Operating Instruction 5.23.2.1 Data Security Classification

Part 1. Purpose
To protect the confidentiality of Minnesota State Institutional Data, and to comply with applicable state and federal laws and regulations, all institutional data must be classified with the appropriate security classification. These operating instructions must be used by data custodians for assigning institutional data to the appropriate data security classification level.

Part 2. Applicability
These operating instructions apply to all institutional data, regardless of media type or format (electronic, paper, or other physical form), and to all uses of that data, wherever located. Colleges and universities may adopt additional requirements, consistent with this operating instructions and Board Policy 5.23 institutional data for which they are responsible.

Nothing in these operating instructions shall be interpreted to expand, diminish, or alter academic freedom, articulated under board policy and system collective bargaining agreements, or the terms of any charter establishing a system library as a community or public library.

Part 3. Definitions
For purposes of these operating instructions, the following definitions apply:

Data custodian
The data custodian is appointed by the data owner to assign the security classifications for institutional data and ensuring the appropriate controls are implemented.

Information technology system (IT system)
Any computer, server, software application, networking infrastructure, storage device or medium, etc., that provides for information processing, transfer, storage, or communications.

Institutional data
Data collected, manipulated, stored, reported, or presented in any format, on any medium, by any unit of the college, university, or system office that are created, received, or maintained by the institution for Minnesota State.

Not public data
Any data classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic as defined in the Minnesota Government Data Practices Act (MGDPA) or equivalent classification in any other relevant state or federal statute or regulation.

Part 4. Operating Instructions

Subpart A. Data security classifications

Using these operating instructions and the table below, the data custodian shall classify all institutional data for which they are responsible. Classification may be done at the data element or IT system level. If data are classified at the IT system level, the entire system must be classified consistent with the most restrictive classification level of any data stored, managed, or transported by the system.

(1) Data security classification table

Data Security Classification	**Definition**	**Highly Restricted Data Elements (This is an Exhaustive List)**
Highly Restricted	Institutional data must be classified as "highly restricted" if the data requires limiting access to only persons with a legitimate need to know, and: • the data elements for which loss of confidentiality could facilitate identity theft; or • by law, regulation, or contract, the data requires high-level security controls, or • the loss of confidentiality could cause significant personal or institutional harm.	• Social security numbers • Credit/payment card numbers and related information • Financial account numbers such as banking or investment account numbers • Security or access codes or passwords used to access highly restricted data • Personal health/medical information including insurance policy ID numbers and any information covered under HIPAA • Non-public investigation data (determined by legal counsel) • Credentials for IT systems that manage data elements in this classification level • Biometric information • Trade secret or intellectual property protected by a non-disclosure agreement
Data Security Classification	**Definition**	**Restricted Data Elements (Not an Exhaustive List)**
Restricted	Institutional data must be classified as “restricted” if it does not classify as “highly restricted” but the data: • by law is not public data, or • requires limiting access to only persons with a legitimate need to know, or	• Student records – admission applications, transcripts, exam papers, test scores, evaluations, grades, student discipline, student class schedule, student worker information, financial aid, and loan collection records • Student directory information that has been suppressed by the student

	• whose unauthorized disclosure will require statutory notification to affected parties (i.e., breach notification).	• Student class lists • College, university, system office, or faculty trade secret or intellectual property • Library use information • Individual demographics including age, race, ethnicity, gender, citizenship, visa status, veteran or disability status, employee home address/phone, dependent information • Faculty/staff employment applications, personnel files, benefits information, birth date, and personal contact information • Donor contact information and non-public gift amounts • Privileged attorney-client communications • College, university or system office internal memos, email, reports, and financial data identified as non-public • Driver's license numbers • Student ID numbers (if not directory data) and passwords • Employee performance information and other private personnel data • Parking lease information • Request for proposal vendor responses and scoring information prior to contract award • Credentials for systems that manage data elements in this classification level and systems classified as Low • Partial social security number • Business continuity and disaster recovery plans • Security information as defined by Minn. Stat. § 13.37
Data Security Classification	**Definition**	**Low Data Elements (Not an Exhaustive List)**
Low	Institutional data must be classified as "Low" if by law it is available to the public upon request.	• Certain employee information name, job title, job description, work location and phone number, employee identifier, salary, gross pension, value and nature of fringe benefits, payroll time sheets, education/training and previous work experience, first and last employment dates, existence and status of complaints, terms of employment settlement disputes, final disposition of discipline, honors and

		awards received or as identified as public in Minn. Stat. § 13.43, subd. 2. • Student information (unless suppressed by the student) name, other information identified as directory information by the college/university in its published FERPA policy • Financial data on public sponsored projects • Course offerings • Invoices and purchase orders • Budgets • "Summary" or statistical data that does not identify an individual • Information authorized to be made available on or through a website that does not require a Minnesota State recognized authentication system (e.g., StarID) • Published research data • Campus maps • Job postings • Information in the public domain

(2) Assigning data security classification
For institutional data not identified in state statute or the table above, the following criteria shall be used by the vice chancellor for information technology to determine if the data is highly restricted, and shall be used by the college or university to determine if the data is restricted.
(a) Negative financial impact as a result of fraud (e.g., money lost)
(b) Potential for regulatory or legal action
(c) Requirement for corrective actions or repairs including breach notification
(d) Potential for identity theft
(e) Damage to the reputation of the college, university, system office, or Minnesota State as a whole
(f) Violation of federal or state law, statute, contract agreements, board policy, system procedure, system operating instructions or, college/university, policy, procedure, standards or operating instructions.

Subpart B. Data collections
Data custodians may assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements must be used. For example, if a data collection consists of a student's name and social security number, the data collection must be classified as Highly Restricted even though the student's name may be considered Low

information. In some cases, a collection of lower class data elements when combined, can result in a higher classification for the collection of data.

Data custodians are encouraged to consult with system legal counsel and the vice chancellor of information technology when in doubt.

Subpart C. Data inheritance and propagation

The process of data classification is not static. Data are often combined and transmitted to produce information on which classification decisions can be made. Once data elements are classified, the security classification travels with the element as it is propagated from an originating system to any other system, collection or medium. Care must be taken by Data Custodians and Data Users to understand that a data element and its associated controls travel with it when it is transmitted and combined with other data. For example: a social security number (a highly restricted data element) remains highly restricted if it is taken out of its system of record e.g. a student system, and placed in a spreadsheet containing other data elements. Moreover, the spreadsheet now inherits some of, if not all of the controls that are associated with the social security number. Thus, the new data collection needs to be classified and treated appropriately. If data are classified at an IT system level, particular care must be used to understand the classification of any data elements that are propagated from the system.

Subpart D. Documentation and dissemination

Data custodians are responsible for: documenting the classification of all institutional data elements for which they are responsible, maintaining an inventory of those data elements, and disseminating the assigned classification information to data users of those data elements.

Subpart E. Data security inventory and reclassification

Data custodians shall review data for which they are responsible at least every three years to ensure a complete and accurate inventory of institutional data elements and their proper security classification and controls.

Subpart F. Implementation schedule

Implementation Requirement	**Required Date of Implementation**
Data security classification definitions	Date of this operating instructions adoption
Data owners and custodians identified	Within three (3) months from date of this operating instructions adoption
Inventory of IT systems containing data for which data owners are responsible	Within nine (9) months from date of this operating instructions adoption
Highly restricted data elements assigned data security classification	Within twelve (12) months from date of this operating instructions adoption

Restricted and Low data elements assigned data security classification	Within eighteen (18) months from date of this operating instructions adoption

---

Date of Adoption: 03/08/17
Date of Implementation: 03/08/17
Date of Last Review:

Date and Subject of Revision:
No additional HISTORY.