Michigan Technological University
Information Technology

Incident Response Procedure

Purpose

This document describes the procedures that should be followed by an individual reporting an incident related to information technology resources. Having an effective incident response is essential in mitigating damage and loss due to an information security incident. Proper handling of such incidents protects the University's information technology resources from future unauthorized access, use or damage.

Scope

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

What is an 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 of confidential information (social security number, grades, health records, financial transactions, etc.) of an individual(s).
- Jeopardize the functionality of the University's IT infrastructure.
- Provide unauthorized access to University resources or information.

Examples of Information Security Incidents include:* Hacking a University system

- Using University IT resources to hack into any non-University computer system
- Using University IT resources to harass or threaten someone
- Suspecting that a machine has been infected with a virus or worm that may lead to data leakage (keystroke logger, password cracker, etc.)
- The loss or theft of a laptop containing University data

Why is reporting an incident important?

An IT related incident could have many consequences for the University. For example:

- Much of the personal information held by the University is covered by external laws and regulations that require proper incident response to ensure that an individual's data is not compromised.
- The intellectual property of the University is valuable.
- The general health of the University resources needs to be maintained

What to do if you suspect an incident has occurred

Please keep in mind: The primary thing that we are trying to accomplish in response to an incident is to preserve as much of the volatile evidence as possible. Because of this we want to do as few things to the affected system as possible before we can image the memory for analysis.

Steps in response to an incident

- 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.
- Contact your support staff to assist with the incident.
    - The help desk can be reached at 7-1111.
    - The IT Security hotline can be reached at 7-0099.
- The individual reporting the incident, or the support staff will need to send as much of the following information as can be gathered to incident@mtu.edu. All of the information may not be easily identifiable in which case you can just list it as N/A and the response team will work on determining it.
    - The name of the detector of the incident along with methods of contact
    - The names and contact information of any other individuals involved with the incident
    - The name and IP address of the computer
    - The physical location of the system
    - The type of incident that is believed to have occurred.
    - Denial of Service
        - Unauthorized Use or Access
        - Compromise of University Data
        - Misuse of IT Resources
        - Malicious Code (viruses or worms)
        - Other
    - A brief description of how the incident was detected

- The purpose of the system (desktop, lab computer, web server, etc.)
- How critical the system is believed to be to University business
- If the system contains "private" data, the type of data it contains (SSNs, credit card information, student grades/addresses, medical information, governmental research data, etc.)

After reporting the incident the response team may contact you for further information. They will be dispatched to analyze the system to determine the extent of the compromise, the potential breach of data, and to clean up the problem.

END OF DOCUMENT
Rev 9/20/16