NDSU Policy 710 Computer and Electronic Communication Facilities
Standards and Procedures

The following standards are required for all computers (servers and desktops).

General Standards
- All servers must be compliant with NDSU Policy 710, Computer and Electronic Communication Facilities.
- All servers must be registered with NDSU IT Division (NDUS Policy 1901.2., section 3.4, “Any device configured as a server must be registered with the campus IT department.”)
  - Servers can be registered via an online process. Click on link below to register a server.
  - https://secure.ndus.nodak.edu/resource/log_in.cgi
- All servers must have a static IP. Static IP addresses can be requested through Network Services. Please contact Valerie Nordsletten at 231-8153l, e-mail: Valerie.Nordsletten@ndsu.edu. Note: prior to obtaining a static IP address, the server must be audited by NDSU IT security and approved by the Vice President for Information Technology.
- Device registration: Any desktop computer and any network addressable device that connects to a campus network should be approved by and registered with the campus IT department. Colleges and departments must maintain a current inventory of all desktops and servers. At minimum, the inventory should contain the NDSU inventory number, the computer’s serial number, software and OEM license numbers of software preloaded through manufacturer, the location, and who the computer is assigned to. (NDUS 1901.2, sections 3.5.6, and 5.1.1)
- Colleges and department shall develop, test, and maintain a disaster recovery and business continuity plan. (NDUS 1901.2, section 1901.2, section 5.1)
- Colleges and departments shall maintain backup and restore procedures. (NDUS 1901.2, section 5.5)
  - Run regular scheduled backups of data. Backups should be stored off-site.
  - Backup and restore procedures should be tested on a regular basis.
  - If your department lacks this capability, ITS can provide these services. Please contact Marc Wallman, Marc.Wallman@ndsu.edu for more information

Data Security Standards
- Colleges and departments must determine and classify types of data stored on servers and desktops. (NDUS 1901.2, sections 3.1.1, 5.7, 5.11, and NDUS 1901.2 Data Classification and Information Security Standard)
- All servers and desktops containing sensitive or confidential data must have methods installed and enabled to protect data. (NDUS 1901.2, sections 2.1-2, 3.3, 3.1.1-2, 3.5.1, 4.1 and 4.3)
- Access should be given only to those who require access to such data. That access should be only what is necessary (e.g., read, write, modify, etc.) (NDUS 1901.2, section 3.5)
- It is recommended that confidentiality agreements be signed and secured from users accessing data which needs to be protected from unauthorized access. An example of a confidentiality agreement can be found here.
Physical Security Standards

- College and department servers must be located in a secure area with up-to-date documentation of who has access. (NDUS 1901.2, section 5.1.1 and the “NDUS Physical Information Technology Security Standards”)
  - Area should be one which is not public and only accessible by those who require access. Doors and windows must be locked when not in use. A log of who has keys to the area must be maintained. Keys must be collected from those who no longer need access to the area.
  - Servers should be located in a climate controlled environment.
  - Use of a UPS (Uninterruptable Power Supply) is recommended. It should have line conditioning for electrical and network cabling.
  - It is recommended that servers are cabled and locked to an immovable surface or stored in a cage that is locked.
  - If desktops are located in a public area, they must be cabled and locked to an immovable surface.
  - Fire suppression services must be available (fire extinguishers).

Logical Security Standards

- Operating systems and applications must be current with all service packs and patches. (NDUS 1901.2, section 3.4 and the “NDUS Server Information Technology Security Standard”)
- Anti-virus software must be installed and current with all recent signatures. (NDUS 1901.2, sections 3.4 and 5.9)
- Install and enable a firewall. (NDUS 1901.2, section 3.4)
  - Configure to allow only necessary/required traffic.
  - Review logs regularly for inappropriate or unneeded access
  - Logs must be kept a minimum of thirty days.
- Review the purpose of the server/desktop to only allow services, applications, and access as they pertain to the purpose. For example: If being used as a Web server, data, or data bases should not be maintained on the same machine. (NDUS 1901.2, section 3.4 and the “NDUS Server Information Technology Security Standard”)
- Run only the services needed on the server. (NDUS 1901.2, sections 3.4, 5.1.2, and the “NDUS Server Information Technology Security Standard”)
  - The services must be related to the role it is serving.
  - Install only software and applications that are needed for the purpose of the machine.
  - Use SFTP (Secure File Transfer Protocol) or SSH (Secure Shell) protocols.
  - Disable Telnet and FTP (File Transfer Protocol) protocols.
  - Disable all services that will not be used.
- Configure all services to log all connections and authentication information. (NDUS 1901.2, sections 3.4, and 5.1.2, and the “NDUS Server Information Technology Security Standard”)
  - Assign appropriate person to review logs and report any unusual activity.
  - Logs must be kept for a minimum period of thirty days.

User Account Standards (NDUS 1901. sections 3.4 and 3.5)

- A unique login and password must be created for each user.
- Password standards must conform to NDSU and NDUS policies and procedures.
  - NDUS password standards can be found here.
  - NDSU password standards can be found here.
The administrator/root account must be renamed and strong password created. Only the individual managing the server should have access to the administrator account.

It is recommended the server is not run in administrator mode. Administrator mode should be used only when necessary.

Force new users to change their password when they first login in.

The guest account must be deleted or renamed and a strong password set.

Disable or delete old accounts/logins that belong to those who no longer need access.
  - For those who are terminated either voluntarily or willfully, the accounts must be locked or deleted.

If account is a shared account, the password must be changed each time someone is added or leaves the group. Password should be changed on a regular basis for these accounts.

Reassignment/Surplus of Electronic Equipment (NDUS 1901, NDUS Server Information Technology Security Standard, and NDUS 1901.2 Data Classification and Information Security Standard)

- Colleges and departments shall use a secure deletion program that conforms to DOD (Dept. of Defense) standards to erase data from hard disks and media prior to reassignment, surplus, or disposal.
- Colleges and departments shall maintain changes to inventory.
- Operating system and any application software that was initially shipped with computer must be reassigned with computer.

Failure to follow established security standards can result in sanctions. (NDUS 1901.2, section 6)

For more information, please contact:

Theresa Semmens, NDSU IT Security Officer
Phone: 231-5870
Theresa.Semmens@ndsu.edu

Galen Mayfield
Executive Director of Enterprise Systems and Enterprise Application
Phone: 231-5843
Galen.Mayfield@ndsu.edu