Metropolitan State University
Information Technology Department

2010 – 2012 Information Security Plan

I. Background

Ensuring the confidentiality, integrity and availability of valuable information and information assets at Metropolitan State University (MSU) is an ongoing concern of the Information Technology Services department. This has been expressed in the IT Mission and Strategic Plans in the past and will remain an important component of future planning. MSU faces a number of challenges due to its heterogeneous provision of information technology services, the need to support three user groups (faculty, staff, and students), and the need to provide secure access to information at all times. An Information Security Plan helps ensure structured management of threats to information assets and minimize disruptions to university operations.

II. Plan Development and Implementation

The Information Security Planning Team includes key ITS personnel and consulting support from Advance IT Minnesota (formerly Center for Strategic IT and Security, a MnSCU Center of IT Excellence at Metropolitan State University):

Information Security Planning Team	
Dawn Syverson	Associate VP for Information Technology & CIO
Tanya Buetow	Network Security Administrator
Garrett Lanzy	Director of Technical Operations
Firasat Khan	Security Project Manager, Advance IT Minnesota

To ensure that it accurately represents the needs and plans of the University, this Information Security Plan (ISP) is subject to review by the IT Advisory Committee and other University advisory and decision-making groups including the following:

University Offices and Groups
Advising Council
AFSCME President
Deans and Directors' Council
IFO President
IFO Technology Committee
MSUAASF President
Office Managers
President's Cabinet
President's Council
Student Senate

III. Key Drivers and Guiding Principles

Key drivers in managing information security at MSU include risk tolerance, asset protection, vulnerability management, and threat mitigation. In order to take a comprehensive approach, existing policies and procedures, mission and plan, and evaluation of existing infrastructure and business processes were considered.

Therefore, the ITS department has developed this Information Security Plan in alignment with the following:

- Information Technology Mission Statement – *Ensure timely and efficient access to information.*
- 2005 – 2007 IT Strategic Plan, Strategic Direction B. 3. *Promote, coordinate, and ensure data integrity initiatives.*
  - *Promote and improve data procedures via web-based activities.*
  - *Better educate users in their responsibilities related to university data.*
- 2005 – 2007 IT Strategic Plan, Strategic Direction C. 2. *Provide secure, satisfactory and dependable IT services.*
  - *Improve backup and disaster recovery procedures.*
  - *Adopt and implement security measures as required by MnSCU.*
- Establish a plan that supports information security-related policies and procedures.
- Identify, assess and mitigate risks to University information assets as discovered through internal and external assessments and evaluations.
- Ensure continued compliance with applicable laws and regulations.

IV. Information Security and Assurance Goals and Objectives

The Information Technology Services department through its staff provides leadership to the University community in safeguarding the confidentiality, integrity and availability of information and computing assets. The department provides strategy definition, security threat assessment, standards development, communication & training, and investigation of threats & incidents.

V. Information Security Plan – Strategic Objectives

Objective 1 – Assess: Evaluate MSU's information security posture periodically to address vulnerabilities, threats and risks related to information access, storage and transfer.

Objective 2 – Prevent: Utilize appropriate loss prevention methods and tools to minimize potential for loss of information assets or disruption of services.

Objective 3 – Manage: Utilize appropriate loss control methods to manage incidents, handle investigations, minimize disruptions and ensure business continuity.

Objective 4 – Minimize Financial Impact: Utilize risk deferment and minimization methods and tools do minimize financial impact of incidents.

VI. Information Security and Assurance Initiatives, Efforts and Practices

Below is a description of activities and initiatives undertaken by the Information Technology Services department in alignment with the four strategic objectives:

Information Security Assessments (ISP Objective 1) –

The University Network Administrator will work to identify potential and actual risks to security and privacy of information across the University. Cabinet members are responsible for identifying all employees in their respective areas who work with data and information that is covered by FSMA, FERPA, or other applicable regulations. Cabinet members will also be responsible for ensuring that appropriate department-level policies and procedures

are documented and current and that employees are knowledgeable about specific procedures for their departments.

In addition, Information Technology Services will work to educate the broader campus community about network security and privacy issues; will publish summaries of findings and "best practices," except in those cases where publication could lead to breaches of security or privacy. Information Technology Services will assure procedures and responses appropriately reflect practices utilized and authorized throughout the MnSCU system and align with standard information security best practices and guidelines.

While Information Technology Services is responsible for the identification of internal and external risk assessment, all members of the university community have a shared responsibility for risk assessment. Technology Services, working in conjunction with the relevant departments and offices, will conduct regular risk assessments and policy reviews.

As a member of the MnSCU system, the university will participate in security assessments offered through the Minnesota State Colleges and Universities (MnSCU) Information Security Program which include:

The Information Security Assessment Program which is one component of a larger, comprehensive. The objective of the Information Security Assessment Program is to gain an understanding of the current campus security practices and posture surrounding **private** digital data. The Program was developed with a goal of improving the system-wide information security posture of all MnSCU institutions, including the Office of the Chancellor and enterprise applications such as the Integrated Statewide Records System. Specifically, the appraisal performed at each campus seeks to identify technical and operational controls around the handling and safeguarding of private data and the systems that host and utilize that data.

Recommendations from this assessment will be used to identify areas for potential improvements and to help guide policy and process development.

Office of the Legislative Audit (OLA) PCI compliance audit: The Office of the Legislative Auditor concluded a campus audit to identify potential issues related to PCI compliance. Specifically issues related to the security of stored paper documents and security of electronic storage of credit card information. While the university had a level B audit which indicated no findings that required additional follow-up or review, information provided through this assessment will be used to ensure no new systems are added to that will violate PCI compliance in the future.

Vulnerability Scanning: The University utilizes an nCircle device for network vulnerability scanning. nCircle is the industry-leading vulnerability management solution which gathers comprehensive endpoint and network intelligence and applies advanced analytics to identify and prioritize the vulnerabilities that pose the most risk to critical systems. The nCircle solution is used to discover and identify all networked assets, internally and on the network perimeter and assessing all systems for vulnerabilities and system configurations for compliance deviations. The results enable the IT security team to focus on the tasks that will most quickly and effectively reduce overall network risk with the fewest possible resources.

Anti Spam/Anti Virus Solution: The University utilizes a combined Anti-Spam/Anti-Virus solution operated by the Office of Enterprise Technology called Secure Mail (Iron Mail). This system protects all state mail (messages sent to the domain @state.mn.us addresses), mail sent to state agencies that use other domains (including metrostate.edu), and mail for many other customers. IronMail uses several techniques to identify spam, including source e-mail server "reputation" and e-mail content inspection.

Policy and Procedures (ISP Objective 2)
MSU has implemented a number of policies and procedures and the Information Technology Services Department will continue to support the evaluation and enhancement of these as needed. Current university policies and procedures containing content related to information security are:

- Section I - a: University-wide Policies
  - 1020 - Student Conduct Code:
  - 1030 - University Community Conduct Code
  - 1040 - Data Privacy
  - 1050 - University E-Mail Policy
  - 1100 - Employee Right to Know
- Section I - b: University-wide Procedures
  - 111 - Principles of University Administration and Procedures for Review of Administrative Operations
  - 112 - Student Conduct Code Procedure
- Section II - a: Academic Affairs Policies
  - 2110 - Intellectual Property and Electronic Courses
- Section IV - a: Administrative Affairs Policies
  - 4050 - Computer Assignment and Replacement Policy
  - 4060 - Web Policy
  - 4120 - Cellular Phone Acquisition and Usage
- Section IV - b: Administrative Affairs Procedures
  - 400 - Guidelines for Administrative Procedures
  - 401 - Building Security
  - 412 - Cellular Phone Acquisition and Usage

Communications and Training (ISP Objective 2)

While department directors and supervisors are ultimately responsible for ensuring compliance with information security practices and providing department-specific and function-specific training, Information Technology Services and Human Resources will continue to provide broad-based training and education programs for all employees who have access to covered data. In addition, specialized training and workshop sessions will be conducted for professionals in information technology who have general access to all university data.

Current Training Initiatives:

- Students are provided information on the code of conduct policy and procedures at university orientation sessions. When accounts are created for systems access, they are also provided a copy of the MnSCU Acceptable Use policy and the University Email policy and are required to indicate their acknowledgement of these policies prior to the account creation being completed.

- Faculty/Non-ITS Staff have been provided online training from MnSCU regarding code of conduct and data security awareness. When accounts are created for systems access, they are also provided a copy of the MnSCU acceptable use policy and the University Email policy and are required to indicate their acknowledgement of these policies prior to the account creation being completed.
- ITS Staff has been provided the same training as other university staff and has also been provided additional security training courses offered by MnSCU specifically related to their role in IT. Systems security is regularly discussed at staff meetings and through professional development opportunities selected by the staff or their managers.

Information Technology Services staff strive to use communications and training tools, services and methods to further the information security and assurance mission.

Communication Methods:

- Information Technology supports policies & standards through leadership discussions at various university committees; email communications on a regular basis and sharing information via the university Safe Computing and Information Assurance web site.
- Informational materials, which includes an informational library hosted by the information security staff containing pamphlets, flyers and informational packets, as well as, regular communications via the IT Happens Newsletter published electronically bi-monthly.
- Regular security reminders and articles are published in the university portals to help educate and inform the university community about security related issues, incidents and best practices.

Technical and Physical Security Solutions (ISP Objective 2)
ITS has continued to use technical solutions to address internal and external threats to information and computing assets. Some of the key approaches are:

- **Service Packs, Patches, and Upgrades:** Information Technology Services assumes the responsibility of assuring that patches and service-level releases for operating systems or software environments are up to date, and will keep records of patching and upgrade activity. ITS will review its procedures for patches and service-level upgrades to operating systems and software, and will keep current on potential threats to the network and its data. Risk assessments will be updated quarterly.

- **Encryption:** Information Technology Services will develop a plan to ensure that all covered electronic information is encrypted in transit and that the central databases, servers and backup tapes are strongly protected from security risks.

- **Virus Protection:** Information Technology will maintain anti-virus, anti-spyware and host intrusion protection software on all university owned equipment. Updates to individual desktop and laptop machines will be provided through automatic updates and user responsible for ensuring these updates are not disabled in any way and are to report any problems or issues with these updates running on their individual workstations to the ITS staff through the regular reporting channels. Information Technology Services will

also maintain licensing and distribution methods for anti-virus and anti-spyware software for home use by the university community and will encourage its use through regular communications and user education.

Information Technology Services will maintain anti-spam/ anti-virus solutions to protect the campus against the annoyances and productivity-stealing aspects of bulk-unsolicited email "advertisements" called spam and to protect against the spreading of viruses and malicious software via the university email systems.

- **Security Response:** Information Technology Services will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

- **Physical Security:** Information Technology Services is responsible for physical security of all central servers that contain covered data and information. ITS will work with other areas of the university to develop guidelines for security of any covered servers in locations outside the central server area which are maintained by staff other than Information Technology Services staff or that are maintained by third-party service providers.

  ITS will work closely with the university Safety and Security Officer to identify potential areas of risk related to physical security of equipment and technology. Current security measures include the use of IP cameras, barrier protection through limited key and punch code access, review and identification of staff access rights on a yearly basis, providing additional locked storage for smaller items, installing security cables where appropriate and utilization of encryption software on all university-owned laptops to protect information in the event of theft.

Systems Access and Authorization (ISP Objective 2)

- **Network Access:** In order to protect the security and integrity of the university network and its data, Information Technology Services maintains a registry of all personnel with account and log-in privileges. ITS will work with departmental directors, supervisors and Human Resources to ensure system access and security accounts are removed promptly upon employment termination. Student account access will be compared on a term-by-term basis to identify students who are no longer affiliated with the university, and rights will be removed per university guidelines related to student admission.

  The university will utilize industry standard firewalls for intrusion prevention, the ability to create protection zones within the university, limiting peer-to-peer file sharing traffic and wireless access control.

- **Student Records System (ISRS):** Information Technology Services, working in cooperation with relevant departments and MnSCU security administrators, will maintain a list of those persons ("module leaders") responsible for each covered data area in relevant software systems (financial, student

administration, development, etc.). These module leaders are responsible for approving and assigning system rights based on job roles and responsibilities. Information Technology Services and the relevant departments will conduct ongoing (at least annual) audits of user system rights.

- **Password Control and Maintenance:** Information Technology Services will implement technology solutions and utilize industry standards for ensuring password strength and regular password maintenance. ITS will also work to educate the university community on issues related password protection and risk mitigation.

Loss Management and Recovery (ISP Objective 3)
ITS uses a considered approach to respond to a wide array of potential information security incidents, whether they are technical or personnel-based. ITS strives to minimize downtime in the event of small incidents or major disruptions.

Avoidance or Minimization of Financial Impact (ISP Objective 4)
ITS works with vendors and external business partners to minimize financial impact to MSU in the event of information security-related incidents. This is done through an array of approaches varying from service level agreements to insurance and the The VP for Finance and Administration and CFO, Associate VP for Technology & Telecommunications and CIO and the Director of Finance will take steps to ensure that all relevant contracts include a privacy clause and that all existing contracts are in compliance with Federal and MnSCU standards, guidelines and procedures.

VII. Roles and Responsibilities

University staff in various roles help focus efforts information security and assurance efforts within the Information Technology Services department and with external stakeholders as necessary.

Service and Support Areas	Roles
Leadership	CIO Director of Technical Operations Network Security Administrator
Network	Network Security Administration Network Analyst Network Administrator
Student	Help Desk Staff (3) University Registrar Vice President of Student Affairs Director of Student Affairs Director of User Services
Staff/Faculty	Help Desk Staff (3) Human Resources Director Director of User Services
Applications/Web	Director of Information Services Web Developers (4) Data Analyst
Communications and Training	CIO Director of User Services

	Director of Technical Operations Network Security Administrator
Physical Security	CIO Network Security Administrator Director of Safety and Security Desktop Support Technicians (4)

VIII. Concluding Statement

This Information Security Plan is subject to periodic review and adjustment. The most frequent of these reviews will occur within Information Technology Services with input and recommendations from the IT Advising Council. Processes in other relevant offices of the university, such as data access procedures and training programs, will undergo annual review. The plan itself, as well as the related data retention policies, will be reevaluated annually to assure compliance with existing and future laws and regulations. Timing of this review should occur as part of the annual external audit.

Over the course of 2010-2012 the goal is to gather additional input from the university community on this plan regarding any missing components or areas needing further clarification or refinement. The Information Technology Services management team will also work to document activities related to and in support of this plan which will highlight activities completed, technology implemented and areas needing to be yet addressed and will share that information for input and review within the university leadership and governance structure.

Dawn Syverson
Associate VP of Technology and Telecommunications & Chief Information Officer
Metropolitan State University
January 2010