NATIONAL DATA
MANAGEMENT AUTHORITY

Access Control 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 measures required to control access to ICT networks.
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 access controls are implemented and 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

Access controls are deemed as a fundamental component of securing an organisation's critical assets. Authentication and authorisation measures stipulated within the Access Control Policy aid in ensuring that users gain access to critical organisation's assets in accordance with their login credentials. Login credentials serves as enhancing data and infrastructure security.

This policy seeks to outline measures that are needed to control access to whole of government ICT network to secure Critical Information Infrastructure and its Critical Information.

5.0. Policy

5.1 Account Management

The Organisation shall define and assign a role to:

5.1.1. Identify and select the following types of information system accounts to support organisational missions and business functions: individual, vendor, temporary, service shared, group, system, guest/anonymous, emergency, developer/manufacturer.

5.1.2. Assign account managers for information system accounts.

5.1.3. Establish conditions for group and role membership.

5.1.4. Specify authorised users of the information system, group and role membership, and access authorisations (i.e., privileges) and other attributes (as required) for each account.

5.1.5. Require approvals by system owners for requests to create information system accounts.

5.1.6. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.

5.1.7. Monitor the use of information system accounts.

5.1.8. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.

5.1.9. Authorise access to the information system based on a valid access authorisation or intended system usage.

5.1.10. Review accounts for compliance with account management requirements in keeping with the organisation's schedule.

5.1.11. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

5.1.12. Employ automated mechanisms to support the management of information system accounts.

5.1.13. Ensure that the information system automatically disables temporary and emergency accounts after usage.

5.1.14. Ensure that the information system automatically disables inactive accounts, in keeping with the organisation's schedule.

5.1.15. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate Information Technology personnel.

5.2 Access Enforcement

The Organisation shall define and assign a role to:

5.2.1. Ensure that the information system enforces approved authorisations for logical access to information and system resources in accordance with applicable access control policies.

5.3 Information Flow Enforcement

The Organisation shall define and assign a role to:

5.3.1. Ensure that the information system enforces approved authorisations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

5.4 Separation Of Duties

The Organisation shall define and assign a role to:

5.4.1. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

5.4.2. Document the separation of duties of individuals.

5.4.3. Define information system access authorisations to support separation of duties.

5.5 Least Privilege

The Organisation shall define and assign a role to:

5.5.1. Employ the principle of least privilege, allowing only authorised access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organisational missions and business functions.

5.5.2. Authorise explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

5.5.3. Require that users of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions.

5.5.4. Restrict privileged accounts on the information system to organisation defined personnel or roles.

5.5.5. Ensure that the information system audits the execution of privileged functions.

5.5.6. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

5.6 Unsuccessful Logon Attempts

The Organisation shall define and assign a role to ensure that the information system:

5.6.1. Enforces a limit of consecutive invalid logon attempts by a user, in accordance with the Organisation's invalid login attempt frequency.

5.6.2. Locks the account/node automatically for the specified time that the Organisation set or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

5.7 System Use Notification

The Organisation shall define and assign a role to ensure that the information system:

5.7.1. Displays to users an approved system-use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance and states informing that:

5.7.1.1 Users are accessing the Organisation's information system.

5.7.1.2 Information system usage may be monitored, recorded, and subject to audit.

5.7.1.3 Unauthorised use of the information system is prohibited and subject to criminal and civil penalties.

5.7.1.4 Use of the information system indicates consent to monitoring and recording.

5.7.1.5 There are not rights to privacy.

5.7.1.6 Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

5.7.2. For publicly accessible systems, the Organisation shall define and assign a role to ensure that the information system:

5.7.2.1. Displays system use information and conditions defined by the Organisation before granting further access.

5.7.2.2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

5.7.2.3. Includes a description of the authorised uses of the system.

5.8 Session Lock

The Organisation shall define and assign a role to ensure that the information system:

5.8.1. Prevent further access to the system by initiating a session lock after the Organisation's defined period of inactivity or upon receiving a request from a user.

5.8.2. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

5.8.3. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

5.9 Session Termination

The Organisation shall define and assign a role to:

5.9.1. Ensure that the information system automatically terminates a user session after the Organisation's specified timeframe.

5.10 Permitted Actions Without Identification Or Authentication

The Organisation shall define and assign a role to:

5.10.1. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.

5.10.2. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

5.11 Remote Access

The Organisation shall define and assign a role to:

5.11.1. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

5.11.2. Authorise remote access to the information system prior to allowing such connections.

5.11.3. Ensure that the information system monitors and controls remote access methods.

5.11.4. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

5.11.5. Ensure that the information system routes all remote accesses through managed network access control points to reduce the risk for external attacks.

5.11.6. Authorise the execution of privileged commands and access to security-relevant information via remote access only for Organisation defined needs.

5.11.7. Document the rationale for such access in the security plan for the information system.

5.12 Wireless Access

The Organisation shall define and assign a role to:

5.12.1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

5.12.2. Authorise wireless access to the information system prior to allowing such connections.

5.12.3. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

5.13 Access Control For Mobile Devices

The Organisation shall define and assign a role to:

5.13.1. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

5.13.2. Authorise the connection of mobile devices to organizational information systems.

5.13.3. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.

5.14 Use Of External Information Systems

The Organisation shall define and assign a role to:

5.14.1. Establish terms and conditions, consistent with any trust relationships established with other organisations owning, operating, and/or maintaining external information systems, allowing authorised individuals to:

5.14.1.1. Access the information system from external information systems.

5.14.1.2. Process, store, or transmit organisation-controlled information using external information systems.

5.14.2. Permit authorised individuals to use an external information system to access the information system or to process, store, or transmit organisation-controlled information only when the organisation:

5.14.2.1. Verifies the implementation of required security controls on the external system as specified in the organisation's information security policy and security plan.

5.14.2.2. Retains approved information system connection or processing agreements with the organisations hosting the external information system.

5.15 Information Sharing

The Organisation shall define and assign a role to:

5.15.1. Facilitate information sharing by enabling authorised users to determine whether access authorisations assigned to the sharing partner match the access restrictions on the information for circumstances that are defined by the Organisation where user discretion is required.

5.15.2. Employ automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

5.16 Publicly Accessible Content

The Organisation shall define and assign a role to:

5.16.1. Designate individuals authorized to post information onto a publicly accessible information system.

5.16.2. Train authorised individuals to ensure that publicly accessible information does not contain nonpublic information.

5.16.3. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

5.16.4. Review the content on the publicly accessible information system for nonpublic information as often as the Organisation requires and removes such information, if discovered.

6.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with this 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
User[1]	Individual or (system) process authorized to access an information system.
Access Control[2]	The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities.

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 Publications (SP): NIST SP 800-53a – Access Control (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164;

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

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