NDMA | NATIONAL DATA
MANAGEMENT AUTHORITY

Personnel Security 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 personnel security safeguards for accessing IT resources.
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 ensure that personnel security safeguards are applied to the access and use of information technology resources and data.

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).

2.0 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 seeks to ensure that the risk of trusted insiders exploiting their legitimate access to an organisation's facilities, assets, systems or people are appropriately managed. It serves to aid in reducing the risk of security breaches resulting from insiders within the Public Sector organisations by increasing the user's awareness about protecting sensitive information.

5.0 Policy

5.1 Position Risk Designation

The Human Resources Department shall:

5.1.1 Assign a risk designation to all positions.

5.1.2 Establish screening criteria for individuals filling those positions.

5.1.3 Review and update position risk designations in keeping with the organisations' defined frequency.

5.2 Personnel Screening

Human Resources and department system and application owners shall:

5.2.1 Screen individuals prior to authorising access to the information systems.

5.2.2 Rescreen individuals according to their organisation's defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening.

5.2.3 Ensure personnel screening and rescreening activities reflect applicable laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

5.3 Personnel Termination

Human Resources, in collaboration with the IT department and/or system owners shall, upon termination of individual employment:

5.3.1 Disable information system access within the organisation's defined time period.

5.3.2 Terminate/revoke any authenticators/credentials associated with the individual.

5.3.3 Conduct exit interviews that include a discussion of the organisation's defined information security topics.

5.3.4 Retrieve all security-related information system-related property.

5.3.5 Retain access to information and information systems formerly controlled by terminated individual.

5.3.6 Notify the organisation's defined personnel or roles within the organisation's defined time period.

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.

5.3.6.1 Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.

5.3.6.2 Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the termination process as directed by Human Resources (HR).

5.3.6.3 Employ automated mechanisms to notify the organisation's defined personnel or roles upon termination of an individual.

5.3.6.4 Disable/purge accounts that are no longer in use.

5.3.6.5 Conduct periodic audits to ensure dormant accounts are properly purged, in keeping with the *Identification Authentication Policy*

5.4 Personnel Transfer

Human Resources, in collaboration with the IT department and/or system owners shall, upon transfer of individual employment:

5.4.1 Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions.

5.4.2 Initiate organisation’s defined transfer or reassignment actions within the organisation’s defined time period following the formal transfer action.

5.4.3 Modify access authorisation as needed to correspond with any changes in operational need due to reassignment or transfer.

5.4.4 Notify the organisation’s defined personnel within the organisation’s defined time period of transfer.

5.4.5 This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

5.5 Access Agreements

Human Resources, in collaboration with the IT department and/or system owners shall:

5.5.1 Develop and document access agreements for information systems.

5.5.2 Review and update the access agreements in keeping with the organisation’s defined frequency.

5.5.3 Ensure that individuals requiring access to information and information systems:

5.5.4 Sign appropriate access agreements prior to being granted access.

5.5.5 Re-sign access agreements to maintain access to information systems when access agreements have been updated or in accordance with organisation’s defined frequency.

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

5.6 Third-Party Personnel Security

Human Resources, in collaboration with the IT department and/or system owners shall:

5.6.1 Establish and document personnel security requirements including security roles and responsibilities for third-party providers.

5.6.2 Require third-party providers to comply with personnel security policies and procedures established by the organisation.

5.6.3 Require third-party providers to notify organisation’s defined personnel of any personnel transfers or terminations of third-party personnel who possess credentials and/or badges, or who have information system privileges within the organisation’s defined time period.

5.6.4 Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organisations providing information system development, information technology services, outsourced applications, and network and security management.

5.7 Personnel Sanctions

Human Resources, in collaboration with the IT department and/or system owners shall:

5.7.1 Employ a formal sanction process for individuals failing to comply with established information security policies and procedures

5.7.2 Notify the organisation's defined personnel within the organisation's defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Sanction processes reflect applicable laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organisations.

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
Authenticator[1]	The means used to confirm the identity of a user, process, or device (e.g., user password or token).
Credential[2]	Evidence attesting to one's right to credit or authority.
Insider[3]	Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks, or systems.
Personnel Security[4]	The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness.
User[5]	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.

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

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

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

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

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