DATA BACKUP AND RECOVERY

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including Highly Sensitive Information protected by law. Maintaining the integrity and availability of this information is an important University function. To this end, Information Security Services deploys a comprehensive framework of *Information Security Standards* of which this document is a part. All members of the University community are required to comply with these requirements. Capitalized terms used herein are defined in the *Information Security* policy or the *Data Classification and Handling* policy. Questions regarding these *Information Security Standards* should be directed to Information Security Services.

This Information Security Standard establishes minimum requirements for the creation and retention of data backups, which are an essential part of disaster recovery and business continuity planning. Clear standards for backing up University Information help to ensure the fast and efficient resumption of business following a system outage or failure. University community members may contact the ITS Solution Center at 928-523-3335 to request data restoration and/or recovery assistance.

1. **File Share Services**. In accordance with the University's *Data Handling Protocols*, all University employees are encouraged to store all University Information they generate or control on University approved network file server drives that are regularly backed up by Information Technology Services or on University approved cloud services such as, but not limited to, Microsoft OneDrive, instead of storing this information locally on desktop, workstation or laptop computers. Storing Sensitive and Highly Sensitive University Information on University approved network file server drives is mandatory.

2. **Backup Regimens**. Effective data backup regimens must be developed and consistently implemented for all network file server drives, database servers, and document management applications.

3. **Backup Types.** Backups shall be designed, implemented and consistently performed in a manner that ensures that operating systems, applications, and University Information is fully recoverable from a system failure. Employ the following types of backup procedures as appropriate as part of a comprehensive computer system backup and disaster recovery strategy:

   3.1. Full. All files and folders selected for the backup are saved

   3.2. Incremental. Only changes made since the last backup are saved

   3.3. Differential. All changes made since the last full backup are saved

   3.4. Virtual Machine Snapshots / Images. An image (replica) of a hard drive's entire contents including the operating system and all application files and data

4. **Backup Frequency**. The frequency of backups shall be determined by the risk associated and the type of backup being performed. Contact Information Security Services for assistance in making these determinations. Suggested backup frequencies are:

   - Hourly
   - Every 4, 8, or 12 hours
   - Daily (once each 24-hour period)
   - Weekly
   - Monthly

The type of backup—full, differential, incremental, or snapshot/image—is an important factor in determining the appropriate backup frequency.

5. **Retention Periods**. The retention period for backups shall be determined by the regulations governing the data. At a minimum, a fourteen (14) day retention period is mandatory. Federal and state regulations, as well as University Records Management Program requirements, must be considered when establishing long-term data backup retention schedules.

6. **Storage**. At least one fully recoverable version of all electronically stored University Information must be secured by physical access controls at a location separate from the University's main secure data center. This second data storage location may be an approved on-campus secure facility or provided by an off-site data storage vendor. All storage locations must be approved by the Chief Information Officer ("CIO"). In some cases, as may be required by law or regulation, backups must be encrypted.

7. **Documentation**.

   7.1. Backup and recovery documentation must include identification of all systems, data, and the procedures for performing backups and recovery. Automated processes and manual steps must be documented, including the tasks necessary for restoration, and be made part of the overall disaster recovery or business continuity plan.

   7.2. All backup and recovery documentation must be reviewed, revised, and updated regularly and as new technology or processes are implemented.

8. **Testing**. Testing of backups and recovery procedures is mandatory. Testing must occur annually at a minimum and should include a review of related documentation and an opportunity to incorporate lessons learned.

9. **Duty to Report**. All University Community Members are obligated to immediately report any IT security threat or suspected or actual release or breach of Sensitive Information**. Dial 928-523-3335 to make a report.** In collaboration with appropriate University stakeholders, Information Security Services is responsible for notifying all affected and responsible parties. The CIO will assemble an incident response team to investigate, preserve evidence, mitigate the situation, and analyze and report on the event. If health or safety may be a concern, the reporting party or Information Security Services shall immediately notify the Northern Arizona University Police Department and any other external entity or governmental agency as appropriate.

10. **Exception Requests**. In the event an information backup regimen cannot be implemented or cannot comply with established standards for an extraordinary reason, an exception request must be made to detail why postponement or deferral is necessary. The CIO must approve all backup-postponement or deferral requests, which must be submitted in writing via the ITS ServiceNow reporting system. Exception requests may be caused by:

    - Production system freeze or change blackout periods preventing the implementation of backups
    - Systems, applications, or devices where alternative backup controls are put in place, documented, and validated