Information security incident management policy template

Why do you need an information security incident management policy?

One of the challenges most businesses face is to have an organised approach when dealing with information security incidents. Since most businesses never anticipate the occurrence of an incident, they fail to update their security infrastructure and open up all sorts of possibilities for hack attacks and insider abuse.

An information security incident management policy can help organizations have a concrete plan, establish appropriate roles and responsibilities, implement proper response procedures and improve security awareness among employees.

Documenting an information security incident management policy not only strengthen the daily operations of your organization but it can also help meet the requirements set by various industry specific compliances such as Health Insurance Portability and Accountability (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS).

Table of Contents

_____<Organization Name>______: Information Security Incident Management Policy

1. Introduction

- All <organization name> employees and contractors should be aware of their responsibilities in securing the confidentiality of sensitive information they handle on a daily basis.
- The policy sets out guidelines to ensure all incidents or weaknesses to <organization name>'s information systems are properly communicated and resolved in an efficient manner.
- An information system can be any asset that stores and processes information, this could include <organization name>'s work station, <CRM>, <ECM> and any other systems used for handling information.

2. Scope

- This policy applies to all employees, contractors and other interested parties with access to <organization name>'s resources.

3. Policy

3.1. Defining an Information Security Incident

- An information security incident is the successful or suspected access to <organization name>'s resources, information technology operations and wilful violation of <organization name>'s acceptable use policy. <define your organization's acceptable use policy here>

Information security incidents can include the following:

- Intrusion to <organization name> computer system.
- Unauthorized disclosure of all data pertaining to <organization name>
- Suspected or actual breaches to <organization name> data and applications.
- Unauthorized changes to the software or systems.
- Denial of service attacks.
- Detection of malicious code.
- Unauthorized probing into <organization name> networks.

  - Compromised user accounts.
  - Loss or theft of <organization name> equipment harbouring sensitive data.

- While the above contains a general overview of the information security incidents that can occur within an organization, not all incidents are required to be assessed and logged such as incidental access by a trusted employee, which would less likely impact the daily operations of the organization and thus would not be classified as an information security incident of severity.
- Nevertheless, a central security incident reporting system would be in place to ensure all incidents whether they are of malicious or accidental origin are appropriately communicated to the <senior management> and other interested parties as soon as they occur.

3.2. Managing Information Security Incidents

3.2.1. Defining Roles and Responsibilities

- <Chief Information Security Officer/IT Manager>: will be the ultimate authority for implementing this policy as well as notifying the <senior management> and other interested parties of the incident and its impact on <organization name>.
- The <Chief Information Security Officer/IT Manager> should create and maintain records of each incident and have them logged within <organization name's centralized log management system>.

- Once the incident is logged for reference, the <Chief Information Security Officer/IT Manager> should conduct a risk assessment at periodic intervals to ensure they do not occur again in the future.
- All records should be maintained and created in accordance with <organization name> retention and disposition schedule.
  <define your organization's retention and disposition schedule>

<Information Security Incident Management Team>: the team would include <organization name>'s <IT Security Team>, <Legal Team>, <PR Team> and <Security Officer>. The responsibilities for each are defined below:

_________<IT Security Team>_________:

- Effectively manage the incident from the moment of its occurrence to its closure.
- Properly assess the business impact and report it to the ____<Chief Information Security Officer/IT Manager>____.
- Have appropriate knowledge on ______<organization name>______'s networks and IT operations and maintain the competency to manage ___<organization name>___ compromised networks and servers.
- Ensure business continuity by conducting tests at regular intervals.
- Gather and properly analyze the evidence in a way that it can be easily admissible in court.

_________<Legal Team>_________:

- Assess the contractual and judicial impact of the incident.
- File complaints.
- Ensure that the incident response activities stay within the confines of ______<organization name>______'s legal and regulatory requirements and policies.

__________<PR Team>__________:

- Answer customers, shareholders and the press.

________<Security Officer>________:

- Ensure physical protection of the organization's premises and ICT infrastructure.

________<Incident Handler>________: the ______<Incident Handler>______ will be a member of the ______<IT Security Team>______ who will be assigned the operational responsibilities to properly manage the information security incident. Their responsibilities would include:

- Instructing other members of the team of the appropriate response actions.
- Help the ___<Chief Information Security Officer/IT Manager>___ prepare a report of the incident, the corrective actions taken and recommendations to prevent its future occurrence.
- Be the internal point of contact within ______<organization name>______.

<Employees>: will be the users of <organization name>'s technology resources. They are expected to recognize any weaknesses to <organization name>'s information systems and immediately report them to the <Incident Handler>. Their responsibilities would include:

- Prompt reporting of the information security incident to the <Incident Handler> or <IT Security Team>.
- Adhere to the <Information Security Incident Management guidelines> set by <organization name>.
- Ensure protection of all information related to the incident.

3.3. Reporting Information Security Incidents and Weaknesses

- The information security incident should be reported as soon as they occur to the <IT Security Team> or any other members of the <Information Security Incident Management Team>.
- All employees of <organization name> shall be reminded of their responsibility to report the incident through a general awareness training, which will be conducted <define time period>.
- The information security incident, whether suspected or actual should be reported as early as possible as it can help minimize the cost of damage and reduce the impact significantly.
- While reporting any weaknesses on <organization name> information systems, employees are cautioned against proving the weakness by testing as it will be seen and logged as system abuse.
- Unauthorized testing could further damage the system and the information it stores leading to the occurrence of an information security incident.

3.4. Assessment of the Information Security Incident

- Once the incident is logged, it shall be analyzed by the <IT Security Team>.
- The analysis would include getting an in-depth understanding of the severity of the incident and its impact on <organization name>'s daily operations.
- The severity will be classified into <three> of the following categories

<Low>: these are incidents with low impacts, such as a minor issue within the system that can cause an inconvenience to the user or customers. This can be fixed any time during the day.

<Medium>: incidents that can have a significant impact on the daily operations of <organization name>. This could include the unavailability of a customer facing service for a substantial amount of time. Incidents of such nature should be fixed by the <IT Security Team> or other <security professionals> if needed, as soon as they occur.

<High>: these would include critical incidents with very high impact. Incidents of <high risk> category would include loss of client confidential information from customer server, data breaches, disclosure of critical business information online, injection of malicious code etc. These too should be immediately rectified by the <Information Security Incident Management Team> right at the moment of its occurrence.

3.5. Conducting a learning and review process

Once the incident is logged and treated, a learning and review process will be conducted to ensure necessary updates to all the existing policies and implementations within <organization name>.

During the review and learning process, the <Incident Handler> under the guidance of the <Chief Information Security Officer/IT Manager> shall properly analyze the incident and provide suggestions on whether additional changes need to be implemented or not.

Some of the steps taken to improve <organization name> information security and ICT infrastructure shall include:

- Prepare a list of emergency contacts and industry experts
- Have appropriate tools to manage hardware and software
- Building an active presence in various online communities
- Give adequate training at periodic intervals
- Create reports of all lessons learned from the incident and incorporate those into the general awareness training
- Review the <Information Security Incident Response Plan>

3.6. Consequences of violating the policy

Breaches to the policy could either result in <disciplinary action> or <instant dismissal> based on the severity of the action. Some of which have been listed below.

<Makes multiple unauthorized copies to company confidential and client confidential records>	<Instant dismissal>
<Accesses client confidential data for the first time without a legitimate business reason or getting appropriate authorization from the concerned manager>	<Final Written Warning>
<An employee purposefully sends out an email containing sensitive information to a recipient not part of organization name or authorized by organization name>	<Instant dismissal>
<The employee legitimately recieves access to personally identifiable data or sensitive data pertaining to organization name or its customers without approval from their concerned manager>	<First Written Warning or Oral Warning>
<An employee is genuinely unaware and opens a file containing sensitive information>	<First Written Warning or Oral Warning>

Information Security Incident Response Form:

Incident Identification Information:

Date and Time of Notification: ____

Incident Detector's Information:

Name: ____

Title: ____

Date and time of detection: ____

Contact Information: ____

Incident Summary:

Type of incident detected: ____

Description of the incident: ____

Actions Performed:

Identification measures: ____

Containment measures: ____

Evidence collected: ____

Mitigation actions: ____

Follow up:

Reviewed by: ____

Recommended actions carried out: ____

Follow up completed by: ____