NATIONAL DATA MANAGEMENT AUTHORITY

Acceptable Use of Information Technology Resources 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 acceptable use of information technology resources.
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 and Benefits

Appropriate organisational use of information and communication technology ("ICT") resources and effective security of those resources require the participation and support of the organisation's workforce ("users"). Inappropriate use exposes the organisation to potential risks including virus attacks, compromise of network systems and services, and legal issues. The purpose of this policy is to define acceptable and unacceptable use of information and information technology infrastructure to protect the confidentiality, integrity and availability of Government of Guyana IT resources.

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

Except for any privilege or confidentiality recognised by law, individuals have no legitimate expectation of privacy during any use of the organisation's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to: all computer files; and all forms of electronic communication (including email, instant messaging, telephones, printing, computer systems and other electronic records). In addition to the notice provided in this policy, users may also be notified with an information banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorised use of the organisation's IT resources is not permissible.

The organisation may impose restrictions, at the discretion of their executive management, on the use of IT resources. For example, the organisation may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the organisation's IT resources (e.g., personal USB drives, iPods).

Users accessing the organisation's applications and IT resources through personal devices must only do so with prior approval or authorisation from the organisation.

5.0 Policy

5.1 Acceptable Use

All uses of Information and Communication Technology (ICT) resources must comply with organisational policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including intellectual property laws.

Consistent with the foregoing, the acceptable use of ICT resources encompasses the following duties:

5.1.1 Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;

5.1.2 Protecting organisational information and resources from unauthorised use or disclosure;

5.1.3 Protecting personal, private, sensitive, or confidential information from unauthorised use or disclosure;

5.1.4 Observing authorised levels of access and utilizing only approved IT technology devices or services; and

5.1.5 Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and/or designated information security representative.

5.1.6 Authorised organisational resources use must have copyrights attached to same.

5.1.7 For security and network maintenance purposes, authorised company or person may monitor equipment, system, and network traffic.

5.2 Unacceptable Use

Inappropriate use of government resources is generally defined as, any use which introduces operational and security risks, and exposes the Government of Guyana to potential legal and financial liability. The following list is not intended to be exhaustive but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorised job responsibilities, after approval from organisational management, in consultation with organisation IT lead (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes, but is not limited to, the following:

5.2.1 Unauthorised use or disclosure of personal, private, sensitive, and/or confidential information;

5.2.2 Unauthorised use or disclosure of organisation information and resources;

5.2.3 Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;

5.2.4 Attempting to represent the organisation in matters unrelated to official authorized job duties or responsibilities;

5.2.5 Connecting unapproved devices to the organisation's network or any IT resource;

5.2.6 Connecting organisational IT resources to unauthorised networks; Connecting to any wireless network while physically connected to the organisation's wired network;

5.2.7 Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with organisational policies;

5.2.8 Using an organisation's IT resources to circulate unauthorised solicitations or advertisements for non-organisational purposes including religious, political, or not-for-profit entities;

5.2.9 Providing unauthorised third parties, including family and friends, access to the organisation's IT information, resources or facilities;

5.2.10 Using organisation IT information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);

5.2.11 Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using organisational IT resources;

5.3 Occasional and Incidental Personal Use

Occasional, incidental and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the organisation's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilisation. Exercising good judgment regarding occasional and incidental personal use is important. Organisations may revoke or limit this privilege at any time.

5.4 Individual Accountability

Individual accountability is required when accessing all IT resources and organisation information. Everyone is responsible for protecting against unauthorised activities performed under their user ID. This includes locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorised disclosure. Credentials must be treated as confidential information, and must not be disclosed or shared.

5.5 Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted organisation, non-public, personal, private, sensitive, or confidential information to or from personal email accounts or use a personal email account to conduct the organisation's business. Users must not store restricted organisational, non-public, personal, private, sensitive, or confidential information on a non-organisational issued device, or with a third-party file storage service that has not been approved for such storage by the organisation.

Devices that contain organisational information must always be attended to or physically secured and must not be checked in transportation carrier luggage systems.

5.6 User Responsibility for IT Equipment

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the organisation and must be immediately returned upon request or at the time an employee is separated from the organisation. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the organisation. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The organisation has the discretion not to issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

5.7 Use of Social Media

The use of public social media sites to promote organisational activities requires written pre-approval from the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation. Approval is at the discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources and may be granted upon demonstration of a business need. Final approval by the Permanent Secretary, Administrative Head, or Head of Human Resources should define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorised, the use of organisational email addresses on public social media sites is prohibited. In instances where users access social media sites on their own time utilising personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to the organisation and staff. These expectations are outlined below.

5.7.1 Use of Social Media within the Scope of Official Duties

The Permanent Secretary, Administrative Head, or Head of Human Resources, or designee, must review and approve the content of any posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of the organisation. However, Permanent Secretary, Administrative Head, or Head of Human Resources approval is not required for postings to public forums for technical support, if participation in such forums is

within the scope of the user's official duties, has been previously approved by his or her supervisor, and does not include the posting of any sensitive information, including specifics of the IT infrastructure. In addition, Permanent Secretary, Administrative Head, or Head of Human Resources approval is not required for postings to private, organisation approved social media collaboration sites. Blanket approvals may be granted, as appropriate.

Accounts used to manage the organisation's social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow information security standards, be unique on each site, and must not be the same as passwords used to access other IT resources.

5.7.2 Guidelines for Personal Use of Social Media

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should respect the privacy of the organisation's staff and not post any identifying information of any staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.

If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. A disclaimer might be: "The views and opinions expressed are those of the author and do not necessarily reflect those of the organisation."

Users should not use their personal social media accounts for official business. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used on organisational devices and IT resources, to prevent unauthorised access to resources if the password is compromised.

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. 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
Personal Information[1]	"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, fingerprints, 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;

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

User[2]	Individual or (system) process authorized to access an information system.
Contract worker[3]	"contract worker" means a person who performs work for another person pursuant to a contract between the employer of the first mentioned person and that other person;
Confidential Record[4]	"confidential record" means a record that would case damage or be prejudicial to national security if made publicly available.
Social Media[5]	Forms of electronic communications, including websites and applications, that enable users to create and share content or to participate in social networking. Examples include: Facebook, YouTube, Whatsapp, TikTok, Instagram etc.

10.0 Contact Information

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

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

[3] *Retrieved from:* Laws of Guyana, Termination of Employment and Severance Pay Act, Chapter. 99:08

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

[5] Retrieved from: NIST Small Business Cybersecurity Corner https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary