



## IT INCIDENT RESPONSE FRAMEWORK AND PLAN

JUNE 2025

**DOC POLICY NO:**

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

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

---

### Executive Summary

The Incident Response Framework and Plan for NSPCL provides a comprehensive structure for effectively managing and mitigating IT and cybersecurity incidents. This framework is designed to enhance the organization's preparedness, ensure swift recovery, and minimize the impact of disruptions on business operations. The plan outlines a strategic approach encompassing key phases of incident response, including preparation, identification, containment, eradication, recovery, and post-incident review. It applies to all IT systems, networks, applications, and data managed by the Information Technology and Security Compliance (ITSC) Department, ensuring a cohesive response to various incidents such as security breaches, system outages, and data losses.



	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE</b> <b>DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>IT INCIDENT RESPONSE FRAMEWORK AND PLAN</b>	

Table of Contents

Commented [OA1]: Format for structure

1.	Purpose .....	3
2.	Scope .....	3
3.	Definitions .....	3
4.	Incident Response Plan .....	3
5.	Review & Revision .....	5

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE</b> <b>DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>IT INCIDENT RESPONSE FRAMEWORK AND PLAN</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

## 1. Purpose

The purpose of this framework is to establish a structured approach for managing and responding to IT and cyber security incidents within NSPCL. This aims to minimize the impact of incidents on business operations, ensure timely resolution, and maintain compliance with regulations.

## 2. Scope

This framework applies to all IT systems, networks, applications, and data managed by the Information Technology and Security Compliance (ITSC) Department. It covers all types of incidents; security breaches, system outages, data loss, and other IT-related disruptions.

## 3 Definitions

- **Incident:** An unplanned interruption or reduction in the quality of an IT service.
- **Major Incident:** A high-impact, urgent incident affecting multiple users or critical business functions.
- **Incident Management:** The process of identifying, analysing, and resolving incidents to restore normal service operation as quickly as possible.

## 4. INCIDENT RESPONSE PLAN

### I. Incident Management Objectives


- Ensure a consistent and effective approach to incident management.
- Minimize the impact of incidents on business operations.
- Restore normal service operation as quickly as possible.
- Maintain compliance with regulatory and legal requirements.
- Continuously improve incident management processes.

### II. Incident Management Process

- Log in to the device using an admin account.
- Download the latest version of the approved antivirus software.
- Run the installer with administrative privileges.
- Accept the license agreement

### 4.2.1 Incident Identification and Logging

- **Detection:** Incidents can be detected through automated monitoring tools, user reports, or IT staff observations.
- **Logging:** All incidents must be logged in the Incident Management System (IMS) with relevant details, including the date and time of occurrence, description, affected systems, and initial severity assessment.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE</b> <b>DEPARTMENT</b>	DOC NO:	
	DOCUMENT TITLE: <b>IT INCIDENT RESPONSE FRAMEWORK AND PLAN</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>	

#### 4.2.2 Incident Categorization and Prioritization

- Categorization: Incidents should be categorized based on the type of issue (e.g., hardware, software, network, security).
- Prioritization: Incidents should be prioritized based on their impact and urgency. Priority levels include:
  - P1 (Critical): Major incidents affecting critical business functions or multiple users.
  - P2 (High): Significant incidents affecting important business functions or a large number of users.
  - P3 (Medium): Moderate incidents affecting non-critical business functions or a limited number of users.
  - P4 (Low): Minor incidents with minimal impact on business operations.

#### 4.2.3 Incident Investigation and Diagnosis


- Initial Assessment: Conduct an initial assessment to determine the scope and impact of the incident.
- Root Cause Analysis: Investigate the root cause of the incident using appropriate diagnostic tools and techniques.
- Documentation: Document all findings, including the root cause, affected systems, and potential solutions.

#### 4.2.4 Incident Resolution and Recovery

- Resolution: Implement appropriate solutions to resolve the incident and restore normal service operation.
- Recovery: Ensure that all affected systems and services are fully operational and functioning as expected.
- Verification: Verify that the incident has been resolved and that no further issues are present.

#### 4.2.5 Incident Closure

- Closure: Close the incident in the IMS once it has been resolved and verified.
- Documentation: Update the incident record with all relevant details, including the resolution steps, recovery actions, and any lessons learned.
- Communication: Communicate the resolution to affected users and stakeholders.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE</b> <b>DEPARTMENT</b>	DOC NO:	
	DOCUMENT TITLE: <b>IT INCIDENT RESPONSE FRAMEWORK AND PLAN</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>	

### 5. 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.