

# ITS Policies & Procedures

<b>Procedure Name:</b> Information Security Incident Response and Notification Procedure	<b>Temporary Review Number:</b> N/A
<b>Classification:</b> Information Technology Services	<b>Supersedes:</b> N/A
<b>Author:</b> Kevin Thompson	<b>Last Review:</b> April, 2007
<b>Authority:</b> MnSCU Standard 5.23.E	<b>Next Review:</b> April, 2008
<b>Application:</b> All University	<b>Effective Date:</b> April, 2007
<b>Distribution:</b> All University	<b>Custodian of Policy:</b> ITS

## PROCEDURE FOR RESPONDING TO INFORMATION SECURITY INCIDENTS:

### Designation of Lead Campus Authority (LCA).

In accordance with MnSCU ITS Standard 5.23.E titled “Notice of Breach of Security,” Minnesota State University, Mankato has designated the Chief Information Officer to serve as the Lead Campus Authority(LCA) when investigating and reporting breaches of information security on campus. The LCA may choose to delegate any function of this role to other qualified persons.

### Reporting a suspected incident.

Pursuant to Minnesota Statute section 13.055 and MnSCU ITS Standard 5.23.E titled “Notice of Breach of Security” any employee of the university that suspects that there has been unauthorized access to or use of university computer systems or that private data may have been lost or stolen must immediately notify his or her supervisor. In addition, any employee that believes that university computer systems have been used to commit a crime or may contain evidence of criminal activity must immediately notify his or her supervisor. Students that suspect unauthorized access to private data or criminal misuse of computer systems should contact campus security. The supervisor or security officer should immediately contact the LCA who will make arrangements for the reporting person to be interviewed. The LCA or designee will contact the data custodian and other departments that need to be made aware of the incident.

- If the security breach involves Information Technology then the LCA or designee will notify the Information Security Manager.
- If the security breach may be linked to a criminal act then the LCA or designee will also notify Campus Security by calling extension 2111.

### Initial Incident Response Process.

After a suspected security incident has been reported to the LCA or designee, he or she will begin creating a detailed accounting of the incident. Notes and supporting documentation should be recorded to the extent that an external auditor could completely reproduce the work of the LCA or designee. The LCA or designee will interview the person reporting the suspected breach and gather notes about the incident, including when it was noticed, how it was noticed, the nature of the information lost, and the scope of the loss (if any). This person will also work with the data owner and any other persons relevant to the suspected breach. Based on these initial findings, the LCA or designee will either conclude the investigation or proceed with the incident response procedure.

### Initial Mitigation Process.

If the security incident results in an ongoing loss of data, then the LCA or designee will work with the Information Security Manager and other members of the ITS department, Campus Security, and IT personnel in the Office of the Chancellor to end the security incident by putting control measures in

place, such as closing down firewall ports, locking out Active Directory accounts, powering down equipment, removing the computing system from the campus network, and physically securing the device if necessary.

#### **Working with Law Enforcement.**

The LCA or designee will consult with Campus Security, the Data Practices and Compliance Officer, Department of Integrated Marketing, and the MnSCU Office of General Counsel before contacting law enforcement agencies if the security incident is believed to involve illegal activities. Information may be shared with law enforcement consistent with applicable data privacy laws. Law enforcement agencies should be informed of the university's incident response and notification procedure when contacted. In some cases, law enforcement officials may present a warrant or subpoena to gather non-public data. Warrants and subpoenas should be reviewed by the Data Practices and Compliance Officer before turning over any non-public data.

#### **Concluding the Investigation.**

The LCA or designee will work with the Information Security Manager and other members of the ITS department, Campus Security, MnSCU Office of General Counsel, and IT personnel in the Office of the Chancellor to create a complete report of when the incident happened, what was the root cause of the incident, what was lost, who was affected, and how this event can be prevented in the future. The LCA or designee will keep detailed records of phone conversations and face to face discussion, and archive any relevant email, log files, and other potential evidence. This group will also review the incident response and notification procedure to ensure that it adequately addressed the situation and update the procedure where appropriate.

#### **Notifying Affected Persons.**

The LCA or designee will work with the Information Security Manager, the Data Practices and Compliance Officer, the Department of Integrated Marketing, and the Office of General Counsel to determine if a notification is required. If notification is required these offices and departments will work together to determine which persons need to be notified, the method by which they will be notified, the wording of the notification, and who will send the notification. The university will strive to provide notification within ten business days of determining that notification is required, however notification can be delayed if necessary for law enforcement purposes or for internal investigation of the security incident.

#### **Internal Disciplinary Action.**

If the security incident involves student or employee misconduct then the LCA or designee will refer the matter to the Human Resources office or the Office of Student Rights and Responsibilities.

#### **Record Retention.**

The LCA or designee will retain copies of all notes, records, notifications and other information relevant to the incident in accordance with the record retention policy.

#### **Authority for Procedure:**

**Minnesota State Colleges and Universities ITS Standard 5.23.E: Notice of Breach of Security**

<http://its.mnscu.edu/security/breachnotification/breachnotifystandard523E.pdf>

**Minnesota Statute Section 13.055: Disclosure of Breach in Security**

[http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT\\_CHAP\\_SEC&  
%20year=current&section=13.055](http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP_SEC&%20year=current&section=13.055)