In keeping with existing UNH and USNH policies it is the duty of the server administrator to maintain their server in a secure fashion. Maintaining each part of the network environment is a crucial step toward the goal of keeping that environment healthy and as secure as possible.

As server administrators you are charged with safeguarding: 1) the server you manage; 2) the data that the server stores; 3) the users of your server; and 4) the network that your server shares.

The first question you need to ask yourself is, do you need to build your own server? Might you be able to provide the services you need through a centralized or contracted service? If so, consider whether or not that might be a better long-term direction for you and your group. Even beyond offloading the day-to-day maintenance issues, you may be able to get help with the legal aspects of data management if you are not managing the server yourself.

The Checklist

Below is a simple check-list of areas that you should consider while building and maintaining a server. This guide will assist you in maintaining not just the 'drivers and wires' portion of server management, but also administering to the population that accesses the server(s) you are responsible for.

- Proper configuration on the base operating system.
- Regular updating/patching of operating system and network accessing applications.
- Installation and maintenance of viable protective software.
- Proper over-sight of user accounts.
- Compliance with all applicable regulations regarding the data stored on, or transmitted through, the server.
- Data Protection
- Regular Log Review
- Proper care taken to the physical security and access of the server.

Section I - The Operating System
Most server operating systems have some form of auto-configuration utility available. Bastille is available for Linux, Windows 2003 has the Server Configuration Wizard. But beyond using canned tools, you should research hardening your operating system.

Make sure you are not running services that you do not need to run.

**Section II - Updating and Patching**

Most operating systems allow for some form of automating patching, some allow for automated downloading of patches for your review before installation. Make best use of patch notification and/or automation as it pertains to your server.

Application patching can be a much trickier task, as many do not have automated patching or notification. It is essential that the server administrator regularly check for updates to any software which accesses remotely stored resources, or provides remote users access to locally stored resources.


**Section III - Protective Software**

All common operating systems offer some form of protective software. Anti-Virus is available for any platform, as well as host-based intrusion detection, anti-spyware, file integrity scanners, host based firewalls, etc. Considering your options and using the appropriate measures can go a long way toward protecting your system. Many people are wary of the overhead of always-on protections like anti-virus, but consider that most packages can be configured to only monitor segments of a drive and can also be regularly scheduled. Impact for most measures can be mitigated, at least to a degree.

**Anti-Virus:**
Most operating systems offer some form of anti-virus software. UNH has licensed software for some operating systems. You can read more at [http://www.virus.unh.edu](http://www.virus.unh.edu).

**Anti-Spyware:**
There are a variety of tools on the market, Microsoft does make their own (Windows Defender) but using more than one, especially if used for periodic scans, is a good way to go.

**Host-Based Firewalls:**
Most operating systems come with some form of host based firewall build into the operating system. Linux has IPChains for example.
File Integrity Scanners:  
(AIDE or Tripwire, are examples)

Host-Based Intrusion Detection:  
Samhain is a popular and well regarded deployment.

Section IV - User Accounts

Because user accounts can be abused and forced, it is necessary to put protections in place to protect the accounts that allow legitimate access to the system. The following are areas to consider when addressing account security

- Password Policies  
  - enforce complex passwords  
  - enforce password life-times.
- Change default account names
- Change default passwords
- Disable unused accounts
- Appropriate access (Give users the access they actually need.)

Section V - Physical Security

When thinking about a server’s physical security there are two main areas to consider.

1. Is the server physically safe in its environment?  
   - Does the server have regulated power? (UPS)  
   - Is the server in danger if there is a fire, flood, etc.?  
   - Is the environment around the server ‘healthy’?  
     - Does it have air-flow?  
     - Is it reasonably free of dust?
2. Is access to the server itself restricted?

Section VI - Data Protection

In a server environment, protecting your data is what most of the previous steps are about. A few additional things to consider though:

- Do you backup regularly?
Service level agreements are available for backups. See http://cis.unh.edu/index.cfm?id=0D95C5C4-C712-5636-C6F2C921D67DD60E for more information.

- Where are your backups stored?
  - Are you storing your backups in a different location that the server?
  - Are those backups in a secure location?
- Do you have a data retention policy?
  - State laws make it extremely important that you have and follow a retention policy for data.

Section VII - Log Review

Regular review of server logs is a critical part of administration. Logs will, many times, provide early signs of problems. Both security problems and technology problems can be often be dealt with before excessive damage is done by make a practice of regular review.

Section VIII - Regulatory Compliance

The University holds a good deal of data that is covered by any number of State and Federal regulations. FERPA, HIPAA, Gramm-Leach-Bliley, etc. Be certain your data handling is in compliance with these regulations.

See UNH and USNH policies

- USNH Security Policy (http://usnholpm.unh.edu/USY/VI.Prop/)
- UNH Acceptable Use (as detailed by the USNH OLPM) (http://usnholpm.unh.edu/UNH/VI.Prop/F.htm)

See other sites regarding securing your serve

- Microsoft Security Central (http://www.microsoft.com/security/default.mspx)
- Cert’s TechTips (http://www.cert.org/tech_tips/)
- SANS Institute (http://www.sans.org/)

Approved for posting as draft 10-16-2007 by CIS IT Security Committee