

Corrective & Preventive Action Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver.**  | **Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 22nd Aug 2013 | First Draft | Rahul Raj |  |  |
| 1.0 | 30th sep 2013 | Initial release | Rahul Raj | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.1 | 10th March 2014 | Updated for including ISO clause reference | Rahul Raj | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.2 | 29th June 2015 | update section 4.0 for certification update | Rahul Raj | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.3 | 3rd May 2017 | update section 4.1 & 4.2  | Rahul Raj | Dhananjay Kumar | Ajay Kr. Zalpuri |

**Table of Contents**

[1. Objectives 4](#_Toc369802594)

[2. Entry Criteria 4](#_Toc369802595)

[3. Inputs 4](#_Toc369802596)

[4. Task 4](#_Toc369802597)

[*4. 1 Continual Improvement* 4](#_Toc369802598)

[*4. 2 Corrective Action* 5](#_Toc369802599)

[*4. 3 Preventive Action* 5](#_Toc369802600)

[*4.4* *Outcome* 5](#_Toc369802601)

[5. Output 5](#_Toc369802602)

[6. Exit Criteria 5](#_Toc369802603)

# Objectives

The objective of the procedure is an effective implementation of Information Security Management System (QMS/ISMS) by proper disposition and corrective and preventive actions.

# Entry Criteria

As soon as any incident/non confirmative raised.

# Inputs

* Systems related incident/non confirmative
* Vulnerability Assessment, Risk Assessment, Penetration Testing etc.
* Feedback from internal and external audits.
* Output from Security Council reviews.
* Security Council minutes of meeting.
* Legal and statutory requirements.
* Need to change QMS/ISMS policies and processes.
* Process related incident/non confirmative
* Analysis of incident reports that have occurred.
* NCs.
* Event logs and other logs.
* Hardware related incident/non confirmative
* Analysis of hardware problems.

# Task

NST should improve the effectiveness of the QMS/ISMS by taking appropriate corrective actions immediately against nonconformities and issues as soon as they are found. It’s an ongoing process.

## *4. 1 Continual Improvement*

NST shall continually improve the effectiveness of the QMS/ISMS through the use of the QMS/ISMS policy, objectives, audit results, analysis of monitored events, corrective and preventive actions and management reviews, as per clause no 8.1 of ISO 27001:2013 & 8.5.1 of ISO9001:2015

## *4. 2 Corrective Action*

* NST shall take action as and when required to eliminate the causes of nonconformities with the QMS/ISMS requirements as per clause no 8.2 of ISO 27001:2013 & Clause 8.5.2 of ISO 9001:2015 in order to prevent recurrence. This also includes recording and reviewing the results of actions taken.

## *4. 3 Preventive Action*

* NST shall determine action as and when required to eliminate the cause of potential nonconformities with the QMS/ISMS requirements as per clause no 8.3 of ISO 27001:2013 & Clause 8.5.3 of ISO 9001:2015 in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems.
* NST shall pay constant attention through risk assessment for any changes in risks and identify preventive action requirements focusing attention on significantly changed risks.
* The priority of preventive actions shall be determined based on the results of risk assessment.

## *4.4 Outcome*

As an outcome of the corrective and preventive actions if any change to the system or the process is required, IT Manager shall review to ensure that the changes are incorporated in the relevant procedures/processes/policies/templates.

# Output

* Records of Corrective Action.
* Records of Preventive Action.
* Closed NC audit report
* Closed event log and other logs
* Closed incident log
* Updated processes/policies/procedures/templates.

# Exit Criteria

Verified Updated records