NSP

NORTH SOUTH POWER

COMPANY LIMITED

WIRELESS AND REMOTE ACCESS POLICY

OCTOBER 2022

DOCUMENT HISTORY AND SIGN OFF

DOCUMENT HISTORY

Document Title	Wireless and Remote Access Policy
Document Reference Number	NSP/EVCIT/2022/118
Initiating Department	Information Technology
Date Created	September 2022
Document Version	Version 1
Effective Date	October 2022
Date of Next Review	October 2024

SIGN OFF AND APPROVAL

S/N	AUTHORIZING OFFICERS ROLE	JOB TITLE	NAME	SIGNATURE	DATE
1	**Created By**	Head, Information Technology	EMMANUEL ABIMBOLA OLOWOOKERE		07-12-22
2	**Reviewed By**	Chief Internal Audit & Risk Management Officer	IKECHUKWU OKOLI		07 - 12 - 22
3	**Approved By**	EVC/CEO	OLUBUNMI PETERS		07-12-22

This sign-off authorizes the immediate implementation of this document.

OVERVIEW

Remote access to North South Power Company Limited (NSPCL) corporate network is essential to maintain our Team’s productivity, but in many cases this remote access originates from networks that might has been compromised or are at a significantly lower security posture than NSPCL corporate network.

2. Purpose

The purpose of this policy is to define the rules and requirements for connecting to NSPCL's network from any host (cell phones, tablets, laptops, desktops etc.). These rules and requirements are designed to minimize the potential exposure to NSPCL from damages which may result from unauthorized use of resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical NSPCL internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all NSPCL Employees, Contractors, Vendors, Interns and Anyone Else with a NSPCL owned or personal computer or workstation used to connect to the NSPCL network. This policy applies to remote access connections used to do work on behalf of NSPCL, including reading or sending email and viewing intranet web resources. This policy covers all technical implementations of remote access used to connect to NSPCL networks.

4. Policy

It is the responsibility of NSPCL Employees, Contractors, Vendors, Interns and Anyone Else with remote access privileges to NSPCL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to NSPCL.

General access to the Internet for recreational use through the NSPCL network is strictly limited to NSPCL Employees, Contractors, Vendors, and Interns. When accessing the NSPCL network from a personal computer, Authorized Users are responsible for preventing access to any NSPCL computer resources or data by non-Authorized Users. Performance of illegal activities through the NSPCL network by any user is prohibited. The Authorized User bears responsibility for any consequences of misuse of the Authorized User’s access.

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with Encrypted Virtual Private Networks (VPNs) and strong passphrases.

4.1.2 Authorized Users shall protect their Login Credentials, even from family and friends.

4.1.3 While using an official computer to remotely connect to NSPCL's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 All hosts that are connected to NSPCL internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

4.1.5 Personal equipment used to connect to NSPCL's networks must meet the requirements of NSPCL-owned equipment for remote access as listed above.

5. POLICY COMPLIANCE

5.1 Compliance Measurement

The IT Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and inspection, and will provide feedback to the appropriate business unit manager.

5.2 Exceptions

Any exception to the policy must be approved by the Team Lead, Information Security and Compliance in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.