NDUS Physical Information Technology Security Standards

Installations with computer and networking resources will implement reasonable security measures to protect the resources against natural disasters, environmental threats, accidents and deliberate attempts to damage the systems.

The networking services and computer operations personnel are responsible for providing adequate disaster recovery plans and procedures for critical systems under their responsibility in the event of a natural or man made disaster.

Access to the networking services areas and computer operations areas are to be restricted only to those responsible for the operation and maintenance of the equipment. No individuals will be allowed in the networking services areas and the computer operations areas unless they are under close supervision of an employee of that area.

Measures shall be taken to ensure that unauthorized individuals can not easily access the server or networking areas. Doors and windows shall be locked at all times and any windows should be of shatterproof glass. Any external crawlspaces should be blocked or alarmed.

During non-business hours, the networking services areas and computer operations areas shall be secured.

Physical access to any peripherals (e.g. storage equipment) or media (e.g. backup tapes) that may contain data or access credentials shall be restricted to only those staff members who have been determined to need access.

Electronic access cards and/or keys are to remain in the possession of the person they are assigned to until such time as the person terminates or is terminated from their position.

Staff who (voluntarily) terminate their employment must return their electronic access cards or keys at the time of their termination or reassignment.

Staff who are (involuntarily) terminated must surrender their electronic access cards or keys at the time they are notified of their dismissal; if the staff member refuses to comply, or the supervisor has failed to collect these items, the electronic access cards are to be canceled immediately and the locks requiring keys are to be re-keyed.

Public computing areas must be protected from theft and vandalism and should be monitored.