NDMA

NATIONAL DATA
MANAGEMENT AUTHORITY

Email 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 email systems.
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

Email represents a vital communications medium through which critical services and sensitive information are disseminated. The purpose of this policy is to enforce the proper use of Government of Guyana, hereafter referred to as 'GoG' email systems and to make users aware of what the GoG deems as acceptable and unacceptable use of its email systems. It also emphasises the importance of only using secured government-issued email addresses to conduct official government business.

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 applies to all Government of Guyana's public sector ministries and agencies and support organisations connecting directly and/or indirectly to the Government of Guyana's Information Communication Technology (ICT) infrastructure.

4.0 Policy

Cybercriminals often use phishing attacks to compromise information systems. Attackers can trivially mimic emails from any source. For instance, the account 'ministerofsecuritygy@gmail.com' can be created by anyone and can be used to look like a real government account. Standardising the use of official government emails for government business is therefore very important as the use of personal emails such as Yahoo, Gmail, and Hotmail creates harmful security risks

4.1 Inappropriate Use

4.1.1 Under no circumstance is an authorised user permitted to engage in any activity that violates existing local and/or international laws as well as the policies and procedures of ethical conduct, safety, and proper business practices while utilising government-issued emails.

4.1.2 The GoG email system shall not be used for distributing or accessing any illegal, disruptive, or offensive messages, including but not limited to profanity, obscenities, derogatory remarks, offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, religious beliefs, or pornography. As a matter of standard business practice, all government electronic communications must be consistent with conventional standards of ethical and polite conduct.

4.1.3 Any offensive material received in email must be reported to the subject ministries' IT Department and Human Resources Department without undue delay.

4.1.4 Sending chain letters or joke emails from a GoG email account is explicitly prohibited.

4.1.5 Technical support personnel may not review the contents of any government employee's email communications out of personal curiosity or at the behest of individuals who have not gone through organisational approved channels.

4.2 Government Business Communication

4.2.1 Public sector employees must use government-issued email accounts for official communication. The use of private/personal email accounts such as third-party email systems like Hotmail, Gmail, Yahoo etc., for official Government communication is strictly prohibited. Institutions/Agencies are required to provide email accounts to employees.

4.2.2 The use of GoG email systems is for GoG business. Personal use of this email system is limited to minimal and incidental providing that its use:

- does not consume more than a trivial amount of system resources,
- does not interfere with productivity, and
- does not pre-empt any government activity. This means that government electronic communication systems must not be used for charitable fundraising campaigns, political advocacy efforts, private business activities, or personal amusement and entertainment.

4.2.3 Where applicable, all non-work-related email is to be saved in a separate folder from work-related email.

4.3 Forwarding Government Emails

4.3.1 Users are prohibited from setting up any rules which automatically forwarding GoG emails to any third-party email system.

4.3.2 Users are prohibited from using third-party email systems and storage servers to create or memorialise any binding transactions or to store or retain email on behalf of GoG. Such communications and transactions should be conducted through proper channels using GoG approved documentation.

4.3.3 Official government emails shall not be forwarded to personal email accounts.

4.3.4 Messages received via official government emails shall not be forwarded to a third party in the absence of express consent from the sender and a clear business objective; except the content of the email received contravenes a prevailing policy or legislation and warrants the intervention of the relevant authorities. In all other cases, forwarding of messages from outside parties to other third parties can only be done if the sender/receiver expressly agrees to this forwarding.

4.3.5 Emails forwarded to email addresses not owned or operated by GOG must not contain any sensitive or confidential information.

4.4 Disabling Email Accounts after suspension or termination of employment

4.4.1 Human Resources and or the Information Technology Division within government ministries and agencies shall immediately disable access to government-issued emails upon either the suspension or termination of employment. This is applicable to all forms of termination of an employee's job, including death, dismissal, or resignation.

4.4.2 Emails shall be retained in accordance with the organisational retention schedule if they qualify as a GoG business record. Emails will be deemed as a business record once there exists a legitimate and ongoing business reason to preserve the information contained in the emails.

4.5 Sharing Account credentials with another individual

4.5.1 Public Sector ministries and agencies shall not encourage sharing of email access credentials unless it is to allow access to a common email account, e.g., frontdesk@agency.gov.gy; or an assistant managing their Minister/Head of Agency's email account.

4.5.2 Requests for the reset of email account passwords must be made by the owner of the email account or a duly authorised individual of the Organisation.

4.6 Email Subscription Lists and Newsfeeds

4.6.1 The use of mailing lists, news feeds, push data updates and other mechanisms for receiving information over the internet must be restricted to material that is clearly related to both government business and the duties of the receiving employee.

4.7 Electronic Messaging and Mail system

4.7.1 Electronic mail accounts must employ personal user-IDs and associated passwords to isolate the communications of different users. Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is forbidden.

4.7.2 The username, electronic mail address, organisational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings. Electronic mail "signatures" indicating job title, name and address of organisation and contact number are required for all official government communication.

4.7.3 In keeping with Intellectual Property rights, employees using Government electronic mail systems must (1) repost or reproduce material only after obtaining permission from the source, (2) quote material from other sources only if these other sources are properly identified, and (3) reveal internal government information only if the information has been officially approved for public release.

4.7.4 Except as otherwise specifically approved by management, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications.

4.7.5 Attachments to electronic mail messages, should be scanned with an organisational authorised virus detection software package at the server level before allowing user access.

4.7.6 Employees are only allowed to use organisational authorised mail clients to access government email.

4.8 Emails received from third parties

4.8.1 Unexpected email received from third parties should be viewed with suspicion. Even if the third party is known and trusted, viruses may still cause an infected email/attachment to be sent from the trusted third-party unknown to them.

4.8.2 Sensitive information must not be forwarded to any party outside government without the prior approval of the administrative head of the government agency.

4.8.3 Messages sent by outside parties should not be forwarded to other third parties unless the sender clearly intended this and unless such forwarding is necessary to accomplish an ordinary business objective. In all other cases, forwarding of messages sent by outsiders to other third parties can only be done if the sender expressly agrees to this forwarding.

4.8.4 Email systems must indicate to recipients whenever emails originate from senders outside of their own domain by placing a banner in the top or bottom of the email to that effect.

4.9 Transfer of sensitive information

4.9.1 If sensitive information must be sent by electronic communication systems, encryption or similar technologies to protect the information must be employed. PGP (Pretty Good Privacy) is recommended as a relatively simple way to send sensitive information in encrypted form over the Internet.

4.10 Email Access and Retention

4.10.1 Emails are to be centrally stored, archived and retained in accordance with established retention schedules and applicable laws of Guyana.

5.0 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 Definition of Terms

Term	Definition
User[1]	Individual or (system) process authorised to access an information system.
Phishing[2]	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
Mobile Device Management (MDM)[3]	The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices.

10.0 Contact Information

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

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

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

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