Hosting A&S NAS copy

A&S provides central file storage for admin and teaching purposes. To improve robustness, ChemIT is pleased to host a copy in our server room.

See also

- Chemistry IT and Arts & Sciences IT

Getting the A&S NAS into Baker

Topic	Comments
Timing? Process?	When start? How long? What staffing required?
Rack space for server and UPS	Ensure adequacy.
Networking	VLAN across buildings? Compliance, relative to expected data on server? If expect "Confidential (Level 1) Information" on server (really?!), see below. Thanks!
Cooling	Anything special?
Physical security, including room access	Room access: No logging, currently. Access by student employees, custodial & facilities staff. Compliance, relative to expected data on server? If expect "Confidential (Level 1) Information" on server (really?!), see below. Thanks!
Hardware and software maintenance	If physical access required, coordinate with ChemIT? Or, provision independent physical access by A&S IT staff? (If that choice, is that OK with CCB researchers?) Using DRAC management? If so, show-and-tell to ChemIT staff? :-)

Confidential (Level 1) Information

Hopefully there will not be any "Confidential (Level 1) Information", as defined by University Policy 5.10, Information Security. (See in particular sections starting at p21.)

NOTE: ChemIT's server room (248 Baker Lab) has no "Confidential (Level 1) Information". Thus, we do not invest or follow the procedure, "Entry must be logged and the logs retained for at least five days."

- We also don't control full access. In addition to ChemIT staff (including student employess), the room can also be independently accessed by custodial staff, water chill repair folks, facilities staff, etc.. They often access the room without our specific knowledge.
- Get a card-access lock instead? AP nearby. CCB just did one nearby, so should be able to easily get accurate cost-estimate. (Notebook logging of in's not an attractive option, but suppose it's an option. Does anything, really?)
- If it helps, there are some extracts from the pertinent policy, below.

Extracts from "University Policy 5.10, Information Security" PDF document, section "PROCEDURES, ITHACA CAMPUS UNITS — IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL1) INFORMATION":

Systems Subject to These Requirements

Thus, for example, a Windows system where the primary user's domain password is sufficient to mount a file server volume and access directories with confidential (Level 1) information would need to be secured as if such information was stored locally.

Confidential (Level 1) Information: Requirements Specific to Application and File Servers

1. All application servers and file servers must be housed in a physically secure computer room or data center. **Entry must be logged and the logs retained for at least five days**.

Suggestion: Where feasible, log exits as well.

* Note: Video monitoring is an acceptable solution to this requirement.

* Note: **Visitors are not permitted except under escort**.

* An individual's access to a store of confidential (level 1) information should be via an account assigned for the sole use of that individual. This requirement is not to be interpreted as disallowing access to an encrypted dataset via a shared encryption key.

2. Confidential (level 1) information should be removed from file servers when it is no longer needed on an operational basis. To the extent feasible, this also applies to confidential (level 1) information stored in databases and other application frameworks.

*Suggestion : Use dual-factor authentication for root/administrator access to these systems. (When campus-wide mechanisms are in place for dual-factor authentication on all standard platforms, this will become a requirement.)