NDUS Network Information Technology Security Standards

Physical access to wiring closet should be restricted to only those staff members who have been determined to need access. Network equipment residing in an area not restricted to networking personnel should be further protected from intentional or accidental access.

Access to network resources should be authenticated and users should be accounted for with appropriate timestamps and IP addresses. Network access logs of users should be retained for no less than 30 days. Firewalls and or access control lists should be used when appropriate, to protect network resources and minimize propagation of viruses and worms.

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

Clocks within all networking devices such as routers and switches should be synchronized with the Universal time servers to ensure the usefulness of timestamps in log files.

Network equipment should be kept current with the manufacturer's firmware and OS patches where possible. All network equipment with remote management capabilities should be password protected and administered over a secure network (e.g. VPN, SSH, or separate VLAN).

Wireless networks should be implemented with a proper site survey to minimize the ability for unauthorized users to connect to the network. Wireless networks should be engineered in such a way as to limit signal propagation to only those areas where coverage is needed.

Network administrators will monitor vulnerability notifications relevant to their devices. Critical networks should be monitored for security violations using intrusion detection and/or other methods. Networks should be proactively scanned by networking staff to identify vulnerabilities of network devices.

Sensitive data such as student records should be encrypted to ensure data confidentiality and integrity when transmitted over a network.

Under no circumstances may an external network be interconnected to act as a gateway to the campus network without coordination and explicit approval from the campus IT department.

Security incidents will be reported to the appropriate officials, including the local campus ITSO.

4/25/05