Policy: Information Technology Security
Document: Incident Response Standards & Procedures
Campus: MSU-Northern
Revised Date: April 2023
Review Date: April 2025
Contact: Chief Information Officer

These standards establish procedures for reporting security incidents response for MSU-Northern policy 1310 Information Technology Security. These procedures apply to information systems, regardless of ownership or location, used to store, process, transmit or access MSU-Northern data as well as all personnel including employees, students, temporary workers, contractors, those employed by contracted entities and others authorized to access MSU-Northern assets and information resources.

This procedure is to be used by any user reporting an incident, including outside sources when applicable.

What is an information technology security incident?

A Security Incident is a violation of computer security policies, acceptable use policies, or standard computer security practices. An "IT security incident" could:

- Result in misuse, exposure or compromise of confidential information of an individual (examples: social security number, grades, financial transactions, etc.).
- Jeopardize the functionality of the university's IT infrastructure.
- Provide unauthorized access to University resources or information.
- Impede or halt authorized use of a systems.

Some examples of Information Security Incidents include:

- Viruses, spyware, or other malicious programs found on your computer.
- Any attempts to break into your computer over the network.
- Any unauthorized disclosure of sensitive information stored on a computer.
- The loss or theft of a laptop containing University data.
- Phishing attempts.

Security Incident Response Procedures

The IT Security Incident Response Procedures outline steps to be followed in the event of a security incident such as a compromised system, a suspected virus, ransomware, unauthorized access, or exposure or leakage of sensitive data.

All members of the university are responsible for promptly reporting any suspected or confirmed security incident involving MSU-Northern data or an associated information system, even if they have contributed in some way to the event or incident.

In order to preserve as much of the volatile evidence as possible, do as few things to the affected system as possible before Information Technology Services can image the system for analysis:

- Do not shut down the computer.
- Do not try to log in to the computer.
- If possible, leave the computer online unless:
    - You believe that data is actively being taken off from the system.
    - You believe that the system is attacking, or being used to stage attacks on other systems.

The person identifying a suspected IT security incident should *immediately* notify the ITS Helpdesk at (406) 265-3765, https://helpdesk.msun.edu, helpdesk@msun.edu, or by visiting the Help Desk in Cowan Hall 117.

The following information should be conveyed to the helpdesk team:

1) Name(s) of the faculty, staff, or student reporting the incident and contact information;
2) a description of the incident that is believed to have occurred (examples: unauthorized use or access; data exposure or leakage; misuse of IT resources; malicious code);
3) a brief description of how the incident was detected;
4) the physical location and purpose of the system(s) that has been impacted (desktop, lab computer, web server, etc.) ; and
5) Whether or not the system(s) contains "confidential" or "restricted" data.
   Examples: social security numbers, financial account numbers, driver's license numbers, health insurance policy ID numbers, protected health information, student ID numbers, etc. (see Data Stewardship Standards for more information on data classifications)

The Helpdesk staff shall then escalate the ticket to the Chief Information Officer (CIO) who organizes the systems and network administration team to begin investigating the incident.

Misuse of access to MSUN's networks, systems, data, and unusual employee behavior such as copying or researching information unrelated to their job can also be reported anonymously through the MUS Compliance Hotline.

MSU-Northern reserves the right to update or revise these standards or implement additional policies and procedures in the future. Users are responsible for staying informed about and compliance with University policies and procedures regarding the use of computing and communication technology.