NDMA NATIONAL DATA
MANAGEMENT AUTHORITY

Information Handling

Ethics Policy

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	Muriana McPherson	20-07-2023
General Manager (NDMA)	Christopher Deen	20-07-2023

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
20-07-2023	1.0		General Manager, NDMA	National ICT Advisor

Summary

1. This policy informs public service/government employees of the ethical and professional way information is to be handled.
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 Government of Guyana has a mission to develop and implement appropriate ICT (Information and Communications Technology) solutions that will transform the delivery of Government services. The numerous roles and responsibilities of the organisation encompass many aspects of information handling and as such, it is of utmost importance that the information gathered from such responsibilities are handled in an ethical, professional, and legal manner. Government of Guyana employees must clearly understand their responsibilities and duties of trustworthiness, confidentiality, and jurisdictional boundaries when accessing the government's digital systems and information.

The purpose of this policy is to inform public service/government employees of the ethical and professional way information is to be handled.

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 and 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

The Government of Guyana is committed to advancing the ethical and responsible use of all network and information resources, and has a zero-tolerance policy regarding illegal, dishonest, improper, or irresponsible use and/or dissemination of its network and information resources. We consider ethics when fulfilling data handling requirements in the discharge of their duties for the following reasons:

4.1 It reduces potential harm to all individuals involved and helps to maintain public acceptability around the work produced.

4.2 It is consistent with good practices in industry around Data security.

4.3 It helps to maintain the reputation of the government as custodians of employees' and third parties' data.

Additionally, users must read the Acceptable Use policy and conform to the prescribed directives on what is acceptable and what is not as it relates to information resources.

Policy

4.4 Ethical Principles[1]

Examining the way, the Government of Guyana works with data using an ethical lens helps to mitigate risk for both individuals and the government. The Government of Guyana's policy shall follow ethical principles that support decision making when working with data. The following details the ethical principles that employees and/or contractors of government organisations must follow.

4.4.1 Purpose of data use must be defined.

4.4.1.1 When using data, the purpose and any proposed actions should be clearly defined upfront.

4.4.2 Transparency is key, and engagement with stakeholders fosters trust.

4.4.2.1 The intent for the use of data should be clearly communicated with data subjects and stakeholders, along with information about how the data will be used. A culture of trust should be fostered between the organisation and data subjects, with clear communication, a foundation for this relationship.

4.4.3 Informed consent must be obtained for collection and use of data.

4.4.3.1 For consent to be informed, data subjects must be aware of what data is collected, how it will be used, and any actions that will result. Data subjects should be given the opportunity to opt out of having their data collected or used. However, opting out may carry consequences which should be communicated to data subjects and those using the data.

4.4.4 Legislation and Policies should be considered a minimum requirement for appropriate data use.

4.4.4.1 The Organisation must comply with all laws of the Cooperative Republic of Guyana, including but not limited to the Cybercrime Act No. 16 of 2018 and the Access to Information Act No. 21 of 2011 while carrying out job functions.

4.4.4.2 Compliance with all Policies and Standards of the Government of Guyana must be achieved.

4.4.5 Strategies should be implemented to minimise harm and reduce bias.

4.4.5.1 An assessment should be conducted to consider potential harms that may arise from the collection, use and storage of data, or interventions resulting from data insights. The possibility of bias should be minimised where possible.

4.4.6 Be aware of and observe relevant government-wide arrangements for trustworthy data access, sharing and use.[2]

[1] Retrieved from: Enterprise Data Ethics Framework https://data.uq.edu.au/enterprise-data-ethics-framework

[2] Retrieved from: Good Practice Principles for Data Ethics in the Public Sector https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf

4.4.6.1 It is the responsibility of public officials to be aware of and build knowledge in the specific governance arrangements, mechanisms, and tools framing data access, sharing and use, to ensure they are respected, applied and used.

4.5 Information Handling

Users are required to:

4.5.1 Adhere to the *Traffic Light Protocol (TLP) Standard* when sharing information.

4.5.2 Adhere to the *Information Classification Standard* so that information entrusted to the organisation is uniformly protected.

4.5.3 Take every precaution to prevent unauthorised access to any passwords, license keys, user identifications or other information that may be used to access network and related assets associated with job duties.

4.5.4 Limit access to information contained in or obtained from the network, related assets, or associated with job functions to authorised persons only.

4.5.5 Treat all confidential information within the network, related assets and obtained via job functions as such.

4.5.6 Seek guidance from existing policies and/or their immediate Supervisor and/or Director whenever they are faced with uncertainty about the correct decision regarding appropriate use, confidentiality, or access, and to do so ***before any*** action is taken on the issue in question.

4.5.7 Do not share, record, transmit, delete, or in any way alter information on the network, or related assets, except when required to perform job duties as authorised.

4.5.8 Report any incidents of non-compliance, system vulnerabilities and use that might result in disruption to their immediate supervisor and/or Director.

4.5.9 Accurately document setup procedures and any modifications done to equipment or software applications (configuration management) and to forward same to their immediate supervisor and/ or change advisory board for approval ***before*** making changes. This is to ensure that others will be informed of procedures and modifications.

4.5.10 Adhere to Original Equipment Manufacturer (OEM) recommendations and or/ recognised industry best practices for system design, rollout, hardening and testing.

4.5.11 Desist from downloading, installing, or configuring any tools, utilities or software that will hinder the requisite monitoring and logging of events on any network asset.

4.5.12 Alert any public sector or private sector organisations whose operations are likely to be significantly affected by an event or omission known. All communication must follow authorised escalation procedures and communication protocols.

4.5.13 Upon receiving information from the different sources: researchers, customers, other teams, Government entities, etc, respond to inquiries in a timely manner, even if it is only to confirm that the request has been received.

4.5.14 Upon receiving information that can either adversely affect or improve safety and security, inform the cybersecurity incident response team about the same, while duly considering confidentiality, privacy laws and regulations, and other obligations

4.5.15 Operate on the basis of verifiable facts. When sharing information, such as indicators of compromise (IOCs) or incident descriptions, transparency regarding evidence and the scope of the issue must be provided. If this is not possible, the reasons for not sharing the evidence and scope should be given with the information.

4.5.16 Review information for accuracy before disseminating. Any inaccurate information should be clearly identified as such.

4.6 Privacy and Confidentiality

Employees are required to:

4.6.1 Respect the privacy rights of other employees, contractors and third-party workers of the organisation they are employed. Their information including data, files, records, or network traffic must not be perused or examined, except as defined by the appointed roles of employees, Government's approved policy framework and/or without the permission of the end user.

4.6.2 Obtain written permission ***before*** conducting risk assessments, probing systems on a network for vulnerabilities or using any remote administration tools.

4.6.3 Respect the right to safeguard confidential information pertaining to employers, clients, and users except as dictated by applicable law.

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, 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. Organisations requesting exceptions should 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 Definitions of Key Terms

Term	**Definition**
Confidential Record[3]	"confidential record" means a record that would case damage or be prejudicial to national security if made publicly available.
Data[4]	A representation of information, including digital and non-digital formats.
Data Subjects[5]	Data subjects are persons to whom data refer.
Personal Information[6]	"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; (b) information relating to the education, medical, psychiatric, psychological, criminal or employment history of the person or information relating to financial transactions in which the person has been involved; (c) any identifying number, symbol or other particular assigned to the person, finger-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; (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;
User[7]	Individual or (system) process authorised to access an information system.

[3] *Retrieved from:* Laws of Guyana, Access to Information Act 2011, ACT No. 21 of 2011.

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

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

[6] *Retrieved from*: Laws of Guyana, Access to Information Act 2011, ACT No. 21 of 2011

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

10.0 Contact Information

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