

**MINNESOTA STATE COLLEGES AND UNIVERSITIES  
BOARD OF TRUSTEES**

**Agenda Item Summary Sheet**

**Committee:** Technology Committee

**Date of Meeting:** June 22, 2011

**Agenda Item:** Information Security Program Review

Proposed  
Policy Change

Approvals  
Required by  
Policy

Other  
Approvals

Monitoring

Information

**Cite policy requirement, or explain why item is on the Board agenda:**

This report will provide the Trustees with information about the security program.

**Scheduled Presenter(s):**

John Hoffoss, Information Security Specialist

**Outline of Key Points/Policy Issues:**

**Background Information:**

The Board of Trustees requested a security program update at the May meeting.

**BOARD OF TRUSTEES  
MINNESOTA STATE COLLEGES AND UNIVERSITIES**

<b>INFORMATION ITEM</b>
Information Security Program Review

**BACKGROUND**

During the May Board meeting, Trustees asked several questions about the systems security program. John Hoffoss will present the following Security Program Review.



Minnesota  
STATE COLLEGE  
UNIVERSITY

# Information Security Program Review

**Board of Trustees Technology Committee Presentation**

**Presenter: John Hoffoss**

**Date: June 22, 2011**



Minnesota  
STATE COLLEGE  
UNIVERSITY

## Overview

- Request for More Information
- Information Security Drivers
- Program Components
- Current Information Security Projects



Minnesota  
STATE UNIVERSITY  
MANKATO



## Program Drivers

Threats constantly shift and change rapidly.

Slide 3



Minnesota  
STATE UNIVERSITY  
MANKATO

“ Information Security is to IT what yellow caution labels are to ladders. Because the users are the same in either case. -- Sam Liles (@selil on Twitter)



## Program Drivers

Technology changes nearly as fast as threats.

Slide 4



Minnesota  
STATE COLLEGE  
AND UNIVERSITY



## Program Drivers

Audit, Regulations, and Law



Slide 5



Minnesota  
STATE COLLEGE  
AND UNIVERSITY

## Information Security Program Mission

Support the System's strategic directions by protecting information resources against unauthorized use, disclosure, modification, damage or loss.

Slide 6



Minnesota  
STATE COLLEGE  
AND UNIVERSITY

## Information Security Office

Information Security Program

Leadership & Governance

**Goals**  
Protect Information Resources

Information Risk Management

Mitigate Risks

Security Lifecycle

Promote Security



Slide 7



Minnesota  
STATE COLLEGE  
AND UNIVERSITY

## Leadership & Governance

- Governance
  - Enterprise Information Security Steering Committee
  - Board Policies, Procedures & Guidelines
- Compliance
  - Payment Card Industry Data Security Standard
- ITS Audit Findings
  - Tracking and responding to IT-related audit findings

Slide 8



Minnesota  
STATE COLLEGE  
AND UNIVERSITY

## Information Risk Management

- Information Risk Management
  - Formalizing risk assessment process
  - Third-party vendor risk assessment tool
  - On-campus Visits with Institution CIOs
- Security Awareness Training
  - Broad training for end-user security awareness
  - Includes training on social engineering, phishing, and other common threats
- Data Center Penetration Testing
  - Addresses several audit findings

Slide 9



Minnesota  
STATE COLLEGE  
AND UNIVERSITY

## Security Lifecycle

- Application Security Program
  - Driven by Software Security Task Force
  - Secure Software Development Standards, Training and Tools
- Software & Hardware Security
  - Vulnerability and Patch Management
  - Secure File Transfer
- Incident Response
  - Support campus staff in resolving viruses, breaches, and other activities that derail operations

Slide 10



Minnesota  
STATE UNIVERSITY  
www.mnstate.edu

## Information Security Program

Leadership & Governance

Information Risk Management

Security Lifecycle

### Review

Proactive

Standards-based

Collaborative

Strategies, Tools,  
Services

Promote Security

Throughout

Information Lifecycle



information  
**SECURITY**

Slide 11



Minnesota  
STATE UNIVERSITY  
www.mnstate.edu

## Information Security Program

Leadership & Governance

Information Risk Management

Security Lifecycle

Planning

Risk Assessment

Asset Management

Secure Development

Program Management

Security Architecture

Access Control

Procurement

Compliance

User Access Management

System Protection

Operate & Maintain

Metrics

Awareness & Training

Contingency Planning

Incident Response

Slide 12