**Incident Management Policy and Procedure**

Doc: POL/IMP

Document Classification: Internal

July 2022

**Document Control Information**

| Document Name | Incident Management Policy and Procedure |
| --- | --- |
| Document ID | POL/IMP |
| Document Owner | Information Security Officer |
| Classification | Internal |
| Approved By |  |

| **Authorization** | | | |
| --- | --- | --- | --- |
| **Stakeholders** | **Read Access** | **Write Access** | **Media Type** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| **Amendment Log** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Author (s)** | **Reviewed By** | **Approved by** | **Brief description of the change** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

[1.0 Introduction 4](#_heading=h.gjdgxs)

[2.0 Purpose 5](#_heading=h.1fob9te)

[3.0 Scope 6](#_heading=h.2et92p0)

[4.0 Incident Definition 7](#_heading=h.1t3h5sf)

[5.0 Incident Classification 8](#_heading=h.2s8eyo1)

[5.1 Malicious Code Attacks 8](#_heading=h.17dp8vu)

[5.2 Denial-of-Service (“DoS”) 8](#_heading=h.3rdcrjn)

[5.3 Unauthorized Access / Theft 8](#_heading=h.26in1rg)

[5.4 Network reconnaissance probes 9](#_heading=h.lnxbz9)

[6.0 Policy 10](#_heading=h.1ksv4uv)

[6.1 Incident Management Coverage 10](#_heading=h.44sinio)

[6.2 Incident Handling Procedures 10](#_heading=h.2jxsxqh)

[6.3 Logging Security Incidents 10](#_heading=h.z337ya)

[6.4 Release of Information 11](#_heading=h.3j2qqm3)

[6.5 Learning from Incidents 11](#_heading=h.1y810tw)

[6.6 Analysis of the Incident 11](#_heading=h.4i7ojhp)

[6.7 Resolution of the Incident 11](#_heading=h.2xcytpi)

[6.8 Documentation of the Incident 11](#_heading=h.1ci93xb)

[6.9 User Awareness 11](#_heading=h.3whwml4)

[7.0 Procedure 12](#_heading=h.qsh70q)

[7.1 Reporting of Incidents 12](#_heading=h.3as4poj)

[7.2 Incident Handling 12](#_heading=h.1pxezwc)

[7.3 Incident Closure 12](#_heading=h.49x2ik5)

[7.4 Contact Details 12](#_heading=h.2p2csry)

[7.5 Containment and Analysis 12](#_heading=h.147n2zr)

[8.0 Reference Documents 14](#_heading=h.23ckvvd)

# Introduction

How you respond to, and handle an attack on, your company’s information systems determines how well you will be able to control the costs and consequences that could result.

For these reasons, the extent to which you prepare for security incidents and work with {Company} will be vitally important to the protection of the user’s key information.

# Purpose

Incident management responsibilities and procedures shall be established to ensure quick, effective and orderly response to security incidents.

1. **Scope**

This policy applies to all incidents involving all employees, apprentice, contractors, consultants, vendors’ temporary staff etc. of {Company} and its information assets. The incidents may cover breach of confidentiality, integrity or availability. The incidents affecting availability of information assets should be addressed by the Business Continuity Management Policy. All are expected to be familiar and comply with this policy.

All incidents involving breaches of confidentiality and integrity of asset will be addressed using this procedure. All incidents involving loss of availability will be addressed by the Business Continuity Management procedure depending on criticality of asset.

# Incident Definition

A security incident can have the following definitions:

* Violation of an explicit or implied security policy;
* Attempts (either failed or successful) to gain unauthorized access to a system or its data;
* Unwanted disruption or denial of services;
* Unauthorized use of a system for the processing or storage of data; and/or
* Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

# Incident Classification

A security incident can be classified under the following categories:

## Malicious Code Attacks

Malicious codes can be programs such as viruses, worms, Trojan applications, and scripts used by intruders to gain privileged access, capture passwords or other confidential information e.g. user account information. Malicious codes attacks are usually difficult to detect as certain viruses can be designed to modify their own signatures after inflicting a system and before spreading to another. Some can also modify audit logs in order to hide unauthorized activities.

The following are some examples of malicious code attacks:

* Worms or viruses rapidly spreading through emails (e.g. I Love You, Melissa Virus);
* Spying codes (e.g. Caligula Virus, Marker Virus, Groove Virus);
* Remotely controlled codes (e.g. Back Orifice, NetBus); and
* Coordinated attack codes (e.g. Trinoo, Tribe Flood Network (TFN))

## Denial-of-Service (“DoS”)

DoS attacks refer to the use of specific tools by intruders to cause networks and/or computers to cease operating effectively or to erase critical programs running on the system. Currently, distributed DoS attacks are becoming prominent where a team of intruders located in various geographical locations launches simultaneous attacks on a victim host. It is generally difficult to trace the source of distributed DoS attacks as perpetrators could launch the attack through multiple different gateways before reaching the victim host. In a DoS attack, DNS, web and mail servers are the most likely targets. While a DoS attack may not be a direct cause of account compromise, it may however be a warning signal for future attacks.

Some examples of DoS attacks are:

* Email related DoS (e.g. mail SPAM, mail bombs);
* Service-related DoS (e.g. Slammer Worm, Chargen DoS); and
* Network jamming DoS (e.g. SYN flood DoS, 'Ping of Death' DoS, Smurf DoS).

## Unauthorized Access / Theft

Unauthorized access ranges from the unauthorized usage of log-on credentials to the tampering of files and directories stored on a system or storage media. It could also entail access to additional computer systems through an unauthorized “sniffer” program or device planted to capture confidential information traversing the network. Most commerce merchants use Secure Socket Layer (SSL) to protect web transactions over the internet. SSL provides server authentication, data encryption and message integrity. Without SSL, most web transactions, including credit card transactions, would travel across the internet in the clear, and would be susceptible to network sniffing i.e. the information could copied, modified or deleted. Internal compromise continues to be the most common and most damaging method of stealing sensitive information. Organized crime groups now actively recruit employees of organizations that process high volumes of user information to steal cardholder data and transaction information.

The following list includes some examples of unauthorized access:

* Employees stealing confidential information;
* System access by using user IDs belonging to ex-employees;
* Unauthorized access by using user IDs that have administrative access rights;
* System access by using special purpose IDs that are no longer required or use weak passwords;
* Unauthorized access by exploiting vulnerability in the company’s information systems, routers or firewalls.
* Access of information by parties affiliated with the process (customer care operations).
* Access of process/application data by application service providers.
* Access of payment information to by third-party payment enablers – Paymate, ITZ card, so on.

## Network reconnaissance probes

The objective of performing reconnaissance probes against a company is to gather information on its network infrastructure. A probe can consist of two natures – host discovery and service ports discovery. Host discovery will determine all active systems in a network, which includes performing Operating System (“OS”) fingerprinting. Port discovery will gather information on the services running on the systems. While a network probe attack may not result in an account compromise, it may however be a warning signal for future attacks.

There are many tools available on the internet for performing these probes such the following examples:

* Host discovery (e.g. Ping sweep, directed broadcast pings, SYN-FIN scans), and
* Service port discovery (e.g. TCP port scan, UDP port scan).

1. **Policy**

Information Security incidents should be reported, resolved, escalated if required and actioned as per defined procedures in a timely manner.

## Incident Management Coverage

* Incident management procedures shall cover all types of potential security incidents, including however not limited to:
  + Theft of computer hardware equipment and communication network
  + Information system failures and loss of service
  + Unauthorized access to a system
  + Deliberate denial of service
  + Virus and worm incidents
  + Errors resulting from incomplete or inaccurate business data
  + Errors resulting from inaccurate processing of data
  + Breaches of confidentiality
  + Non conformities found during the internal audits
  + In addition to normal contingency plans to recover from such incidents, incident management procedures must cover:
  + Analysis and identification of the cause of the incident
  + Planning and implementation of remedies to prevent recurrence
  + Collection of audit trails and similar evidence
  + Communication with those affected by or involved with recovery from the incident
* All incidents must be classified in five categories as described in the Personnel Security policy.
* Note: Scheduled downtimes are excluded from the scope of Incident Management.

## Incident Handling Procedures

* Action to correct and recover from security breaches and system failures must be controlled. The procedures for Incidence response must ensure that:
  + Clearly identified and authorized staff are allowed access to production systems and data
  + All emergency actions taken are documented in detail.
  + Emergency action is reported to management and reviewed in an orderly manner.
  + The integrity of business systems and controls is confirmed with minimal delay.
  + Audit trails and similar evidence must be collected and secured, as appropriate, for:
  + Internal problem analysis
* Use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings
* Negotiating for compensation from software and service suppliers
* Settlement of Insurance claims, wherever applicable
  + All day to day security incidents should be reported to Management Representative
  + An incident shall be immediately reported to the Head – IT and Management Representative, if the attack has been on the network or software.
  + The statistics / details about the incidents should be reported to the Management during the regular Management meetings.
  + After an incident computers affected by the attack shall be cleaned and restored using a known clean set of software.
  + Patterns of incidents (including previous) should be reviewed to identify potential security breaches and minimize the chances of similar incidents in the future.

## Logging Security Incidents

* + A written log shall be kept for all security incidents, which are under investigation
  + The information shall be logged in a location and format that cannot be accessed and altered by others.
  + The types of information that must be logged are:
    - Date and time of incident and receipt of information
* Names of information system components (e.g. systems, programs or networks) that have been affected.
* People contacted
* Emergency actions taken
* Cost of the assets reported as lost / missing

## Release of Information

* Control of information during the course of a security incident or investigation of possible incident is very important. Providing information to the wrong people can have undesirable side effects, especially if the news media is involved.
  + - All information during the course of a security Incident or investigations of a possible incident must be controlled.
    - Management shall be the only party to authorize the release of any information.

## Learning from Incidents

* + A follow-up analysis of the incident must be performed after an incident has been fully managed and all systems have been restored to a normal mode of operation.
  + The incident log book must be updated and the incident details should be shared with Management on quarterly basis for advice and action.

## Analysis of the Incident

* Management Representative shall analyze the incident log book and comment on adequacy of corrective action taken.
* Management Representative shall present analysis of incidents to Management. Learning from the incident shall be used to strengthen the processes and take preventive actions if necessary.

## Resolution of the Incident

* It is the responsibility of the Department Head along with Management Representative to resolve the incidents within his / her department. Management Representative along with Department Head shall take corrective actions to resolve the incident.
* Corrective action shall be documented at each stage of resolution. All results from the investigation shall be reported to Management.

## Documentation of the Incident

* The incident log book shall be stored for future reference.
* Incidents shall be categorized based on the nature of each incident. For more details on the incident categorization refer to the Personnel Security Policy and Procedure.

## User Awareness

* User awareness programs shall be conducted periodically to upgrade awareness in identification and escalation of suspicious activities.
* Media such as emails, internal newsletters, training programs, notice boards shall be used as common channels for increasing the awareness amongst the users.
* User awareness programs shall be conducted as mentioned in ISMS Policy and Personnel Security Policy and Procedure.

1. **Procedure**

## Reporting of Incidents

* The users should report all security incidents to Management Representative via e-mail.
* The procedure for reporting of incidents shall be made aware to the new joinees by way of awareness programs at the time of induction.
* The users, in the case of reporting any security incidents are expected to follow the following procedures:
* Note the symptom of problem; and
* If a security breach is suspected, the user should inform Management Representative immediately for appropriate remedial action.
* If the incident is related to any IT equipment, then the IT equipment should be disconnected from the network and should not be plugged back till clearance is obtained from the Head – IT for usage of the IT equipment.
* Do not access or alter compromised systems (i.e. do not log on at all to the machine and change passwords, do not log on as ROOT);
* If an employee is involved in any security violation, the disciplinary process as mentioned in Personnel Security Policy and Procedure should be followed.
* The users should be warned not to attempt to resolve any incident on their own. The same shall be considered as breach of security and may form a base for disciplinary actions.

## Incident Handling

The process to be followed for handling incidents should be as given below:

* For incidents of ‘Low’ and ‘Moderate’ severity, the Management Representative should handle the incidents. Management Representative should send a monthly report of the ‘Low’ and ‘Moderate’ severity incidents.
* For ‘Critical’, ‘High’ and ‘Medium’ severity incidents, the Management Representative should be immediately informed. These incidents should be resolved by the Management Representative in discussion with Head - HR and respective Delivery / Department Head.
* An incident shall be immediately reported to the Head – IT and Management Representative, if the attack has been on the network or software.
* The statistics of the ‘Low’ and ‘Moderate’ severity incidents and details about the ‘Critical, ‘High’ and ‘Medium’ severity incidents should be reported to the Management during the regular Management meetings.
* The IT team will raise the ticket via Service Desk for unauthorized software’s (the software’s which are installed without raising Change Request and Service Desk) and virus related incidents.

## Incident Closure

* Management Representative should take the lead in resolving the incidents reported. Management Representative may take help from the concerned teams (e.g. IT Team for any technical incident, HR Team for any disciplinary process) for the timely resolution of the incident.
* The resolution details like actions taken, results of root cause analysis, results of mitigation process, and lessons learnt should be recorded in the Incident Log Book.
* Information collected through "Lessons learned" section should form as the input for the revision of the Information Security Policies and Procedures.

## Contact Details

The contact details for the Information Security Team can be found in the ‘Organization of Information Security Policy’.

## Containment and Analysis

The Management Representative should visit the location (place, computer, server etc.) to collect further details immediately and make appropriate steps to isolate and contain the incident if it is capable of spreading to other assets.

If the team is unable to identify the probable cause and the probable resolution it may contact the vendors or any other appropriate personnel.

In special circumstances, the Head – India (CEO) and Management Representative shall decide when and why an investigation should be conducted, and whether to involve law enforcement agencies. Privacy issues need to be considered prior to such investigations. It is best to consult the {Company} legal department in such circumstances.

The Head – India (CEO) and Management Representative, based on the consultation with the legal department shall convene a special committee to liaise with the law enforcement agencies to address the following issues:

* Establishing a prior liaison with law enforcement agencies.
* Deciding when and if to involve these agencies.
* Setting up means of reporting such crimes.
* Planning for and conducting investigations.
* Involving senior management and the appropriate functions, internal audit and human resources
* Establishing procedures for handling and processing reports of computer crime.
* Ensuring the proper collection of evidence, this includes identification and protection of the various storage media.

# Reference Documents

* ISMS Overview Policy
* ISO 27001:2013
* Statement of Applicability for ISO27001:2013
* Computing Environment Procedure
* Business Continuity Management Policy
* Incident Log Book
* Organization of Information Security Policy
* Personnel Security Policy and Procedure