NDMA NATIONAL DATA
MANAGEMENT AUTHORITY

Configuration Management 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 configuration management.
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 Information Technology (IT) resources are inventoried and configured securely in compliance with Information Technology security policies, standards, and procedures within the Public Sector 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 policy. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This policy 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 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

This policy is applicable to all departments and users of IT resources and assets.

5.0 Policy

5.1 Baseline Configuration

IT Department shall:

5.1.1. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.

5.1.2. Review and update the baseline configuration of the information system in keeping with the organisation's maintenance schedule.

5.1.3. Review and update the baseline configuration of the information system when required as a result of the organisation's defined circumstance and as an integral part of information system component installations and upgrades.

5.1.4. Retain one previous version of baseline configurations of information systems to support rollback.

5.1.5. Keep backup configuration of critical equipment.

5.2 Configuration Change Control

IT Department shall:

5.2.1. Determine the types of changes to the information system that are configuration controlled.

5.2.2. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.

5.2.3. Document configuration change decisions associated with the information system.

5.2.4. Implement approved configuration-controlled changes to the information system.

5.2.5. Retain records of configuration-controlled changes to the information system in accordance with organisation's defined time period.

5.2.6. Audit and review activities associated with configuration-controlled changes to the information system.

5.2.7. Coordinate and provide oversight for configuration change control activities through the organisation's defined configuration change control element (e.g., committee, board) that convenes with the organisation's defined frequency and organisation's defined configuration change conditions.

5.2.8. Test, validate, and document changes to the information system before implementing the changes on the operational system.

5.3 Security Impact Analysis

IT Department shall:

5.3.1. Analyse changes to the information system to determine potential security impacts prior to change implementation.

5.4. Access Restrictions For Change

IT Department shall:

5.4.1. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

5.5. Configuration Settings

IT Department shall:

5.5.1. Establish and document configuration settings for information technology products employed within the information system using the organisation's defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.

5.5.2. Implement the configuration settings.

5.5.3. Identify, document, and approve any deviations from established configuration settings for the organisation's defined information system components based on the organisation's defined operational requirements.

5.5.4. Monitor and control changes to the configuration settings in accordance with policies and procedures.

5.6 Least Functionality

IT Department shall:

5.6.1. Configure the information system to provide only essential capabilities.

5.6.2. Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.

5.6.3. If required, disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

5.6.4. Prevent programme execution in accordance with policies regarding software programme message and restrictions and rules authorising the terms and conditions of software programme usage.

5.6.5. Identify software programmes not authorised to execute information systems.

5.6.6. Employ a "deny-all", "permit-by-exception" policy to prohibit the execution of unauthorised software programmes on the information system.

5.6.7. Review and update the list of unauthorised software programmes annually.

5.7 Information System Component Inventory

IT Department shall:

5.7.1. Develop and document an inventory of information system components that:

5.7.1.1.Reflects the current information system accurately.

5.7.1.2.Includes all components within the authorisation boundary of the information system.

5.7.1.3.Is at the level of granularity deemed necessary for tracking and reporting.

5.7.1.4.Includes information deemed necessary to achieve effective information system component accountability.

5.7.2. Review and update the information system component inventory in keeping with the organisation's defined frequency.

5.7.3. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.

5.7.4. Employ automated mechanisms quarterly to detect the presence of unauthorised hardware, software, and firmware components within the information system.

5.7.5. Take the following actions when unauthorised components are detected:

5.7.5.1.Disable network access by such components, or

5.7.5.2.Isolate the components and notify the Head of the Information Technology Department.

5.7.6 Verify that all components within the authorisation boundary of the information system are not duplicated in other information system component inventories.

5.7.7 Configuration Management Plan

IT department shall develop, document, and implement a configuration management plan for the information system that:

5.7.7.1.Addresses roles, responsibilities, and configuration management processes and procedures.

5.7.7.2.Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.

5.7.7.3.Defines the configuration items for the information system and places the configuration items under configuration management.

5.7.7.4.Protects the configuration management plan from unauthorised disclosure and modification.

5.7.8 Software Usage Restrictions

IT Department shall:

5.7.8.1.Use software and associated documentation in accordance with contract agreements and copyright laws.

5.7.8.2.Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

5.7.8.3.Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorised distribution, display, performance, or reproduction of copyrighted work.

5.7.9 User-Installed Software

IT Department shall:

5.7.9.1.Establish policies governing the installation of software by users.

5.7.9.2.Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.

5.7.9.3.Monitor policy compliance in accordance with the organisation’s defined frequency.

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**
Configuration Management[1]	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.
Information System[2] Component	“A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system…”

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

[2] *Retrieved from:* NIST Information Technology Laboratory – Computer Security Resource Center information system component - Glossary | CSRC (nist.gov)

User[3]	Individual or (system) process authorized to access an information system.
Whitelisting[4]	1.An approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition. 2.An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments.
Blacklisting[5]	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.
Baseline Configuration[6]	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
Configuration Management Plan[7]	A comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems.

10.0 Contact Information

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

Reference

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Configuration Management (CM)

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

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

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

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

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