

**Incident Management Process**

**Version History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. No.** | **Release Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 13th Aug 2013 | Draft Version | Rahul raj | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.0 | 10th Nov 2013 | Baseline | Rahul raj | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.1 | 29th July 2015 | Clause 6.2 included for Responding to the incident with expected time of resolution | Rahul raj | Dhananjay Kumar | Ajay Kr. Zalpuri |

**Table of Contents**

[1. Introduction 4](#_Toc381029366)

[2. Scope 4](#_Toc381029367)

[3. Terms & Definitions 4](#_Toc381029368)

[4. Entry Criteria 4](#_Toc381029369)

[5. Inputs 4](#_Toc381029370)

[6. Process 5](#_Toc381029371)

[6.1 Incident Logging 5](#_Toc381029372)

[6.2 Incident Reporting and Analysis 6](#_Toc381029373)

[6.3 Incident & Event Resolution 6](#_Toc381029374)

[6.4 Learning from the incident 7](#_Toc381029375)

[7. Outputs 7](#_Toc381029376)

[8. Exit Criteria 7](#_Toc381029377)

# Introduction

The purpose of incident management procedure is to handle and resolve the incident.

An information security incident is indicated by a single or a series of unwanted and unexpected information lost that has a significant probability of compromising business operations and threatening information security. They are included but not limited to:

* Denial of Service
* Malicious Codes
* Inappropriate Usage
* Unauthorized access
* Information Security Incident data shall be reviewed for all ISMS related controls and procedures improvement.

# Scope

This procedure is applicable to NST employee.

# Terms & Definitions

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. Information Security Event data shall be reviewed for daily operation processes improvement.

**Information Security Incident**

An information security incident is indicated by a single or a series of unwanted and unexpected information lost that has a significant probability of compromising business operations and threatening information security. They are included but not limited to:

* Denial of Service
* Malicious Codes
* Inappropriate Usage
* Unauthorized access
* Information Security Incident data shall be reviewed for all ISMS related controls and procedures improvement.

# Entry Criteria

Any incident is raised and logged in Incident tracker.

# Inputs

1. Incidents reported through Incident tracker:

* IT
* Admin
* HR
* Physical security
* IT Security
* Finance

1. Potential incidents recorded in Management review Meeting

# Process

This process is subdivided into following sub-processes:

1. Incident Logging
2. Responding to the incident with expected time of resolution
3. Incident Reporting and Analysis
4. Incident & Event Resolution
5. Learning from the Incident

## 6.1 Incident Logging

1. All incidents will be logged in proper incident tracker with following details:

* Incident Description
* Type of Incident
* Incident Reported By
* Incident Reported to/ Attended By
* Severity
* Priority
* Impact
* Incident Date
* Status of the Incident
* Closure Date
* Workaround
* Root Cause Analysis
* Steps taken to resolve
* Lesson Learn/Suggestions for further improvement
* Remarks

1. Severity can be of 3 types – High, Medium and Low. It is up to department head/ IT manager to decide the priority of the incident.

* For IT Incidents and Admin incidents,

**Severity 1**

Incident disrupts business continuity and affects critical information systems, network or business process, either internally or externally

Incident impacts long-term perception of the organization

**Severity 2**

Incident disrupts normal work of an internal system or network

Incident affects critical business process(es)

Incident indicates a confirmed threat of imminent attack

**Severity 3**

Incident affects non-critical business process(es)

Incident indicates a potential threat of imminent attack

1. In Impact column, mention the impact in detail.
2. Besides logging the incident, report each incident to Security Council.
3. Incident status can have 3 values – Raised, WIP and Resolved:

* When incident is logged for the first time (as soon as incident occurs), its status is ‘Raised’.
* When work starts on the incident then its status should be updated to ‘WIP’.
* When actions taken to resolve the incident has resolved the incident then update the status of the incident to ‘Resolved’.

1. Collection of evidence to be done for information security events/incidents.

## 6.2 Responding to the incident with expected time of resolution

## Every incident which is reported, it will be allotted to “respective owner” for further action. The response will be sent to initiator of the incident with “respective owner” connect, who is handling the incident resolution. In consultation with “respective owner”, the expected time of resolution along with workaround (if possible) will also be communicated.

## 6.3 Incident Reporting and Analysis

Incident can be either an IT issue or Admin issue or some event discussed in Security Council meeting. Some examples of incidents are as follows:

* Machine infected from virus
* Hacking attack
* Network (LAN/Internet) down
* Machine theft
* Machine damaged
* Access Control mechanism not working
* Server crash
* Some internal team issue

Once incident has been reported, department head/project manager will analyze the incident to know its impact and root cause for it.

## 6.4 Incident & Event Resolution

1. Once root cause and impact of an incident is known, department head/IT Manager will try to resolve the incident by taking appropriate action.
2. There can be incidents where root cause is not known then in that case, department head/IT manager will try to find some workaround to solve the incident.

## 6.5 Learning from the incident

1. The learning gained from the incident shall be logged against the incident or in learning database and should be implemented so that incident can be prevented from occurring in the future. If the learning is being logged against the incident then it can be logged in ‘Suggestions for Further Improvement’ column. Lessons learnt/suggestions will be monitored in Security Council meetings.

# Outputs

1. Updated Incident log trackers
2. Updated Process Improvement log

# Exit Criteria

Incident is closed.