NATIONAL DATA
MANAGEMENT AUTHORITY

Software Installation 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 all relevant issues pertaining to appropriate software installation and deployment of software.
2. This is a living document which will be updated annually or as required.
3. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0. Purpose and Benefits

The purpose of this policy is to address all relevant issues pertaining to appropriate software installation and deployment in compliance with Government of Guyana IT security policies, standards, and procedures.

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

Allowing employees to install unauthorised software on organisation computing devices can leave the organisation open to unnecessary exposure. The introduction of malware from infected software, unlicensed software, and unapproved software installations can be used to infiltrate an organisation's network are all examples of problems that can be introduced when employees install software on organisation equipmnt. For this reason, it is necessary to outline requirements around installation of software on Government of Guyana computer systems to minimize the various risks that can accompany unapproved software installations.

5.0. Policy

5.1. Disclaimer on Software

5.1.1.The Organisation strictly forbids any employee from installing any of the following type of software (including portable or standalone software that may or may not require administrative rights to execute):

5.1.1.1 Unauthorised Software-

5.1.1.2 Pirated copies of any software

5.1.1.3 Any title not listed in the organisation's *Supported Software List,* which is maintained by the Organisation's relevant personnel/role designed to maintain the supported software list. Any software that infringes on Intellectual Property Rights, including software licenses.

5.1.1.4 Any software not installed in accordance with this policy.

5.2 Supported and Restricted Software

The organisation shall design and assign a role/department to:

5.2.1 Develop and maintain a current list of supported software, operating systems, and categories of restricted software.

5.2.2 Address exceptions regarding the addition of software to the list of supported software.

5.2.3 Address software installation requests from employees within the organisation.

5.3 Software Installation Requests

5.3.1 If an employee requires software to be installed on their system, approval must first be obtained from the role assigned in section **5.2** of this policy**.**

5.3.1.1 The assigned role reserves the right to reject software installation requests for justified reasons but must inform the requesting employee via approved communication protocols (i.e., written notice, email etc.).

5.3.2 Software installation requests from employees must be filled out using an organisation designed *Software Request Form* and submitted to their supervisor for forwarding to the relevant personnel/role.

5.3.3 Software requested must be aligned with the facilitation or execution of the duties and responsibilities of the requesting employee.

5.4 Software Installation

5.4.1 Software installed are only to be installed on organisation owned equipment by the appropriate role/department staff.

5.4.2 All software installed on the organisation's computer systems (including all commercial and shareware products) must be used in compliance with all applicable licenses, notices, contracts, agreements and must follow Government of Guyana IT security policies, standards, and procedures.

5.4.3 The role defined in section **5.2** of this policy shall uninstall any unapproved software from an organisation owned computer system.

5.5 Software Audits

5.5.1 The role assigned in 5.2 must:

5.5.1.1 Monitor software installation and usage on the organisation's computer systems.

5.5.1.2 Conduct scheduled periodic, unannounced, and/or random audits to ensure compliance with this policy. During such audits, scanning and elimination of computer viruses and vulnerabilities must be proactive and performed in accordance with the *Vulnerability Scanning Standard* and all other applicable standards and policies.

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 time-frame 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
Computer System[1]	Means a device or group of interconnected or related devices, which follows a computer programme or external instruction to perform automatic processing of electronic data; and Includes, but is not limited to, a desktop computer, a laptop computer, a netbook computer, a tablet computer, a video game console, internet connected devices, a smart phone, a personal digital assistant, a smart television or a video camera.
Software[2]	All or part of the programs, procedures, rules, and associated documentation of an information processing system.

10.0Contact Information

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

[1] *Retrieved from*: Laws of Guyana, Cybercrime Act 2018, N0.16 of 2018

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