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

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 NDSU 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

Keep operating system updated – Use automatic updates – restart your computer when asked to after updates have been installed

Use antivirus protection (Worms, Trojans, Viruses)

Install and enable adware prevention software
Common Sense Security

Use due diligence – Follow standards and guidelines as outlined by current NDUS/NDSU policies and procedures

Bandwidth/downloading copyright protected files:
Using excessive resources and downloading copyright protected materials is against NDUS/NDSU policy and procedure

Viewing unacceptable content, violating laws and regulations, using the computer to harass, stalk, or create harm, or use for unlawful purposes is a violation of NDUS/NDSU policy and procedure and can be a basis for a criminal complaint if in violation of state and federal laws.
Software Installation

- Must be approved by administration and placed into inventory
- Software downloaded from the Internet
  - Safety precautions taken?
- Read the EULA – Know what the terms are
- Rule of Thumb: One piece of software = One license per machine
  
  Do not “share” with others
Best Practices

• Computer must be protected with login and password
• If you need to leave your computer, be sure to log off your computer or lock your desktop.
• Use a screensaver with a password.
• Log off or turn your computer off when you are done for the day.
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!
Guests should not be able to see data on computer screen
Computers in public areas

• Must not have access to confidential and/or sensitive data.
• Must require authorized user access.
• Access to data restricted only to what is necessary.
• Should be secured to a solid surface with lock and cable.
Paper security in the work area
Confidential data is covered when not used
Confidential Files stored in locked cabinets
Hard Copy Information

Files in open storage –
In area not accessible to public or unauthorized staff.
Responsible person in attendance at all times.
Door is locked during inactivity.
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.
Staff/Faculty Mailboxes

- Located from public view.
- Should be in a reasonably restricted area.
- Important for administration to determine how to handle mail stamped sensitive or confidential.
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

• All wireless mobile devices used by NDSU employees to access NDSU data e.g., email, must use the NDSU secure wireless. More information can be found at www.ndsu.edu/its/internet/wireless/.

• NDSU recommends that you do not connect a mobile device containing NDSU data to public network such as a cyber cafe or other public areas where “free” wireless is available.
PDA (Personal Digital Assistant) Security

- Treat same as your wallet.
- Enable power-on authentication.
- Enable password protection on the device.
- Encrypt of any sensitive data that will be stored on the PDA.
Mobile Device Security

• Encrypt sensitive data stored on the device and on any external memory cards added to the device.

• Back up data to a folder on your Computer’s hard drive.

• Wireless Access – Ensure that all data and connections are encrypted.
Removable Media

Removable Media: any memory device that can be removed from or connected to a device, e.g., flashdrives.

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

• North Dakota University System Computer Use Policy 1901.2

• NDSU Policy 158: Acceptable Use for Electronic Devices

• NDSU Policy 158.1: Email as an official means of communication for employs

• NDSU 710: Computer and Electronic Communication Facilities

• NDSU Student Code of Behavior
If you have questions, contact:

NDSU Chief IT Security Officer:
Theresa Semmens
IACC Building, Room 210D
701.231.5870
Theresa.Semmens@ndsu.edu
Protection of Data and Electronic Resources