INFORMATION TECHNOLOGY PROCEDURES

INFORMATION AND TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

Procedure number:	P-01
Procedure title:	**ITS SECURITY INCIDENT RESPONSE PROCEDURE**
Date issued:	May 1,2012
Date last reviewed:	August 25, 2016
Version number:	2.0
Approval authority:	Chief Information Security Officer
Responsible office:	Information and Infrastructure Assurance

Table of Contents

I. Overview

This document describes the Information and Technology Services (ITS) process for reporting and responding to an information security incident. It specifies appropriate incident response actions based on the nature and severity of the incident, the data involved, and other factors. This process is a unit-level implementation of the *Information Security Incident Reporting* (SPG 601.25) and the *Information Security Incident Management Guidelines for University Units.*

This process applies to information security incidents relating to all data networks, network hosts, applications, workstations and servers managed by ITS. It also applies to computers and devices not administered by ITS, but which are used by ITS employees or other associated individuals to access information resources managed by the university.

Information security incidents covered under this procedure meet the definition of information security incidents in SPG 601.25.

ITS Service Management (ITSM) is responsible for incident processes related to a significant deterioration, degradation, or disruption of an ITS business process or service (detailed information is available at https://backstage.its.umich.edu/policies/business). IIA is responsible for incident processes, running in parallel to the ITSM process, related to significant security incidents. While investigating a particular significant incident, it may become evident or there may be indications that the source or origin is IT security-related. Examples of security-related incidents include: unauthorized access to systems or data; loss or theft of equipment; a denial of service attack; or intentional interference with the intended use of an IT resource. IIA is responsible for handling, centrally tracking, and investigating all security incidents within ITS. During a significant incident, if ITS staff suspect that an outage or service disruption may be security-related, the ITS Security Incident Response Process should be followed. The significant incident coordinator will report the incident to security@umich.edu as promptly as possible. If it is determined that the incident is not IT security-related, IIA will discontinue its participation in that significant incident process.

II. Purpose

The goals in managing an incident are to:

A. Collect as much information as possible about the nature of the incident;
B. Block or prevent escalation of the damage caused by the incident, if possible;
C. Repair, or coordinate the repair of, damage caused by the incident;
D. Preserve evidence of the incident, as appropriate;
E. Restore service as soon as possible;
F. Ensure that incidents are promptly reported and escalated per SPG 601.25;
G. Take proactive steps to mitigate future incidents.

III. Definitions

A. **Information Security Incident**: As defined in SPG 601.25, an information security incident tis an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied responsible use policy (as defined in SPG 601.07). Examples of information security incidents include (but are not limited to):

1. Computer security intrusion
2. Unauthorized use of systems or data
3. Unauthorized change to computer or software
4. Loss or theft of equipment used to store private or potentially sensitive information
5. Denial of service attack
6. Interference with the intended use of information technology resource

7. Compromised user accounts

B. **Information Security Roles and Responsibilities:**
ITS has the following information security roles:

1**. Information and Technology Services (ITS) Staff:** As service owners and users of IT resources, ITS staff is expected to recognize potential security incidents. Responsibilities include:

a. Promptly reporting all security incidents to security@umich.edu before taking any remediation steps;
b. Working with Information and Infrastructure Assurance (IIA) to follow this ITS Security Incident Response Process. This includes checking with IIA *prior* to communicating with any external unit or department about issues or problems that may have security-related components;
c. Incident information is considered sensitive data and should be appropriately protected;
d. Ensuring incidents are promptly reported to management and appropriate business owners as appropriate;
f. Incidents involving suspected child pornography should be reported directly to the Department of Public Safety and Security (DPSS).

C. **Information and Infrastructure Assurance (IIA):** IIA is the team of IT security professionals within ITS assigned to handle the information security needs for ITS. Responsibilities include:

1. Receiving notification of detected or reported information security events and incidents from users and service owners of IT resources, automated detection systems, or other sources.
2. Maintaining security@umich.edu as the mailbox to report all security incidents within ITS.
3. Accepting, logging, and tracking all security incidents. Information about security incidents will be retained for five years.
4. Executing incident mitigation and containment actions.
5. Providing expert technical advice and guidance.
6. Forwarding discovered incidents that did not originate within ITS to the appropriate unit.
7. Identifying post-incident security training and mitigation needs.
8. Coordinating all incident-related communications, including to senior management, business process and service owners, ITS staff, and external units such as the Office of Public Affairs.

IV. Procedure

The IIA team will follow the Incident Response Procedure and capture all relevant data. This data will then be aggregated and stored in a secure tracking system.

The following steps need to be taken in response to an incident. Although they are listed in a typical order, some steps may be taken concurrently or in a different order, depending on the circumstances. Further, the incident information logged throughout the incident may need to be updated periodically, and specific information, such as severity level, may change as further analysis is performed.

A. Initial Report and Assignment

1. Initial Event Notification: An information security incident begins when a security-related event is reported. This could come from an automated system diagnostic, a trouble ticket submitted by a user, or other source. Security incidents should be sent to security@umich.edu. The ITS staff reporting the incident should not take any containment steps before reporting the incident. The person on the IIA team who receives the initial notification opens an incident log in the tracking system (with a unique incident identifier) and adds available details, including some preliminary assessment of the incident severity, if it can be immediately determined

2**. Assign Incident Administrator:** The incident is assigned to an incident administrator, a member of the IIA team who is responsible for investigating the incident and coordinating the response until the incident is resolved and closed. When an incident administrator has been confirmed, that individual will promptly contact the person who reported the incident.

3**. Detail Incident Log Entry in IIA:** Tracking system Incident documentation should include the data fields found in the *Information Security Incident Management Guidelines for University Units*. Use the table below to clarify the data fields that are to be initially provided. This information should be entered and updated as necessary in the tracking system.

Information to be Documented	Description/Note
Date of event	
Time of event	Including time zone
Who or what reported the event	Include full name, location, telephone number, and email of person reporting the incident. If an automated system reported the event, include the name of software package, name of the host where the software is installed, physical location of the host, host or CPU ID of the host, network address of the host, and MAC address of the host if possible.
Detailed description of the event	Include as much information as available.
Identification of the host(s)	Specify the host or system that the event is related to/occurred on. Include the hardware manufacturer, operating system type and version, name of the host, UM asset ID tag, physical location of the host, host or CPU ID of the host, network address of the host, and MAC address of the host if possible.
Names or Descriptions of Others	If the event involves suspicious modifications or behavior of a computer that is accessible to many people and a person is reporting the incident, then ask the person for the names or descriptions of others in the area prior to and just after the event.
Physical Security Controls	If there is limited physical access to the computer, document the physical security controls that limit access (ask the person reporting the event to describe what they have to do to access the computer).

B. Notification and Escalation

There are many factors to weigh in determining appropriate notification and escalation of an incident, including the severity of the incident, the scope of the compromise, cost to the university of supporting a criminal investigation, and the proprietary and confidential university information that might become public if a criminal investigation occurs. When evidence shows that ITS has been victimized by a computer or communications crime, a thorough investigation usually involving law enforcement must be performed. In coordination with appropriate ITS staff, IIA will conduct a forensic investigation when necessary. The incident administrator takes the following steps:

1. Review and verify incident documentation, event reports and information entered in the Incident Tracking System;
2. Verify the assigned severity level based on available information;
3. Acquire the resources necessary to respond to the incident;

4. Notify the University Incident Response Coordinator of any serious incidents;
5. Notify the HIPAA Compliance Officer of all incidents involving PHI;
6. Notify UMOR of all incidents involving human subjects' personal information;

7. Participate in a Computer Security Incident Response Team (CSIRT) that may be convened relating to a serious incident in ITS.

C. Severity Assessment: The *Information Security Incident Management Guidelines for University Units* define two severity levels for information security incidents: serious and non-serious. For serious incidents, the owner(s) or operator(s) of the affected hosts should be directed not to use or modify the system in any way until the incident administrator contacts them and instructs them to do so. Examples of non-serious incidents include a malware infection on a workstation that does not contain sensitive information, a compromised web-server that is not mission-critical, or a stolen laptop that does not contain sensitive information. IIA will prioritize responding to serious incidents over non-serious incidents.

1. **Non-serious Incidents**: Once the incident has been classified as a non-serious incident, the following procedure will be pursued. The incident administrator classifies the incident severity based on the following:

a. Sensitivity of potentially compromised data
b. Legal issues
c. Magnitude of service disruption
d. Threat potential
e. Expanse – how widespread the incident is
f. Public engagement – level of potential public interest or concern

i**. Containment:** The incident should be contained as quickly as possible, pending further investigation by IIA. The Incident Response Coordinator and the incident reporter will devise a plan to contain the incident. In most cases this can be accomplished by removing the network cable of a suspected compromised system. In the case of a serious incident, do not remove the network cable as this removes the option of performing more invasive forensic monitoring of an intruder.

ii**. Analysis:** The Incident Response Coordinator will work with the appropriate ITS IT end users to identify the root cause of the incident. This includes answering the following questions about the incident:

- How long was the incident active before it was noticed?
- From where did the incident originate?
- What level of unauthorized access, if any, was gained?
- Were any other University resources affected?

iii**. Closure:** Based on the characteristics of the incident, a plan will be devised to restore affected systems to normal operation and prevent reoccurrence. The appropriate business owners will be notified and the incident will be closed. IIA will aggregate statistics about non-serious incidents and provide periodic reports to leadership.

2. Serious Incident and Assessment Questions: The following questions are intended to help classify serious risks, and are meant as specific examples of applying severity levels to security incidents:

a. **Is sensitive, confidential or privileged data at risk?**

If there is imminent danger (the act is in progress) that sensitive, confidential or privileged information can be read, modified, or destroyed by an unauthorized entity or the disclosure or access already occurred, then assign the incident severity level serious.

b**. Is business continuity at risk?**

If there is imminent danger of disruption of business due to security issues or malicious acts or the disruption is in progress, then assign the incident severity level serious.

c**. Does the incident involve Protected Health Information (PHI)?**

The Health Information Portability and Accountability Act (HIPAA) sets strict guidelines on the release of the health information of patients. Any violation of HIPAA standards is assigned a serious severity level and the HIPAA Compliance Officer is contacted.

d**. Does the incident involve personal information about a human subject?**

If personally identifiable human subject information is potentially compromised, the incident is assigned severity serious and the University of Michigan Office of Research (UMOR) is contacted.

Notification of serious incidents should occur as soon as possible and no later than 24 hours from the time the incident was initially detected. Notification of serious incidents should include the data fields specified in the *Information Security Incident Management Guidelines for University Units.*

Condition	Contact	Contact Information
Any incident	IIA	security@umich.edu

i**. Containment:** After assessing that an incident has occurred and notifying the appropriate parties, the next step is to contain the damage. This procedure may be unique for each incident and incident administrators should use their best judgment when devising a containment plan.

In the case of a serious incident, containment includes restricting access to the affected systems or otherwise ensuring that university resources are protected while the incident is under analysis. The longer the perpetrator of an incident has access to or control of a system, the higher the risk of long-term negative impact to the university. In the case of non-serious incidents, an appropriate level of containment, if any, should be applied. In certain cases, gathering information about an active attack may be prioritized over containing an incident.

For example, if the serious incident is network-based, the incident administrator should work with the appropriate *Business Owners* and administrators of the system to plan a network disconnection of the affected systems. Since this will affect business continuity within ITS, the incident administrator should ensure that the Business Owners understand the potential impact of the incident, the implications of disconnecting the systems from the network, and, if possible, include a timeline for re-enabling access to the system. If the appropriate parties are unavailable, or an agreement cannot be reached, the incident administrator may unilaterally enact a containment plan. If possible, the system should remain powered on but with its network access restricted. Turning a system off could erase potentially valuable volatile data. Actually disconnecting the system from the network could involve physically removing the network cable or reconfiguring network hardware to disallow access to the system. Every possible means of remote access should be disabled, including every network port and modem.

Once disconnection is complete, it is important to verify that the system is indeed unreachable by testing remote connectivity. If the incident involves a network-based denial of service attack, containment may be more difficult. The incident administrator should coordinate with upstream network service providers to identify the source of the problem and devise a containment plan. The containment plan, the parties involved, the actions

taken, who took them, and when should be included in a detailed log entry in the incident tracking system.

ii**. Analysis**

Analysis will vary greatly from incident to incident, but the overall methodology should be consistent. If a serious incident involves law enforcement, IIA will work with DPSS to ensure appropriate measures are taken when gathering and handling forensic evidence. The incident administrator should analyze the incident in order to answer the following:

- What was the incident and how did it occur?
- From where did the incident originate?
- What level of unauthorized access, if any, was gained?
- Did an unauthorized party access sensitive data?
- Were any other university resources affected?

A variety of tools should be used to collect information about the affected systems. The incident administrator should carefully weigh the side effects of collecting information. For instance, running a virus scanner on a potentially compromised host will overwrite the last access time for every file scanned, forever losing valuable information. If at any point it is determined a detailed forensic analysis is appropriate, the incident coordinator may employ various forensic toolkits in the investigation. In the case of a compromised host, information such as system logs, application logs, and active network connections will aid in reconstructing the incident. Other information that is stored outside the host being investigated, such as firewall logs, network logs, or IDS (intrusion detection system) alerts should be gathered and correlated. A log in the Incident Tracking System should be kept detailing the methodology and results of the analysis. If any information is collected, include what it is, who acquired it, how it was acquired, and when it was acquired.

iii**. Closure:**

D. **Complete Incident Documentation in Incident Tracking System**

The incident administrator should document any hypothesis, how evidence supports or contradicts it, actions taken to discover evidence or test the hypothesis, important or influential interactions with other people, relevant thoughts at the time, and anything else that will prompt accurate recall of the investigation. The final incident report should include the time and date for each entry in the incident notes, as well as the following information:

1. How the incident was detected
2. Dates:
    a. Inferred date of compromise
    b. Date the compromise was detected
    c. Date the incident was finally resolved
3. Names
    a. People added to the Incident Roles for this incident
    b. Person responsible for the IT Resource
4. Person compromising the resource, if known
5. Scope
    a. Cause of the incident
    b. Impact of the incident
    c. Nature of the resolution
6. Proposed improvements to security systems

E. **Store Other Incident Information:** All logs and data associated with the incident should be saved in accordance with ITS policies unless otherwise required by IIA. Forensic files, such as dumps or traces, should be collected and stored in a secure manner.

F. **Sensitive Data Status of Incident Information**: Due to the sensitivity of incident-related information, strict authorization and access controls will be maintained to ensure information is available only to authorized staff. The Chief Information Security Officer is the data steward and manager for IT security-related information and the ultimate authority for determination of access to the information and data.

G. **Lessons Learned Review:** For all serious level incidents, a Lessons Learned Review must be conducted that will typically use information captured in the incident tracking system. The review documentation should contain detailed information about the event, investigation, and conclusions. All data used in the review should reference information collected and be verifiable.

H. **Executive Summary Report:** Once a serious incident is closed, an Executive Summary Report is required. This report will be generated and provided to executive management, and other groups involved in the incident response. The Executive Summary Report should contain:

1. A high-level description of the incident and its scope
2. The impact on the University
3. Actions taken or planned for to prevent further occurrences
4. Recommendations for further action

V. References

Responsible Use of Information Resources (SPG 601.07)

Describes University community responsibilities for exercising high ethical standards when accessing and handling University IT resources. Violations may constitute security incidents.

Institutional Data Resource Management Policy (SPG 601.12)

Sets policies and responsibilities for managing and protecting institutional data resources.

Information Security Incident Reporting (SPG 601.25)

Requires prompt reporting of all security incidents and central reporting of serious incidents.

Information Security Incident Management Guidelines for University Units

For additional information, please contact IT Policy and Compliance Lead, Information and Infrastructure Assurance, Information and Technology Services at ajlevy@umich.edu or 734-764-7791.