NATIONAL DATA
MANAGEMENT AUTHORITY

Software Acquisition 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 outlines the rules governing the acquisition of software for Government of Guyana agencies.
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 outlines the rules governing the acquisition of software for Government of Guyana agencies.

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

Acquiring software for organisation computing devices can leave an organisation open to unnecessary exposure if done incorrectly. Software resources enable organisations to conduct their critical operations. These resources may store and transmit confidential, restricted, and other sensitive information about Government of Guyana assets. If compromised, such data on software platforms would introduce significant security, privacy, legal and financial risks. It is therefore necessary to outline requirements around acquisition of software on Government of Guyana computer systems to minimize the various risks that can accompany poor software acquisition.

5.0. Policy

5.1. Requesting Software

Requests for software must consider that software acquisition is guided by:

5.1.1 A needs assessment must be conducted to determine the software requirements, and where applicable, appropriate software and/or vendor selection tools must be used.

5.1.2 All software acquisition must be planned and included in the budget for approval prior to procurement.

5.2 Conducting Software Evaluations

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

5.2.1 Prior to the acquisition of any software, conduct an evaluation, in compliance with the appropriate policies, standards and guidelines and in alignment with the Agency's strategic plan.

5.2.2 Establish and maintain *Software Acceptance Testing and Evaluation* procedures. This includes procedures for: conducting document evaluations; evaluating software development plans (if acquiring custom made software); creating software evaluation forms; documenting corrective actions; ensuring corrective actions are completed; and establishing a software acceptance checklist.

5.2.3 Ensure that developers or any other party responsible for the sale or marketing of the software being required are not allowed to perform evaluations or acceptance testing. However, those parties would be permitted to observe the process.

5.3 Procurement of Software

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

5.3.1 Assume responsibility for the acquisition of all software and must be guided by the rules and regulations of the National Procurement and Tender Administration Board (NPTAB), under the *Procurement Act Cap. 73:05 (2003),* and all other relevant national laws and standards.

5.3.2 Acquire software from intellectual property owners or authorized resellers.

5.3.3 Reach out to the Intellectual Property Owners to ensure that the acquisition of the software does not violate the intellectual property rights by validating it is acquired through authorized vendor channels and that it is fit for purpose (non-grey market or partner license). All procurement must be validated by the Organisation's ICT Endorsement / Procurement Process.

5.4 Receiving Software

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

5.4.1 Upon receiving software, follow established *Check-in Procedures* to ensure that software is included in the approved and secure Agency software register before any installation is done. Installation must be done in accordance with the Software Installation policies and all other relevant policies, standards, and procedures that guarantee appropriate testing.

5.4.2 Keep copies of all original documentation for reference purposes in an approved central Software Register. The department is also required to make copies of the End User License Agreement (EULA), Software License Terms (SLT) and manuals available to all relevant departments.

5.4.3 Track and update the Software Register on a regular basis to ensure proper licensing and compliance. The management of the Software Register is intended to control costs by informing, purchasing, upgrading, renewing and cancellation decisions, advising on the correct type of license, taking advantage of such measures as volume licensing discounts; and optimising software value by potentially reusing or redistributing software to other

departments/divisions. Annual reports on the Software Register must be submitted to the Head of Agency.

5.5 Distributing Software

5.5.1 After Check-in procedures are competed, the department assigned in 5.4 must schedule software installation in accordance with the Agency's approved Software Installation policies, standards, guidelines, and procedures that guarantee appropriate testing.

5.5.2 The department must retain the following information for each employee who received software: name, email address, telephone number, department, job title.

5.5.3 If software needs to be re-installed, the employee must contact the relevant department to perform the reinstallation and must copy his/her supervisor.

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.

10.0 Contact 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