

NDUS Data Classification and Information Technology Security Standards

Any electronic data asset of the NDUS or Institution shall be classified as Public, Private or Confidential according to the following standards.

Public Data - Public data is defined as data that any entity either internal or external to the NDUS can access. Open record laws of North Dakota may apply.

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

Confidential Data - Confidential data is information that is not to be publicly disclosed. The disclosure, use, or destruction of Confidential Data can have adverse affects 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.

Examples of NDUS Data Classification Schema

PUBLIC

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 time sheets
- . Home address (unless employee has requested non-disclosure (suppress))
- . Home Telephone number (unless employee has requested non-disclosure (suppress))

Student Directory information (The following information is Public, unless the student has requested non-disclosure (suppress)).

- . Name
- . Address
- . Telephone number
- . Electronic (e-mail) address
- . Dates of enrollment
- . Enrollment status (full/part time, not enrolled)
- . Major
- . Adviser
- . College
- . Class
- . Academic awards and honors
- . Degree received

Other

- . Financial data on public sponsored projects
- . Course offerings
- . Invoices and purchase orders
- . Budgets

PRIVATE

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

Non-directory Student Information (May not be released except under certain prescribed conditions.)

- . Grades
- . Courses taken
- . Schedule
- . Test scores
- . Advising records
- . Educational services received
- . Disciplinary actions
- . Student ID

CONFIDENTIAL

- . Legal investigations conducted by the Institution
- . Sealed bids
- . Trade secrets or intellectual property such as research activities
- . Social security number
- . Gross pension
- . Value and nature of fringe benefits
- . Health records
- . Passwords

The owner of a data item is that person, department or office that is responsible for the integrity of the data. It shall be the responsibility of the owner of the data to classify the data. However, all individuals accessing data are responsible for the protection of the data at the level determined by the owner of the data or as mandated by law. Any data not yet classified by the owner shall be deemed Confidential. Access to data items may be further restricted by law, beyond the classification systems of the NDUS or Institution.

All data access must be authorized under the principle of least privilege and based on minimal need and all access to Confidential data must be authenticated and logged.

When an individual that has been granted special access changes responsibilities or leaves employment, all their access rights must be reevaluated and any unneeded access revoked.

When necessary, data transmission and storage should be encrypted. Sensitive data such as student records should be encrypted to ensure data confidentiality and integrity when transmitted over a network.

Data having value beyond the person that created it or data critical to the mission of the NDUS or the Institution shall be located, or backed up, on centralized servers maintained by the NDUS or institution, unless otherwise authorized by the campus or University System CIO or ITSO.

Appropriate effort shall be taken to protect data integrity, confidentiality and availability wherever it may reside: on a production server, on a disk array, on tape, on CDROM, et. al.

Prior to redistribution of media all data must be scrubbed from any media not scheduled for destruction.

4/26/05