Guidance on Network-Attached Storage (NAS) Usage

Faculty of Medicine – Deputy CIO Medicine

What is Network-Attached Storage?

A Network-Attached Storage (NAS) device is a dedicated file storage system with the ability to store files for users on a network. It allows multiple users and devices to retrieve and store data from a centralized location.

Use of NAS Devices

The Faculty of Medicine (FoM) Deputy CIO Medicine (DCIO-M) advises against the use of self-managed NAS devices due to the security risks they pose to UBC's network and concerns regarding the safety and classification of stored data. Usage guidelines:

- NAS devices must not be used to store student or administrative data, which are governed and owned by UBC.
- Use of NAS should be limited to research-related data, particularly large experimental, scientific, or archival datasets, where a Principal Investigator is ultimately responsible for the data.

UBC Storage Solutions

UBC provides centrally managed file storage solutions that:

- Meet institutional security and privacy requirements across all data classification levels.
- Include physical security, resiliency, and backup capabilities.
- Are supported and maintained by central IT.

Recommended services include:

- TeamShare: https://it.ubc.ca/services/web-servers-storage/teamshare-storage-service
- OneDrive: http://it.ubc.ca/services/web-servers-storage/microsoft-onedrive
- ARC Compute & Storage: https://arc.ubc.ca/compute-storage

If the recommended storage options do not meet your unit's needs, please contact DCIO-M at dcio.medicine@ubc.ca to discuss alternatives.

Acceptable Use & General Requirements

Units within FoM considering NAS solutions should first assess whether UBC's institutional storage offerings meet their needs more securely and cost-effectively. If a standalone NAS is still justified:

- Approval must be obtained from the Administrative Head of Unit in consultation with DCIO-M
- The device must be tagged and registered with DCIO-M for asset tracking.
- The intended use and data classification must be documented.
- The NAS must meet the minimum-security requirements outlined below.

Data Classification and Storage Requirements

Self-managed NAS devices are not permitted to store personal health information (PHI). UBC-approved storage solutions must be used for PHI and similarly sensitive data.

Data Type	Storage on NAS	Requirements
Low-Risk Published manuscripts / Public	Case-by-case. Requires additional approvals	Consult DCIOM for review
Medium-Risk Non-personal but proprietary research data	Case-by-case. Requires additional approvals	Consult DCIOM for review
High-Risk Personal information / De-identified human datasets (non-health)	Case-by-case. Requires additional approvals	Must meet ethics board and security standards
Very High-Risk PHI / Biometric data / Identifiable human genetic data / Biospecimens	🚫 Not allowed	Use UBC-approved infrastructure only

Minimum Security Requirements

NAS devices must meet these security requirements to align with UBC's Information Security Standards (ISS).

- Support AES-256 encryption at the volume level to protect data at rest. [U5]
- Use secure transfer protocols: SMB3, HTTPS, SFTP, or TLS 1.2+ for data in transit. [U3, M10]
- Support individual admin and user accounts; shared accounts are prohibited. Integration with enterprise directory services (e.g., UBC LDAP or Active Directory) is recommended. [M2, M3]
- Disable local admin accounts where possible. If required, rename them, use unique credentials, and comply with UBC's password and privileged account management policies. [U2, M3]
- Enable logging of user logins, file access, and administrative actions. These logs must be retained for at least 90 days. [M8]
- Must not be directly accessible from the internet. All remote access should be routed through internal networks via VPN. The administrative interface must be segregated from general user access and only available to authorized IT staff through a UBC VPN. [M10, U6]
- Must actively receive regular vendor firmware and security updates. [M5]
- Must allow you to disable insecure protocols like Telnet, FTP, or SMBv1. [M10]
- Uninstall or disable unnecessary third-party apps or features bundled with the NAS software to reduce risk. [M5]
- Must be in a locked, access-controlled room or data center, not physically accessible in open offices or shared lab spaces. [U7, M9]

NAS Device Approval and Pre-Purchase Security Review

Individuals wishing to use a NAS device must contact DCIO-M at dcio.medicine@ubc.ca prior to purchase to review and confirm that the device meets the required security standards.