# Information Security Incident Response Standard Procedure

# Jan 05 2020


| | |
|---|---|
| Document Title: | Information Classification and Handling Policy |
| Author(s) | Rajesh Kumar Singh, Rushi Luhar |
| Version Number: | V1.0 |
| Document Status: | Approved |
| Date Approved: | Jan 05 2020 |
| Approved By: | Executive Board |
| Effective Date: | Jan 10 2020 |
| Date of Next Review: | Jan 05 2021 |

## 1.1 Overview

This information security incident response procedure establishes an integrated approach for SentiSum to respond to security incidents. The procedure outlines the information passed to the appropriate personnel, assessment of the incident, the integrated response, documentation, and preservation of evidence.

## 1.2 Purpose

- Ensure a rapid, documented and controlled response to information security incidents
- Verification that an incident occurred.
- Maintain or restore business continuity
- Minimize the impact of the incident
- Determine how the incident was executed and prevent similar incidents in the future
- Improve security and incident response
- Keep the management informed of the situation and response

## 1.3 Scope

This policy applies to all employees, consultants and contractors who lead or respond to an information security incident.

## 1.4 Policy Statements

I. Any suspected Information Security Incidents are to be reported to the Director, Information Technology or CTO on an urgent basis. The CTO, when applicable, will evaluate, qualify and report the incident to the CEO.

II. Corrective measures will be prescribed according to the type and severity of the incident.

III. Employees, consultants and contractors may be engaged on an urgent basis to support remediation efforts.

IV. In all cases, the first response to an incident will be to identify and execute such measures as contain or otherwise minimize the incident or threat. This may involve immediately terminating network circuits, user accounts, or the rapid shutdown of any IT System, at the discretion of the Director, Information Technology or CTO.

## 1.5 Roles and Responsibilities

Roles and responsibilities for the various parties involved in all the steps of the incident response process are outlined below.

### 1.5.1 Incident Detection and Recording

Incidents may be discovered and reported by a client, a SENTISUM employee or a partner/vendor. The individual discovering an incident should immediately contact the IT Service Desk and the CTO.

All SENTISUM employees being alerted to a suspected or confirmed incident, (whether part of the IT Service Desk or not) should endeavour to capture the following incident details as clearly as possible:

1. The name of the individual who discovered the incident, and their contact details.
2. Date and time of the reported incident.
3. The nature of the incident, how and when it was detected.
4. The IT Systems or persons involved, and locations.
5. Name of system being targeted, along with operating system, IP address, and location.
6. Any information about the origin of the attack, including IP addresses, if applicable.
7. Preliminary evaluation of the severity or impact of the incident.

Immediately upon observation or notice of any suspected Security Event, Personnel shall use reasonable efforts to promptly report such knowledge and/or suspicion to the Information Security Department at the following address: **InformationSecurity@sentisum.com**

### 1.5.2 Incident Ownership, Monitoring, Tracking and Communication

The IT Director and dedicated Systems Security Specialists will be principally responsible for the Incident Ownership, Monitoring, Tracking and Communication.

The IT Director will engage the assistance of relevant subject matter experts and form a joint Computer Security Incident Response Team (CSIRT). The CSIRT will consider the following:

- Is the incident still in progress?
- What data or property is threatened and how critical is it?

- What is the impact on the business should the attack succeed?



- What system or systems are targeted, where are they located physically, and on the network?
- Is the incident inside the trusted network?
- Is an urgent response necessary?
- Can the incident be contained?
- What type of incident is this? Ex: virus, worm, intrusion, abuse, damage.
- What is the degree of confidence that the nature and impact of the Incident is fully understood?

A security incident report will be created. The incident will be categorized into the highest applicable level as detailed below.

LEVEL I - A threat to public safety or life

LEVEL II - A threat to data

LEVEL III - A threat to computer systems

LEVEL IV - A disruption of services

### 1.5.3 Containment

a. Team members from the CSIRT will follow an established procedure to contain or otherwise minimize the impact of the incident, such as procedures provided within Anti-Virus Software.
b. If there is no applicable procedure, the CSIRT will engage subject matter experts as may be required, including external experts, to contain the impact of the Incident, and will fully document the procedure followed.
c. Following the conclusion of the incident, this procedure will be appropriately communicated to enable use in future incidents.

### 1.5.4 Resolution and Recovery

a. CSIRT members will use forensic techniques including reviewing system logs, searching for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses, to determine the root cause of the incident.
b. Personnel will be granted system access for this purpose by the Director, Information Technology. Such personnel will vary in accordance with the incident.

c. CSIRT members will recommend changes to prevent a recurrence of the incident and/or to prevent infection of other systems. Such changes will be implemented per the Change Management procedure, or may be executed on an urgent basis. Team members will restore



the affected system(s) to the uninfected state. Restoration tasks may include, but are not limited to the following:

i. Re-installation of the affected system(s) from scratch, with a restoration of data from backups if necessary. Team members may be required to preserve evidence before doing this.
ii. Reset User passwords if passwords may have been compromised.
iii. Ensure that the system has been hardened by turning off or uninstalling unused services.
iv. Ensure that the system is fully patched.
v. Ensure that real time virus protection and intrusion detection is running.
vi. Ensure that the system is logging the correct events, at the appropriate level of detail.

### 1.5.5 Documentation

The following information will be documented using the attached Incident Report form.

1. All information collected in the *Incident Detection and Recording* section above.
2. The category of the incident. (Level I to IV)
3. How the incident occurred, whether via email, firewall, etc.
4. Origin of the attack, such as an IP address or computer/user name.
5. Other information related to a potential attacker
6. The response plan, including all preventative actions that were developed.
7. What was actually done to respond to the Incident?
8. The overall assessed effectiveness of the response.

### 1.5.6 Evidence Preservation

If evidence preservation is deemed appropriate, it may be appropriate to engage the services of Third Party Forensic Technology Services, per sections above, and notify the legal counsel.

If this is not indicated:

- Retain copies of logs, email, and other communication
- Make a list of witnesses, statements and contact details

- Retain all evidence until instructed otherwise by the CTO.



### 1.5.7 Incident Closure Report

A final report of the incident shall be prepared by the by the Director, Information Technology, with copies to the CTO. In addition to the information previously identified, the report shall contain:

i. Assessment of damages and/or costs. A review of the response policy and an update to any relevant policies. A plan for the prevention of a recurrence of the incident.
ii. Requirements for additional policies, procedures or training that may have prevented or lessened the impact of the incident.
iii. An analysis of the appropriateness and timeliness of the response, and opportunities for improvement.
iv. Availability of subject matter experts during the Incident.
v. Any other lessons arising from the incident.

## 1.6 Enforcement

Failure to comply with this policy may result in actions which include but are not limited to the following:

i. Denial of access to the `s information and information technology assets.
ii. Contractual remedies, as may be appropriate for third party suppliers, consultants and/or contractors, such as provisions for breach or termination of contract.
iii. Disciplinary action for employees, including, but not limited to, written warnings, suspensions with or without pay, and/or immediate termination of employment for cause without notice or other obligation.

## 1.7 Definitions

| Term | Definition |
|---|---|
| **Information Assets and Information Technology Assets** | Computer equipment (including laptop and desktop computers), software, operating systems, storage media, network accounts, electronic mail, internet access, portals, gateways, network devices, mobile devices, servers, telephones and telephone systems, multifunction printers, personal/home computers and devices while they are connected to the network either directly or over a VPN connection, information assets (whatever the media or format type) such as business or personal information, and any other thing that may be considered by the to be an information and information technology. |
| **Information Security Incident** | A security incident is an electronic or physical activity which may result in or threaten the loss of availability, compromise of integrity, or breach of confidentiality or privacy of the IT systems or information. Events and actions may be declared or reported as security incidents ahead of an actual breach or impact occurring. Security incidents can occur as a result of accidental or intentional breach of security policies and standard practices. Examples of security incidents include:<br>• Penetration of, or denial of service attacks on, networking infrastructure, servers, workstations, applications and websites<br>• Unauthorised access to sensitive corporate or personal information or client data |

| Term | Definition |
|---|---|
| | • Compromise of user or administrator accounts or credentials<br>• Loss or theft of end user devices, portable storage devices and hard copies of sensitive information<br>• Malware infection on the IT systems<br>• Social engineering attacks<br>• Unauthorised disclosure of protected information through electronic or physical means<br>• Use of the IT Systems for illegal purposes such as launching cyber-attacks, distributing illicit material or relaying spam<br>• Other violations of the Privacy and Security Framework Polices |
| **IP Address** | An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP Address is more commonly represented in the following format; **172.16.254.1**, although any of the numbers within each of the four decimal separated values can exist between 1 and 254. |
| **CSIRT** | A joint /IT Service Vendor technical team that responds to the security incident and if appropriate for that incident, engages external resources for containment and/or resolution/recovery. |