NATIONAL DATA
MANAGEMENT AUTHORITY

Physical and Environmental 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 physical and environmental security measures for ICT 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 Information and Communications Technology (ICT) resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorised physical access.

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 and physical infrastructure, 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 Policy

4.1 Physical Access Authorisations

The organisation shall define and assign personnel to:

4.1.1 Develop, approve, and maintain a list of individuals with authorised access to the facilities where the information systems reside.

4.1.2 Issue authorisation credentials for facility access.

4.1.3 Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.

4.2 Physical Access Control

The organisation shall define and assign personnel to:

4.2.1 Enforce physical access authorisations by verifying individual access authorisations before granting access to the facility.

4.2.2 Control ingress/egress to the facility using organisations' defined physical access control systems/devices and/or guards.

4.2.3 Maintain physical access audit logs for organisations' defined entry/exit points.

4.2.4 Provide organisations' defined security safeguards to control access to areas within the facility officially designated as publicly accessible.

4.2.5 Escort visitors and monitors visitor activity in the organisations' specified areas.

4.2.6 Secure keys, combinations, and other physical access devices.

4.2.7 Inventory of organisations' defined physical access devices should be conducted in keeping with the organisations' defined frequency.

4.2.8 Change combinations and keys in keeping with organisations' established maintenance schedule and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

4.3 Facility Penetration Testing

The organisation shall define and assign personnel to:

4.3.1 Employ a penetration testing process that confirms with the organisations' schedule, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

4.4 Access Control for Transmission Medium

The organisation shall define and assign personnel to:

4.4.1 Control physical access to the organisations' defined information system distribution and transmission lines within its facilities using the organisations' defined security safeguards.

4.5 Access Control for Output Devices

The organisation shall define and assign personnel to:

4.5.1 Control physical access to information system output devices to prevent unauthorised individuals from obtaining the output.

4.5.2 Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorised individuals only, and placing output devices in locations that can be monitored by personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

4.6 Monitoring Physical Access

The organisation shall define and assign personnel to:

4.6.1 Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.

4.6.2 Review physical access logs based on organisations' defined frequency and upon occurrence of the organisations' defined events or potential indications of events; and coordinate results of reviews and investigations with the organisational incident response capability.

4.7 Visitor Access Records

The organisation shall define and assign personnel to:

4.7.1 Maintain visitor access records to the facility where the information system resides in keeping with organisations' defined time period; and reviews visitor access records in accordance with organisations' defined frequency.

4.8 Power Equipment and Cabling

The organisation shall define and assign personnel to:

4.8.1 Protect power equipment and power cabling for the information system from damage and destruction.

4.8.2 Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organisational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

4.9 Emergency Shutoff

The organisation shall define and assign personnel to:

4.9.1 Provide the capability of shutting off power to the information system or individual system components in emergency situations.

4.9.2 Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorised activation.

4.10 Emergency Power

The organisation shall define and assign personnel to:

4.10.1 Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; transition of the information system to long-term alternate power in the event of a primary power source loss.

4.10.2 Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

4.11 Emergency Lighting

The organisation shall define and assign personnel to:

4.11.1 Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

4.11.2 Provide emergency lighting for all areas within the facility supporting essential missions and business functions.

4.12 Fire Protection

The organisation shall define and assign personnel to:

4.12.1 Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

4.12.2 This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

4.13 Temperature And Humidity Controls

The organisation shall define and assign personnel to:

4.13.1 Maintain temperature and humidity levels within the facility where the information system resides at organisations' defined acceptable levels.

4.13.2 Monitor temperature and humidity levels in accordance with organisations' defined frequency to include alarms or notifications of changes potentially harmful to personnel or equipment.

4.14 Water Damage Protection

The organisation shall define and assign personnel to:

4.14.1 Protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

4.14.2 This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organisations.

4.15 Delivery and Removal

The organisation shall define and assign personnel to:

4.15.1 Authorise, monitor, and control entering and exiting the facility and maintain records of those items delivered and removed from facility.

4.15.2 Effectively enforcing authorisations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Alternate Work Site

The organisation shall define and assign personnel to:

4.15.3 Employ organisations' defined security controls at alternate work sites.

4.15.4 Assess as feasible, the effectiveness of security controls at alternate work sites.

4.15.5 Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

4.15.6 Alternate work sites may include, for example, other government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Staff may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

5.0. 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.

6.0. 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.

7.0. Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this policy.

8.0 Definitions of Key Terms

Term	Definition
User[1]	A person, organisation entity, or automated process that accesses a system, whether authorised to do so or not.

9.0 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 – Physical and Environmental Protection (PE), NIST SP 800-46, NIST SP 800-73, SP NIST 800-76, SP NIST 800-78, SP NIST 800-116; Intelligence Community Directive (ICD): 704 705; Department of Defense (DoD): Instruction 5200.39 Critical Program Information (CPI) Protection; Personal Identity Verification (PIV) in Enterprise Access Control System (E-PACS) (2012)

[1] *Retrieved from*: SANS Glossary of Security Terms T-U - https://www.sans.org/security-resources/glossary-of-terms/