Remote Access Standard

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 standard establishes controls 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 standard is to establish authorised methods for remotely accessing resources and services securely. Major security concerns with remote access include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, the availability of internal resources to external hosts, potential damage to resources, and unauthorised access to information.

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 standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard 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 addresses all information, regardless of the form or format, which is created or used in support of business activities. It is the user's responsibility to read and understand this standard and to conduct their activities in accordance with its terms.

4.0 Standard

Remote access is allowed when there is a clear, documented business need. Access may be allowed from organisation-issued or personally owned devices, at the discretion of the organisation and in accordance with the standards below. Such access must be limited to only those systems necessary for needed functions.

4.1 Approved Methods of Remote Access

Approved methods of remote access to systems are listed in order of preference.

4.1.1. **Portals** - a server that offers access to one or more applications through a single centralised interface that provides authentication (e.g., web-based portal, virtual desktop interface (VDI)).

4.1.2. **Direct Application Access** – accessing an application directly with the application providing its own security (e.g., webmail, https).

4.1.3. **Remote System Control** – controlling a system remotely from a location other than the organisation's internal network.

4.1.4. **Tunneling** - a secure communication channel through which information can be transmitted between networks (e.g., Virtual Private Network (VPN)).

4.2 Required Controls

4.2.1.1 Any method of remote access must use a centrally managed authentication system for administration and user access.

4.2.1.2 Devices and software used for remote access must be approved after review by the Information Security Officer/designated security representative. Blanket approvals may be provided based on this review.

4.2.1.3 The authentication token used for remote access must conform to the requirements of the appropriate assurance level.

4.2.1.4 Remote access sessions must require re-authentication after 30 minutes of inactivity.

4.2.1.5 Remote access sessions must not last any longer than 24 hours.

4.2.1.6 The organisation must monitor for unauthorised remote connections and other anomalous activity and take appropriate incident response action as per the Cyber Incident Response Standard.

4.2.2 Tunneling specific controls:

4.2.2.1 No split tunneling is allowed.

4.2.2.2 Network controls regulating access to the remote access endpoint and between remote devices and networks are required.

4.2.2.3 When a remote access device will have access to other networked devices on the internal network, the remote device must be authenticated such that configuration of the device is compliant with applicable policies.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with this standard 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.

6.0 Exceptions

Requests for exceptions to this standard 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

7.0 Maintenance

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

8.0 Definitions of Key Terms

Term	Definition
Remote Access[1]	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).
Unauthorised Access[2]	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
Internal Network[3]	A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology provides the same effect. An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
Authentication[4]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Token[5]	Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity.
Token Authenticator[6]	The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.

9.0 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 https://csrc.nist.gov/glossary/term/remote_access

[2] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/unauthorized_access

[3] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/internal_network

[4] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/authentication

[5] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/token

[6] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/token_authenticator