Minnesota State Colleges and Universities
System Procedures
Chapter 5 – Administration
Procedures associated with Board Policy 5.23

5.23.2 Data Security Classification

Part 1. Purpose
This procedure establishes data security classifications for Minnesota State institutional data, data ownership, custodianship, and user roles and responsibilities. To protect the security and confidentiality of Minnesota State data and to comply with applicable board policy as well as state and federal laws and regulations, all institutional data must be classified with the appropriate security classification.

Part 2. Applicability
This procedure applies to all institutional data, wherever located, regardless of media type or format (electronic, paper, or other physical form), and to all uses of that data. This procedure and associated operating instructions establish minimum requirements for classifying institutional data. Colleges, universities, and the system office may adopt additional conditions of use consistent with this procedure and Board Policy 5.23 for information technology resources under their control.

Nothing in this procedure 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 this procedure, 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 that the appropriate controls are implemented.

Data owner
An individual with authority and accountability for specified information (e.g., a specific business function) or type of institutional data. Included in this authority is the ability to grant and deny access to data or portions of institutional data under his or her authority. This individual shall assign responsibility to the appropriate data custodian(s) to ensure the protection of institutional data. The data owner is typically in a senior or high-level leadership position. There may be more than one data owner at a college, university, or the system office, depending on the authority and accountability for specified information (e.g., a specific business function) or type of institutional data.

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
"Not public data" are 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. Procedures
Authorizing administrators are expected to implement and oversee this procedure for business-related purposes in accordance with board policy, other applicable system procedures and law.

Subpart A. Data security classification
All institutional data must be classified in one of the following security classifications:

1. **Highly restricted**
   Institutional data that are not public data (1) the disclosure of which may compromise a person's identity in financial transactions; or (2) which by law, regulation, or contract requires high-level security controls; or (3) when the loss of confidentiality could cause significant personal or institutional harm.

2. **Restricted**
   Not public data that are not classified as highly restricted.

3. **Low**
   Institutional data that by law are available to the public upon request.

Subpart B. Data security classification roles and responsibilities

1. **Data owners**
   a) The chancellor and the presidents of each college and university shall designate a data owner for all departments and/or administrative units that collect, create, or maintain institutional data. Data owners may assign administrative responsibilities to data custodians in regards to management of data under their control. The chancellor and presidents shall have ultimate responsibility for data practices compliance at his/her respective institution or office.
   b) The data owner shall maintain an inventory of private and confidential data sufficient to ensure compliance with Minn. Stat. § 13.025, subd. 1. The data owner shall ensure implementation of appropriate security controls to limit access to institutional data classified as highly restricted or restricted to those individuals whose work responsibilities require access.

2. **Data custodians**
   Data custodians are appointed by the data owner and shall work at the direction of the data owners to assign the appropriate data security classification to institutional data and identify to the data owner the appropriate information security controls. Data custodians must also communicate the data security classifications to affected groups and individuals.

3. **Data users**
   Data users shall access or use highly restricted or restricted data only for business purposes that reasonably require access and follow all applicable laws and Minnesota State policies, procedures, and operating instructions related to data classification and access.

   The vice chancellor for information technology shall issue systemwide data classification directives.

Subpart C. Data reclassification
On a periodic basis, the data custodian shall reevaluate the classification of institutional data to ensure the assigned classification remains appropriate based on changes to legal and contractual obligations. Conducting an evaluation on an annual basis is encouraged; however, the data custodian must determine what frequency is most appropriate based on available resources. If at any time a data custodian determines that the data has changed such that it warrants reclassification, an analysis of existing security controls must be performed and controls changed if necessary.

Subpart D. Disputes
Disputes as to the classification of institutional data must be referred to the appropriate administrator at a college or university or the system office. The vice chancellor for information technology, working with system legal counsel, may be called upon to make a final determination in any data classification dispute.

Date of Adoption: 02/17/17
Date of Implementation: 02/17/17
Date of Last Review:

Date and Subject of Amendments: