Policy

All University Colleges and Divisions are responsible for adopting the minimum security standards as established by this policy and all supporting Information Security Standards and Procedures. Standards and Procedures establish the minimum level of security required by the University. Colleges and Divisions are encouraged to work with the Information Security Staff on how they can exceed these minimums for the protection of the University's information resources. In cases where University data or systems are actively or imminently under threat of compromise, the Vice President for IT Solutions and Chief Information Officer (CIO) or designee will act in the best interests of the University.

Nothing in this policy shall be interpreted to expand, diminish or alter academic freedom, articulated under MnSCU Board Policy, Minnesota State University Policy, collective bargaining agreements, or the terms of any charter establishing a system library as a community or public library.

Colleges, Divisions, Faculty, Staff, Students, Emeriti, and/or Affiliates who are subject to, but do not comply, with MnSCU Board Policy, this policy, supporting standards or procedures will be subject to remedial action in accordance with applicable Federal and State Statutes, MnSCU Board Policy, Minnesota State University Policies and Procedures and/or collective bargaining agreements. Violations of this policy may result in loss of privileged access, administrative sanctions, and/or personal civil or criminal liability.

State Asset Computing Devices

All computing devices purchased with University funds and/or for official University programs with the ability to permanently store data must have a State of Minnesota Asset Tag affixed to it and must be inventoried according to MnSCU Board Procedure 7.6.3 Capital Assets. All computer assets will be the accountability of the Vice President or Dean of the respective Division or College. Each computer asset will be assigned to an individual. The individual will be responsible for the proper security of the device as outlined in MnSCU Board Policy Procedure 5.22.1 Acceptable Use of Computers and Information Technology Resources. Individuals will also be responsible for the proper inventory tracking of the device(s) assigned to them.

Any transfer of state asset computing devices must be reported to the IT Solutions Center (servicedesk@mnsu.edu). When a transfer of responsibility occurs, the computer must be submitted to IT Solutions (ITS) for erasure and re-installation in order to ensure the privacy and security of any remaining data on the device. All state asset computing devices no longer needed by a division or department must be disposed of through ITS by contacting the IT Solutions Center.
All state asset computing devices must meet ITS computing device standards and have an operating system image approved by ITS that meets Minnesota State University, Mankato Information Security Standards. Devices that do not meet ITS computing device standards are subject to review by the CIO and/or designee.

Data Classification

According to Minnesota State Statutes Chapter 13 Section 13.03 Minnesota Government Data Practices Act, all University Data is considered public data and may be inspected or copied by everyone, unless otherwise classified by Federal Statute, State Statute, MnSCU Board Policy, System Procedure, System Guideline, University Policy, Standard or Procedure. While data contained within University Information Technology resources may be public, ITS takes every reasonable effort to protect the security and privacy of the University’s Information Technology resources and data. The ITS staff of Minnesota State University, Mankato will not monitor or inspect data contained within Information Technology systems except in limited circumstances detailed in supporting Information Security Standards and Procedures.

Exceptions

Exceptions with a documented business need may be requested by contacting the IT Solutions Center (servicedesk@mnsu.edu). Upon review of the risk to the University, the CIO may grant exceptions to this policy and/or supporting standards and procedures. All approved exceptions are subject to periodic review and re-certification. Approved exceptions may be revoked at any time as circumstances change.

Support

Any actual or suspected compromise must immediately be reported to ITS. The CIO or designee will consult with necessary stakeholders to determine an appropriate course of action based on the risk to the University.

Responsibilities

The CIO will be accountable for ensuring the responsibilities of this policy and supporting standards and procedures are carried out in the spirit of protecting the security and privacy of the University’s data, systems, Faculty, Staff, Students, Emeriti, and Affiliates. In cases where the privacy or security of the University are actively or imminently under threat of compromise, the CIO or designee will act in the best interests of the University. The CIO will have final decision making authority over all matters related to Information Security Policy, Standards and Procedures. In case of un-documented or contradicting situations, the Information Security Staff will attempt to clarify and further document the situation with the CIO having final authority over decisions.

All Administrators, College Deans and Division Vice Presidents will be responsible for ensuring their respective areas are following proper Information Security Policy, Standards and Procedures. All Faculty, Staff, Students, Emeriti, and Affiliates are responsible for immediately reporting violations of Information Security Policy, Standards and Procedures to ITS.

Revisions to this policy will be subject to the University Policy Development policy. Revisions to supporting Information Security Standards and Procedures will be subject to review by the CIO. University Shared Governance groups will be consulted as needed upon review by the CIO.

Rationale

Data and access to it is increasingly ubiquitous, and expectations and needs for access to data has become a critical aspect of our University's strategic health and viability. As we need to make access to data easy and usable to those at our institution who need it, it is equally critical that we protect our data
from those who should not have access to it. Threats to and attacks on data in both professional and personal arenas are becoming increasingly commonplace. Universities and higher education institutions are especially vulnerable to these threats and attacks because of our industry's inclination toward openness and collaboration. Data breaches from these threats and attacks are on the rise for higher education institutions (Schauffhauser, 2013; Zalaznik, 2013). As a University, we have a duty to our students and ourselves to diligently protect the “confidentiality,” “integrity,” “availability,” and “accountability” of the University's data. All Faculty, Staff, Students, Emeriti, and Affiliates must make every reasonable effort to ensure the privacy and security of all data of the University.

The purpose of this policy and related standards and procedures is to ensure that all University Faculty, Staff, Students, Emeriti, and Affiliates understand their duty and responsibility in reducing the risk of compromise through appropriate security measures. Access to University data is a privilege, not a right, and implies a duty and responsibility to adequately protect the University from compromise.

This policy is focused on the protection of the University's information resources. Related Information Security Standards and Procedures establish the minimum security standards in accordance with MnSCU Board Policy 5.22 Acceptable Use of Computers and Information Technology Resources, MnSCU Board Policy 5.23 Security and Privacy of Information Resources as well as related MnSCU Board Policy Procedures. All Minnesota State University, Mankato Information Security Standards and Procedures are enforceable through this policy.

Definitions

**Accountability** – Accountability is the assurance that actions taken on University Information Systems are traceable to a source in the event of an Information Security Incident. It is also the assurance that the actions of an end-user are appropriately attributed to themselves without question for the protection of the end-user.

**Affiliate** – Affiliate is any individual or entity with an official relationship with the University whether paid or volunteer. Affiliates are subject to all Information Security Policy, Standards and Procedures.

**Attack** – Attack is any successful or unsuccessful unauthorized disclosure of University Data or unacceptable use or attempted use of University Information Systems.

**Availability** – Availability is the degree to which Data and/or Information Systems are accessible to University Faculty, Staff, Students, Emeriti, and/or Affiliates.

**Breach** – Breach is any unauthorized use or disclosure of University data or Information Systems

**CIO** – Vice President for IT Solutions and Chief Information Officer

**Confidentiality** – Confidentiality is the assurance that University data or Information Systems are available only to those who are authorized to access or use data or Information Systems.

**Data** – Data is any information accessed, stored, transmitted or overseen by the University

**Data Owner** – The Data Owner is the person(s) that can authorize or deny access to certain data and is responsible for its accuracy, classification, integrity and timeliness. IT Solutions staff are typically not data owners.

**Data Custodian** – The Data Custodian is responsible for ensuring that data systems and controls conform to requirements as set forth by the Data Owner. Data Custodians can be a subordinate of the Data Owner and/or the IT Solutions Staff.
**Incident** – An incident is any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy.

**Information System** – Information System is any device or software used to access, store, transmit or oversee University data.

**Integrity** – Integrity is the assurance that systems are adequately protected and free from tampering of any kind.

**Risk** – Risk is the possibility of suffering harm or loss or the potential for realizing unwanted negative consequences to University Data or Information Systems.

**Risk Assessment** – Risk Assessment is an evaluation of University Data or Information System to qualify and/or quantify identified risks, their potential severity and potential for compromise.

**Related Information**

- [University Information Security Standards and Procedures](#)
- [MnSCU Board Policy 5.22 Acceptable Use of Computers and Information Technology Resources](#)
- [MnSCU Board Policy 5.23 Security and Privacy of Information Resources](#)
- [Minnesota Government Data Practices Act](#)