Who’s Looking at Your Data?
Guidelines for Protecting Sensitive Data

North Dakota State University
Presentation Overview

• In today's universe, protecting confidential data is crucial.
• NDSU is a custodian of personal data belonging to students, staff, faculty, researchers, and those who use its outreach services.
• What can you as a good steward do to protect that information?
• This presentation will outline standards and guidelines as they pertain to federal laws on what is needed to protect personal and confidential information.
Federal Laws & Policies

• FERPA
  – Family Education Rights and Privacy Act, 1974
    • Protects students’ personal information

• GLBA
  – Graham Leech Bliley Act – 2002
    • Protects personal financial information such as financial aid, credit and financial information

• HIPAA
  – Health Insurance Portability Accountability Act – 1996
    • Protects individuals’ personal health information
State Laws, Policies, etc

• ND Privacy Law
  – Passed in 2006
    • Protects personally identifiable information. Entity is required to report to owner of information if information has become compromised or stolen

• North Dakota Public Records Law
  – Defines what is and isn’t a public record

• PCI-DSS (Payment Card Industry Data Security Standards)
  – Online Credit Card Transaction Requirements
  – Requires all entities that accept credit to follow strict security standards
NDUS & NDSU Policies

• North Dakota University System Policy 1901.2, Acceptable Use for Computers
  *This policy outlines data classification

• NDSU 710: Computer and Electronic Communication Facilities

• NDSU 158: Acceptable Use of Electronic Communication Devices

• NDSU 158.1: Email as an Official Method of Communication for Employees

• NDSU Employee Policy Handbook
NDSU’s Responsibility

• To secure and protect personal, financial, student, and health related data from
  – Misuse
  – Theft
  – Corruption
  – Unauthorized disclosure
Your Responsibilities

• To follow policy & procedure
• Use due diligence
• Incorporate recommended standards & guideline for protection of private and confidential data
NDUS Data Classification Standard

• **Public Data**: defined as data that any entity either internal or external to the NDUS can access. Open Records Law of ND may apply.

• **Private Data**: includes information that the NDUS or Institution is under legal or contractual obligation to protect. Private information may be copied and distributed with the NDUS only to authorized users. Private information disclosed to authorized external users must be done so under a non-disclosure agreement.
NDUS Data Classification Standard

- **Confidential Data:**
  - Information that is not to be publicly disclosed. The disclosure, use, or destruction of Confidential Data can have adverse effects on the NDUS or Institution and possibly carry significant civil, fiscal, or criminal liability. This designation is used for highly sensitive information whose access is restricted to selected, authorized employees.
  - The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information.
  - Confidential information must not be copied without authorization from the identified owner.
Ownership of Data

• **Data Owner**: Person of data such as SSN and date of birth or entity that has created what is term “confidential data” such as aggregated personally identifiable data or documents such as contracts or is the owner of

• **Data Custodian**: NDSU – employees, department, colleges, research centers, extension offices
Due Diligence of Care

• All NDSU employees responsible for managing, storage and manipulation of data are responsible for
  – Classification of data (Confidential, Private, Public)
  – Integrity of data (complete and unaltered)
  – Availability of data (accessible when needed)
  – Confidentiality of data (protected from misuse)
Private & Confidential Data

• Information that is not to be publicly disclosed

• Custodians of protected information have a responsibility not to reveal the contents to another individual/group unless there is a valid “need to know”

• Such information must not be copied without authorization from the identified owner
Confidential Data Elements

- Social Security Number
- Gross pension
- Value and nature of fringe benefits
- Health records
- Passwords
- Legal investigations conducted by the Institution
- Sealed bids
- Trade secrets or intellectual property such as research activities
- Credit Card numbers and related information
Private Data Elements

- Employee ID Number (EMPLID)
- Employee Date of Birth
- Location of Assets
- Donors
- Gender
- Ethnicity
- Citizenship
- Citizen Visa Code
- Veteran and Disability Status
Public Data Elements

• Employee Information
  – Name
  – Salary
  – Expense reimbursements
  – Job titles
  – Job description
  – Education and training
  – Previous work experience
  – First and last employment
  – Existence and status of complaints
  – Terms of buy-out agreements
  – Final disposition of disciplinary action
  – Work location
  – Work phone number
  – Honors and awards received
  – Payroll and time sheets
Social Security Numbers

• Do not use as an identifier on
  – Files
  – Spread sheets
  – Data bases
  – Correspondence

• Any files/documents containing SSN data must be secured and available only to those who have a need to know

• If possible, remove the SSN from the document
Credit Card Information

• All NDSU entities that accept and/or process financial information must be compliant with NDSU Policy 509, Electronic Financial Transactions
  – Do not store
    • Full credit card number (only last four digits)
    • CVV2 number
    • Exp. Date
  – Receipts
    • Only allow last four digits on receipt
    • No CVV2 number
    • No exp. Date
  – Do not accept credit card transactions over email
  – If received over voice mail, delete immediately
  – Must have separation of duties for acceptance of credit cards
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
• Computer must have login and password activated
• Do not share computer with family/friends
Common Sense Security

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

Use antivirus

Install and enable anti-spy ware prevention software

Install and enable firewall
Common Sense Security

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

• Must be approved by Supervisor
• Administration must place software into inventory
• Software downloaded from the Internet
  – Safety precautions taken
• Read the EULA (End User License Agreement)
  – What are you agreeing to?
• One piece of software = 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
Public Disclosure

- Flaunt your backside!
  Guests should not be able to see data on computer screen
- If necessary, use a screen diffuser
Confidential Files = Locked Cabinets
Cabinets should be located in a private area
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.
Laptops, Tablets, & Smart Phones

• Maintain copies of important data somewhere other than the device. Consider using an external portable storage device.

• Be sure to back up all data, and make use of encryption features when you do so.

• Hard drive and external storage is encrypted.

• Device must be labeled and identified
Wireless Security

• Must be secure transmission
• Use a VPN client (Virtual Private Network) or the NDSU secure wireless client to transmit data.
• Use encryption for confidential information.
• Do not use public wireless kiosks for transmitting NDSU information.
Smart Phones

• 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 device.
Smart Phones

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

• Back up data stored on PDA or Smart phone to a folder on your Computer’s hard drive.

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

Includes: CDRoms, DVDs, USB flash drives, external portable hard drives, memory sticks

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

• For computer related security issues contact your supervisor
• Document reasons you suspect breach of data
• Do not move, touch, alter equipment or anything related to the breach
• Do not attempt to do your own investigation
If you have questions

NDSU Chief IT Security Officer:
Theresa Semmens
IACC Building, Room 210D
231-5870
Theresa.Semmens@ndsu.edu
Theresa Semmens
NDSU IT Security Officer