NATIONAL DATA
MANAGEMENT AUTHORITY

Remote Access Policy

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This policy addresses the requirements for securely accessing remote ICT resources.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

The purpose of this policy is to define rules and requirements for connecting to the Government of Guyana's (GOG) network from any host. These rules and requirements are designed to minimise the potential exposure to GOG from damage which may result from unauthorised use of resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical GOG internal systems, and fines or other financial liabilities incurred as a result of those losses.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this policy. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This policy encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It specifically addresses remote access connections used to do work on behalf of the Government of Guyana, including reading or sending emails and viewing intranet web resources. This policy covers all technical implementations of remote access controls used to connect to the Government of Guyana's network. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organisation's Information Security Policy and its associated standards.

4.0 Information Statement

Remote access to the Government of Guyana's corporate network is essential to maintain productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than the corporate network. It is crucial to mitigate these external risks to the best of our ability.

5.0 Policy

General access to the Internet for recreational use through the Government of Guyana's (GOG) network is strictly limited to GOG employees, contractors, vendors, and agents (hereafter referred to as "Authorised Users"). When accessing the GOG's network from a personal computer, Authorised Users are responsible for preventing access to any GOG computer resources or data by non-Authorised Users. Performance of illegal activities through the GOG network by any user

(Authorised or otherwise) is prohibited. The Authorised User bears responsibility for and consequences of misuse of the Authorised User's access.

5.1 Requirements

5.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For further information see the *Acceptable* Use Policy, Encryption Standard, and the Password Protection Policy.

5.1.2 Authorised Users shall protect their login and password, even from family members. For further information, see the Password Protection Policy.

5.1.3 While using a GOG owned computer to remotely connect to the corporate network, Authorised Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorised User or Third Party.

5.1.4 Use of external resources to conduct GOG business must be approved in advance by InfoSec and the appropriate business unit manager.

5.1.5 All hosts that are connected to GOG internal networks via remote access technologies must use an anti-virus software that has the latest virus definition updates, this includes personal computers.

5.1.6 Personal equipment used to connect to GOG's networks must meet the requirements of GOG-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access* to GOG Networks.

6.0. Compliance

This policy shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with the policy may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

7.0 Exceptions

Requests for exceptions to this policy shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

8.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this policy.

9.0 Definitions of Key Terms

Term	Definition
Workstation[1]	A computer used for tasks such as programming, engineering and design.
User[2]	Individual or (system) process authorized to access an information system.

10.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[1] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center (CSRC) - https://csrc.nist.gov/glossary/term/workstation
[2] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user