

MnSCU INFORMATION SECURITY OFFICE CHARTER

PURPOSE

The mission of the Information Security Office is to deliver and maintain MnSCU's Information Security Program that safeguards information and system assets against unauthorized use, disclosure or modification, and damage or loss. The administrative responsibilities include establishing and maintaining a security organization, developing a cost-effective and integrated security program that supports the accomplishment of MnSCU goals and priorities.

SCOPE

The Information Security Program is an integrated program including Disaster Recovery, and information security for all MnSCU institutions and the System Office. Physical security is within the scope of the program as required to protect information technology assets. It is essential for the success of the security program that it is integrated with the following components: security awareness and training; policies, standards and procedures; risk assessment and analysis; monitoring and reporting; and enforcement.

GOALS

The MnSCU information security program foundation will be built on the Control Objectives for Information and Related Technology (COBIT) framework. We will use British Standard BS7799 as a technical reference and possible certification in the future. Within the framework of (COBIT), the goals are:

- No incidents causing public embarrassment
- Immediate reporting on critical incidents
- Installation of suitable environment and physical controls which are regularly reviewed for their proper functioning
- Alignment of access rights with organizational responsibilities
- Reduced number of new implementations delayed by security concerns
- Full compliance, or agreed and recorded deviations from minimum security requirements
- Reduced number of incidents involving unauthorized access, loss or corruption of data
- Cost-effective use of security countermeasures to achieve minimum security risk

BACKGROUND

The Chief Information Security Officer who reports to the MnSCU Chief Information Officer directs the Information Security Office located, within the Information Technology Services division. Although the Security Office is a central function of MnSCU, information security administration is distributed throughout MnSCU institutions requiring security administrators at each Data Center and with responsibilities delegated to a Director at each institution. Local area network system security is the responsibility of the campus CIO. The local campus CIO usually is the designated Security Director for the institution. MnSCU's WAN (wide area network) and the System Office's LAN security is the responsibility of Information Technology Services Division's Director of WAN. In addition, each business system on the campus requires a security coordinator, which has custodial responsibilities for data security. The business systems include financial, human resources and student records. These business systems have authorized designees responsible for system-wide data ownership. These functional areas of technology must be integrated into a comprehensive security program based on architecture that includes MnSCU's over-all security program.

An essential factor in the information technology architecture of MnSCU is the impact of administrative systems used by all institutions. The Integrated Student Record System (ISRS), the primary administrative system for MnSCU, will drive the system security architecture for an integrated security program. In addition, academic systems and web-based applications are significant components of the information technology architecture. Given the need for the users to access ISRS through local network and local applications, it is critical to the success of the security program that institutions' security policies, standards and procedures are consistent and follow system-wide standards for the protection of administrative and academic system data assets.

The following proposed security organization reflects the distributed functions and applications from the central security administration to the local responsibilities at each institution (see attachment A. Organizational Structure).

GENERAL RESPONSIBILITIES

All MnSCU employees have a responsibility to comply with information security policies, standards and procedures. A successful information security program requires all employees to be aware of security implications in the daily execution of their job duties. Given the integrated and system-wide features of our administrative and academic applications and our networks, we are particularly vulnerable to threats at many possible points of intrusion. The responsibilities for network (LAN and WAN) administration, Data Center management, and data ownership are major components of our information security infrastructure. The system can only be as strong as the weakest link.

Information Security Office

- Design, plan, maintain and manage information security program
- Manage and monitor Disaster Recovery
- Develop, recommend and promulgate security policies, standards and procedures

- Monitor and assess the effectiveness of the information security program including policies, standards, procedures, practices and results
- Manage and support the Information Security Steering Committee and coordinate with other ITS steering committees.
- Periodically report on the effectiveness of the Information Security Program
- Review, evaluate, and recommend information security requirements for information system applications (best practices).
- Coordinate information security plans and program actions with the ITS Leadership and management Teams, MnSCU Office of Internal Auditing, and Office of General Counsel
- Sponsor and provide information security training and awareness

Board of Trustees

- Establish general information system security policy foundation for MnSCU's Information Security Program
- Review the general effectiveness of the Information Security Program

MnSCU Chancellor

- Support establishment of policies and standards needed to protect the integrity of MnSCU information technology systems and data
- Establish and enforce information security policies, standards and procedures as delegated by the Board of Trustees

Chief Information Officer

- Ensure the security and protection of MnSCU's information assets through the successful planning, design and implementation of the Information Security Program

Information Security Steering Committee

- Review and recommend MnSCU system-wide information security policies, standards and procedures as a foundation of the Information Security Program
- Assess the cost effectiveness and quality of the Information Security Program
- Recommend information security principles and goals for the Information Security Program
- Review and recommend security needs and policies for MnSCU including requirements for proposed information system infrastructure and applications. This requires coordination with other ITS' steering committees and MnSCU's Information Technology Roundtable.
- Best Practice identification and advocacy role
- Coordinate security policy and standard development efforts with other ITS steering committees with specific focus on the Infrastructure and Administrative Steering Committees
- Review existing policies and recommend changes

Information Security Office Staff Responsibilities

MnSCU Information Security Officer

The Information Security Officer (ISO) directs the planning, implementation, and maintenance of the Information Security Program. Development of the Security Program for MnSCU requires setting information security goals and objectives that support the business needs of MnSCU. The ISO will develop and monitor security policies and practices to ensure that MnSCU's information systems and data are secure for unauthorized access, protected from inappropriate alteration, physically secure, and available to authorized users in a timely fashion. The ISO's duties include training in and dissemination of security policies and practices as well as developing strategies and plans to provide for timely business resumption in the event of serious disruption.

ISRS Security Administrator

- Monitor security policy and procedure compliance in computer center and data warehouse operations. Primary responsibilities are focused on data centers, ISRS, and MnSCU's Data Warehouse.
- Coordinate Data Center and Data Warehouse security audit reviews with internal and external auditors.
- End user security administration for ISRS, replicated database and data warehouse so that user access is managed within security policies, procedures, standards, and system availability is maintained at acceptable levels.
- Provide periodic reports on ISRS information security violations, vulnerabilities, and recommendations for changes to security policies, standards, and procedures.
- Provide technical assistance, coordination, training and security awareness, controls, policies, and procedures for campuses' Information Security Officers to ensure effective administration of end user access and controls for ISRS, Data Warehouse, replicated data bases.
- Campus Service Unit (CSU) user security administration for ISRS, replicated database and data warehouse so that CSU users access is managed within security policies, procedures and standards and system availability is maintained at acceptable levels.
- State wide security administration for System Office and Auditors, both internal and OLA for ISRS, replicated database and data warehouse so that these users access is managed within security policies, procedures, standards, and system availability is maintained at acceptable levels.
- Provide technical assistance, coordination of ISRS administration of new and or modified security screens as released from Quality Control into production.
- Administer High-level security rights as in Duplicate Resolution statewide.

Information Security Administrator

- Monitor and maintain Data Centers' Disaster Recovery Plans including periodic test and evaluations. Provide technical assistance to campus Security Directors on Business Continuity and Disaster Recovery planning.

- Participate in the design reviews, development and implementation of any new applications integrated or interfaced with ISRS and on-going enhancements and change releases to ISRS to ensure new applications will MnSCU's information security policies, procedures and standards.
- Develop and promote a system-wide Security Awareness and training program.
- Formulate and promulgate system-wide security standards and review relevant policies and procedures in context of these standards. Make recommendations for security policy changes for Security Steering Committee review.
- Plan, implement, and maintain a system-wide Computer Security Incident Response Team (CSIRT) and reporting system.
- Perform an annual performance assessment of MnSCU's information security program including written assessment report with recommendations for improvements

Network Security Administrator

- Monitor and assess LAN and WAN security program compliance and performance.
- Provide technical assistance and training to campus technical staff and business managers.
- Collaborate with and periodically lead a Computer Emergency Response Team (CERT) to in response to security and disaster incidents.
- Assist with the planning and implementation of the Security Office's Security Awareness and Training Program.
- Employ automated and manual tools to identify and demonstrate network security vulnerabilities.
- Assist with the evaluation, recommendation, and planned implementation of network security products (including virus protection), tools, and methodologies.
- Develop, evaluate, and recommend improvements on network (LAN and WAN) security standards, policies, and procedures.
- Monitor, assess, and report on firewall, router, and network operating system (access points) logs.

The purpose of this document is to describe and communicate the structure, responsibilities, and relationships of the MnSCU Information Security Office as a foundation for MnSCU security infrastructure. The document will be modified periodically to reflect changes and improvements in the security architecture and organization of MnSCU.