

REVISED: July 2009

Information & Technology Services System Hardening Policy

Overview and Purpose

This policy is intended to create a reasonably secure operating environment and prevent unauthorized access to Minnesota State University, Mankato Information Systems. The policy provides direction for Information & Technology Services (ITS) to develop configuration standards for systems that it manages and provides authority to those configuration standards.

Scope

This policy applies to all devices and systems managed by Information & Technology Services (ITS). In some circumstances this policy may apply to devices and systems which are not managed by ITS.

Policy

- ITS will develop configuration standards for the operating systems, services, and infrastructure it manages.
- All devices and systems managed by ITS and currently in a production state must adhere to the applicable configuration standards for that device or system.
- ITS may require a device which is not administered by ITS to conform to configuration standards before providing services to that device. For example, ITS may require a desktop computer at another institution to meet a configuration standard before being granted access to the ImageNow service which is managed by ITS.
- Devices and systems that do not comply with applicable configuration standards may lose access to services provided by ITS. This may include a devices ability to access wired and wireless networks.
- Configuration standards and exceptions will be reviewed every year. Configuration standards may be reviewed more frequently to incorporate security changes.

Exceptions

- Exceptions to the configuration standards may be granted by the Vice President of Information & Technology Services or that person's designee.

Effective and Review Date

- This policy is effective July 1, 2009.
- This policy will be reviewed on July 1, 2010 and every three years after that.