



Protection of Data and Electronic Resources

Laws and Regulations

Privacy Laws – Geared towards protecting the individual

- FERPA – student privacy and protection of information
- GLBA – personal financial information
- HIPAA – personal identifiable health information

<http://www.ag.ndsu.nodak.edu/agcomm/accs/support/conference/laws.htm>

ND Open Records Law

Public Records – Files and Folders stored on state owned electronic resources that are not classified as confidential or sensitive in nature

Confidential Data

- Information that is not to be publicly disclosed
- The recipients or “keepers” of confidential information have a responsibility not to reveal the contents to another individual/group unless there is a valid “need to know”
- Confidential information must not be copied without authorization from the identified owner

Examples of Confidential Data

Student Records

Grades, disciplinary action, demographic information

Personnel Records

Demographic information, health information

Intellectual Information

Research, copyright protected property, contracts, etc.

Financial Records

Best Practice

- Consider all data entered into the State network as confidential and/or sensitive
- Only share confidential information with those who have a need to know

Best Practices

- Never leave your computer turned on and unattended. If you need to leave your computer, be sure to log off your computer or lock your desktop
- Use a password protected screensaver
- Log off or turn your computer off when you are done for the day

Common Sense Security

Vaccinating your computer...

- Operating system updated
- Office suite software current
- Use antivirus protection (McAfee)
- Use adware protection (Spybot S&D)

Common Sense Security

Use due diligence -

Confidentiality – Data is protected

Integrity - Data is complete, true

Availability – Those who have a need to know have access to the data

Bandwidth/downloading files – Using excess bandwidth is considered a violation of NDUS policy – excessive waste of resources

Security Standards

- Only authorized personnel/students and equipment allowed on the network.
- Authentication and Authorization
 - Login and password for users
 - Devices registered and identified

Software Installation

- Approved by administration?
- Administration – Software Inventory
- Downloaded from the Internet?
 - Safety precautions taken?
- Read the EULA
- One license per machine
 - Do not “share”

Strong Passwords

- Should be a combination of alpha, numeric, capital and lower case letters and special characters (*!@^)
- Should be at least 8-12 characters long
- Changed on a regular basis

Example: MC*sJ12-34

Translation: My cat is Jasper

Show your backside!



Computers in public areas

- Should not have access to confidential/sensitive data.
- Should require only authorized user access.
- Access to data restricted only to what is necessary.
- Should be secured to solid surface with lock and cable.

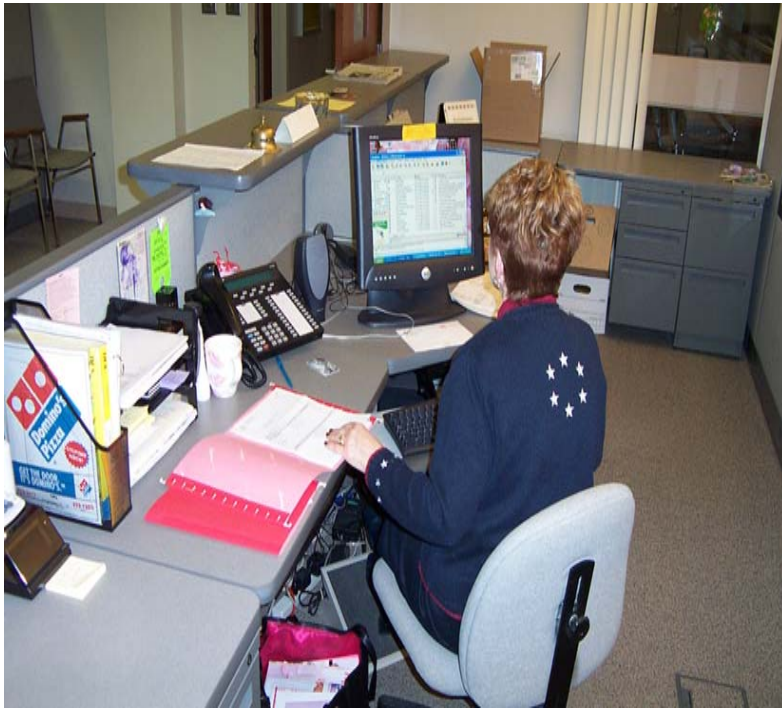
Paper security in the work area



Files stored in locked cabinets



Working Files



- Use file or binder for protection.
- If file is not in use, it should be covered or stored away.
- Time Slips – keep out of sight.
- Paycheck stubs – should be behind the counter or in possession of designated person.

Computer Backup & Restore Procedures

- Regular scheduled backups of all electronically stored documents
- Rule of thumb: Six weeks of backups maintained and rotated
- Restore procedures for “lost” documents need to be tested periodically

Laptops

- Maintain copies of important data somewhere other than the laptop. You might consider using an external portable storage device.
- Be sure to back up all data, and make use of encryption features when you do so.
- Use a locking cable to secure your laptop to your desk or workstation.

Wireless Security

- Use a VPN or similar security to transmit data.
- Use encryption for confidential information.

Removable Media

- When not in use, keep in safe place.
- Dispose of properly.
- Encrypt sensitive data.
- Share only with those who have a “need to know”.

Surplus & Disposal

- Surplus/reallocation
 - Wipe down hard drive with DOD program
- Disposal (environmental standards apply here)
 - Incinerate
 - Smash!
- <http://www.state.nd.us/csd/surplus/computer.htm>

Acceptable Computer Use Policies

Acceptable Computer Use Policies to become familiar with:

- North Dakota University System Computer Use Policy 1901.2

http://www.ndus.nodak.edu/policies_procedures/ndus_policies

- NDSU 710: Computer and Electronic Communication Facilities
- NDSU Student Code of Behavior

If you have questions, contact:

NDSU IT Security Officer:

Theresa Semmens

IACC Building, Room 210A

231-5870

Theresa.Semmens@ndsu.edu

This is reality:

Bad things are out there, disguised as good things...and we must use our computers safely and wisely.

www.ircbeginner.com/opvinfo/trojan-virus.html