Malware Incident Response Standard Operating Procedure (SOP)

JUNE 2025

DOC POLICY NO:

Developed By

Assistant General Manager, Information Technology and Security Compliance

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: 1 DATE OF ISSUE: xxxxxx REVISED DATE: **N/A**
	DOCUMENT TITLE **MALWARE INCIDENT RESPONSE STANDARD OPERATING PROCEDURE (SOP)**	

Table of Contents

Commented [OA1]: Format for structure

NSP	**INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT**	DOC NO: 1 DATE OF ISSUE: xxxxxx REVISED DATE: **N/A**
	DOCUMENT TITLE **MALWARE INCIDENT RESPONSE STANDARD OPERATING PROCEDURE (SOP)**	

1. Purpose

The purpose of this procedure is to provide a structured, systematic approach for identifying, containing, eradicating, and recovering from malware incidents affecting North South Power Company Limited's IT assets and infrastructure. Prompt and coordinated response help minimize damage, reduce recovery time, and prevent future occurrences.

2. Scope

This procedure applies to all systems, users, devices, and third parties within the organization that are subject to malware threats or indicators of compromise (IOCs).

3. Roles & Responsibilities

Commented [OA2]: Is this the IR Team? If so, title it as that

Role	**Responsibility**
IT Security Team	Lead the response, analyse infections, coordinate containment, and document incident resolution.
System Administrators	Assist in isolating affected systems, applying patches, and restoring functionality.
HR/Legal	Handle compliance, disciplinary action, and communication
End Users	Report any suspected malware activity immediately and avoid interacting with affected systems.
Management	Authorize escalations and approve decisions requiring service disruption or legal involvement.

4. Incident Response Steps

Step 1: Detection & Reporting

- Receive alerts via antivirus, IDS/IPS, SIEM tools.
- Users should immediately report suspicious activities (e.g., slow performance, pop-ups, unauthorized access) to the IT Help Desk.
- IT systems with real-time scanning may also automatically alert the IT Security Team.
- Log initial incident details: source, type, device, user, time.
- Assign severity level based on predefined criteria (low, medium, high, critical).
- Notify the incident response team (IR Team).

Commented [OA3]: Please provide the meaning of shortcuts in a mini definition section

Step 2: Containment

- Short Term: Disconnect the infected device from the network (wired/Wi-Fi) effectively isolating the affected systems from the network to prevent spread.
- Long Term: Disable affected user accounts, shared drives, quarantine files, restrict access and revoke user credentials, if applicable.
- Preserve forensic evidence, log containment actions taken and affected assets before proceeding to eradication.

Step 3: Analysis

- Analyse logs, alert data, and malware behaviour to determine:
    - Type of malware (e.g., Trojan, ransomware, spyware).
    - Infection vector (email, USB, network).
    - Affected data and system integrity.

Step 4: Eradication

- Use updated anti-malware tools to remove the infection and clean the systems.
- Delete malicious files, registry entries, and scripts.
- Apply security patches, revoke compromised credentials, and reset configurations.
- If cleaning fails, perform a full reinstallation of the affected system(s).

Step 5: Recovery

- Restore data from verified backups, if needed.
- Monitor systems for residual infection or unusual behavior.
- Reconnect systems to the network after verification and under controlled observation.
- Confirm normal operations and user access.

Step 6: Containment

- Conduct a post-incident review
- Document the incident, actions taken, and lessons learned.
- Update threat signatures, security policies and SOPs based on findings if necessary.
- Submit final report to IT Leadership.

Commented [OA4]: Head of ITSC team

5. Escalation Matrix

Formatted Table

Severity	Description	Escalate To
Low	Isolated system infection, no data loss	System Admin
Medium	Multiple systems infected, potential data exposure	IT Security Lead
High	Widespread infection, confirmed data compromise or ransomware	CIO, Legal, External Authorities if needed

6. Documentation & Records

Maintain full lifecycle details (all incident logs, screenshots, reports, and post-incident analysis) in the **Cybersecurity Incident Register** for a minimum of 2 years.

7. Review and Revision

	INFORMATION TECHNOLOGY AND SECURITY **COMPLIANCE DEPARTMENT**	DOC NO: 1 DATE OF ISSUE: xxxxxx REVISED DATE: **N/A**
	DOCUMENT TITLE **MALWARE INCIDENT RESPONSE STANDARD** **OPERATING PROCEDURE (SOP)**	

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.