Secure Configuration 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 secure configuration.
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 baseline configurations for information systems that are owned and/or operated by the organisation. Effective implementation of this standard will maximise security and minimise the potential risk of unauthorised access to information and technology.

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

Standard secure configuration profiles based on any one or more of the industry consensus guidelines listed below, must be used in addition to the latest vendor security guidance. Alterations to the profile must be based on business need, policy, or standard compliance, developed in consultation with the Policy Coordinator, documented and retained for audit purposes.

4.1 Industry Consensus Guidelines:

4.1.1 The following resources can be consulted for guidance on setting the security configurations of operating systems and applications:

4.1.1.1 Center for Internet Security (CIS) Benchmarks [1]

4.1.1.2 National Institute of Science and Technology (NIST) National Checklist Program [2]

4.1.2 The initial setup, software installation, and security configuration of new systems must be performed in a secure environment isolated from other operational systems with minimal communication protocols enabled.

4.1.3 Changes to configurations must be formally identified, proposed, reviewed, analysed for security impact, tested, and approved prior to implementation in accordance with the

[1] Retrieved from: Center for Internet Security (CIS) Website: https://www.cisecurity.org/cis-benchmarks/
[2] Retrieved from: NIST National Checklist Program: https://ncp.nist.gov/repository

change management procedures. Individuals conducting security impact analysis must possess the necessary skills and technical expertise to analyse the changes to information systems and the associated security ramifications.

4.1.4 Organisations must maintain configuration management plans that define detailed processes and procedures for how configuration management is used to support secure system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the secure system development life cycle.

4.1.5 A configuration monitoring process must be in place to identify undiscovered or undocumented system components, misconfigurations, vulnerabilities and unauthorised changes.

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
Configuration[3]	The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.

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

Configuration Management[4]	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Misconfiguration[5]	An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.
Vulnerability[6]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

9.0 Contact Information

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

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

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

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