Policy

Responsibility of All Users
All employees at Minnesota State University, Mankato will make every reasonable effort to ensure the privacy of non-public data stored or sent on the university's network. Information and Technology Services (ITS) cannot guarantee the privacy of data transmitted through the network or data stored on any computer or other storage device. The protection, privacy and integrity of non-public data is reliant on all employees adhering to the information privacy procedures described below.

Users are also reminded of their responsibility to refrain from sharing passwords or circumventing security mechanisms as detailed in the Minnesota State Colleges and Universities Acceptable Use of Computers and Information Technology Resources. Departments should work with the Information Security Manager to develop safeguards for protecting their non-public data.

Privacy of Information Systems
The e-mail and network activity of computer users are considered private. The contents of university-supplied e-mail folders and file server folders marked “My Documents” are also considered private. Additionally, the hard drive contents of non-state-owned computers delivered to ITS for repair are considered private. The ITS staff of Minnesota State Mankato will not monitor or inspect private network activity, private folders, or private drives except in limited circumstances detailed in this document. Network equipment such as switches, routers, firewalls, intrusion detection systems, DHCP and DNS servers are configured to log activity for trend analysis purposes, troubleshooting, and to detect and track malicious activity. ITS staff will not use this information to invade the private communication of users.

The contents of university-supplied folders that are available to a general audience such as “My_Public_Files” and “My_Website” are considered public and shall not be used to store non-public information. Users should not expect any degree of privacy over the contents of these folders.

Encrypting Non-Public Data
For acceptable encryption technology and recommended products for protecting non-public data please contact the IT Service Desk.
Procedures

Protection of Non-Public Data
Any electronic non-public data that is being transmitted over a public network must be encrypted or sent over an encrypted connection such as VPN or SSL. Non-public electronic data stored on a device that is not housed in a physically secure location (such as the University's data center) must be encrypted as well.

Non-public data cannot be stored on cell phones, iPods, MP3 players or other electronic devices that do not support the encryption technology. Non-public data that is stored on portable media such as external hard drives, USB thumb drives, flash memory cards, CD or DVD media must be encrypted and should be physically controlled at all times. Non-public data on portable media that is no longer needed must be securely destroyed. CD and DVD media can be shredded while hard drives, flash drives, and other reusable electronic storage devices must be securely erased compliant with NIST SP 800-88. ITS provides this service at no cost for state asset machines.

Desktop and notebook computers that access or contain non-public data should use full-disk encryption software. Users are encouraged to limit their printing of non-public data, and must retrieve documents from the printer immediately that contain non-public data. Paper records containing non-public data must be stored in a physically secure location. When record retention schedules allow for the disposal of paper records containing non-public data these documents must be shredded prior to disposal or placed in a Minnesota State Mankato Document Destruction Box.

Privacy of Network Activity and Folders
General monitoring of network activity and folder content by ITS staff is permitted for trending and analysis purposes and for maintaining the health of systems.

ITS staff may come into contact with a specific user's private network activity, folders, and disks while carrying out their routine job functions. For example, if a user reported that he or she was having trouble receiving e-mail, the e-mail administrator may have to go into that user's e-mail folders to troubleshoot and resolve the problem. In doing so, the e-mail administrator may be exposed to the user's private data.

ITS staff may be directed to inspect a user's private folders, network activity, disks or other digital information as part of an investigation into workplace misconduct, information security breaches, violations of university or Minnesota State Colleges and Universities policies, or violations of state and federal statutes. The Information Security Manager will act as the liaison between ITS and all internal and external departments for all investigations regarding information technology resources. The investigation owners will provide a letter in writing to the Information Security Manager appointing any designee for the areas they are responsible for. If a designee is not provided only the following individuals may direct an investigation. For faculty and staff accounts, this direction must come from the Director of Human Resources (or designee) and for student accounts this direction must come from the Vice President for Student Affairs and Enrollment Management (or designee). The Vice President of Information Technology (or designee) can direct system administrators to inspect any user's private folders, network activity, or disks as part of an investigation into an information security breach. The President of the University (or designee) can direct system administrators to inspect and user's private folders, network activity, or disks in response to a valid court order or subpoena.

ITS staff will not copy or make use of information that they encounter in a user's private folders or disks without the consent of the information owner. However, ITS staff must report to their supervisors if while performing their approved duties they encounter evidence of a crime or evidence that a person's health or safety is in jeopardy. It is the supervisor's responsibility to pass the information on to the appropriate parties.
Definitions

Non-public data: For the purposes of this policy, non-public data are defined as data that is protected by the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Minnesota Government Data Practices Act (MGDPA), or any other State or Federal regulation or policy approved by Minnesota State Mankato or the Minnesota State Colleges and Universities Board of Trustees. In addition to these data, proprietary or sensitive information not covered by other laws but that would be detrimental to the university if misused is also considered non-public.

Public Network: Any network not owned and operated by Minnesota State Mankato such as the Internet or the network of another state agency. Because Minnesota State Mankato is unable to verify or audit the security posture of a network that it does not own and operate, the assumption must be made that the network is configured as a public network.

Malicious activity: Computer use designed to compromise the confidentiality, integrity, or availability of non-public data. Examples include hacking or creating a denial of service condition on the network.