



Antivirus Installation & Update 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 ANTIVIRUS INSTALLATION & UPDATE STANDARD OPERATION PROCEDURE (SOP)	

Table of Contents

1. Purpose 3

2. Scope 3

3. Roles and Responsibilities 3

4. Antivirus Installation Procedure 3

5. Antivirus Update Procedure 4

6. Monitoring & Reporting 4


7. Review and Revision 4

8. Audit & Compliance 4

9. Review & Revision 5

10. Related Documents 5

Commented [OA1]: TOC should be formatted for structure

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: 1
	DOCUMENT TITLE ANTIVIRUS INSTALLATION & UPDATE STANDARD OPERATION PROCEDURE (SOP)	DATE OF ISSUE: xxxxxx REVISED DATE: N/A

1. Purpose

This Standard Operating Procedure (SOP) outlines the standardized process for installing, configuring, updating, and maintaining antivirus software on all devices used within North South Power Company Limited. This ensures consistent protection against malware and other malicious threats across the organization.

2. Scope

This SOP applies to all end-user devices (desktops, laptops, mobile devices), servers and virtual machines, networked devices with operating systems and any third-party devices granted access to North South Power Company Limited’s systems.

3. Roles & Responsibilities

Role	Responsibility
IT Security Team	Evaluate, select, and maintain antivirus solutions
	Support antivirus installation and troubleshooting
System Administrators	Ensure all systems are compliant with antivirus standards
End Users	Ensure antivirus is not disabled or tampered with on their devices


4. Antivirus Installation Procedure

Step 1: Pre-Installation Checks

- Ensure the device is authorized and enrolled in asset inventory.
- Confirm compatibility with the company-approved antivirus software.
- Uninstall any existing conflicting antivirus software.

Step 2: Containment

- Log in to the device using an admin account.
- Download the latest version of the approved antivirus software.
- Run the installer with administrative privileges.
- Accept the license agreement and configure installation settings:
- Enable antimalware
- Enable advanced threat control
- Enable anti exploit
- Enable process changes
- Enable application blacklisting
- Enable web access control

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: 1 DATE OF ISSUE: xxxxxx REVISED DATE: N/A
	DOCUMENT TITLE ANTIVIRUS INSTALLATION & UPDATE STANDARD OPERATION PROCEDURE (SOP)	

- Enable data protection
- Enable anti phishing
- Enable network attack defence
- Enable anti tampering
- Enable device control
- Enable monitoring of WIFI Connections
- Enable real-time scanning/traffic scan
- Enable automatic quarantine
- Enable web protection (if applicable)
- Complete installation and reboot device if prompted.

Step 3: Analysis Post-Installation Configuration

- Perform a full system scan.
- Verify that the antivirus is actively running and signatures are up to date.

5. Antivirus Update Procedure

Step 1: Signature Updates

- Enable automatic updates by default.
- Configure systems to check for updates at least every 6 hours.
- Perform manual update verification weekly on critical systems.

Step 2: Software Updates (Engine/Program)

- Schedule monthly review for available software version upgrades.
- Test updates in a sandbox environment before wide deployment.
- Deploy stable upgrades to all systems using centralized deployment tool.

6. Monitoring and Reporting


- Antivirus logs must be enabled and maintained on the BitDefender GravityZone Business suite for Endpoint & Microsoft Defender for email security.
- Alerts for malware detection, outdated software, and disabled antivirus must be acted on within 72 hours.
- **Monthly compliance reports will be generated** and reviewed by the IT Security Manager.

Commented [OA2]: Monthly reports will be generated b
who or what?

7. Troubleshooting & Escalation

- If installation fails or the antivirus malfunctions:
- Log a helpdesk ticket with the error details and device information.
- Escalate to **Tier 2 support** if unresolved in 72 hours.
- In case of mass update failure or outbreak, initiate the Malware Incident Response Procedure.

Commented [OA3]: What is Tier 2 support?

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: 1
	DOCUMENT TITLE ANTIVIRUS INSTALLATION & UPDATE STANDARD OPERATION PROCEDURE (SOP)	DATE OF ISSUE: xxxxxx REVISED DATE: N/A

8. Audit & Compliance

- Random checks will be conducted quarterly on devices across departments.
- Non-compliant systems will be disconnected from the network until resolved.
- Records of installations and updates must be retained for a minimum of 12 months.

9. Review & 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.