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

5.23.3 Information Security Requirements and Controls

Part 1. Purpose
This procedure defines the roles and responsibilities regarding information security requirements and the methods for determining the appropriate security controls to meet information security requirements.

Part 2. Applicability
This procedure applies 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.

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 shall be appointed by the data owner to assign the security classifications for institutional data and ensuring 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 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.

Information security controls
Technical, administrative, management, or physical methods or safeguards that, when applied, satisfy information security requirements. For example, an information security requirement may state, “Confidential data in transit over a public network (i.e., the Internet) must be unreadable to any unauthorized individual.” The information security

control for meeting this requirement could be to apply encryption to any confidential data when transmitted over the Internet.

Information security requirements
Information security obligations that must be met or implemented. Information security requirements are defined by, for example, federal or state law or regulation, industry regulations, state statute, board policy or procedures, third-party contracts, college or university policy, or any other information security protection requirement identified by the data owner.

Information technology service provider
An internal or external entity that provides or manages an information technology system.

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.

Part 4. Procedures

Subpart A. Responsibilities for determining information security requirements

It is the responsibility of the data owner to identify information security requirements applicable to any institutional data or IT system for which he or she is responsible. Additionally, the data owner is responsible to ensure that any information technology service provider that provides an IT service meets applicable requirements

Subpart B. Determining appropriate information security controls

Data custodians, acting on the data owner's behalf, shall use Operating Instructions 5.23.3.1 Information Security Controls to determine the appropriate security controls to meet information security requirements for the IT systems and data for which they are responsible. Operating Instructions 5.23.3.1 prescribes minimal controls needed to protect institutional data. It does not preclude colleges, universities, or the system office from applying additional controls.

Subpart C. Application of information security controls

Colleges, universities, and the system office shall implement all required information security controls identified in Operating Instructions 5.23.3.1 and any other operating instructions under this procedure for institutional data and IT systems for which they are responsible.

Subpart D. Operating Instructions Development Responsibilities
The vice chancellor of information technology shall develop operating instructions to implement these procedures per Board Policy 1A.1.

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

Date and Subject of Amendments: