



## VULNERABILITY AND PATCH MANAGEMENT POLICY

JUNE 2025

DOC POLICY NO:

-----  
Developed By  
-----

Assistant General Manager, Information Technology and Security Compliance

---

### Executive Summary

North South Power Company Limited's Vulnerability and Patch Management Policy is designed to protect the company's IT infrastructure by systematically identifying, evaluating, and mitigating vulnerabilities. The policy ensures that vulnerabilities are regularly scanned and assessed, prioritized based on risk, and remediate through timely deployment. This proactive approach helps maintain the security and integrity of the company's assets, while continuous monitoring and improvement processes ensure the policy remains effective against evolving threats.

The policy assigns clear roles and responsibilities to the IT Security Team, System Administrators, and all employees and contractors, ensuring a coordinated effort in managing vulnerabilities and applying patches. Compliance with this policy is mandatory, with non-compliance potentially resulting in disciplinary action. By adhering to this policy, North South Power Company Limited aims to maintain a secure IT environment, protect its assets, and ensure operational continuity.



	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>VULNERABILITY AND PATCH MANAGEMENT POLICY</b>	

Table of Contents

Commented [OA1]: Format for structure

1.	Purpose .....	3
2.	Scope .....	3
3.	Policy Statement .....	3
4.	Roles and Responsibilities .....	3
5.	Vulnerability Management Process .....	4
6.	Patch Management Process .....	4
7.	Continuous Monitoring and Improvement .....	5
8.	Compliance and Enforcement .....	5
9.	Review and Revision .....	5

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>VULNERABILITY AND PATCH MANAGEMENT POLICY</b>	

### 1. Purpose

The purpose of this policy is to establish a comprehensive approach to identify, evaluate, and mitigate vulnerabilities within North South Power Company Limited's IT infrastructure. This policy defines a structured and consistent approach for identifying, assessing, prioritizing, and remediating vulnerabilities in North South Power Company Limited's IT environment. It aims to minimize exposure to known vulnerabilities, ensure timely deployment of vendor-released patches, maintain compliance with security best practices and standards and protect critical systems and business data from exploitation.

### 2. Scope

This policy applies to:

- All hardware and software components, including servers, desktops, laptops, mobile devices, and network infrastructure.
- Operating systems, databases, applications (on-premises and cloud-based), and third-party software used across the organization.
- All North South Power Company Limited personnel (employees, contractors, and interns) and third-party service providers with access to the company's IT systems.

### 3. Policy Statement

North South Power Company Limited is committed to maintaining a secure IT environment by:

- Performing vulnerability scans at defined intervals and after significant changes.
- Applying security patches and updates according to risk-based prioritization.
- Ensuring that all patching actions are tested, documented and tracked.
- Establishing and maintain roles and workflows for timely resolution of vulnerabilities.
- Training all stakeholders on responsibilities related to patch & vulnerability management.

### 4. Roles and Responsibilities

#### IT Security Team


- Conduct vulnerability scans.
- Manage the vulnerability assessment lifecycle.
- Coordinate remediation efforts and report metrics to leadership.

#### System Administrators

- Apply, test, and validate patches.
- Ensure backup procedures before deployment.
- Maintain accurate records of patching activities.

#### Employees & Contractors

- Promptly report unusual system behaviour.
- Avoid delaying system updates.
- Follow safe computing and security guidelines.

	<b>INFORMATION TECHNOLOGY AND SECURITY</b> <b>COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>VULNERABILITY AND PATCH</b> <b>MANAGEMENT POLICY</b>	

## 5. Vulnerability Management Process

### 5.1 Identification

- Use approved scanning tools (e.g., Nessus, OpenVAS) to scan all assets at least quarterly and after major updates or deployments.
- Capture asset inventory with current patch levels, versions, and configurations.

### 5.2 Evaluation

- Classify vulnerabilities based on CVSS score and business impact.
- Tag critical assets (e.g., finance servers, domain controllers) for heightened attention.

### 5.3 Prioritization

- Assign severity levels (Critical, High, Medium, Low).
- Focus on vulnerabilities:
  - With known exploits in the wild.
  - Affecting exposed or critical systems.
  - With regulatory/compliance impact (e.g., ISO 27001, NDPR).

### 5.4 Remediation

- Apply fixes via patches, configuration changes, or network segmentation.
- Define timelines:
  - Critical = within 72 hours
  - High = within 7 days
  - Medium = within 14 days
  - Low = within 30 days

### 5.5 Verification

- Retest resolved vulnerabilities.
- Perform root cause analysis on repeated or unaddressed findings.

## 6. Patch Management Process

### 6.1 Patch Identification


Monitor advisories from:

- Vendor web sites (Microsoft, Cisco, etc.)
- Security databases (NIST NVD, MITRE)
- Subscription alerts (e.g., US-CERT, CISA)

### 6.2 Patch Testing

Use staging environments to:

- Evaluate impact on performance and system compatibility.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>VULNERABILITY AND PATCH MANAGEMENT POLICY</b>	

- Ensure continuity of critical applications before production deployment.

**6.3 Patch Deployment**

- Schedule patching during approved maintenance windows.
- Follow change management protocol with rollback plans.
- Use centralized patch management systems (e.g., WSUS, SCCM, ManageEngine).

**6.4 Patch Verification**

- Validate successful installation using automated tools or manual logs.
- Document issues and resolutions.

**6.5 Documentation**

Maintain logs of:

- Applied patches (name, CVE ID, date, system)
- Known issues and workarounds
- Approval records from change management

**7. Continuous Monitoring and Improvement**

North South Power Company Limited shall:

- Continuously monitor assets for emerging threats and newly disclosed vulnerabilities.
- Review scan findings with trends, risk dashboards, and remediation metrics.
- Conduct post-incident reviews to strengthen the patch management lifecycle.
- Integrate vulnerability intelligence into IT governance and procurement decisions.

**8. Compliance and Enforcement**

- Failure to adhere to this policy may result in disciplinary actions, including access restriction, contract termination, or legal consequences.
- The IT Security Team will perform random audits and quarterly compliance checks.
- Exceptions to this policy must be approved by the head of ITSM or designated authority, with justification and documented risk acceptance.

Commented [OA2]: ITSC

**9. 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 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.