NDUS Server Information Technology Security Procedures

For purposes of these Procedures a server is defined as any device that provides computing service to multiple computers or individuals.

Systems administrators shall configure their servers based on the assumption that the network they are connected to is insecure. All unused services shall be disabled. Any access to a server other than a "public" server (i.e. public web server) shall be authenticated and access permissions based on minimal need. File access permissions shall be set to restrict access to confidential or sensitive data to authorized personnel only.

When an individual who has been granted special physical or electronic access changes responsibilities or leaves employment, all access rights must be re-evaluated and revised or revoked if not needed.

Server administrators shall regularly check for new services installed that allow access from the network (i.e., normal UNIX user installs apache Web server on port 40404).

Software with security vulnerabilities should be patched in a timely manner. In situations where an identified vulnerability cannot be quickly patched, action such as increased monitoring or further restricting access to the affected application will be taken. System administrators should monitor vulnerability notifications relevant to their platform(s) and application(s).

Servers that have been compromised shall be disconnected, fixed and documented prior to reconnecting to the network.

Remote access to the server for server administrators should be restricted to only those clients who need it using a software firewall or VPN or similar method. User remote access will be authenticated and may be further restricted based on the function of the server.

If the server only needs access to the internal network, external access shall be filtered (i.e., dedicated DHCP server, an internal Web server).

System administrators will respect the presumed confidentiality of all data, looking at it only when given permission or where required to maintain the proper functioning of the server. The use of scanners or monitors is prohibited without the explicit permission of the campus ITSO or the NDUS ITSO.

Any exchange of authentication information between the client and the server shall be done over an encrypted connection. Any connection that has the potential to transmit confidential or sensitive data shall be encrypted. Sensitive or confidential data such as student records shall be encrypted to ensure data confidentiality and integrity when transmitted over a network.

Servers shall be configured to log any activity relevant to the purpose of the server as well as any security related events. Such logs shall be retained for a minimum of 30 days. Access log backups will be kept for a minimum of 30 days. Servers' clocks shall be synchronized with Universal time servers to ensure the usefulness of timestamps in log files.

Data shall be protected against disaster by making regular backups. A second set of backups for mission critical data should be maintained off-site in a secured protected area.

Data shall be properly scrubbed from any server hardware and media before being surplussed or scrapped to prevent the unintended release of data.

Security incidents will be reported to the appropriate officials, including the local campus ITSO. End users will be notified in the event that a security incident results in the disclosure or possible disclosure of confidential data.

All servers will be registered with the campus IT department.

4/25/05