



ANTI-VIRUS AND MALICIOUS CODE PREVENTION POLICY

JUNE 2025

DOC POLICY NO:

Developed By

Assistant General Manager, Information Technology and Security Compliance

Executive Summary

North South Power Company Limited is dedicated to safeguarding its IT infrastructure through a comprehensive Anti-virus and Malicious Code Prevention Policy. This policy aims to protect the company's assets, ensure data integrity, and maintain operational continuity by implementing and maintaining up-to-date anti-virus and anti-malware solutions. Regular system scans, continuous monitoring, and prompt response to malware incidents are key components of this policy.

The policy assigns clear roles and responsibilities to the IT Security Team, System Administrators, and all employees and contractors, ensuring a coordinated effort in preventing and managing malware threats. Regular training sessions and user awareness programs are conducted to educate employees on safe computing practices and the importance of malware prevention. 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 and resilient IT environment.


	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: N/A
	DOCUMENT TITLE: ANTI-VIRUS AND MALICIOUS CODE PREVENTION POLICY	

Table of Contents

1. Purpose 3

2. Scope 3

3. Definitions 3

4. Policy Statement 3

5. Roles and Responsibilities 4


6. Anti-virus and Malware Prevention Process 4

7. User Awareness and Training 6

8. Compliance and Enforcement 6

9. Review and Revision 7

Commented [OA1]: Table of contents should be properly formatted

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: N/A
	DOCUMENT TITLE: ANTI-VIRUS AND MALICIOUS CODE PREVENTION POLICY	

1. Purpose

The purpose of this policy is to define a structured approach for the prevention, detection, mitigation, and reporting of malware and malicious code threats across North South Power Company Limited's IT ecosystem. By enforcing this policy, the company aims to:

- Safeguard the confidentiality, integrity, and availability of its data and systems.
- Prevent unauthorized access, data corruption, and system outages caused by malware.
- Reduce the organization's exposure to internal and external cyber threats.
- Ensure timely and coordinated response to malware incidents.

2. Scope

This policy applies to:

- All information systems (servers, workstations, laptops, mobile devices, and cloud-hosted environments) owned, operated, or managed by North South Power Company Limited.
- All employees, contractors, consultants, third-party enabled staff who use or access North South Power company's information resources.
- All software, applications, databases, and network components within the organization's control.

3. Definitions

- Malware: Software designed to disrupt, damage, or gain unauthorized access to systems.
- Antivirus Software: A program used to detect, prevent, and remove malware.
- Endpoint Protection: Security solutions installed on devices like laptops, desktops, and servers.
- Zero-Day Attack: A threat exploiting an unknown vulnerability.


Commented [OA2]: This is not used in the policy

4. Policy Statement

North South Power Company Limited is committed to maintaining a robust information security posture by:

- Implementing industry-recognized anti-virus and anti-malware technologies.
- Conducting routine and on-demand malware scans across all systems and endpoints.
- Continuously monitoring systems for abnormal behavior and threats.
- Promoting safe digital habits through regular training and awareness programs.
- Enforcing compliance to ensure proper usage and protection of IT assets.

Commented [OA3]: I suggest this is defined alongside the endpoint protection in Clause 3

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: N/A
	DOCUMENT TITLE: ANTI-VIRUS AND MALICIOUS CODE PREVENTION POLICY	

5. Roles and Responsibilities

To ensure comprehensive malware protection, the following responsibilities are assigned:

IT Security Team

- Select, configure, and manage centralized anti-virus and malware defense tools.
- Monitor alerts and logs to detect and respond to infections in real-time.
- Maintain incident response procedures for malware-related events.
- Maintain and enforce policy compliance, including reviews.

System Administrators

- Ensure anti-virus software is installed, activated, and updated on all managed systems.
- Schedule and verify completion of regular scans.
- Report and document any unusual system behaviors or suspected infections to the IT Security Team.

IT Audit & Risk Management Team

- Perform reviews and audit of antivirus & malware policy as well as its implementation across the company and its infrastructures.

Employees and Contractors

- Adhere to safe computing practices as outlined by the IT Security Team.
- Avoid downloading or executing unauthorized software or attachments.
- Promptly report suspected malware incidents or phishing attempts.
- Complete all assigned security awareness training sessions.

6. Anti-virus and Malware Prevention Process


6.1 Installation

All corporate devices, including desktops, laptops, servers, and mobile devices, must have company-approved anti-virus and anti-malware software installed prior to deployment. The company approved antivirus and antimalware tools are BitDefender GravityZone Business suite for Endpoint, Microsoft Defender for email security.

6.2 Central Management

All antivirus software must:

- Be centrally managed via a Security Operations Centre (SOC) or Endpoint Detection & Response (EDR) platform.

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: N/A
	DOCUMENT TITLE: ANTI-VIRUS AND MALICIOUS CODE PREVENTION POLICY	

- Support real-time scanning, ~~behavioural~~behavioral detection, and automatic quarantining.

6.3 Updates

Anti-virus software must be configured to update virus definitions and threat signatures automatically. Regular updates to software patches must be managed and verified by the IT Security Team. All proprietary updates by OEM may be treated as emergency updates when the need arises.

Emergency updates may include:

a. Security Fixes

- Patch for a zero-day vulnerability
- Disabling a compromised user account or API key
- Removing malicious code or backdoors
- Updating SSL/TLS certificates due to a breach or expiration

b. Service Restoration

- Rolling back a failed deployment
- Restarting services or application servers
- Reverting to a previous stable version due to critical bugs
- Clearing corrupted cache or sessions to restore normal behavior

c. Data-Related Fixes

- Correcting corrupted or critical production data
- Running emergency scripts to restore lost transactions
- Removing or quarantining harmful or inconsistent data
- Fixing broken data integrations or syncs

d. Configuration Changes

- Switching to a backup database or failover node
- Temporarily increasing system resources (CPU/memory)
- Disabling a broken feature or component via config flags
- Updating connection strings or credentials for third-party services

e. Incident Response Actions


- Blocking IPs or disabling endpoints under attack (DDoS, brute force, etc.)
- Modifying firewall or WAF rules
- Temporarily restricting user access to mitigate damage

f. Dependency or Integration Fixes

- Updating broken third-party API credentials or tokens
- Disabling external integrations causing application crashes
- Applying hotfixes from a vendor or internal dev team

g. Logging and Monitoring Adjustments

- Enabling debug logging temporarily to diagnose an issue
- Adding custom alerts for unstable modules

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: N/A
	DOCUMENT TITLE: ANTI-VIRUS AND MALICIOUS CODE PREVENTION POLICY	

6.4 Malware Protection (Email Protection)

- All inbound and outbound emails must be scanned.
- Suspicious attachments or links should be blocked or quarantined automatically.

6.5 Malware Protection (Web Filtering & Removable Media)

- Block access to known malicious domains or suspicious downloads.
- Log and audit web activity for anomaly detection.
- Removable media must be scanned automatically on insertion.
- Usage should be restricted and monitored.

6.6 Scanning

- Full system scans shall be scheduled weekly.
- Quick scans shall be performed daily or during system startup.
- On-access scanning (real-time protection) must remain enabled at all times.

6.7 Monitoring

All security tools must support centralized logging and alerting, with malware detection alerts configured to immediately notify appropriate personnel for rapid response. Upon detection, infected systems must be promptly isolated, and the IT Security Team must execute a malware response plan that includes

- containment of the affected systems,
- removal or isolation of malicious code,
- restoration from backups as needed
- and conducting a root cause analysis with full documentation of the incident.

6.8 Exception

Any deviation from this policy requires a formal risk assessment and written approval from the Head of ITSC.

7. User Awareness and Training


To strengthen the human layer of defense:

- The IT Security Team will conduct biannual cybersecurity awareness training.
- Employees will receive periodic email bulletins and infographics on safe computing.
- Simulated phishing tests may be conducted to assess user vigilance.
- New hires must complete security onboarding training within their first month.

8. Monitoring, Compliance and Enforcement

Commented [OA4]: Is this currently a position at NSP, Mr Wale?

Formatted: Indent: Before: 1.27 cm, No bullets or numbering

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: N/A
	DOCUMENT TITLE: ANTI-VIRUS AND MALICIOUS CODE PREVENTION POLICY	

All individuals covered under the scope of this policy are expected to comply with its provisions. Failure to adhere may result in:

- Formal warnings or written reprimands.
- Suspension of access privileges.
- Disciplinary action being taken by the disciplinary ~~committee as~~committee may be formed by management.

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 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.