NATIONAL DATA
MANAGEMENT AUTHORITY

Clean Desk 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 the securing of sensitive/confidential materials when not in use.
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 establish requirements for maintaining a “clean desk”- where sensitive/critical information about users, intellectual property and third-party vendors is securely stored.

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 applies to all users of Information systems and 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 all sensitive/confidential materials are secured when not in use or a user leaves his/her workstation. It serves to aid in reducing the risk of security breaches within the Public Sector organisations by increasing the user’s awareness about protecting sensitive information.

5.0 Policy

5.1 Users are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the close of business and when they are expected to be gone for an extended period.

5.2 Computer workstations must be locked when workspace is unoccupied.

5.3 Computer workstations must be shut completely down at the end of the day’s work.

5.4 Any restricted and sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the close of business.

5.5 File cabinets containing restricted and sensitive information must securely locked when not being in use.

5.6 Keys used for retrieving restricted and sensitive information must not be left at the unattended desk.

5.7 Passwords must not be left on sticky notes, posted on or under a computer, nor may be left written down in an accessible location.

5.8 All restricted and sensitive information when being disposed of must be shredded in the official shredder bins or placed in the lock confidential disposal bins.

5.9 Restricted and sensitive information must be erased from any medium used to display information e.g. whiteboards.

5.10 Portable computing devices such as laptops and tablets must be securely stored when not in use. All storage devices such as CDROM, DVD OR USB drives must be treated as sensitive and must be securely stored in a locked drawer.

5.11 All printers and fax machines must be cleared of papers as soon as they are printed; this helps to ensure that sensitive information is not left in printer trays.

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 9.0 Definitions of Key Terms

Term	Definition
Workstation[1]	A computer used for tasks such as programming, engineering and design.
User[2]	Individual or (system) process authorized to access an information system.
Password[3]	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

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 (CSRC) - https://csrc.nist.gov/glossary/term/workstation

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

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