**Contents**

[1. Introduction 2](#_Toc112073357)

[2. Purpose 2](#_Toc112073358)

[3. Roles and Responsibilities 2](#_Toc112073359)

[4. Process Flow 4](#_Toc112073360)

[5. Guidelines for incident response 4](#_Toc112073361)

[5.1 Insider threat 4](#_Toc112073362)

[5.2 Interactions with Law Enforcement 5](#_Toc112073363)

[6. Enforcement and Compliance 6](#_Toc112073364)

[7. Policy Statements 6](#_Toc112073365)

[8. Verification activities 7](#_Toc112073366)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **Change Reference** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

An IT security incident is any event that poses a threat to the security of an organization's information or IT systems. These events can range from a major data breach to simple virus infection, and they can have serious consequences for businesses of all sizes. An effective IT security incident management process is essential for mitigating the damages of an incident and getting your business back up and running as quickly as possible.

# Purpose

The purpose of an IT security incident response process is to ensure that incidents are dealt with in a timely and effective manner. This process should be designed to minimize the impact of incidents on the organization and to help the organization learn from and prevent future incidents.

# Roles and Responsibilities

* Security Incident Manager: This is the individual who is responsible for coordinating the response to the incident. They will work with all other team members to ensure that the incident is dealt with efficiently and effectively.
* Security Analyst: The security analyst is responsible for investigating the incident and gathering all relevant information. They will work closely with the security incident management to understand the scope of the incident and determine the best course of action.
* Security Engineer: The security engineer is responsible for implementing the technical solutions necessary to mitigate the incident. They will work closely with the security analyst to understand the requirements and ensure that the solutions are properly implemented.
* Communications Manager: The communications manager is responsible for coordinating all communication related to the incident. This includes communicating with external stakeholders such as law enforcement or shareholders, as well as internal stakeholders such as employees or customers.
* Incident handler- The person in charge of organising resources and handling communication when responding to a security incident. The first responder should perform the function to the best of their knowledge, skills, and abilities up until an Incident Handler has been identified
* Information security team- The team comprises of security incident management,
* Business Continuity Manager: The business continuity manager is responsible for ensuring that the organization can continue to operate despite the incident. They will work with all other team members to identify critical functions and develop plans to keep them running during and after the incident.

# Process Flow

**Suspicious activity identified**

**Inform SEC Team**

**Event is noted**

No

Yes

**Final report created and presented to stakeholders**

**Incident remediation**

**Handler begins the investigation**

**Incident handler is assigned**

**Create an incident response plan**

**Sends Preparatory report to Sec team**

**Event is logged**

**SEC team interacts with stakeholders/client and revise the procedure**

# Guidelines for incident response

## 5.1 Insider threat

* The Incident Response Coordinator will designate alternative Incident Response Handlers to the incident if a specific Incident Response Handler is a person of interest in the incident.
* The Incident Security Manager will act in place of the Incident Response Coordinator or select a designee to act on their behalf if the Incident Response Coordinator is a person of interest in an incident.
* The Chief Information Officer (CIO) will select a designee to act on their behalf if the Information Security Manager is a person of interest in an incident.

## Interactions with Law Enforcement

All discussions with outside law enforcement agencies are conducted only after seeking advice from the Office of General Counsel. When OGC has given the go-ahead, the organization consults with CMU local jurisdiction authorities to establish their information needs and shares the bare minimum of data needed for incident response.

|  |  |  |  |
| --- | --- | --- | --- |
| **IT Security Incident Report** | | | |
| **Report details** | | | |
| **Report Date:** | 20-12-22 | | |
| **Report Number:** | SEC-225-80 | | |
| **Created by:** | Kunal T | | |
| **Role:** | Security Supervisor | | |
| **Incident Details** | | | |
| **Date of incident:** | 19-12-22 | | |
| **Time of Incident:** | 1:42 PM GMT | | |
| **Incident Type:** | Virus | | |
| **Location of Incident:** | The user's laptop; device #112-4445-90130 | | |
| **Status of Report:** | In Documentation Process | | |
| **Incident Description:** | The user received an E-mail from an external user, which had an attachment. The content of the E-mail specified that the attached form needs to be filled in ASAP, otherwise his storage space on the exchange server will run out and he won't be able to send/receive E-mails. The user opened the attachment, and the virus was able to install a Trojan horse on the company's server. The user admits that he acted foolishly and failed to notice that the origin of the mail wasn't the organization's IT department. | | |
| **People affected by the Incident** | | | |
| **Name** | **Role** | | **Equipment Affected** |
| Tracey Zakazian | Site designer | | 1) The user's laptop 2) The company's cloud server |
| **Follow up actions** | | | |
| **Action** | | **Responsible** | **Comments** |
| Detach the user's laptop from the company's internal site | | Kunal T | Done |
| Clean up the server from all viruses | | Checkpoint | 3rd party vendor, cost: $4,500 |
| **Approval of Documentation** | | | |
| **Name** | | Patty Crawford | |
| **Role** | | VP of IT | |
| **Date of Approval** | | 26-12-22 | |
| **Signature:** | |  | |

# Enforcement and Compliance

The Information Security Officer will review this policy on a regular basis to ensure that it is being followed. All IAU units (Deanships, Departments, Colleges, Sections, and Centres) are responsible for maintaining continual compliance monitoring in their respective areas. IAU's environment could be harmed (e.g., loss of trust and reputation, operational disruptions, or legal violations) if the information security directives are ignored or violated, and the fallible individuals will be held accountable, which could result in disciplinary or corrective actions (e.g., dismissal) and legal investigations. Employees who are suspected of breaking security instructions must be treated correctly and fairly (e.g., disciplinary action). Management and the Human Resources Department must be informed about policy infractions and deal with them.

# Policy Statements

* The Information Security Officer, in collaboration with the Deanship, will create an "Information Security Incident Management Form" to report all security violations/occurrences and to create a swift reaction mechanism for information security incidents.
* All workers must understand and be able to recognize any strange or unexpected behavior on the assets that could indicate a software failure. The following are examples of security occurrences, but they are not exhaustive.

a. System alterations that are uncontrollable.

b. Inadequate access (e.g., password sharing).

Physical security breaches are c.

d. Hacking or manipulation of systems.

e. Confidentiality of data is jeopardized (e.g., data theft).

f. Data integrity is jeopardized (i.e., damage to data or unauthorized modification).

a. Misuse of data, assets, or services.

h. Infection of a system with a malicious or illegal program.

i. An effort to gain access to a computer without authorization.

Changes to hardware, software, or infrastructure configuration that are not approved.

3. If a security incident is discovered, users must take the following steps:

a. Take note of the symptoms and any error messages that appear on the screen.

b. If an infection is suspected, disconnect the workstation from the network (with the help of the ICT Deanship).

c. Do not utilize any contaminated removable media (e.g., USB memory sticks).

4. All IAU workers are required to notify the Deanship of any suspected security-related events.

Information such as, but not limited to, the following must be provided:

a. The individual who reported the incident's name and phone number.

b. The type of data or equipment that is being used.

c. Whether the loss of the information poses a threat to any individuals or other data.

d. The incident's location

e. Any impacted equipment's inventory numbers

f. The time and date of the security breach.

g. The location of the affected data or equipment

h. The incident's type and circumstances

# 8. Verification activities

The audit activities are planned in this activity. Planning must consider the following issues:

* Which services need to have their security issues audited?

This is dependent on the volume and gravity of security incidents for each service, as well as the significance of the service.

* What is the audit's scope?

What scope does the audit have—a thorough audit or just a cursory examination of a few indicators?

* auditing technique? Will an audit be completed through checks, practical tests, or just a questionnaire?
* How frequently is the audit required?

This is dependent on the volume and seriousness of security incidents experienced by each service, its significance, and the degree to which it is exposed to both internal and external threads.

* Who does the audits?

To ensure that the auditor is unbiased, unaffected by options or customer relationships, and motivated to preserve the auditing contract, auditors should be changed frequently.