NATIONAL DATA
MANAGEMENT AUTHORITY

Identification and Authentication 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 user identification and authentication best practices.
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

To ensure that only properly identified and authenticated users and devices are granted access to Information Technology (IT) resources in compliance with Government of Guyana IT security policies, standards, and procedures.

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 users of information systems, and systems that are automated or 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 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

The goal of the Identification and Authentication policy is to manage risks from user authentication and access to Government of Guyana's information assets through the establishment of effective identification and authentication programmes. This policy is important to help the Government of Guyana to implement identification and authentication security best practices.

5.0. Policy

5.1. Identification And Authentication

IT Department shall:

5.1.1 Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of organisation users.

5.1.2 Ensure that information systems implement multifactor authentication for network access to privileged accounts. Where not possible, compensating controls must be implemented.

5.1.3 Ensure that information systems implement multifactor authentication for network access to non-privileged accounts where possible.

5.1.4 Ensure that information systems implement multifactor authentication for local access to privileged accounts where possible.

5.1.5 Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.

5.1.6 Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilises a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.

5.2. Device Identification And Authentication

IT Department shall:

5.2.1 Ensure that all devices on the network are authenticated before providing access.

5.3. Identifier Management

IT Department, through department information systems owners, shall:

5.3.1 Ensure that the organisation manages information system identifiers by receiving authorisation from organisation defined personnel or roles to assign an individual, group, role, or device identifier.

5.3.2 Select an identifier that identifies an individual, group, role, or device.

5.3.3 Assign the identifier to the intended individual, group, role, or device.

5.3.4 Prevent reuse of identifiers for 90 days.

5.3.5 Disable the identifier after 30 days of inactivity.

5.4 Authenticator Management

IT Department shall:

5.4.1 Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

5.4.2 Establish initial authenticator content for authenticators defined by the organisation.

5.4.3 Ensure that authenticators have sufficient strength of mechanism for their intended use.

5.4.4 Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

5.4.5 Change default content of authenticators prior to information system installation.

5.4.6 Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.

5.4.7 Change/refresh authenticators every 90 days.

5.4.8 Protect authenticator content from unauthorised disclosure and modification.

5.4.9 Require individuals and devices to implement specific security safeguards to protect authenticators.

5.4.10 Change authenticators for group/role accounts when membership to those account changes.

5.4.11 Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.

5.4.12 Ensure passwords must contain characters from at least four of the following five categories:

5.4.12.1 Uppercase characters of English language (A through Z)

5.4.12.2 Lowercase characters of English language (a through z)

5.4.12.3 Base 10 digits (0 through 9);

5.4.12.4 Non-alphanumeric characters ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/; and

5.4.12.5 Any Unicode character that is categorised as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

5.4.13. Require passwords to have a minimum length of 8 characters.

5.4.14. Enforce at least one changed character when new passwords are created.

5.4.15. Store and transmit only cryptographically-protected passwords.

5.4.16. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.

5.4.17. Prohibit password reuse for 12 generations.

5.4.18. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

5.4.19. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

5.4.20. Enforce authorised access to the corresponding private key.

5.4.21. Map the authenticated identity to the account of the individual or group.

5.4.22. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

5.4.23. Require that the registration process to receive organisation defined types of and/or specific authenticators be conducted in person or by a trusted third party before organisation defined registration authority with authorisation by organisation defined personnel or roles.

5.4.24. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy [organisation defined token quality requirements].

5.5 Authenticator Feedback

IT Department shall:

5.5.1 Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorised individuals.

5.6 Cryptographic Module Authentication

IT Department shall**:**

5.6.1 Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for such authentication**.**

5.7 Identification And Authentication

IT Department shall:

5.7.1 Ensure that information systems uniquely identify and authenticate non-organisation users or processes acting on behalf of non-organisation users.

5.7.2 Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.

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 time-frame 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
Authentication[1]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Cryptography[2]	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification
Identification[3]	The process of discovering the identity (i.e., origin or initial history) of a person or item from the entire collection of similar persons or items.
Password[4]	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
User[5]	Individual or (system) process authorized to access an information system.

10.0Contact 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/authentication

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

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

[4] https://csrc.nist.gov/glossary/term/password

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