NDMA NATIONAL DATA MANAGEMENT AUTHORITY

Password Protection 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 establishes requirements for the selection and protection of passwords.
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 establish requirements for the creation of strong passwords and the protection of those passwords.

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, 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 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

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of our resources. All staff, including contractors and vendors with access to Government of Guyana's Information systems, are responsible for taking the appropriate steps, as outlined in this policy, to select and secure their passwords.

5.0 Policy

5.1 Password Creation

5.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

5.1.2 Users must use a separate, unique password for each of their work-related accounts in the absence of single sign on (SSO) systems. Users must not use any work-related passwords for their personal accounts.

5.1.3 User accounts that have system-level privileges granted through group memberships or programmes such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

5.2 Password Change

5.2.1 Passwords should be changed when there is reason to believe a password has been compromised.

5.2.2 Password cracking or guessing may be performed on a periodic or random basis by the IT Team. If a password is guessed or cracked during one of these scans, the user will be required to change it to follow the Password Construction Guidelines.

5.3 Password Protection

5.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Government of Guyana information.

5.3.2 Passwords must not be inserted into email messages, or other forms of electronic communication, nor revealed over the phone to anyone.

5.3.3 Passwords may be stored only in "password managers" authorised by the organisation.

5.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers.)

5.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

5.4 Application Development

5.4.1 Application developers must ensure that their programs contain the following security precautions:

5.4.1.1 Applications must support authentication of individual users, not groups.

5.4.1.2 Applications must not store passwords in clear text or in any easily reversible form.

5.4.1.3 Applications must not transmit passwords in clear text over the network.

5.4.1.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

5.5 Multi-Factor Authentication

5.5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

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**
Password[1]	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
User[2]	Individual or (system) process authorized to access an information system.
Workstation[3]	A computer used for tasks such as programming, engineering and design.

9.0 Contact Information

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

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

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

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