Welcome to the document imaging annual user training!

Each year, as delegated by the NDSU Vice President of Information Technology and Chief Information Officer, the NDSU Chief IT Security Officer conducts an audit of all departments that use a document imaging system to ensure compliance for “NDUS Policy 1901.4, Imaging Systems.”

Policy 1901.4 requires users to receive annual training. The quiz that accompanies this training will serve as a record that you have satisfied the necessary training requirements for the current year.
The purpose of this training is to...

- Meet compliance for federal laws, university system and NDSU policies regarding document imaging

- Emphasize and reinforce the level of security required for handling student records, employee records, and other protected records stored within a document imaging system

- Ensure all users receive, on an ongoing basis, training and education related to using the document imaging system
**IMPORTANT POLICIES**

- **NDUS Policy 1901.4: Imaging Procedures** serves as the basis for the campus document imaging audit.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** protects the privacy of student educational records (*also covered by NDSU Policy 600*).

- **NDSU Policy 713: Records Retention** applies to all documents classified by NDSU that have required retention and disposal periods.
IMPORTANT POLICIES/PROCEDURES

• NDSU Policy 158: Acceptable Use of Electronic Communications Devices applies to general usage of campus computers by university employees

• NDUS 1901.2: Computing Facilities defines user privileges, responsibilities, and protective measures when accessing computing and networking resources

• NDUS 1901.3: Information Technology Project Management states that state board of higher education will manage and regulate IT planning and services for institutions under its control
• **NDUS 1912.1: Information Security Procedures** complies with the provisions of The Financial Services Modernization Act of 1999 (Gramm Leach Bliley).

• **NDUS 1912.2: Student Records – Directory Information** defines which information is not protected and can be publicized.

• **NDUS 1912.3: Employee Personal Information** defines elements considered to be personal and protected information related to person (SSN, gender, ethnicity, etc.)
NDUS Policy 1901.4

See the complete policy on the NDUS web site at:
www.ndus.edu/makers/procedures/ndus/default.asp?PID=341&SID=62

Purpose:
The purpose of this procedure is to establish an imaging procedure for all NDUS institutions that create, use, and manage digital images on optical imaging systems.
Procedure Summary:

1. Institutions shall create and use procedures that comply with standards established by the NDUS and also defined in procedures for managing digital images.

2. Institutions shall create and follow documentation that outlines and describes system hardware and software specifications and written policies and procedures that document the creation, maintenance, use and preservation of digital images within the system.
NDUS Policy 1901.4

Procedure Summary:

3. Training schedules that include initial instruction as well as regular, ongoing training must be implemented to ensure that employees understand the policies and procedures and any changes that may occur.

4. Audit mechanisms and processes to monitor the reliability and authenticity of the digital images must be activated, understood, and used.
NDUS Policy 1901.4

Procedure Summary:

5. Hardware and software shall be monitored for reliability, integrity, and security of the system.

6. Institutions must periodically review all document imaging policies, procedures, and guidelines making necessary updates to meet regulatory changes.
NDUS 1901.4 Procedures

• Individuals with access to the system and data will be given appropriate training regarding policies and procedures for the security and safety of the data stored and used within the system. The training will be ongoing and up-to-date.

How do we comply?
The material contained in this training session will be used to educate users about the policies, procedures, and security related to using a document imaging system. Completing the accompanying quiz will be required annually.
NDUS 1901.4 Procedures

• All who use the system must undergo basic training on handling and use of confidential data and have signed confidentiality agreements.

How do we comply?
All users must complete the “NDUS Data Privacy Training” (which is also required to access Peoplesoft) and have a signed “Employee Confidentiality Agreement” on file prior to accessing records in the document imaging system.
CONFIDENTIALITY AGREEMENT

All NDSU staff with access to the document imaging system need to annually review and sign an employee confidentiality agreement (like the one shown below).

EMPLOYEE CONFIDENTIALITY OF STUDENTS RECORDS ACKNOWLEDGMENT

Under the Family Educational Rights and Privacy Act (FERPA) of 1974, North Dakota State University has a legal responsibility to assure students that their education records are protected and kept confidential. All employees, including student employees, have a responsibility to adhere to the strict privacy of student records in accordance with state and federal laws and the rules of NDSU.

The University will treat the breach of this responsibility in a very serious manner. Employees who sign this agreement acknowledge that they understand the responsibility they have to not look up the records of students for personal use or to otherwise improperly disclose such records and that they realize the seriousness of this matter. Violation of law or regulation can result in disciplinary action, and in some cases wrongly disclosing confidential records can be a criminal violation.

Further, some employees may come into contact with private medical records and/or records containing protected health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). For more information regarding HIPAA, please see www.ndsu.edu/hipaa. Employee acknowledges the responsibility to comply with the privacy provisions of this law as well.

My signature represents that I have read and understand the above.

Department:
Employee Name [print]:
Employee Signature:  Date:

©2016-2017 North Dakota State University
NDUS 1901.4 Procedures

• An individual in each department/office must be assigned the responsibility to oversee and manage the training of assigned personnel.

How do we comply?
Each office that uses the document imaging system must designate a person as their office’s ImageNow “Manager”. This person will serve as their office’s point of contact, coordinate and supervise user training, and oversee system security for their office’s users and documents.
NDUS 1901.4 Procedures

• *Training logs for individuals are maintained by those who manage the oversight of those who use the system.*

**How do we comply?**
Each ImageNow “Manager” must record which users have received which types of training and when that training was completed.
NDSU Policy 713: Records Retention

• Formally documented procedures are established to ensure that only authorized individuals can create, copy, annotate or access digital images within the system. The access given is granted based on a specific need for use of the system.

How do we comply?
All users begin with minimal access. Additional access is granted upon request and only after the access need is confirmed by the ImageNow “Manager”.

©2016-2017 North Dakota State University
NDUS 1901.4 Procedures

- Access is removed from those individuals who no longer have a need to use the system.

How do we comply?
Each ImageNow “Manager” is responsible for making sure inactive users are removed from all associated sub-groups, deactivated in the system, and a request sent to the ITS Help Desk to have their imaging access removed. Be sure to alert your office’s ImageNow Manager of any changes in a user’s account status.
NDUS 1901.4 Procedures

• Formally document procedures for imaging of documents and provide such documentation to individuals who have been given access or duties related to imaging documents.

How do we comply?
Make users aware of the “ImageNow User Manual” and create internal tutorials to provide first-time user training to individuals who are new to document imaging.
The “ImageNow User Manual” may be accessed several different ways:

• Clicking “Help” on the main ImageNow toolbar and selecting “ImageNow User Help”

• While ImageNow is open, press the [F1] key on the keyboard to launch the “ImageNow User Help”

• Locate and open the “ImageNow6-UserGuide” PDF file (along with other tutorial files) stored on your department’s network SHARED drive
Upon the establishment of a new user account, first-time users should be trained on how to:

- Log in & log out (*explain the automatic log-off feature*)
- Button functions on the main ImageNow toolbar
- How to Search and View Documents
- Viewing and Routing Documents in Workflow
- Deleting Documents (*if security allows*)
- Recovering Deleted Documents from the Recycle Bin
NDSU Policy 713: Records Retention

• There is a separation of duties in place for individuals who have been given access to the imaging system. For example, the person who scans in a document does not have the ability to delete the document after it has been linked.

How do we comply?
Individual users are assigned to task-based User Groups that contain permissions for certain processes. For example, only users in the “Power Users” group have the ability to delete documents from the system.
NDUS 1901.4 Procedures

- Those who perform the scan or validation function have received additional training on document quality assurance.

How do we comply?
Separate tutorials for the scanning process will be made available to users assigned to scanning. Users will be trained to ensure the scanned image matches the original.
SCANNING & LINKING TRAINING

In addition to searching and viewing documents in ImageNow, some users may be responsible for capturing and indexing new documents, which requires additional training for:

• Capturing Documents (*via Scanner, IN Printer, File Upload*)
• Validating Document Quality
• Using Application Plans to Link the Index Keys
• Populating Custom Properties
• The process for Retaining Original Hard copies
NDSU Policy 713: Records Retention

• A process to validate that the scanned document matches the original documents is in place. The process must be documented and conducted quarterly.

How do we comply?
Offices must perform and record a document validation process, which compares the quality of randomly selected imaged documents to their original hard copies every three months.
DOCUMENT VALIDATION PROCESS

• Compare Imaged Documents to Hard Copies
  1. Search imaged documents by a random creation date
  2. Randomly select 3-5 documents from the search results
  3. Locate selected documents in hard copy archive
  4. Confirm quality of the imaged document
  5. Record validated documents in spreadsheet log

• Compare Hard Copy Documents to Imaged Docs
  1. Randomly select 3-5 documents from hard copy archive
  2. Search for corresponding documents in ImageNow
  3. Confirm quality of the imaged document
  4. Record validated documents in spreadsheet log
NDUS 1901.4 Procedures

• Logs are collected, monitored, and documented to verify reproduction accuracy and reliability according to the original document.

How do we comply?
Results from the document validation process including creation dates of selected documents, document types, student names, ID or invoice numbers, and date the validation was conducted are recorded into a spreadsheet log.
NDUS 1901.4 Procedures

- Digital images that are the records of documented business processes have been linked to the business processes that created them.

How do we comply?
Documents “owned” by a specific office will be linked to a corresponding “drawer” associated with that office. In the event the “ownership” of a document changes during the document’s lifecycle, the drawer name will be reassigned to the office that assumes ownership of the document.
NDUS 1901.4 Procedures

• All data that is stored as an image is classified according to NDUS policy and procedure 1901.2.

How do we comply?
Electronic data of the NDUS and NDSU shall be classified as either “Public”, “Private”, or “Confidential” according to the following standards.

Confidential and other document types not meant to be destroyed must be assigned to protected drawers with additional security and limited user access.
NDUS Policy 1901.2

Public – Data that any entity either internal or external to the NDUS can access (*ND open records laws may apply*)

Private – Data that the NDUS or Institution is under legal or contractual obligation to protect. It may be copied & distributed to authorized NDUS users and to authorized external users under a non-disclosure agreement.

Confidential – Data that is not to be publicly disclosed and whose access is restricted to selected, authorized employees. Cannot be copied without owner’s consent.
EXAMPLES OF “PUBLIC” DATA

Employee Information
• Name
• Salary
• Job title & description
• Work location
• Work phone number
• Education & training
• Work experience
• Expense reimbursements
• Honors & awards
• Payroll time sheets
• Home address
• Home phone number

Student Information
• Name
• Address
• Phone number
• Email address
• Enrollment dates
• Major
• Adviser
• College
• Class level
• Academic awards & honors
• Degree received
EXAMPLES OF “PRIVATE” DATA

Employee Information
- Employee ID number
- Birth date
- Gender
- Ethnicity
- Citizenship
- Citizen visa code
- Veteran & disability status
- Location of assets
- Donors

Student Information
- Student ID
- Grades
- Courses taken
- Class schedule
- Test scores
- Advising records
- Educational services received
- Disciplinary actions

©2016-2017 North Dakota State University
**Examples of “Confidential” Data**

- Legal investigations conducted by institution
- Sealed bids
- Trade secrets or intellectual property such as research activities
- Social security number
- Gross pension
- Value and nature of benefits
- Health records
- Passwords
NDUS 1901.4 Procedures

• All digital images are destroyed according to NDSU Policy 713, Records Retention.

How do we comply?
Documents need to be purged based on the document retention schedule. Additional information and requirements can be found on the NDSU Records Management web site at: www.ndsu.edu/recordsmanagement.
FERPA

What is FERPA?

• The Family Education Rights and Privacy Act of 1974 is a federal law designed to protect the privacy of student educational records.

• It applies to all educational agencies & institutions that receive funds by the Secretary of Education

• It provides guidelines for appropriate use & release of student educational records

• It establishes that students are the “owners and institutions are the “custodians” of the records

©2016-2017 North Dakota State University
**Types of Records**

*Educational Record* — any record maintained by the institution related to a student, including:

- Personal Information (name, ID, etc.)
- Enrollment records
- Grades
- Class schedules & rosters
- Student exams or papers
- Student financial records
- Student employment information
TYPES OF RECORDS

Storage Media — may exist in any of the following formats:

• Electronic document or email
• Computer printout
• Class list on a desktop
• Notes taken during an advising session
• Database
• Documents and materials that are handwritten, taped, saved on disk or film, etc.
**Types of Records**

Exceptions to Educational Record Definitions:

- “Sole possession” records or private notes that are not accessible or released to other personnel
- Law enforcement records created for a legal purpose (ex. Subpoena)
- Employment records (not based on student status)
- Medical/psychological treatment records protected under HIPAA
- Alumni records
DIRECTORY INFORMATION

Releasable items that are not considered sensitive:

• Name, Address, Email address, Phone number
• Height, weight, and team photos *(if member of athletic team)*
• Major and Minor field of study
• Class level
• Dates of attendance
• Enrollment status
• Previous institutions attended
• Participation in officially recognized activities & sports
• Honors/awards received
• Degree earned and date of earned degrees
• Photographic, video, or electronic images of students taken and maintained by the institution
**NON-DIRECTORY INFORMATION**

Confidential data that may not be released without a student’s written consent:

- Date and Place of Birth
- Race
- Gender
- SSN
- Student ID number
- Grades
- GPA
- Country of Citizenship
- Religion
GUIDELINES FOR ALL EMPLOYEES

• All NDSU employees are responsible for protecting the confidentiality of student education records.

• “Need to Know” — Access to student data is to perform job responsibilities and role with University.

• Data stored/transmitted electronically must be secure and only available to those entitled to it.

• Be vigilant and report any FERPA violations.
Additional information on the FERPA student privacy policy can be found at:

• **FERPA Guidelines for Faculty & Staff**
  ([https://www.ndsu.edu/fileadmin/registrar/facstaff/ferpa.pdf](https://www.ndsu.edu/fileadmin/registrar/facstaff/ferpa.pdf))

• **Notification of Rights Under FERPA**
  ([https://www.ndsu.edu/registrar/records/ferpa/](https://www.ndsu.edu/registrar/records/ferpa/))

And all employees should complete the following upon starting their position:

• **NDUS Data Privacy Training**
  ([https://community.ndus.edu/course/view.php?id=113](https://community.ndus.edu/course/view.php?id=113))
END OF TRAINING MATERIAL

This concludes the training material.
Please proceed to the ImageNow Training Quiz.

(This material can be referenced while taking the quiz.)

GOOD LUCK!