THE UNIVERSITY OF TEXAS HEALTH SCIENCE CENTER AT SAN ANTONIO

# IMS-ISA Incident Response Guideline

## Incident Response

**Information Security and Assurance**

**12/31/2009**

This document serves as a guideline for Information System Owners and their staff to create an incident Response Plan for their information system. This document defines what constitutes a security incident, as well as, lists any necessary requirements for documenting the incident, what conditions and to whom they should notify, and recommended reporting timelines. It provides examples of security incident types, but does not detail the various types of security incidents as that would be too impractical.

This page has been left blank intentionally

# Document History Page

| Revision Number | Summary of Changes | Date |
|---|---|---|
| Version 1.0 | Final Document | 12/31/2009 |
| | | |
| | | |

This page has been left blank intentionally

# Table of Contents

Document History Page ..... iii
Introduction ..... 1
Purpose ..... 1
Scope ..... 1
Objective ..... 1
Guidelines ..... 1
Mission Criticality for Information Systems ..... 2
Extent and Duration ..... 2
Preparing for Incidents ..... 3
Preparing to Handle Incidents ..... 3
Preventing Incidents ..... 4
Detection and Analysis ..... 4
Indications of an Incident ..... 4
University of Texas System Guidelines ..... 4
Containment ..... 5
Eradication ..... 6
Recovery ..... 6
Post Incident Activities ..... 6
Appendices ..... 7
Appendix A – Definitions and Acronyms ..... 7
Appendix B – References ..... 8
Appendix C – Documentation Requirements ..... 9
Basic Data Fields ..... 9
Incident Handler Data Fields ..... 9
Appendix D ..... 10

# List of Figures

Figure 1 – Incident Response Life Cycle ..... 1

# List of Tables

Table 1 - Security Incident Severity Matrix ..... 3
Table 2 - Incident Categories and Reporting Timeframes ..... 10

This page has been left blank intentionally

# Introduction

Incident response is a key element to any organization's information security program and its ability to meet its mission and business functions. Organizations and especially information system users, administrators, owners and security officers must know how to properly handle security incidents. With the number of security incidents as varied as the different types of information systems, specialized incident response plans must be developed and maintained for each system. Developing incident response plans for all information systems at the Health Science Center is too much for any one department. Thus, this document serves as a guideline to those persons to assist them in developing their own incident response activities. Effective incident response requires well documented process, procedures, as well as, knowledgeable and trained personnel. Information systems owners should task their staff to develop such capabilities to assure the appropriate level of availability, confidentiality and integrity is maintained.

## Purpose

The purpose of this document is to provide guidance to the reader on what information is necessary to develop an Incident Response Plan and provides some recommendations on how to handle a security incident.

## Scope

This guideline is general in its content and designed to provide guidance to any person handling a security incident that is or may affect a system at the University. The reader should consult his or her department's or information system's incident response plan for detailed procedures and other pertinent information.

## Objective

After reading this guide, the reader should be able to:

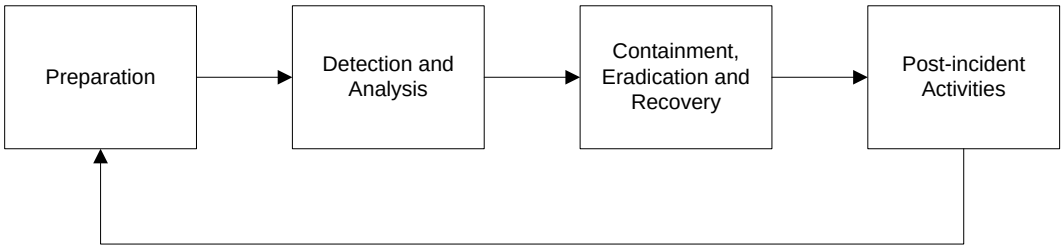
1. Detect and analyze incidents
2. Contain, eradicate and recover from them; and
3. Conduct post-incident activities
4. Draft an Incident Response Plan for information system their organization owns, operates and maintains.

There is some information on how to effectively prepare for handling incidents as well.

# Guidelines

The Incident Response Life Cycle is organized into four major phases. The phases are shown below. An incident response plan can be organized in a similar order.

**Figure 1 – Incident Response Life Cycle**




Preparation is the most cost-effective part of the process. Detection and analysis is the critical starting point of the response process. Incident responders should consult *NIST Special Publication 800-61, Revision 1 - Computer Security Incident Handling Guide*, dated March 2008 for more detailed guidance on how to detect and analyze security incidents. Containment, eradication and recovery make up the third phase of the process. Lastly, any incident response capability should conduct post-incident activities to help improve internal procedures and to document and communicate lessons that were learned during the latest security incident.

Before one can respond to a security incident, one should know what one is. Therefore, a security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Any event that fits this general definition should be considered a security incident. How quickly an organization responds to a security incident will depend upon how critical that information system is to their mission or related business functions. The following sections provide guidance on how to determine the severity of a security incident.

## Mission Criticality for Information Systems

Information system owners should classify the criticality their information systems. This will aid in determining how quickly they should address security incidents. An information system should be classified as one of the following. The guidelines can assist in classifying the criticality of an information system.

- Mission-Critical Information System: any system that is vital for an organization to complete its mission or business-related function, and whose loss would result in the severe or catastrophic failure to accomplish that mission or business-related function
- Mission-Essential Information System: any system that is necessary for an organization to complete its mission or business-related function, and whose loss would result in a significant adverse impact to accomplishing that mission or business-related function
- Mission-Support Information System: any systems that is not required for an organization to complete its mission or business-related function, and whose loss would result in a limited adverse impact to accomplishing that mission or business-related function

## Extent and Duration

The final set of decision points refer to the extent and duration of the security incident and associated damages. Each of these items will be rated as objectively as possible as low, moderate, or high. One or more of these three items may also map into the mandatory and UT System areas.

Extent – the degree to which something extends as a range of values or locations.

- Low – the incident was restricted to a single system
- Moderate – the incident was restricted to systems within the owning department
- High – the incident extended to other departments or to systems outside the University

Duration – the period of time during which the incident continues; this includes the event itself and its associated cleanup and recovery periods

- Low – the incident occurred and was recovered in 6 hours or less
- Moderate – the incident occurred and was recovered in 6 to 48 hours
- High – the incident occurred and was recovered in greater than 48 hours

Extent and duration and their associated ratings, can be mapped out on a simple three-by-two matrix.

**Table 1 - Security Incident Severity Matrix**

| | Low | Moderate | High |
|---|---|---|---|
| **Extent** | | | |
| **Duration** | | | |

A high in any category would necessitate a formal SIR, as would two or more moderates, though a moderate severity rating could also require a formal SIR. All other combinations would require the less formal approach.

## Preparing for Incidents

The first part to any incident handling process is to prepare for them. This includes establishing an incident response capability as well as conducting activities to prevent incidents from happening. Preparation is a key part of the process. Implementing industry best security practices and a layered defense strategy are just two ways personnel can prepare themselves.

### Preparing to Handle Incidents

Responders should have a set of tools and resources, including hardware and software when handling an incident. Examples include:

- Contact Information
- On-call Information
- Incident reporting mechanisms (i.e. phone numbers. Email addresses and online forms)
- Pagers or cellular devices
- Incident response center or meeting place

Hardware and software that users should consider implementing are:

- Laptops
- Spare desktops, servers, networking devices
- Blank storage media
- Printers, copiers, facsimile machine

If a Computer Incident Response Team (CIRT) exists, then they should have access to laptops, desktops or servers with:

- computer forensics software
- Sniffers or port analyzers

- Evidence gathering accessories

Responders should also have available:

- Clean software (i.e. OS boot disks)
- Security patches
- Backup images

## Preventing Incidents

There are several key practices that are necessary for preventing incidents from occurring. System owners and administrators should implement good patch management processes and procedures. Applying industry best practices for hardening the systems or host security is also highly recommended. Personnel should work with IMS staff to ensure that the necessary measures are in place at the network level to ensure an adequate level of security exists. Administrators should install software to prevent incidents from malicious code to exploit the system. Lastly, owners, administrators and users should participate in regular security awareness or training.

## Detection and Analysis

There are too many different types of incidents making a list of them are not practical and so are developing a set of procedures for handling every incident. The best that University personnel can do is to prepare generally to handle any type of incident and more specifically to handle common incident types. The incident categories listed below are neither comprehensive nor intended to provide definitive classification for incidents; rather, they simply give a basis for providing advice on how to handle incidents based on their primary category:

- Denial of Service—an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- Malicious Code—a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host
- Unauthorized Access—a person gains logical or physical access without permission to a network, system, application, data, or other IT resource
- Inappropriate Usage—a person violates acceptable use of any network or computer policies41
- Multiple Component—a single incident that encompasses two or more incidents.

Some incidents fit into more than one category. An incident response team should categorize incidents by the transmission mechanism—for example:

- A virus that creates a backdoor should be handled as a malicious code incident, not an unauthorized access incident, because the malicious code was the only transmission mechanism used.
- A virus that creates a backdoor that has been used to gain unauthorized access should be treated as a multiple component incident because two transmission mechanisms were used.

This section focuses on recommended practices for handling any type of incident.

## Indications of an Incident

### University of Texas System Guidelines

To further assist information system users, administrators and owners UT System has established eleven (11) guidelines for determining if an incident is significant and should be reported to the UT Systems

through their Security Incident Reporting Tool. Those personnel should report any incidents like the following to IMS-ISA. IMS-ISA will report any qualifying event to UT Systems and other state agencies.

1. Has a University owned computer or other University owned computing device been lost or stolen?
2. Was there an unauthorized disclosure or compromise of the security, confidentiality, or integrity of Sensitive Digital Data or Personal Identifying Information confidential or sensitive information?
3. Does the incident involve a harmful virus, worm or other attack that propagates through the network?
4. Could the attack be propagated to other state systems beyond the control of the institution?
5. Was there an unwanted disruption or denial of service?
6. Were there successful attempts to gain unauthorized access to a mission critical information resource or confidential/sensitive data?
7. Was a University information resource used for the processing or storage of data such as illegal file sharing or for distribution of illegal materials?
8. Were there attacks on the Internet and widespread automated attacks against Internet sites including website defacement?
9. Did the incident involve new types of attacks or new vulnerabilities?
10. Were University information resources used to attack others?
11. Were there failures in change management processes or unauthorized changes to mission critical hardware, firmware, data or software?

## Containment

Once an incident as been detected and analyzed, it is important to choose the proper containment strategy. During such times, it is best to have predetermined containment actions. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

The criteria should be documented clearly to facilitate quick and effective decision-making. Criteria for determining the appropriate strategy include—

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Incident response teams should consider delaying containment or invoking containment and the affect it may have upon the system; both could have adverse impacts.

Incident response personnel should collect the following information during an incident.

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer)
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence was stored.

Security incidents should be escalated to the IMS-ISA when it has been determined that the security incident will affect or has affected information systems or personnel outside its accreditation boundary.

## Eradication

After the incident has been contained, it I necessary to eradicate elements of the incident such as malicious code or unauthorized user accounts.

## Recovery

During recovery it is important to restore the system to its normal operating parameters. This may involve installing clean software or a complete system rebuild.

## Post Incident Activities

One of the most important activities in the process is learning and improving. Questions to be answered in the lessons learned meeting include—

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

The greater the impact of the security incident, the greater effort needed for post-incident. All post-incident activities should be documented in a report for future reference and training.

# Appendices

## Appendix A – Definitions and Acronyms

Security Incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Any event that fits this general definition should be considered a security incident.

IMS-ISA – Information Security and Assurance department

NIST – National Institutes of Standards and Technology

SP – Special Publication

## Appendix B – References

Scarfone, K., Grance, T., Masone, K., Computer Security Incident Handling Guide, NIST Special Publication 800-61, Revision 1, March 2008, Gaithersburg, MD

# Appendix C – Documentation Requirements

The following are required fields necessary for handling any security incident.

### Basic Data Fields

- Contact Information for the Incident Reporter and Handler
  - Name
  - Organizational unit (e.g., school, department, division, team)
  - Email address
  - Phone number
  - Location (e.g., mailing address, building and room number)
- Incident Details
  - Date/time when the incident was discovered
  - Estimated date/time when the incident started
  - Type of incident (e.g., denial of service, malicious code, unauthorized access, inappropriate usage)
  - Physical location of the incident (e.g., city, state)
  - Current status of the incident (e.g., ongoing attack)
  - Source/cause of the incident (if known), including hostnames and IP addresses
  - Description of the incident (e.g., how it was detected, what occurred)
  - Operating system, version, and patch level
  - Antivirus software installed, enabled, and up-to-date (yes/no)
  - Description of affected resources (e.g., networks, hosts, applications, data), including systems' hostnames, IP addresses, and function
  - Mitigating factors
  - Estimated technical impact of the incident (e.g., data deleted, system crashed, application unavailable)
  - Response actions performed (e.g., shut off host, disconnected host from network)
  - Other organizations contacted (e.g., software vendor)
  - If any confidential/high risk data (e.g. SSN, CCN, EPHI,PII, etc) was compromised during the incident, what type of data it was
- General Comments

### Incident Handler Data Fields

- Current Status of the Incident Response
- Summary of the Incident
- Incident Handling Actions
  - Log of actions taken by all handlers
  - Contact information for all involved parties
  - List of evidence gathered
- Incident Handler Comments
- Cause of the Incident (e.g., misconfigured application, unpatched host)
- Cost of the Incident
- Business Impact of the Incident

# Appendix D

Both the Texas Administrative Code 202, Subchapter C Rule §202.76 and the UTS Policy 165 both nave requirements for various persons or the organization's designated representative to report security incidents in a timely manner. The table below

### Table 2 - Incident Categories and Reporting Timeframes

| Category | Name | Description | Reporting Timeframe |
|---|---|---|---|
| CAT 0 | Exercise/Network Defense Testing | This category is used during state, exercises and approved activity testing of internal/external network defenses or responses. | Not applicable; this category is for each department's internal use during exercises. |
| CAT 1 | *Unauthorized Access | A person gains logical or physical access without permission to a federal department network, system, application, data, or other technical resource. | Within one (1) hour of discovery/detection. |
| CAT 2 | *Denial of Service (DoS) | An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS. | Within two (2) hours of discovery/detection if the successful attack is still ongoing and the department is unable to successfully mitigate activity. |
| CAT 3 | *Malicious Code | A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. Departments are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software. | Daily Note: Within one (1) hour of discovery/detection if widespread across department. |
| CAT 4 | *Inappropriate Usage | A person violates acceptable use of any network or computer use policies. | Weekly |
| CAT 5 | Scans/Probes/ Attempted Access | This category includes any activity that seeks to access or identify a federal department computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. | Monthly Note: If system is classified, report within one (1) hour of discovery. |
| CAT 6 | Investigation | Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. | Not applicable; this category is for each department's use to categorize a potential incident that is currently being investigated. |

The IMS-ISA will submit summary reports of security-related events shall be sent to the Department of Information resources (DIR) on a monthly basis no later than nine (9) calendar day after the end of the month.

NOTE: * Any incident that involves compromised PII must be reported to IMS-ISA at (210) 567-5900 and infosec@uthscsa.edu within 1 hour of detection regardless of the incident category reporting timeframe.