NORTH SOUTH POWER COMPANY LIMITED

END - USER GUIDELINES FOR MALWARE PREVENTION

JUNE 2025

DOC POLICY NO:

Developed By

Assistant General Manager, Information Technology and Security Compliance

Table of Contents

Commented [OA1]: Formatted for structure

1. Purpose 3
2. Scope 3
3. Key Guidelines 3
4. Reporting & Response 3
5. Training & Acknowledgement 4
6. Review and Revision 4

NSP	**INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT**	DOC NO: 1 DATE OF ISSUE: xxxxxx REVISED DATE: **N/A**
	DOCUMENT TITLE **END-USER GUIDELINES FOR MALWARE PREVENTION**	

1. Purpose

To equip employees and contractors with practical, clear guidance on how to prevent malware infections and protect North South Power Company Limited's digital environment.

2. Scope

This document applies to all users (employees, contractors, interns) with access to company-owned or managed devices, systems, applications, and data.

3. Key Guidelines

Safe Browsing & Downloads

- Only browse work-related websites.
- Do not download files or software from unverified or personal sources.
- Avoid clicking on pop-ups or suspicious links.

Email Hygiene

- Be wary of unexpected emails, even from known contacts.
- Do not open attachments or click on links in suspicious emails.
- Report phishing or suspicious emails immediately to IT Security.

Use of External Devices

- USB drives and other removable media must be scanned with antivirus software before use.
- Avoid connecting personal USBs or mobile devices to company systems.

Software & Updates

- Do not install unapproved software.
- Ensure your device is set to automatically receive antivirus and system updates.
- Restart your system regularly to apply updates.

Device Handling

- Lock your computer when away from your desk.
- Report lost or stolen devices immediately.
- Do not share passwords or allow others to use your login credentials.

4. Reporting & Response

- If you suspect malware or unusual activity, report it to the Helpdesk or IT Security immediately.
- Do not attempt to remove or quarantine the threat yourself.

5. Training and Acknowledgment

- All users are required to complete annual cybersecurity awareness training.
- Acknowledgment of this guideline is a condition for access to corporate systems.

Commented [OA2]: is it annual or bi annually?

Commented [OA3R2]: It is bi annually in Anti Virus and Malicious prevention?

6. 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.