

BOARD OF TRUSTEES
MINNESOTA STATE COLLEGES AND UNIVERSITIES
INFORMATION ITEM

Security Issues Update

BACKGROUND

As part of the ongoing focus on information security, the following update provides a review of information security issues, actions taken to address them and plans for future enhancements to the security environment.

Minnesota State Colleges and Universities System maintains one of the largest and most complex networks in the State. Significant amounts of private information are stored and maintained within the System, so there is a responsibility to students, faculty, and staff to maintain the confidentiality, integrity and availability of that data, and ensure that critical information is safe and only viewed by properly authorized personnel. Balancing the need for security with the need for an open, service-driven networking environment while supporting thousands of users, computers, servers, several data centers and a variety of operating systems presents significant challenges to ensuring network security.

The System has experienced tremendous growth in the amount of data maintained for example, the demands for data warehouse reports and on-line learning. At the same time the numbers of threats and vulnerabilities to IT systems have also increased significantly. New regulatory requirements from Homeland Security to the Gramm-Leach-Bliley Act must also be addressed.

An effective, well defined information security program must take into account the different user groups; academic, administrative and residential. It must accommodate visitors, students with their own computers, research activities, remote access, libraries and the wide variety of new technologies becoming available, such as wireless. As the numbers of websites, e-mails and electronic files increase, and the ways to access them become more flexible, the threats to information security increase.

Security measures must go beyond IT systems and cannot rely just on technology solutions. A comprehensive program requires executive level support, formal policies and procedures, risk assessment and management, training and awareness, technology standards and guidelines, compliance measures, and ongoing commitments to the program.

As part of the effort to ensure a high level of security for the Systems information resources, the MnSCU Information Technology Services division recently completed an external review of Information Security policy, standards, and network architecture and configuration. During the remainder of this year, ITS will be revisiting the overall information security strategy and implementing recommendations to enhance the exiting security environment and to ensure that it comprehensively meets the System's security needs.

Information Security Program

ITS planning efforts are currently underway to develop and formally adopt, implement and maintain a comprehensive, system wide security program that address strategies, awareness, and tactical implementation, over a 2-5 year timeframe. Significant progress has been made toward improving the security environment; however, continual work remains to achieve an enterprise wide security program which is defined, followed and managed. What follows is an update on progress and plans related to various program components.

Policies, Standards and Guidelines

Standards: The existing program framework is designed to comply with International Security Standards ISO 17799, which is the generally accepted industry standard within the security discipline for security architecture and configuration. Past efforts have focused on development of technical standards to be implemented by all Colleges/Universities, and are a component of a larger security program. Typically this implementation occurs in steps with the most critical areas addressed first. Development of guidelines and best practices to assist Colleges/Universities in implementing these technical standards is underway with emphasis on server configuration guidelines.

Remaining areas of the technical framework which will be developed include network traffic segmentation, encryption and specific firewall configuration change standards and guidelines. The standards documentation must also be made more usable by mapping guidelines to the MnSCU standards in a web based format creating a consistent level of technical detail across the standards. Efforts are currently underway to address all of these areas.

Role Based Authorization for ISRS

Certain staff within the Office of the Chancellor and particularly the ITS division have access to the application and institutional databases. General roles for employees and related job duties for each role have been established for these employees. Security access varies depending on the roles and responsibilities of each individual staff member. Reports and procedures were also created to monitor compliance.

Security and Privacy Policy and Procedures

The following security policy and procedure has been formally adopted.

Board Policy 5.22: Acceptable Use of Computers and Information Technology Resources
This policy establishes responsibilities for acceptable use of Minnesota State Colleges and Universities information technology resources. Adopted 7/16/03

System Procedure 5.22.1: This procedure establishes responsibilities for acceptable use of Minnesota State Colleges and Universities information technology resources. Adopted 1/23/04

A draft policy addressing “Security and Privacy of Information Resources” is currently being developed with the assistance of the Office of General Counsel and the policy, and related procedures, will be widely distributed for review and input, with expected completion early next year.

Compliance Metrics

Measuring compliance is critical in determining the effectiveness of the security program and to evaluate whether the program objectives and risk mitigation requirements are being met. The strategy for compliance measurement requires decisions about who measures compliance, what is measured, how it is measured, and consequences for non-compliance.

As a starting point, ITS developed ISRS security monitoring tools for College/University use. Security reports by ISRS Modules were created for each College/University to monitor ISRS security and are available on the Data Warehouse. Biweekly reports listing employees whose jobs status has changed or individuals that have separated from the systems during a pay period are sent to College/University HR Directors and CIO's so changes can be made to ISRS access rights where required. A project to identify incompatible functions and establish guidelines and options for campuses to use when assigning and reviewing individual user access on ISRS has been completed for the Accounts Receivable module.

Risk Management

Security Risk Assessment is one of the fundamental building blocks in any information security management system. Risks may involve the unauthorized disclosure or modification of data, loss of information resources or improper use of computer resources. The security risk assessment is a living document, subject to revisions and updates.

Risk management offers alternative strategies for dealing with risk and making it more acceptable. It involves identifying risks, prioritizing them, proposing strategies for mitigation, and allocating resources to carry them out and validating those strategies.

A Risk Assessment tool was developed and includes: data, applications (administrative, academic and network), servers, client computers, public workstations, network devices and peripherals, telecommunications, cable plant, roles and goodwill. An assessment was completed for the Metro data center. The primary focus of the existing risk assessment template is on the technology aspects of information security and is available to all Colleges/Universities through the ITS website.

However, Risk Management is an enterprise wide concern and needs to extend beyond the data center and technology focus and become an ongoing process. Future risk assessments need to address higher level issues such as executive level support, budget and staffing, both at the Office of the Chancellor and College/University levels. It will include also strategies to report significant risk levels to the CIO and Cabinet members to prioritize options to minimize risk levels to an acceptable level. Significant efforts will be made in this area over the next 6 months.

Training and Awareness

Security is an ongoing process that requires the participation of all users of system IT resources. Training and awareness programs are critical for communicating risks, defending against viruses, worms and hackers, improving system security, and for understanding the new regulations such as HIPAA and Gramm-Leach-Bliley requirements and their implications.

The size of the system, numbers of individuals and various audiences (Office of the Chancellor, campuses, support staff, faculty, students and IT professionals), each having different knowledge

base, makes awareness training challenging. While specific training sessions have been provided primarily to IT professionals and some business office staff, options for a system-wide comprehensive training and awareness program are currently being planned by the Security Steering Committee, which is composed of Office of the Chancellor and College/University management staff.

Future efforts will focus on developing a comprehensive awareness program that will be College/University directed and managed and deliver a system-wide consistent message. Efforts are underway with the assistance of the Office of General Counsel to develop a series of training modules that address the needs of various user groups. Plans are also underway to look at skills needed by technical support teams both at the office of the Chancellor and Colleges/Universities.

Business Continuity Planning

Business continuity is not just about restoring an IT system; it is about preserving the ability to do business. The Business Continuity Plan establishes actions and procedures to recover the major/critical business operations and resources in the event of an extended interruption of operations, and implement recovery strategies and actions that are designed to minimize the financial and operational impacts of such interruptions. Business Continuity Plans were developed for the Office of the Chancellor at Wells Fargo Place and ETC Building.

Network

Providing necessary network connectivity to a variety of users while ensuring protection to the business is a major task. Hundreds of devices such as firewalls and routers, each containing thousands of rules, are installed to monitor and manage network access system wide. Some devices are centrally managed and others are managed by the Colleges/Universities. These rules help protect against untrusted connections and potential access to protected data. While a recent external review of the network architecture and configuration indicated that current process and procedures met or exceeded industry best practices or regulatory requirements in many areas, additional effort is being focused on implementing additional security controls as recommended.

Resources Deployed to Focus on Security Issues

In response to the recent OLA follow-up report on MnSCU Information Security issues, we are taking several key actions. We have created a new, high level technical security analyst position, which we plan to fill within the month. This position was created by moving an open position from the Systems Development group, and will significantly enhance our ability to make progress on the many highly technical aspects of information security. We also have formed a high level group of senior managers representing various disciplines who are integrating the planning of our activities related to regulatory requirements such as Gramm-Leach-Bliley, Information Security Awareness, and other related issues. This effort will enable us to develop and implement a comprehensive Information Security Program from a strategic viewpoint which is not focused solely on technology issues, but incorporates a broader, system-wide vision. Finally, we have contracted with a respected and experienced IT and business professional to help oversee the development and implementation (integrating the many individual elements we already have in place) of a Minnesota State Colleges and Universities Information Security Program. This significant increase in resources focused on making continued progress in information security will result in even great strides forward over the next year than the significant progress we have made over the last year.