



## COMMUNICATION PLAN FOR INCIDENT MANAGEMENT

JUNE 2025

**DOC POLICY NO:**

-----  
**Developed By**  
-----

**Assistant General Manager, Information Technology and Security Compliance**

---

### Executive Summary

The Communication plan for Incident Management at NSPCL establishes a comprehensive strategy for effectively conveying information during IT and cybersecurity incidents. This plan ensures that all stakeholders, including employees, management, and external partners, receive timely and accurate updates regarding incident status, response actions and recovery efforts. The plan outlines key communication protocols, responsibilities and channels to be used during an incident.

By defining clear messaging strategies tailored to different audiences, NSPCL aims to maintain transparency, minimize uncertainty, and uphold stakeholder confidence throughout the incident management process. This structured approach not only facilitates coordination among teams but also aligns communication efforts with regulatory compliance and organizational objectives.


	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>COMMUNICATION PLAN FOR INCIDENT MANAGEMENT</b>	

Table of Contents

1. Purpose ..... 3

2. Objectives ..... 3

3. Stakeholders ..... 3


4. Communication Channels ..... 4

5. Communication Phases ..... 4

6. Escalation Procedure ..... 5

7. Review and Revision ..... 5

Commented [OA1]: This is to be formatted for structure

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>COMMUNICATION PLAN FOR INCIDENT MANAGEMENT</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

### 1. Purpose

The purpose of this communication plan is to ensure timely, accurate, and effective communication with all relevant parties during the incident management process. This plan aims to keep users and stakeholders informed about the status of incidents, response actions, and resolution progress.


### 2. Objectives

- Provide clear and consistent communication to all stakeholders.
- Ensure transparency and build trust during incident management.
- Facilitate coordination and collaboration among incident response teams.
- Minimize misinformation and manage stakeholder expectations.

### 3. Stakeholders

Identify the key stakeholders who need to be informed during an incident:

- **Internal Stakeholders:**
  - Executive Management (EVC/CEO, CTO, Chief Internal Audit & Risk Officer)
  - Information Technology and Security Compliance (ITSC) Department
  - Affected Department Heads
  - Incident Response Team (IRT)
  - All Employees
- **External Stakeholders:**
  - Customers
  - Vendors and Partners
  - Regulatory Bodies
  - Law Enforcement (if applicable)
  - Media (if applicable)

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>COMMUNICATION PLAN FOR INCIDENT MANAGEMENT</b>	

#### 4. Communication Channels

Utilize various communication channels to reach different stakeholders effectively.

- **Email:** For detailed updates and formal communication.
- **Phone Calls:** For urgent and direct communication.
- **Intranet/Portal:** For internal updates and resources.
- **Meetings:** For in-depth discussions and coordination.
- **SMS/Instant Messaging:** For quick alerts and notifications.
- **Press Releases:** For public announcements (if necessary).

#### 5. Communication Phases

##### 5.1 Preparation

- Maintain updated contact information for all stakeholders.
- Define roles and responsibilities for communication during incidents.
- Conduct regular training for the incident response team on communication protocols and tools.

##### 5.2 Detection and Analysis

- Inform the Incident Response Team and relevant department heads immediately upon detection of an incident.
- Provide an initial assessment of the incident, including potential impact and affected systems.


**Commented [OA2]:** Who provides?  
The ITSC team

##### 5.3 Containment

- Regularly update stakeholders on containment efforts and progress.
- Share short-term containment plans and any immediate actions taken to mitigate the incident.

##### 5.4 Eradication

- Communicate findings from the root cause analysis and steps taken to eradicate the threat.
- Confirm that the threat has been eliminated, and systems are secure.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>COMMUNICATION PLAN FOR INCIDENT MANAGEMENT</b>	

#### 5.5 Recovery

- Inform stakeholders about the progress of system restoration and testing.
- Notify when systems and services are fully operational, and any residual issues have been resolved.

#### 5.6 Post-Incident

- Share the outcomes of the post-incident review, including lessons learned and recommendations for future improvements.
- Provide a comprehensive incident report to executive management and other key stakeholders.

#### 6. Escalation Procedures

- *Please refer to the Escalation Procedures for Major incident Document.*

#### 7. Review & Revision

This document will undergo a formal review every two (2) years to ensure its continued relevance and effectiveness. The review will be conducted by the IT Security Team in collaboration with key stakeholders. If significant changes in technology, regulatory requirements, or threat landscape arise before the next scheduled review, an addendum will be issued and attached as an update to relevant sections of the policy. Such interim updates will remain in effect until the next comprehensive review and integration into the core policy.