Password Construction Guidelines

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

Formatted Table

Document History and Version Control

<table>
<tr><th>Date</th><th>Version</th><th>Description</th><th>Authorised By</th><th>Approved By</th></tr>
<tr><td>31-03-2023</td><td>1.0</td><td></td><td>General Manager, NDMA</td><td>National ICT Advisor</td></tr>
<tr><td colspan="5"><b>Summary</b>
1. This guideline addresses best practices for the creation of strong 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.</td></tr>
</table>

Formatted Table

1.0 Purpose

The purpose of these guidelines is to provide best practices for the creation of strong passwords for users and accounts within Agencies and Ministries of The Government of Guyana.

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

3.0 Scope

This guideline 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 guideline and to conduct their activities in accordance with its terms.

4.0 Information Statement

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

5.0 Guideline

5.1 Strong passwords are long, the more characters you have and the more complexity in them contribute to having a stronger password.

5.2 It is recommended that users create a password that is a minimum of eight (8) characters long.

5.3 In addition, it is highly encouraged the use of passphrases which are passwords made up of multiple words, with the addition or substitution of numbers. Examples include:

5.3.1 "It'sTime4GuyanaTo$hine"

5.3.2 "Ice-CreamC0ffeeC@ke"

5.4 Passphrases are both easy to remember and to enter, and they also meet the password complexity requirements.

5.5 Poor or weak passwords can have the following characteristics:

5.5.1 Contains less than eight (8) characters.

5.5.2 Contains personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends etc.,

5.5.3 Contains simple patterns such as "aaabbb", "qwerty", "zyxwvuts", "123456789".

5.5.4 Contains some variation of the word “password” such as “P@ssw0rd”.

5.6 In addition, every account should have a different, unique password. To enable users to maintain multiple passwords, it is recommended that the organisation utilises a “password manager” software that is authorised and provided by the organisation’s IT department.

6.0 Compliance

These guidelines shall take effect upon publication. Compliance is expected with all organisational guidelines, policies, and standards. Failure to comply with the guidelines 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 guideline 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 guideline.

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.
Passphrase[2]	A passphrase is a memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage, but is generally longer for added security.

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

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

User[3]	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.

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