NATIONAL DATA MANAGEMENT AUTHORITY

Risk Assessment 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 conducing periodic risk assessments.
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

To ensure that Information Technology (IT) performs risk assessments in compliance with IT security policies, standards, and procedures of the Government 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 users of information systems, and systems that are 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

Conducting periodic risk assessments is a necessary first step towards strengthening an organisation's cybersecurity posture as it helps in the identification of the potential threats and vulnerabilities to the confidentiality, integrity, availability (CIA) of its Information Technology resources and systems. It is also necessary to conduct these assessments on potential threats to confidential and proprietary electronic information, and to develop strategies to efficiently and effectively mitigate the risks that affect these resources.

5.0 Policy

5.1 Security Categorisation

IT Department shall:

5.1.2 Apply proper security controls to data categorised as confidential by system owners, including protected health information and personally identifiable information (PII), in accordance with applicable laws, directives, policies, regulations, standards, and guidance

5.1.3 Document the security controls (including supporting rationale) in the security plan for the information system.

5.2 Risk Assessment

IT Department shall:

5.2.1 Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorised access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

5.2.2 Document risk assessment results in annual IT Risk Assessment.

5.2.3 Review risk assessment results quarterly.

5.2.4 Disseminate risk assessment results to stakeholders.

5.2.5 Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

5.3 Vulnerability Scanning

IT Department shall:

5.3.1 Scan for vulnerabilities in the information system and hosted applications quarterly and/or randomly in accordance with the Organisation's defined process/procedure and when new vulnerabilities potentially affecting the system/applications are identified and reported.

5.3.2 Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

5.3.2.1 Enumerating platforms, software flaws, and improper configurations.

5.3.2.2 Formatting checklists and test procedures.

5.3.2.3 Measuring vulnerability impact.

5.3.3 Analyse vulnerability scan reports and results from security control assessments.

5.3.4 Remediate legitimate vulnerabilities within one month in accordance with an organisational assessment of risk.

5.3.5 Share information obtained from the vulnerability scanning process and security control assessments with the Information Security Officer (*ISO)/designated security representative* to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

5.3.6 Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

5.3.7 Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported.

5.3.8 Ensure that information systems implement privileged access authorisation to all systems for selected vulnerability scanning.

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
Confidential Record[1]	"confidential record" means a record that would case damage or be prejudicial to national security if made publicly available.
PII[2]	Personally Identifiable Information; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
Personal Information[3]	"personal information" means information about a person, including- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, marital or family status of the person;

[1] *Retrieved from:* Laws of Guyana, Access to Information Act 2011, ACT No. 21 of 2011.
[2] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/pii
[3] *Retrieved from:* Laws of Guyana, Access to Information Act 2011, ACT No. 21 of 2011

	(b) information relating to the education, medical, psychiatric, psychological, criminal or employment history of the person or information relating to fmancial transactions in which the person has been involved; (c) any identifying number, symbol or other particular assigned to the person, fmger-prints, blood type or DNA profile of the person; (d) the postal and email addresses, and telephone number of the person; (e) the personal opinions or views of the person except where they relate to another person; (f) correspondence sent to a public authority by the person that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence; the views or opinions of another person about the person; and the person's name where it appears with other personal information relating to the person or where the disclosure of the name would reveal other personal information about the person; (g) the views or opinions of another person about the person; and (h) the person's name where it appears with other personal information relating to the person or where the disclosure of the name would reveal other personal information about the person;
Risk[4]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence
Risk Assessment[5]	The process of identifying risks to organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Security Control[6]	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

[4] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/risk
[5] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/risk_assessment
[6] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/security_control

Threat[7]	Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
User[8]	Individual or (system) process authorized to access an information system.
Vulnerability[9]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

10.0 Contact Information

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

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

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

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