DATA TYPE EXAMPLES

The capitalized terms used herein are defined in the Data Classification and Handling policy.

DATA TYPE EXAMPLE CATEGORIES INCLUDE:

- Directory Information
- Employee Records
- Financial Records
- Health Records
- Institutional Records
- Law Enforcement Records
- Library Records
- Personally Identifiable Information
- Student Records
- University Research

In addition to data being evaluated against the listed data types and classifications ISS may also change the classification of data against the following considerations:

SENSITIVE PII (SPII) DATA

SPII is generally defined as any PII that if lost, stolen, or disclosed without authorization could result in significant harm to an individual including embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and risk to safety.

Determining SPII relies on additional context, including what other pieces of PII data are connected to this data point, because of this, any PII may become SPII when it is combined with other known pieces of PII. Specific care must be taken when Accessing PII data and additional evaluations may be required. If you are combining multiple data types, regardless of the classification level and are uncertain what level of classification is now required, contact the ISS team for an evaluation and guidance.

Sensitive PII (SPII) requires special handling due to the increased risk of harm to University Community Members or the University itself if it is compromised.

Information involving matters of personal privacy

The University may conduct business with University Community Member acting as private citizens. While the University may disclose data about University Community Members, under appropriate legal circumstances, data collected from interactions with University Community Member acting as private citizens is held to a higher privacy standard.

Data Type	Level 1 Public Data	Level 2 Internal Data	Level 3 Sensitive Data	Level 4 Highly Sensitive Data

DRAFT

Directory Information	Employee titles and campus email address and telephone numbers, if not marked as restricted NAU User ID (NAU UID) – not to be listed in a public forum or large aggregate lists Student directory information, if not marked as restricted - name, major, officially recognized sports/activities participation - enrollment status - degrees and awards received - dates of attendance, most recent previous colleges/institutions attended - weight and height of athletic team members - address (local and permanent), telephone number, email address		Employee personal telephone number, personal email address, personal mailing address Parent or other family member names, emergency contact information Student directory information as listed in level 1, if marked as restricted	
Employee Records	Employee titles and campus email address and telephone numbers, if not marked as restricted Explanations of general employment benefits		Background checks and investigations Benefits elections Employee evaluations Employment history	
Financial Records		University financial or budgetary information	Bank account information Student financial aid	Payment Credit Card Industry Data Security Standards (PCI-DSS) data, such as credit card numbers with or without extra data (cardholder name, security code) used in transmission

DRAFT

Health Records			Personal medical or counseling records	Medical records used to document care provided to students and employees Medical records used to document care provided to outside parties interfacing with NAU academic health programs
Institutional Records	Factual reporting required by law (*e.g.*, enrollment figures, state budget information) Job postings Public event calendars or press releases The University's website and campus maps intended for public use	Information security vulnerabilities Intranet – internal web sites (*e.g.*, SharePoint sites) Network diagrams, building blueprints, critical infrastructure plans Purchasing, contracting, grants, sponsored projects University financial or budgetary information	Building safety plans, HVAC monitoring and control data Information proprietary to the University Information protected by the attorney-client privilege or any other applicable privilege Sealed bids prior to purchasing awards and contracts Security camera recordings	
Law Enforcement Records			Law enforcement records	Criminal Justice Information Services (CJIS)
Library Records	Library catalog information Library Learning Resources		Library registration records or circulation records related to individual patrons	
Personally Identifiable Information	Directory photos uploaded by the user	Employee ID (also known as PeopleSoft ID) NAU UserID (NAU UID) Pronoun(s)	Biometric Information (fingerprint, voice recording, DNA) Birth date (full: mm-dd-yy or partial: mm-dd only)	Level 3 Sensitive Data when combined with other personally identifiable information

DRAFT

			Birth date combined with last four digits of Social Security Number (SSN) Birthplace (city, state, country if not USA) Driver License, Passport, or other forms of Personal Identity Information Ethnicity ~~Gender~~Sex Gender Identity Marital Status Mother's Maiden Name Photograph Physical description Social Security Number Tax Identification Numbers	
Student Records		Prospective student and student applicant personal information	Educational records, including disciplinary records Educational services received Employment Records for Students, unless covered under another data release policy	
University Research	Anonymously recorded data (human subjects data) posing no harm to participants (as determined by the Institutional Review Board)		Identifiable interview / survey information (human subjects data) Limited Data Sets obtained from a covered	Controlled Unclassified Information (CUI) Defense Federal Acquisition Regulation Supplement (DFARS) Export controlled research information (International Traffic in

DRAFT

	Research data from any public source, such as US Census public data Research data or findings intended for public disclosure Research data that has been de-identified (human subjects data) and poses no harm to participants (as determined by the Institutional Review Board)		healthcare entity through a Data Use Agreement Research data containing identifiable bio-specimen data Research proposals, methods, protocols, and disclosures Restricted Data Sets - data with indirect identifiers (human subjects data) - data obtained through an external data owner with an agreement containing restrictions Unpublished research data	Arms Regulation (ITAR) and Export Administration Regulations (EAR)) Human subjects research, deemed by the Institutional Review Board to pose harm Medical records used in research (Protected Health Information (PHI)) Research data subject to federal regulations Research involving vulnerable populations as determined by the Institutional Review Board

DRAFT