Business & Finance Information Security Incident Response Policy

University of Michigan

http://www.umich.edu/~busfin/

BUSINESS & FINANCE

Document Version:	**10**
Effective Date:	6/1/2006
Review Date:	7/31/2009
Responsible:	Seth Meyer ISSO, B&F Security Committee
Approval Authority:	Laura Patterson, AVP
Contact:	Security & Network Services
Telephone:	(734) 615-7045
E-mail:	mais.tio.sns@umich.edu

Policies/Guidelines Supported:

University of Michigan:

- SPG 601.25, Information Security Incident Reporting Policy
- Information Security Incident Management Guideline

Business & Finance:

- Information Security Policy: Incident Response

Table of Contents

Purpose

This document describes the Business & Finance procedure for 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. The procedure supplements the University's *Information Security Incident Reporting Policy* (SPG 601.25), and the *Information Security Incident Management Guideline*.

This procedure is specifically amended to the Business & Finance Incident Response Policy and serves as the associated procedure to that policy statement.

Scope

This procedure applies to information security incidents relating to all data networks, network hosts, workstations and servers administered by Business & Finance. It also applies to computers and devices not administered by the B&F IT admins, but which are used by Business & Finance employees or other individuals associated with the units to access information resources managed by the University. This would include workstations and computing infrastructure managed by Business & Finance IT.

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

Goals

The Security & Network Services team is responsible for handling security incidents within specific units of Business & Finance. The goals of the Security & Network Services team in an incident are to:

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

Definitions

Terms used in this document may be found in the *Common Definitions* document located in the BFSC public folder.

See SPG 601.25 for the definition of an information security incident.

Information Security Roles and Responsibilities

Standard information security roles are explained in the *Roles and Responsibilities* document located in the BFSC public folder.

Note: One individual may be responsible for more than one of the unit roles listed below.

Business & Finance has the following information security roles:

Security & Network Services Team (SNS)

The SNS is the group of IT security professionals who have gone through the IIA security administrator training (or equivalent) and are assigned to handle the information security needs for the unit.

Responsibilities include:

- Receiving notification of detected or reported information security events and incidents from IT Resource Users, automated detection systems, or other sources;
- Accepting, logging, and tracking security incidents;
- Responding to incidents - executing incident mitigation and containment actions;
- Performing other core security services and risk assessments for the unit;
- Providing expert technical advice and guidance to the unit;
- Maintaining the Central Logging Servers, Virtual Firewall policy and Network Intrusion Detection devices;
- Forwarding discovered incidents that didn't originate within Business & Finance to the appropriate unit or to NOC;

Business & Finance Unit Security Officer (USO)

The USO is a member of the Business & Finance Security Committee who (in addition to the above) is assigned to coordinate incident response for the unit. This role may be rotating or permanent as determined by the Business & Finance Security Committee (see below).

Responsibilities include:

- B&F focal point for tracking, investigating, and coordinating incident response for assigned incidents;
- Reporting SERIOUS and MEDIUM incidents to the ISSO and other parties as appropriate;
- Business & Finance focal point for incident status reporting and communications;

Note: Once an incident is classified as SERIOUS, the ISSO assumes the responsibility of the focal point for incident communications.

Business & Finance Security Committee (BFSC)

Each USO is a member of the Business & Finance Security Committee. The Committee convenes quarterly to review appropriate incidents and discuss security initiatives in the B&F Three Year IT Security Plan. The committee is chaired by the Business & Finance ISSO.

Responsibilities include:

- Appointing USOs to each division within Business & Finance;
- Reporting the USO appointments to IIA for a university response framework;
- Reviewing previous SERIOUS and MEDIUM incidents with the ISSO and other parties as appropriate;
- Coordination with B&F communication officers about tactical responses to incidents;
- Review this incident response document and make appropriate updates;

Business & Finance Information Systems Security Officer (ISSO)

The ISSO is the manager of the SNS team, who is also the designated *Information Security Coordinator* for designated Business & Finance units.

Responsibilities include:

- Ensuring Business & Finance has established appropriate unit-level security procedures that are consistent with University policies and guidelines;
- Ensuring Business & Finance is following information security policies and procedures;
- Ensuring incidents are promptly reported to B&F unit management, appropriate Business Owners, IIA, the HIPAA Officer, and OVPR, as needed;
- Serving as B&F focal point for SERIOUS incident communications;
- Collaborating with IIA on the response and mitigation of SERIOUS incidents;
- Championing information security education and awareness for the unit;
- Providing feedback to IIA of special security needs, priorities, and concerns;
- Identifying security training needs for the unit;

Information Security Incident Response Procedure

The SNS Team and unit USO will use the security technologies at their disposal to respond to the incident. This may include data traffic interception, redirection or system disconnection. In an external attack, SNS will work with law enforcement agencies and upstream data service providers, as appropriate, to stop an attacker's access.

The SNS team and USO will follow the Incident Response Procedure and capture all relevant data. This data will then be aggregated in a SNS maintained secure database to be shared with law enforcement and IIA as necessary.

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.

1. Initial Event Notification

An information security incident begins when a security-related event is reported to the USO or ISSO. This could come from an automated system diagnostic, a trouble ticket submitted by a Data User, or other means.

The primary method to be used for submitting a security incident to SNS should be via the BFIT Lead Team Outlook Help Desk ticket system. All tickets submitted with a category value of "Security Incident (SNS)" will be assigned by the BFIT Lead Team to SNS and an e-mail notification to SNS will be automatically generated.

The person on the SNS Team who receives the initial notification opens an Incident Log in the SNS Tracking File System, (with a unique incident identifier) and adds available details, including some preliminary assessment of the incident severity, if one can be immediately determined.

2. Assign Incident Administrator

According to Business & Finance procedure, the incident is assigned to a incident administrator, a member of the SNS Team (with assistance from the appropriate USO) who is responsible for investigating the incident and coordinating the response until the incident is resolved and closed.

When a incident administrator has been confirmed, that individual will contact the person who reported the incident and provide incident Contact information.

3. Detail Incident Log Entry in SNS Tracking System

Incident documentation should include the Incident Data Fields found in the *Information Security Incident Management Guideline.* Use the table below to clarify the data fields that are initially provided. This information should be entered and updated, as necessary, in the SNS Incident Tracking System, a secured file system of reports.

Information to be Documented	**Description/Note**
Date of event	
Time of event	Including time zone
Who or what reported the event	If a person reported the event include their full name, location, telephone number, and e-mail. If an automated system reported the event include the name of software

Information to be Documented	Description/Note
	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 possible.
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. If the host has a modem connected to it, document the telephone number of the connected line or the wall jack number.
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).

4. Severity Assessment

The *Information Security Incident Management Guideline* defines three severity levels for information security incidents: Low, Medium, and Serious.

LOW-severity incidents should be tracked for statistical aggregation purposes and do not require taking the additional steps described below.

The incident administrator classifies the incident severity based on the following:

- Sensitivity of potentially compromised data
- Legal issues
- Magnitude of service disruption
- Threat potential
- Expanse – how widespread the incident is
- Public appeal – level of potential public interest

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:

- **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.

- **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.

- **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 Officer is contacted.

- **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 OVPR is contacted.

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.

Note: An incident severity classification may change based on subsequent events or greater knowledge of what happens during the incident.

5. 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.

The incident administrator must notify the ISSO of any SERIOUS or MEDIUM incidents in a timely manner.

The Business & Finance ISSO takes the following steps:

- Review and verify incident documentation, event reports and information entered in the SNS Incident Tracking System;
- Verify the assigned severity level based on available information;
- Acquire the resources necessary to respond to the incident;
- Notify IIA of any SERIOUS incidents;
- Notify the HIPAA Officer for all incidents involving PHI;
- Notify the OVPR for all incidents involving human subjects' personal information;
- Notify the University Office of Communications of SERIOUS incidents;

- Notify others as necessary, including Business Owners, DPS, OGC, unit communications, and unit IT Service Providers;
- Participate in a Computer Security Incident Response Team (CSIRT) that may be convened relating to a SERIOUS incident at the unit.

Notification of SERIOUS incidents (to IIA, HIPAA, or OVPR) should occur as soon as possible and no later than 24 hours from the time the incident was initially reported. Notification of SERIOUS incidents should include the data fields specified in the *Information Security Incident Management Guideline*.

For SERIOUS incidents, the Business & Finance ISSO confers with the University Chief Information Technology Security Officer (CISO) at IIA to determine whether the incident warrants legal action and whether the Department of Public Safety and the Office of General Counsel need to be contacted. The Business & Finance ISSO is responsible for periodically communicating the ongoing status of the response and investigation to the CSIRT, IIA, unit management and law enforcement as needed.

Business & Finance USO Contacts

Unit	USO	Contact Information
AEC	James Dormal	jdormal@umich.edu, 5-2250
BFIT	John Hufziger	hufziger@umich.edu, 6-7596
DPS	Stephen Dudek	mule@umich.edu, 3-3434
HRAA	Marjory Falconer	mefalcon@umich.edu, 7-5756
IIA	Esther Friedman	estherf@umich.edu, 7-5357
MAIS	Seth Meyer	smeyer@umich.edu, 5-7045
Michigan Business Svcs	Jim Householder	jhouse@umich.edu , 7-0693
OSEH	Eric Kolb	ekolb@umich.edu, 3-9106
Parking & Trans Svcs	Ray Hodel	hodel@umich.edu, 3-7311
Plant Operations	Ted Gerutta	tgerutta@umich.edu, 7-0823
University Audit	Matt Toaz	mtoaz@umich.edu, 7-7523

Condition	Contact	Contact Information
Any SERIOUS incident	IIA University Office of Communications	IIA@umich.edu (734) 615-2761 (734) 936-5190
Incident involves Protected Health Information	University HIPAA Officer	Jeanne Strickland (734) 615 4759 jeanst@umich.edu
Incident involves human subject research or other sensitive research information	Office of Vice President for Research (OVPR)	UMresearch@umich.edu (734) 764-1185
Incident involves criminal activity	Department of Public Safety (DPS) Office of General Counsel (OGC)	http://www.umich.edu/~safety/ (734) 763-3434 Emergencies – call 911 ovpgc@umich.edu (734) 764-0304

6. 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 administrator should use their best judgment when devising a containment plan.** The incident administrator may choose to coordinate the containment plan with SNS, if a SNS team member is not participating.

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.

For example, if the SERIOUS incident is network-based, 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 Business & Finance, ensure the Business Owners understand the potential impact of the incident and the implications of disconnecting the systems from the network. 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 should coordinate a plan with the Business & Finance ISSO.

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, 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.

Include a detailed log entry in SNS Incident Tracking System of the containment plan, the parties involved, the actions taken, who took them, and when.

7. Analysis

Analysis will vary greatly from incident to incident, but the overall methodology should be consistent. If a SERIOUS incident involves law enforcement, DPS and IIA will work with Business & Finance to ensure appropriate measures are taken when gathering and handling forensic evidence. For other SERIOUS incidents, the B&F incident administrator may choose to involve IIA in the analysis. For non-SERIOUS incidents, incident administrator should perform an appropriate level of analysis.

The incident should be analyzed by incident administrator 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?
- Was sensitive data accessed by an unauthorized party?
- 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 involve IIA or employ IIA 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 alerts should be gathered and correlated.

A log in the SNS 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.

8. Incident Closure

Complete Incident Documentation in SNS Incident Tracking System

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. Include the time and date for each entry in the incident notes, as well as the following information:

- How the incident was detected
- Dates
    - Inferred date of compromise
    - Date the compromise was detected
    - Date the incident was finally resolved
- Names
    - People added to the Incident Roles for this incident
    - Person responsible for the IT Resource
- Person compromising the resource, if known
- Scope
    - Cause of the incident
    - Impact of the incident
    - Nature of the resolution
- Proposed improvements to security systems

Inform IIA

The Business & Finance ISSO is required to notify IIA when a SERIOUS incident has been discovered. The B&F ISSO should include relevant documentation from the SNS Incident Tracking System.

Store Other Incident Information

All logs, and data associated with the incident should be saved in accordance with Business & Finance policies. Forensic files, such as dumps or traces, should be collected and stored in a secured folder.

9. Lessons Learned Review

For all MEDIUM and SERIOUS level incidents, a Lessons Learned Review must be conducted, which will typically use information captured in the the IR log maintained by SNS. 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.

For SERIOUS incidents, the Lessons Learned Review will take place in a private meeting between IIA and the Business & Finance ISSO no later than 48 hours after the conclusion of the SERIOUS incident.

10. Executive Summary Report

Once a SERIOUS incident is closed, an Executive Summary Report is required. This report will be generated by the Business & Finance ISSO and provided to IIA, executive management, and other groups involved in the incident response.

The Executive Summary Report should contain:

- A high-level description of the incident and its scope
- The impact on the University
- Actions taken to prevent further occurrences
- Recommendations for further action

References

SPG 601.7 – Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan

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

http://spg.umich.edu/pdf/601.07-0.pdf

SPG 601.12 – Institutional Data Resource Management and Protection Policy

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

http://spg.umich.edu/pdf/601.12.pdf

SPG 601.25 – Information Security Incident Reporting Policy

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

Information Security Incident Management Guideline

Data Resource Management and Protection Roles and Responsibilities Guideline

This document defines information security responsibilities at all levels of the University.

Data Resource Management and Protection Common Definitions

This reference document lists commonly-used information security terms and acronyms.