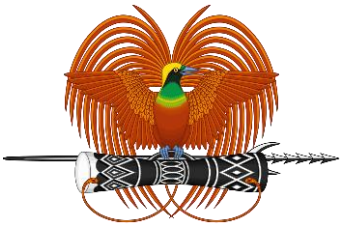

Papua New Guinea

Department of Information and Communications Technology

Government

Email Standards and Guidelines

2023

Document Control:

Document Name:	***PNG Government Email Standards & Guidelines* 2023**
Prepared by:	Department of Information and Communications Technology
Edition:	Version 1
Approved by:	Public Service ICT Steering Committee
Date Approved:	29th May 2023
Effective Date:	1st July 2023
Next Review Date:	

Papua New Guinea Government Email Standards and Guidelines **2023.**

ARRANGEMENT OF CLAUSES.

Papua New Guinea Government Email Standards and Guidelines **2023.**

PART 1. - PRELIMINARY.

1. NAME.

This instrument is the PNG Government Email Standards and Guidelines 2023.

2. COMMENCEMENT.

This instrument commences on [1 July 2023].

3. AUTHORITY.

This instrument is made under Section 64 of the Digital Government Act 2022.

4. SIMPLIFIED OUTLINE.

(1) This instrument prescribes the standards and guidelines for all government emails. All public bodies must comply with this instrument.

(2) This instrument has been produced by the Department of Information and Communications Technology (DICT).

(3) Part 1 sets out preliminary matters.

(4) Part 2 contains Standard 1 and Standard 2, and it is mandatory for all public bodies to comply with these standards.

(5) Part 3 contains guidelines for emails, and it is recommended that public bodies follow these guidelines.

(6) Part 4 contains other matters with Appendix 1.

(7) Notes are included in this instrument to help understanding by drawing attention to other provisions information or explanations. The notes are in small type, so that they don't disrupt the text. They do not contain statements of law.

5. DEFINITIONS.

The defined terms used in this instrument are set out in this section -

"content" means a message delivered to a customer, prospect, or subscriber's inbox via an automation platform, a dedicated email builder, or by hand;

"email" means electronic mail which is a method of exchanging messages ("mail") between people via electronic devices;

"email archiving" means a method for storing email content in a digital format that may be saved, indexed, searched, and retrieved;

"email hosting" means a service that runs email servers and delivers email services to consumers and companies;

"email retention policy" means the procedure for determining how long emails should be kept in an archiving system before being deleted;
"email security" means the protection of access to email accounts, content, and conversation;
"email standards" means a specification, established by consensus, and approved by a recognized body, and that provides for a common approach to email addressing;
"government domain" has the same meaning as in the ***Digital Government Act*** **2022**;
"mis-directed emails" means an electronic mail that is sent to the incorrect recipient which is also known as a misaddressed email;
"Public body" has the same meaning as in the ***Digital Government Act*** **2022**;
"recipient" means a person who is to receive email from either an individual or a business;
"role-based emails" means a generic email address assigned to a particular group, function, or service within an organization. This can also be known as a functional email address.

6. OBJECTS OF STANDARDS AND GUIDELINES.

The objects of these Standards and Guidelines are to -

(*a*) establish a format that is flexible and standardized for creation of all government emails; and
(*b*) maintain a consistent image of government accessibility; and
(*c*) ensure simplicity and is intuitive to use; and
(*d*) facilitate ease of identification of official government emails; and
(*e*) provide strategies for effective and consistent communication.

7. SCOPE AND APPLICATION.

(1) This instrument applies to all public bodies and all government emails using the government domain .gov.pg.

(2) Non-government bodies may comply with this instrument. However, these bodies must not use the government domain and the PNG Government crest must not be used for non-government emails.

8. GOVERNMENT EMAILS.

(1) A public body must establish official government emails for the use of both the public body and its employees.

(2) This government email must use the government domain .gov.pg.

(3) A public body using a domain, other than the .gov.pg domain, for any its emails must, as soon as practicable after this instrument comes into force, ease using that other domain and use the .gov.pg domain.

(4) An email of the public body that does not use the .gov.pg domain is not considered to be an official email of the public body.

PART II. - GOVERNMENT EMAIL STANDARDS.

9. OVERVIEW.

(1) This Part sets out the Government Email Standards.

(2) This Part prescribes Standard 1 which sets out naming conventions for government emails and Standard 2 which are email solutions.

(3) The objects of the Government Email Standards are to:
(*a*) ensure availability of new email addresses; and
(*b*) maintaining a consistent and predictable way of naming government emails; and
(*c*) provide recommended solutions for effective and consistent communication.

(4) All public bodies must comply with the Government Email Standards.

STANDARD 1. - NAMING CONVENTIONS.

Standard 1.1. - Role-based emails.

(1) Public bodies must use the following syntax when creating role-based emails.
[functionalname]@[publicbody].gov.pg

Example:

info@ict.gov.pg; or
digital.services@ict.gov.pg.

(2) In which case the:

[functionalname] is the name of the division, group, or service within the public body.

[publicbody] is a common term, acronym, or abbreviation for the public body e.g., 'ict', finance, defense, finance, labour, cis, etc. The name of the public body should contain an alias or its acronym. For instance, the Department of Information and Communication Technology (Department of ICT or DICT) uses 'ict'.

gov.pg is the government domain 'gov' is sponsored top-level domain (sTLD), referring to the Papua New Guinean government and 'pg' is the Internet country code top-level domain (ccTLD) for Papua New Guinea.

(3) When the [functionalname] comprises of more than one word, a single operator must be used to indicate the space between each word. The above example demonstrates this.

(4) [publicbody].gov.pg must be the public body's registered domain and must adhere to the PNG Government Domain Name Standards.

(5) Appendix 1 sets out a list of role-based email addresses that public bodies may use.

Standard 1.2. - Creation of personal email addresses.

(1) Public bodies must use the following syntax when creating personal emails.

[firstname].[lastname]@[publicbody].gov.pg

Example:

john.doe@ict.gov.pg.

(2) In which case the:

[firstname]	is the individual's legal or preferred name.
[lastname]	is the individual legal last name/surname. The last name may be more than one.
[publicbody]	is a common term, acronym, or abbreviation for the public body e.g., ict, finance, defense, finance, labor, cis, etc. The name of the public body should contain an alias or its acronym. For instance, the Department of Information and Communication Technology (Department of ICT or DICT) uses 'ict'.
gov.pg	is the government domain. 'gov' is sponsored top-level domain (sTLD), referring to the Papua New Guinean government and 'pg' is the Internet country code top-level domain (ccTLD) for Papua New Guinea.

(3) The [firstname] and the [lastname] must be written in lowercase.

(4) [publicbody]. gov.pg must be the public body's registered domain and must adhere to the PNG Government Domain Name Standards.

(5) All email addresses must be unique. In circumstances where there are duplicates, in which the first name and last name combination has been used already, this can be resolved by adding a middle initial letter or by adding a number to the [lastname].

Example:

john.doe1@ict.gov.pg.

STANDARD 2. - EMAIL SOLUTIONS.

Standard 2.1. - Email Hosting.

(1) All public bodies must use an email hosting service approved by the Department of Information and Communication Technology.

(2) Microsoft provides an email hosting service that is highly recommended by the Department of Information and Communication Technology. If a public body chooses to use this hosting service, it must use either Microsoft 365, or Microsoft Exhange 2019 or any version higher.

Standard 2.2. - Email Security.

(1) All public bodies must implement an Email Security Solution.

(2) All public bodies must use an email security solution approved by the Department of Information and Communication Technology.

(3) In compliance with the PNG Government Cybersecurity Standards and Guidelines 2023, all public bodies must ensure compliance with third-party email security.

(3) The following lists solutions highly recommended by the Department of Information and Communication Technology:

(*a*) Barracuda Email Security;
(*b*) Proofpoint Email Security;
(*c*) TrendMicro Email Security;
(*d*) FortiMail.

Standard 2.3. - Email Archiving.

(1) All public bodies must employ email archiving to maintain a tamper-proof copy of the emails.

(2) Barracuda Message Archiver is a solution highly recommended by the Department of Information and Communication Technology.

(3) The email archiving solution must be approved by the Department of Information and Communication Technology.

(4) Note that this email archive solution is also important in defining email retention policies.

PART III. - GOVERNMENT EMAIL GUIDELINES.

10. OVERVIEW.

(1) This Part sets out the Government Email Guidelines, containing recommendations for email usage, management, and governance.

(2) The objects of these guidelines are to promote proper email etiquette as well as providing essential guidelines for email usage, security, and management.

(3) It is recommended that public bodies follow these Guidelines.

Guideline 1. - Email Policy.

(1) Develop email policies for the access, management, and security for government emails within a public body.

(2) This policy will describe how to:

(*a*) understand the security responsibilities associated with government emails;
(*b*) understand responsibilities when using official government emails;
(*c*) determine which emails are kept and which can be deleted;
(*d*) how to manage government emails in a way that maintains their integrity and authenticity.

(3) This should also include policies for email security, email hosting and email archiving, including email retention policies (as mentioned in Standard 2 Email solutions).

Guidelines 2. - Email Security.

(1) Always practice protecting and keeping email accounts secure from unauthorized access, loss and compromise.

(2) Note that it also means to be aware of all cyber risks associated with emails, for instance, phishing and social engineering.

(3) Government email users should keep in mind the following factors of email security:
(*a*) Privacy of government emails;
(*b*) Authentication of email accounts;
(*c*) Integrity of emails sent.

(4) Public bodies should consult the National Cyber Security Centre (NCSC) to ensure that they comply with the appropriate minimum ICT Security standards for the protection of email and email systems.

(5) Public bodies should conduct security awareness training annually to reduce security risks such as phishing emails or malware attacks through emails.

Guideline 3. - Privacy.

(1) The PNG Digital Transformation Policy will help guarantee that personal information about citizens is safeguarded. Email content, and in some cases the email address itself (if it contains a specific address or addresses) may contain personal information.

(2) Any personal information gathered by a public body should be handled in conformity with general data protection principles, pending the enactment of data protection laws.

Guideline 4. - Appropriate use of government emails.

(1) It is important that each employee understands when to use official government emails.

(2) All employees are required to use official government emails when conducting government businesses and services, this includes when an individual is working outside of the office.

(3) When sending an email to a recipient, always maintain email etiquette in both role-based and personal emails.

(4) The following are some guidelines for proper communication over email:
(*a*) Create a clear subject, by using the subject line to state the purpose of the email;
(*b*) Always use appropriate languages when communicating;
(*c*) Use CC and BCC appropriately. CC when copying an individual publicly and BCC when copying an individual privately. Always recheck if the right recipient is copied and for errors in the recipient's email address;
(*d*) Proof-read every email that will be sent to avoid grammatical errors;
(*e*) Always acknowledge and reply to all the emails sent to the government email.

Guideline 5. - Email Signatures.

(1) Public bodies should use email signatures.

(2) The email signature creates a consistent brand image, establishes rapport, and make use of the time-tested communication medium.

(3) Contact information, pronouns, social media, a photo, and/or a logo can all be included in signatures. When emailing, the specifics in your signature can increase your and your brand's legitimacy. It may feel safer to respond to an email that appears professional and includes contact information.

Guideline 6. - Misdirected emails.

(1) Public body email systems should include informative messages in bounced/undeliverable email whenever possible.

(2) Bounced/undeliverable emails are typically a non-delivery notification sent to the sender's address, such as one indicating that the recipient's address is incorrect, or that the message size exceeds allowed limits, and so on.

PART IV. - MISCELLANEOUS.

1.1 IMPLEMENTATION SCHEDULE.

(1) The Email Standards and Guidelines are effective from [01.07.2023].

(2) All public bodies must adopt the mandatory standards in Part 2 on or before [01.07.2024].

12. COMPLIANCE AND MONITORING.

The Department may conduct an assessment and evaluation report of the compliance of public bodies with this instrument.

13. SUPPLEMENTAL STANDARDS AND GUIDELINES.

The Department may issue supplemental standards and guidelines to support the PNG Government Email Standards and Guidelines.

APPENDIX.

Appendix 1. - Role-Based Email Addresses.

The following shows examples of a few common role-based email addresses that each public body may have.

recruitment@; jobs@; careers@	These emails are used for recruitment by organizations.
help@; support@	Emails used for help or support within organizations.
sales@	Emails used for sales or marketing.
info@	Emails for inquiries and getting information from organizations.