



## ESCALATION PROCEDURES FOR MAJOR INCIDENTS

JUNE 2025

**DOC POLICY NO:**

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

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


---

### EXECUTIVE SUMMARY

The Escalation Procedures for Major Incidents at NSPCL provide a critical framework for swiftly addressing and resolving significant IT and cybersecurity incidents that could disrupt business operations. This document outlines a structured approach to ensure that major incidents are identified, communicated, and escalated efficiently to minimize their impact and facilitate timely resolutions.

These procedures delineate clear roles and responsibilities for all stakeholders involved in the incident management process. By establishing defined escalation paths, this framework ensures that incidents are addressed at the appropriate levels of the organization, facilitating quick decision-making and resource allocation.


The focus of these procedures is to enhance the organization's ability to manage high-impact incidents effectively while maintaining operational continuity and compliance with regulatory obligations. By fostering a proactive approach to incident escalation, NSPCL aims to mitigate risks, restore services promptly, and protect the integrity of its IT infrastructure, ultimately reinforcing stakeholder trust and organizational resilience.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>ESCALATION PROCEDURES FOR MAJOR INCIDENTS</b>	

**Table of Contents**

Commented [OA1]: Format for structure

1.	Purpose .....	3
2.	Criteria for Escalation .....	3
3.	Roles & Responsibilities .....	3
4.	Escalation Levels and Points .....	4
5.	Escalation Process .....	5
6.	Post Escalation Review .....	5
7.	Compliance & Enforcement .....	5
8.	Review & Revision .....	5

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>ESCALATION PROCEDURES FOR MAJOR INCIDENTS</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

1. Purpose

The purpose of this document is to establish a standardized escalation process to ensure timely and appropriate handling of major IT and cybersecurity incidents. Prompt escalation mitigates operational risk, protects critical infrastructure, and promotes business continuity through the engagement of the correct level of expertise and authority. This policy enhances North South Power Company Limited’s ability to:

- Minimize damage caused by incidents.
- Coordinate technical and managerial responses.
- Ensure timely communication and decision-making.
- Maintain compliance with internal policies and external regulations.

2. Criteria for Escalation

Escalation is warranted when incidents meet one or more of the following criteria:

- Severity: Disrupts critical services or affects a large number of users.
- Scope: Impacts multiple business units, systems, users or geographic locations.
- Duration: Remains unresolved beyond standard response time thresholds.
- Complexity: Requires specialized skills or cross-functional support.
- Regulatory Impact: May lead to legal or compliance violations.
- Public Relations: Could attract media attention or damage the company’s brand.


Each incident is initially categorized based on these metrics to determine the appropriate escalation path.

Commented [OA2]: Is this the criteria/ definition for an incident to be categorized as a Major incident.

3. Roles and Responsibilities

Role	Responsibility
ITSC Team	First responders, incident classification, initial troubleshooting.
Incident Manager	Tactical coordination, technical triage, escalation decision-making.
Head of ITSC	Strategic direction, resource deployment, executive reporting.
CIARMO	Risk oversight, regulatory coordination, policy alignment.
EVC	Business impact mitigation, final decision authority, public messaging.

Commented [OA3]: Who is this? Just for clarity. Is this the department manager or an ITSC manager

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>ESCALATION PROCEDURES FOR MAJOR INCIDENTS</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

#### 4. Escalation Levels and Points

##### Level 1: Initial Response Team (ITSC)

- Trigger: All reported or detected incidents.
- Responsibilities:
  - Log, categorize, and prioritize the incident.
  - Attempt immediate resolution using SOPs.
  - Initiate impact assessment.
- Escalation Point: Incident Manager.

##### Level 2: Incident Manager

- Trigger: Incidents unresolved at Level 1 or that meet any escalation criteria.
- Responsibilities:
  - Oversee technical and procedural response.
  - Engage subject matter experts.
  - Notify Head of ITSC if escalation is needed.
- Escalation Point: Head of ITSC Department.

##### Level 3: Head of ITSC Department


- Trigger: High-severity or prolonged incidents; operational disruption.
- Responsibilities:
  - Make decisions regarding resource allocation.
  - Coordinate internal and external support.
  - Provide real-time updates to management.
- Escalation Point: Chief Internal Audit & Risk Management Officer (CIARMO).

##### Level 4: Chief Internal Audit & Risk Management Officer (CIARMO)

- Trigger: Regulatory, reputational, or high-risk implications.
- Responsibilities:
  - Manage risk and ensure policy compliance.
  - Notify external regulators or partners if applicable.
  - Coordinate with legal, compliance, and PR teams.
- Escalation Point: Executive Vice Chairman.

##### Level 5: Executive Vice Chairman/CEO (EVC/CEO)

- Trigger: Business-wide impact, reputational crisis, or board-level intervention.
- Responsibilities:
  - Make final decisions on company-wide communications and remediation.
  - Report to the Board of Directors.
  - Lead public relations efforts if necessary.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>ESCALATION PROCEDURES FOR MAJOR INCIDENTS</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

## 5. Escalation Process

### 5.1 Initial Notification

- Step 1: Incident logged by ITSC with relevant metadata (timestamp, severity, systems).
- Step 2: Initial troubleshooting begins. Escalation to Incident Manager if unresolved within threshold.

### 5.2 Escalation to Higher Levels

- Step 3: Incident Manager reviews logs, escalates to Head of ITSC if required.
- Step 4: Head of ITSC evaluates operational impact and engages CIARMO.
- Step 5: CIARMO performs enterprise risk evaluation, escalates to EVC/CEO as necessary.

### 5.3 Communication During Escalation

- Stakeholder Notifications: Triggered at each level through defined communication channels.
- Status Reporting: Regular, timestamped updates shared with internal teams and affected departments.
- Documentation: All decisions, escalations, and resolutions are logged in the Incident Register.

## 6. Post-Escalation Review

Once the incident is resolved, a formal Post-Incident Review (PIR) must be conducted within 5 business days. This includes:

- Root cause analysis.
- Timeline of escalation decisions and actions taken.
- Review of impact, response effectiveness, and escalation accuracy.
- Documentation of Lessons Learned.
- Updates to escalation procedures or training programs as needed.

**Commented [OA4]:** What team conducts this?

## 7. Compliance and Enforcement

Failure to comply with these escalation procedures may result in:

- Delays in incident resolution.
- Legal or regulatory penalties.
- Disciplinary actions against responsible personnel.

All employees and contractors involved in IT operations or incident management must undergo mandatory training on these procedures annually.

## 8. Review and 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.