Arkansas State University

ITS Cloud, Network, and Local Storage Guidelines

Version 1.1

Effective Date: January 28, 2025
Revised Date: February 14, 2025

1. Purpose

To ensure secure and reliable data management, this document outlines the guidelines for utilizing cloud storage, network storage (file share), and local storage at A-State, with a focus on the use of Microsoft OneDrive as the approved platform for confidential and internal data.

2. Scope

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

3. Definitions

- **Cloud Storage:** Storing data over the internet through a service provider, offering flexibility and redundancy.
- **Network Storage (File Share)**: Data stored on a centralized, approved file share managed by ITS within the A-State network, allowing multiple users to access and share files while maintaining security and backup options.
- **Local Storage:** Data saved directly on a machine or external device without automatic backups.

4. Guidelines

4.1. Cloud Storage Overview

Cloud storage allows data to be stored and accessed over the internet, offering flexibility, security, and redundancy. Using these platforms ensures that sensitive information is stored securely and can be accessed anywhere, anytime, with proper authorization.

4.1.1. Why Use Cloud Storage?

Approved Cloud Storage provides the following benefits:

- **Accessibility:** Access files from any device with an internet connection.
- **Collaboration:** Share documents and collaborate in real-time with colleagues.
- **Security:** Meets A-State's security standards for handling confidential data.
- **Redundancy:** In the event of local hardware failure, data stored in the cloud remains safe.

4.2. Cloud Storage vs. Local Storage vs Network Storage

- **Cloud Storage:** These services provide a secure and backed-up environment. Data stored in the cloud is protected by multiple layers of security and redundancy.
- **Local Storage:** Data saved on a local machine or external device is not backed up by A-State. In the event of hardware failure, this data can be lost permanently. Therefore, local storage should not be used for critical A-State data.
- **Network Storage:** Files stored on A-State's network file shares (SMB) are centrally managed and regularly backed up. This storage option allows secure file sharing within the organization while maintaining access controls and data protection policies. Network storage is recommended for departmental and shared files that require security and redundancy but should not be used for storing personal files or collaborating with colleagues.

4.3. Approved Services

- **Microsoft OneDrive:** The primary, approved cloud storage solution for storing confidential and internal data. OneDrive meets A-State's security standards, ensuring data is protected and accessible from authorized devices
    - Each user is allocated a default storage quota on OneDrive. Users who require additional storage beyond this standard limit can contact security@astate.edu to begin the approval process for an increased storage allowance.
- **Kaltura:** For large media files, such as video, Kaltura is the recommended platform, optimized for high-volume storage and streaming of multimedia content.
- **Canvas LMS:** Canvas offers an integrated solution for storing academic materials, designed specifically for educational content.
- **Dropbox:** Limited support is available for Dropbox, and specific use cases must be reviewed and approved by security@astate.edu prior to Dropbox use. All existing users of Dropbox with institutional accounts should aim to migrate content to OneDrive if feasible.

4.4. Cloud Storage Guidelines

- **Sharing Files:** When sharing files, ensure you only grant access to individuals who need it. Confidential data should not be shared with external parties without prior authorization from relevant authorities.

- **Data Synchronization:** Confidential data must not be synchronized to non-A-State-owned devices. Keep data secure by only accessing it via trusted devices that meet security standards.

4.5. Local Storage Guidelines

- **Avoid Local Storage for Critical Data:** Do not store important or sensitive data on local devices (laptops, desktops) as they are not backed up. In the event of hardware failure, local data may be lost permanently.

4.6. Network Storage (File Share) Guidelines

- **Access Control:** Access to file shares is controlled by ITS, and permissions should adhere to the principle of least privilege where access is only granted to those that need to use this to perform day to day business operations.
- **Intended Use:** File shares should primarily be used a source to receive automated reports from Banner, Automic/UC4, or other A-State platform. These file shares should not be used for personal or collaborative documents.
- **Backup and Storage:** Network file shares are regularly backed up; however, users should avoid storing non-essential or personal files in these locations. Ensure critical files are saved to designated OneDrive storage for data protection.

5. Roles and Responsibilities

- **A-State IT Department:** Responsible for maintaining and updating these guidelines and ensuring that only approved cloud storage platforms are used.
- **All Employees and Students:** Required to follow these guidelines to ensure the security and proper management of A-State's data.

6. Compliance

Compliance will be monitored by the A-State IT department. Unauthorized use of unapproved cloud services or improper handling of confidential data is prohibited. Violations of these guidelines may be a violation of the Appropriate Use of Information & Technology Resources ASU System Policy or other applicable policies.

7. Review and Maintenance

These guidelines will be reviewed as needed to ensure they remain up to date with current technologies and legal requirements.

8. Frequently Asked Questions

8.1. What is cloud storage?

Cloud storage refers to storing data on the internet through a service provider (e.g., Microsoft OneDrive) that manages and secures the data, allowing access from anywhere with an internet connection.

8.2. Why is cloud storage important for A-State?
Cloud storage ensures that data is protected against loss, is accessible remotely, and meets security standards for confidential information.

8.3. What happens if I use an unapproved cloud service?
Using unapproved cloud services such as Google Drive for storing confidential or internal data could potentially lead to a data breach or security incident.

8.4. What are the risks of using local storage?
Local storage is vulnerable to hardware failure. If your machine crashes, data stored locally could be lost forever. Cloud storage provides a backup in case of these incidents.

8.5. Why should I use cloud storage instead of local or network (file share) storage?
Cloud storage ensures your data is backed up and recoverable even in the event of device failure or loss. Local storage (e.g., saving files directly to your computer) does not offer this protection and can result in permanent data loss. Network storage is a viable option for restricted, and limited access data but should primarily be used to store reports generated from institutional systems.

8.6. Why isn't local storage recommended?
Local storage is not backed up by A-State's IT infrastructure. In the event of hardware failure, theft, or corruption, any important files stored locally will be lost without recovery options. Using cloud storage provides redundancy, ensuring your files are safe.

Versioning

1.0 Original Document Approved on 1/28/25

1.1 Inclusion of Network Storage option on 2/14/25