Weill Cornell Medicine

Service Policy

Devices: Network-Attached Storage

Responsible Executive: Chief Information Officer, WCM
Original Issued: July 20, 2017
Last Updated: July 20, 2017

Contents

1. What are network-attached storage devices? 2
2. NAS vs. ITS File Sharing Storage 2
3. Use of NAS Devices 2
   3.01 Minimum Security Requirements 2
4. Supported Models 2
5. Procedures 3

1. What are network-attached storage devices?

A network-attached storage device, or NAS, is a standalone server with the ability to store files for users on a network.

2. NAS vs. ITS File Sharing Storage

ITS provides several sustainable and scalable digital storage solutions for WCM users. ITS storage solutions are centrally managed, meet security and privacy requirements permitting the storage of high risk data, and account for physical security, resiliency, and offsite backup. For additional information about ITS storage solutions, please visit the ITS website at http://its.weill.cornell.edu/services/storage-servers/file-sharing.

3. Use of NAS Devices

NAS devices managed individually and not stored within a WCM data center introduce added security risk. WCM is responsible for maintaining an asset inventory of WCM data. Departments who wish to use a NAS device must have the device "tagged" by ITS for asset tracking. The use and intent of the NAS device, including the type of data it will store, must be documented. Furthermore, the NAS device must meet the minimum security requirements in the section below.

NAS devices are not permitted to store protected health information as they do not offer offsite data backups to meet HIPAA requirements. ITS storage solutions must be used instead.

3.01 Minimum Security Requirements

NAS devices must meet the following minimum security requirements:

- Event logs must be enabled on the device to capture such events when users are accessing the system, modifying files, or transferring data
- Event logs must be available to ITS in the case of incident response activities and should be forwarded to the ITS security and event information management system
- Embedded, enabled, and updated antivirus software
- Configured with centralized authentication against ITS directories, such as Active Directory or LDAP
- Any local accounts used to manage the system should be disabled; if absolutely necessary, default passwords must be changed to meet ITS policy 11.15 – Password Policy & Guidelines
- Unnecessary, insecure, or legacy services must be disabled, such as telnet, FTP, SMBv1, etc.
- Direct remote access to the NAS device (or any web interface to manage the device) must be disabled as WCM's existing remote access services should be utilized instead
- Encryption (full disk or file and folder) should be enabled across all storage drives and exceptions should follow the existing process defined in ITS policy 11.06 - Device Encryption
- Disable or uninstall any unnecessary third-party applications offered with the NAS device software
- Install security updates released by the vendor upon release
- Physically secure the NAS device to reduce the risk of theft, including the theft of individual hard drives

ITS will regularly review NAS device configurations to ensure they continue to meet the above requirements.

4. Supported Models

ITS has reviewed various NAS devices. Many Synology and QNAP devices are capable of supporting the above security requirements (with added configuration). For some sample devices, please reference the models below:

- Synology DiskStation DS216, DiskStation DS416
- QNAP TS-251, TS-431

5. Procedures

Individuals wishing to utilize a NAS device should contact their ITS departmental liaison prior to purchase to ensure the device will meet the above security requirements. ITS Security will review and evaluate these requests.