

# University Policies

<b>Policy Name:</b> Campus Information Technology Privacy	<b>Effective Date:</b> January 1, 2009
<b>Custodian of Policy:</b> Vice President for Technology/Chief Information Officer	<b>Last Review:</b> January, 1996
	<b>Next Review:</b> September, 2013

## 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 depends 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 MnSCU Acceptable Use of Information Technology Resources policy. Departments should work with the ITS Information Security Manager to develop procedures for protecting their non-public data.

### Privacy of Personal Data:

Whenever possible, the purposes for which personal data are collected will be specified at the time of collection. The subsequent use of personal data must be limited to the fulfillment of those purposes for which it was collected and other uses that support those purposes for which it was collected. Personal data must not be disclosed, made available or otherwise used for purposes that were not specified at the time of collection except with the consent of the data subject or by the authority of law. Personal data must be protected by reasonable security safeguards against such risk as loss, unauthorized access, improper modification, or unauthorized disclosure. Individuals have the right to confirm if the University has data relating to him or her and to have that data communicated in a reasonable time and format

### Privacy of Network Activity, Folders and Disk Drives:

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\_Private\_Files" 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. Network administrators 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 should not be used to store non-public information. Users should not expect any degree of privacy over the contents of these folders.

## Privacy of visitors to Minnesota State University Web Servers:

Minnesota State Mankato will respect the privacy of all web site visitors to the extent permitted by law. ITS configures all servers to log detailed information for performance trend statistics, and to track malicious activity. Visits to the University's web site will generate network traffic logs and web site visit logs which will be used to maintain the security and performance of the University's networks and computer systems. Web servers create cookies to maintain session data and to identify a user for future web site visits. In addition, some information may be voluntarily provided by the visitor, such as the act of applying for admission online. This information is considered private and will not be disclosed to outside parties except as provided by law. A link to this privacy procedure must be included on all University web pages.

## Encrypting non-public data:

The Campus Encryption Standard provides a list of acceptable encryption technology and recommended products for protecting non-public data. A link to the Campus Encryption Standard is provided at the end of this document.

## Resolving Conflicts:

Should some section of this policy conflict with State or Federal law in such a way that the two cannot be reconciled then the State or Federal law will preempt that section of this policy.

## Procedures:

### Protection of non-public data:

Any electronic non-public data that are being transmitted over a public network must be encrypted or sent over an encrypted connection such as VPN or SSL. For example, a person at home sending mail over MavMail to other users on campus need not take any additional steps to protect those data. However, sending a sensitive report to another state agency would require encryption of either the report itself or the connection to protect that information. 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. The Campus Encryption Standard provides a list of acceptable encryption technology and recommended products.

Non-public data cannot be stored on cell phones, iPods, MP3 players or other electronic devices that do not support the encryption technology listed in the Campus Encryption Standard. Non-public data that are stored on portable media such as external hard drives, USB thumb drives, flash memory cards, CDs 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 can be scrubbed of data. ITS provides this service at no cost.

Desktop and notebook computers that access or may contain non-public data must encrypt those data and should use full-disk encryption software such as PointSec or BitLocker available through ITS. Disk encryption software helps reduce the risk of a security breach if the computer is lost or stolen by making it nearly impossible to read the disk's contents. The Campus Encryption Standard lists several acceptable disk encryption technologies for the most common operating systems. 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 Systems Administrators is allowed for trending and analysis purposes and for maintaining the health of systems.

System administrators 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.

System administrators may be directed to inspect a specific user's private folders, network activity, or disks as part of an investigation into workplace misconduct, information security breaches, violations of university or MnSCU policies, or violations of state and federal statutes. 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 Associate 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 any user's private folders, network activity, or disks in response to a valid court order or subpoena.

System administrators will not copy or make use of information that they encounter in a user's private folders or disks. However, system administrators will report to their supervisors if while performing their approved duties they encounter evidence of a serious crime or evidence that a person's health or safety is in danger.

## Definitions:

**Non-public data:** For the purposes of this policy, non public data are defined as data that are protected by the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Privacy 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 computer network not owned and operated by Minnesota State University, Mankato such as the Internet or the computer 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 or integrity of non-public data or use designed to make computer resources unavailable. Examples include hacking, or creating a denial of service condition on the network.

## Authority:

MnSCU Board Policy 5.23: [Security and Privacy of Information Resources](http://www.mnscu.edu/board/policy/523.html)  
<http://www.mnscu.edu/board/policy/523.html>

Minnesota Statutes 13.05 Subd 5: [Minnesota Government Data Practices Act](http://www.revisor.leg.state.mn.us/bin/getpub.php?type=s&year=current&num=13.05)  
<http://www.revisor.leg.state.mn.us/bin/getpub.php?type=s&year=current&num=13.05>

Minnesota Statutes 13.15: Minnesota Government Data Practices Act  
<http://www.revisor.leg.state.mn.us/bin/getpub.php?type=s&year=current&section=13.15>

See also:

MnSCU Board Policy 5.22: Acceptable Use of Information Technology Resources  
<http://www.mnscu.edu/board/policy/522.html>

Minnesota State University, Mankato Campus Encryption Standard  
[http://www.mnsu.edu/its/security/encryption\\_standard.pdf](http://www.mnsu.edu/its/security/encryption_standard.pdf)

Minnesota State University, Mankato Student Records Policy  
<http://www.mnsu.edu/acadaf/policies/StudentRecordsPolicy.pdf>