University System of New Hampshire

SHARED ELECTRONIC FILE STORAGE MANAGEMENT STANDARD

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: Designated Reviewers Only
Status: In-Force

1 PURPOSE

This Standard aims to establish procedures and policies for shared electronic file storage management of the University System of New Hampshire's (USNH) information technology resources.

2 SCOPE

This standard applies to all USNH business and academic units and USNH-owned information systems that collect, store, process, share or transmit institutional data. Personally owned devices that connect to the University Campus Network must meet the requirements of the End-Point Management Standard.

3 AUDIENCE

All USNH community members who access USNH information technology resources should be familiar with this Standard

4 STANDARD

4.1 SHARED ELECTRONIC FILE STORAGE - A shared, or network, drive permits centralized network file storage and sharing, which is especially valuable when a project requires collaboration with multiple users, or when a record of institutional value must be accessible to multiple users. This document is intended to offer guidance regarding the value of managing a shared drive and provides best practice techniques for more efficient management of a shared drive.

These guidelines encourage use of shared drives in a manner that will create a navigable drive with appropriate restrictions and offers guidance in the following areas:

- Structuring a shared drive.
- Techniques for efficient management on a shared drive.
- Maintaining continued accessibility of records stored on a shared drive.

Compliance with the recommendations laid out in this document will support more efficient document retrieval, free up network space, mitigate migration costs, and improve the agency's ability to respond to public records and e-discovery requests.

4.2 STRUCTURING SHARED STORAGE

- Shared storage must be navigable by other users, present and future. To encourage continued accessibility of documents stored on the shared drive, structure the folders and sub-folders logically.
- Rely on the structure of the file system to provide context to individual records. The file path need not be apparent in the file title, assuming the file structure is logical.
- Avoid creating hierarchies more than 4-5 folders deep. This will ensure that documents are not lost in a deep folder and keep duplicate documents off the shared storage (leaving more space for everyone).

Deep folder hierarchies also pose challenges when moving content or upgrading a system.

- Decide early on which documents to file by case and which to file by subject. A good rule of thumb is to follow the file plan created for paper records in organizing digital documents.
- File administrative and reference records by subject or function, not by project, as projects do not retain meaning over time.
- If records must be filed by project or case, a good practice is to keep documents in a well-labeled project folder for the project's duration but transfer the final product to the correct topical folder upon project completion. Remove any records with no retention schedule, such as document drafts or outside research, from the shared drive upon project completion or completion of the final copy. However, filing records by subject and function from the beginning is ideal.

4.3 FILE AND FOLDER NAMING CONVENTIONS - Efficient management of electronic records begins with accurate and meaningful file naming. This requires that file names (as well as folder structures) make sense to everyone, not just their creator. A file, folder, or sub-folder name should be:

- Interpretable by others in the department in which the file resides.

- Interpretable by future users of the shared storage.
- Distinguishable from files with similar subjects, and from different versions of the same file.
- Consistent across the department or workgroup, and in compliance with established naming conventions.

Additionally, folder names should not repeat information contained elsewhere. Incorporate the following elements within the file name:

- Title descriptive of the document's content.
- Date of creation or of modification (YYYYMMDD).
- Version number (v1.0, v2.0) o When updating existing documents, use the current version number as a reference for internal changes (e.g., v1 becomes v1.1, v1.2, etc. while being edited internally and v2.0 upon publication).

4.4 SAVING DOCUMENTS CORRECTLY - Employees should save documents to the correct location the first time. This reduces the amount of work involved when identifying records and organizing storage drives later. Each drive has different documents that are appropriate and inappropriate. Employees should not save documents of a personal nature (vacation photos, personal emails, etc.) on any shared storage. These items make it more difficult to find relevant information, create a significant burden for IT systems to back up, and use resources and storage for information that is unrelated to work. Additionally, these items could potentially become subject to a public records request or e-discovery. In addition to saving documents in the correct location the first time, users should avoid placing duplicate documents on a shared storage. When a document is ready for placement on shared storage, place it in the appropriate existing folder or create the requisite folder.

4.5 ACTIVE HOUSEKEEPING - Unless responsibility for a folder has otherwise been delegated, each user of the shared storage is responsible for the folders and documents he or she creates. Users should regularly audit their documents to determine which records to retain and which to delete from the storage. If placing a document on shared storage on a specific drive for someone else to quickly pick up, users should remove those documents immediately after they retrieve them. Managers and IT staff should schedule an annual (or more frequent) cleanup day, to ensure periodic cleansing of unnecessary files and folders. Documents and folders to consider for deletion include:

- Draft versions of finalized documents.
- Documents and folders that no longer serve a purpose after sharing with someone.

- External documentation (e.g., research, downloaded files) after project completion.
- Duplicates and redundant files.
- Documents that no longer have administrative or reference value or which have met their retention requirements.
- Empty folders.

4.6 EMPLOYEE SEPARATION - Each department should have a procedure in place regarding the records of employees who leave or are separated from employment. Best practices call for employees to share files with the supervisor of that position so that the supervisor can determine what to retain. Ideally, supervisors will review employee files and shared drives before an employee leaves and make determinations about the files. To avoid confusion about files, an employee should describe his or her files and folder structure to a supervisor prior to leaving USNH or include a .txt or MS Word document with a detailed description of its organization.

4.7 SECURE ACCESS, SHARING, AND PERMISSIONS - Be cautious when sharing and setting permissions for data stored in the cloud. Limit file sharing to only those with a legitimate need to know for purposes of conducting University business. Share files with specific individuals, never with "everyone" or the "public," unless that is your intention and you have confirmed that the information at issue can be properly shared with the recipients. Avoid sharing files with the default "Anyone with the link can edit" permission, which allows the person you shared that file with to further share the file with anyone for the same level of access. Never use anonymous guest links, especially when sharing confidential or restricted data. Periodically review sharing privileges in your Shared File Electronic Storage Systems i.e. OneDrive/Teams/SharePoint folders. Remove individuals when they no longer need access to your files or folders. Your Desktop/Laptop Computer should not be considered safe or durable storage since the University does NOT back up any of the files stored directly on the drives contained in your desktop computer or laptop. If the drive on your computer crashes, if your machine comes down with a virus, catches ransomware, or if your laptop is lost or stolen, we cannot recover any of the materials you may have stored there.

4.8 SENSITIVE AND CONFIDENTIAL INFORMATION - Keep confidential information off the network storage or, at minimum, place appropriate restrictions on folder access. Records that are subject to confidentiality restrictions include but are not limited to:

- Sensitive information described in the USNH Information Classification Policy.
  Personally identifiable information as defined in G.S. §§132-1.1, 1.2, §125-19, §§126-22, 24, and others.

University System of New Hampshire

- Data protected by state or federal statutory law, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Family Educational Rights and Privacy Act of 1974 (FERPA), the Gramm-Leach-Bliley Act of 1999 (GLB), and G.S. §130A-476.
- Some administrative information related to personnel functions and financial matters.

4.9 EDUCATION AND TRAINING - Employees are responsible for their own records and bear full responsibility for folder system management. It is crucial that they understand their responsibilities as users of the shared storage and custodians of the public record. Lack of knowledge about proper procedures is the main cause of shared storage issues. We strongly encourage departments to train new employees on proper use of shared storage and good file naming conventions. ET&S is a resource if additional training is required.

4.10 REMOVABLE MEDIA GUIDELINES - Removable media is a term that refers to several types of portable devices, including but not limited to USB flash drives, memory cards, external hard drives, and more. The use of removable media is discouraged as their portability introduces additional risk as such devices can easily be lost, stolen, and/or compromised with malicious software.
When alternatives are not feasible, the following apply to minimize the risk to the confidentiality, integrity, and availability of USNH resources:

- Never connect unknown removable media or devices to a USNH computer.
- Never share passwords used for removable media or devices with anyone.
- Never store non-public USNH data on a personal device.
- Any removable media shall be properly encrypted according to USNH-approved encryption technologies.
- Never connect USNH removable media or devices to a personal computer.
- If connecting removable media to a USNH device, anti-virus software shall be used to scan for malware.
- Lost or stolen removable media containing sensitive, protected, or restricted data shall be reported immediately to the designated authority for each department or institution.

University System of New Hampshire

5 MAINTENANCE OF PROCESSES AND PROCEDURES RELATED TO THIS STANDARD

As part of the mandatory annual review of this Standard required by the *USNH Cybersecurity Policy*, the processes and procedures that support the requirements defined in this Standard shall be reviewed and, where needed, updated to ensure currency and continuous improvement.

6 ENFORCEMENT

Failure to comply with this Policy puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., student conduct and/or applicable personnel policies).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

7 DEFINITIONS

- File Storage
- Naming Convention

8 RELATED POLICIES AND STANDARDS

University System of New Hampshire Cybersecurity Policy

University System of New Hampshire Acceptable Use Policy

Endpoint Management Standard

Network Security Standard

University System of New Hampshire

CONTACT INFORMATION

For USNH community members: Questions about this Standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, and Compliance (GRC) via this Support Form.

All other requests can be submitted here: Submit an IT Question.

DOCUMENT HISTORY

Effective Date:	April 16, 2023
Approved by:	Dr David A Yasenchock, Interim CISO
Reviewed by:	Dr David A Yasenchock, Director, Cybersecurity GRC
Revision History:	V 1.1