.

5. Why prefer cloud over network or local storage?

Cloud storage provides automatic backup, remote access, and better collaboration. Network storage is for internal, restricted-access reports—not ideal for collaboration or personal storage.

6. Why avoid local storage?

Local devices are not backed up by ITS. Files may be lost permanently in case of failure or damage.

Version History

- **1.0:** Initial document approved – *January 28, 2025*
- **1.1:** Added network storage guidelines – *February 14, 2025*

Revision #4

Created 2025-06-02 15:31:55 UTC by Josh Breytspraak

Updated 2026-07-28 20:07:11 UTC by Jacob Weaver