Good Practices for Network Printers and Copiers
5/10/2010

In accordance with USNH and UNH IT policy, all network devices must be maintained in a manner which insures the protection of the device, the data that is handled by the device and the UNH network. UNH IT recommends the following practices for protecting network printers and copiers. When a network printer or copier is installed, the administrator should insure that the installer or provider has identified all default settings – including, but not limited to recommendations 1 through13 of this list - that should be reviewed or changed by the administrator to achieve appropriate data security. Administrators should also check the manufacturers instructions and/or website for additional information on protection options for specific models.

1. Enable Administrative Password
2. Change all default passwords
3. All passwords must meet USNH strong passwords standards
4. Disable DHCP
5. Disable unused protocols, including IPv6
6. Disable unused services, including FTP and Telnet
7. Disable unused ports
8. Change default names, such as SNMP community names. Utilize naming conventions that cannot be easily guessed by an attacker
9. Turn off SNMP if it is not SNMP Version 3 or higher
10. Disable incoming SNMP traffic by default
11. If device stores data, it must not be readable by any other device. Alternatively, enable encryption on the device
12. Enable automatic overwrite of data to protect legally protected information
13. If remote configuration and support is to be utilized, utilize secure protocols (https and SSL) over port 443
14. Register the device with static IP address and subject to security scans. Request a security scan when device is installed.
15. The firmware must never be more than two revisions old.
16. Prevent inappropriate access: use access list or restrict to local IP addresses
17. Access controls are to be IP filtered, MAC filtered or through the use of network print servers
18. Maintain current patch levels for security standards and anti-virus for the operating system
19. Wipe all data storing media before device removal or transfer
20. Defeat malicious scans and attacks: enable device based firewall if available and shut down the device when not in use such as after hours, weekends and holidays
21. Report security breaches: see http://it.unh.edu/itsecurity for reporting requirements, including State of NH Data Breach requirements, and contact information