



THIRD-PARTY ANTIVIRUS & MALWARE COMPLIANCE ADDENDUM

JUNE 2025

DOC POLICY NO:


Developed By

Assistant General Manager, Information Technology and Security Compliance

Executive Summary

The North South Power ITSC Disaster Recovery Plan (DRP) establishes the framework, responsibilities, and procedures to enable the timely recovery and continuity of critical IT systems and services following a disaster event. This plan ensures that disruptions caused by cyberattacks, hardware failures, natural disasters, or network outages do not compromise the integrity, availability, and confidentiality of North South Power's business operations. The DRP supports North South Power's commitment to service resilience, regulatory compliance, and continuous improvement of its business continuity strategy.

Commented [OA1]: This is not the correct executive summary for this policy. this is fro DRP

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO:
	DOCUMENT TITLE: THIRD-PARTY ANTIVIRUS & MALWARE COMPLIANCE ADDENDUM	DATE OF ISSUE: REVISED DATE: N/A

1. Purpose

To ensure all third-party vendors and service providers who access or manage North South Power Company Limited systems comply with our antivirus and malware prevention standards.

2. Scope

Applies to all vendors, contractors, and partners with access to:

- Company data
- Internal networks or applications
- Devices connected to company systems

3. Third-Party Responsibilities

Third parties shall:

- Install and maintain up-to-date antivirus and antimalware solutions on all systems used to access North South Power Company systems.
- Ensure antivirus software is configured for real-time protection and automated updates.
- Cooperate fully with the company during any malware incident or investigation.
- Adhere to secure coding practices (for development vendors) to reduce malware risk.

4. Access Conditions

- No third party shall connect to the company network without verification of compliant antivirus software.
- Periodic audits may be conducted to validate malware prevention controls.
- Any devices found non-compliant may be denied access until remediated.

5. Notification Requirements

- Third parties must notify North South Power Company Limited within 24 hours of any malware-related security incident that could impact the company.
- A formal incident report must be submitted within 5 working days.

6. Enforcement

Non-compliance may result in termination of access, financial penalties, or contract suspension and continued access is contingent on adherence to this addendum.

7. Policy Review

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.