k

IT INCIDENT RESPONSE POLICY & PROCEDURES

JUNE 2025

DOC POLICY NO:

Developed By

Assistant General Manager, Information Technology and Security Compliance

Executive Summary

The IT Incident Response Policy for NSPCL is designed to provide a comprehensive framework for effectively managing and responding to IT and cybersecurity incidents. This policy aims to minimize the impact of such incidents on business operations, facilitate a swift resolution process, and ensure compliance with relevant regulatory requirements.

Table of Contents

Commented [OA1]: Format for structure

1.1 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 requirements.

1.2 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, including security breaches, internet downtime, service disruption, system outages, data loss, and other IT-related disruptions.

1.3 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.
- **Response Time:** The maximum time allowed to acknowledge the incident and begin initial assessment or action.
- **Resolution Time:** The maximum time allowed to resolve the issue and fully restore service functionality.
- **RPO (Recovery Point Objective):** The maximum acceptable amount of data loss measured in time. It defines how much data the business can tolerate losing.
- **RTO (Recovery Time Objective):** The maximum acceptable time allowed to recover from an incident before significantly impacting business operations.
- **Response Time:** Time taken to acknowledge and begin triaging the incident.
- **Resolution Time:** Time taken to fully resolve the incident and restore services to normal.

1.4 Roles and Responsibilities

- **Incident Manager:** Responsible for overseeing the incident management process, coordinating response efforts, and ensuring timely resolution.
- **ITSC Team:** Responsible for detecting, logging, categorizing, investigating, and resolving incidents.
- **Users:** Responsible for reporting incidents promptly and providing necessary information to the ITSC team.
- **Stakeholders:** Responsible for supporting the incident management process and ensuring compliance with policies and procedures.

1.5 Incident Turnaround Time (TAT) Table

Incident Category	Definition	Response Time	Resolution Time	RPO	RTO
Low	Minor issue with no impact on operations; workaround available	≤8 business hours	≤ 3–5 business days	Up to 24 hours	Up to 5 business days
Medium	Issue affects a single user or non-critical function; limited operational impact	≤ 4 business hours	≤ 1–2 business days	Up to 12 hours	Up to 2 business days
High	Significant impact on multiple users or a critical function; no workaround	≤ 1 hour	≤ 8–12 business hours	Up to 4 hours	≤ 12 hours
Emergency	Complete outage of a critical system or data loss; severe operational impact	Immediate (≤ 15 minutes)	≤ 4 hours	Near-zero (≤ 1 hour)	≤ 4 hours

- Times are measured in defined **business hours**, unless a 24/7 support model is used.
- Emergency and high-severity incidents may trigger **escalation protocols**.

Commented [OA2]: Where is this used?

1.6 Communication and Escalation

- Communication Plan: *Please refer to the Communication Plan for Incident Management Document.*
- Escalation Procedures: *Please refer to the Escalation Procedures for Major incident Document.*

1.7 Continuous Improvement

- Post-Incident Review: Conduct post-incident reviews to identify lessons learned and areas for improvement.
- Metrics and Reporting: Track and report key incident management metrics, such as incident volume, resolution time, and user satisfaction.
- Process Improvement: Continuously review and improve the incident management process based on feedback and performance data.

1.8 Review and Revision

This policy 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.