The Republic of The Gambia

Government Email Policy

[2023-2027]

FINAL

MINISTRY OF COMMUNICATIONS & DIGITAL ECONOMY (MoCDE)
MOCDE | Tenengfara Business Complex, Bertil Herding Highway, Bakau, KM, Digital Address F889+WWH

Table of Contents

1. Abbreviations and Acronyms

The following are the list of Abbreviations and Acronyms for certain key words in this policy document:

- ***ICT/ICTs***: Information and Communication Technology/Technologies
- ***R&D***: Research and Development
- ***GoTG***: Government of The Gambia
- ***ECOWAN***: ECOWAS Wide Area Network
- ***NBN***: National Broadband Network
- ***ACE***: Africa Cost to Europe (International Fiber Optic Link)
- ***NICI***: National Information and Communication Infrastructure
- ***ICT4D***: ICT for Development
- ***IC Act***: Information and Communication Act
- ***MOCDE***: Ministry of Communications and Digital Economy
- ***LAN***: Local Area Network
- ***MDAs***: Ministries, Departments and Agencies
- ***GMD***: Gambia Dalasi (Gambia Local National Currency)
- ***E-Mail***: Electronic Mail
- ***Mailbox***: Email Account (Electronic E-Mail Account Mailbox)
- ***PS***: Permanent Secretary
- ***MOPS***: Ministry of Public Service
- ***PSC***: Public Service Commission
- ***PMO***: Personnel Management Office
- **S/MIME**: Secure Multipurpose Internet Mail Extensions
- **SMS**: Short Message Service
- **MMS**: Multimedia Message Service
- ***SLA***: Service Level Agreement
- ***IT***: Information Technology
- ***eBooks***: Electronic Book (Electronic Book Format)
- ***SSL***: Secure Socket Layer
- ***PGP***: Pretty Good Privacy
- ***Cc***: Carbon Copy (Email Carbon copy)
- ***Bcc***: Blind Carbon Copy
- ***PDF***: Portable Document Format
- ***NRS***: National Records Service
- ***NAO***: National Audit Office
- ***IAO***: Internal Audit Office
- ***DR***: Disaster Recovery (Disaster Recovery Site)

2. Executive Summary

As part of the execution of its mandate, the Ministry of Communications and Digital Economy has identified the strengthening of the government email platform as an integral component to the realization of its broad goals and objectives. The implementation of this email policy is also driven by the recognition of the significance of timely, effective, and reliable electronic communications.

The purpose of the email policy is to provide robust guidelines on the management and utilization of the government email platform. The policy sets out standard procedures geared towards enhancing the effective and efficient use of the government email services.

The policy begins by defining the management framework which is underpinned by clearly defined roles and responsibilities as assigned to the manager of the email platform- MoCDE, MDAs and other potential users. The policy also makes provisions for the adoption of Service Level Agreements between MoCDE and various institutions, in order to have a robust reference on the respective functions and obligations of the respective beneficiary institutions and individuals.

The government email policy 2023-2027 is anchored on ten (10) pillars that holistically spell out the entire governance structure as well as procedures for the utilization of the email service, these includes:

- ✓ Eligibility criteria,
- ✓ Email account creation,
- ✓ Ownership,
- ✓ Email specific procedures,
- ✓ Email account transfer,
- ✓ Email account deactivation,
- ✓ Acceptable and unacceptable Use,
- ✓ Security, privacy, and confidentiality,
- ✓ Retention, Archiving and Deletion
- ✓ Exceptions

The eligibility criteria cover The Presidency, all active Cabinet Ministers, Civil and Public servants using the government email platform, as well as a provision for potential users including the consultants, volunteers, interns, and researcher's contingent on approval from the management of MoCDE. The policy provides for the creation of emails to be centrally handled by MoCDE in order to ensure effective traceability, monitoring and evaluation of the platform and the usage of its associated services.

Additionally, in order to ensure transparency and accountability, the email policy also articulates the requisite processes relating to email ownership, email account transfer and email deactivation as and when necessary. There are also comprehensive provisions which outline acceptable and unacceptable use or behaviour with the government email. The policy also

catered for salient guidelines which will help address security, privacy, and confidentiality issues. These also include provisions relating to email and email content retention, archiving and deletion as an when necessary or in line with the national records service act and other applicable laws or regulations.

Moreover, the government email policy also inculcates resounding measures to support monitoring and compliance. This will be aided by the adoption of robust monitoring systems and tools to be complimented by audit mechanisms as an, when necessary, to help boost compliance to the various procedures and standards identified. The policy also further provides solid basis to address malpractices through the solid guidelines on violations and consequences.

In line with standard practice, the Government email policy also recommends for a comprehensive review to be conducted four years after implementation or periodic annual review or when the need arises. The review process will allow MoCDE and stakeholders the opportunity to identify gaps and proffer more sustainable solutions for improved outcomes in the next phase of implementation. This review is of more prominence given the unprecedented rate of technological evolution and the discourse around Cybersecurity, Data Protection and Privacy.

3. Introduction

Communication has been the catena gluing societies from the very dawn of human history up to date. Each epoch in history has its own unique way of conveying information through communication tools, systems, or platforms, from one end to another. With time though, generations relatively improved, in terms of effectiveness and efficiency in communication compared to its preceding generations. This upgrade can be attributed to constant development and innovations in ICTs especially in the domain of digital infrastructure and services.

Today's generation, which is often referred to as the knowledge and digital age, is underpinned, powered, and driven by ICT, which has brought about a new paradigm shift in communication and created an environment that enables communication and sharing of information seamlessly with little or without daunting human intervention.

The GoTG, understanding the potentials and benefits of ICT for socio-economic transformation and growth, and recognizes what ICT can offer in enhancing information sharing and communication, decided to ally with and leverage on ICT for its public sector transformation and modernization.

To achieve such, GoTG decided to rollout a holistic e-Government Programme in 2010, guided by an e-Government strategy and action plans. This e-Government programme has been implemented in three (3) five-year phases and the first phase includes the establishment of an ICT Cadre in Government to serve as a support structure to government in mainstreaming ICT in MDAs, followed by the establishment of an e-Government data center hosting government application and services including the government main email communication platform.

Over the years, this e-Government programme has registered successes and as well challenges, more so challenges related to the proper functioning of the government email platform due to many different factors. As a result, many government officials do away from using the government email services for official communication and rather uses private emails for official communication, which is risky and often resulted in loss of official information.

To remedy such challenges, the only possible option was to institutionalize a government email policy to ensure all government employees use the government email services for all official email communication within government. However, the government email policy can only be institutionalized if the government email platform is stable. Recognizing such, MoCDE recently endeavored to address the challenges surrounding the Government email platform by transitioning to a new, more stable, more secure, and sustainable email platform.

Nevertheless, even with a more stable, reliable, and secure email platform for government, there must be an email policy institutionalizing and guiding the administration and usage of the government email platform, thus this government email policy is developed to ensure that all government institutions and employees uses only their government emails for all official communication within government.

This Government Email Policy (GEP) is expected to; ensure that the Government email platform ultimately replace all manual correspondence (hard-copy letters and documents) or serves as an alternative to manual correspondence concurrently, save lot of cost as government can do away from the need of using vehicles (including fuel and lubricants) to dispatch letters between institutions, optimize resources by removing the need of having different email platforms for each institution, enhance efficiency in delivery of correspondence within government as with a button click an information can be sent and received from one end to the other and also ensure security and preservation of government information or contents communicated via email from being lost forever, damaged or compromised.

3.1. Policy Formulation Process & Life Cycle

A standard policy formulation process goes through various processes, in which there are methods or procedures to follow, and different policies may have different scope and requirements, however methods or procedures of formulation can sometimes be the same, similar, or different. In this policy, the following methods were employed from pre-formulation, during formulation, and post formulation.

Firstly, immediately after a decision was made by MoCDE for a Government email policy to be formulated, a benchmarking approach was devised, which investigated; existing tools or guidelines for email policy formulation, existing email policies formulated in developed or developing countries based on international best practice and existing email policies in the sub-Saharan African region.

The policy benchmarking process investigated the details of the structure of those existing email policies and the context in which they were developed, which was followed by putting up a well-organized and standardized table of content containing all the needed elements for the formulation of a standard email policy for government and public service use, putting in consideration all the use cases of the GoTG email platform.

Secondly, since a standard policy formulation process is usually done through a multi-stakeholder consultative process, similarly for this policy, an email policy survey questionnaire was developed, carefully reviewed internally, and adopted by MOCDE, which was then shared with all relevant MDAs to collect the basic data needed to serve as an input and set out the basis of the formulation of this email policy.

Moreover, the basic data collected and collated from the stakeholders using the email survey questionnaire has informed that at least four (4) government institutions out of twenty (21) institutions have their own or uses their own private email systems or services, in which the four (4) institutions are paying a minimum amount of GMD 750,000 annually for operation and maintenance of their private email systems or services, which will be very costly and unsustainable in the long run and practically impossible for government to afford and sustain if all government institutions are to have or use their own email systems and associated services, which will cost government a minimum of GMD 16,000,000 for twenty (21) Ministries annually compared to a minimum of GMD 6,426,376 annually if the Government email platform is used by all institutions.

The email survey also informed that at least 67% of government employees assigned with a government email address uses their private emails for official communications while (47%) usually perform unacceptable act on their official email accounts including deleting official emails and not retaining or archiving emails. Notably, at least 30% of government employees never use the Government email system, 85% of government employees interchangeably use their private email accounts and their government email accounts, 90% of institutions show interest in using the government email platform and would want their staff use it as well and 10% of institutions think otherwise with the believe that the government email platform has never been stable.

Additionally, the data collection and analysis process was followed by the policy formulation process and upon completion of the policy formulation process, this policy; was shared as draft for internal review within MOCDE, shared online on the MOCDE website for all MDAs to review and send in their comments/suggestions, in which both MoCDE staff and MDAs sent their comments and inputs to MoCDE for review, consideration and consolidation into the draft policy.

After incorporating all the relevant comments, inputs and suggestions from MDAs, a validation workshop is organized to validate the policy and the validated policy document is sent to Cabinet for adoption and once adopted by Cabinet, the Policy will be implemented by the Policy Implementing Entity.

The Figure (1) below depicts the Government E-Mail Policy Formulation process and its entirelife cycle from pre-formulation, during-formulation to after-formulation:

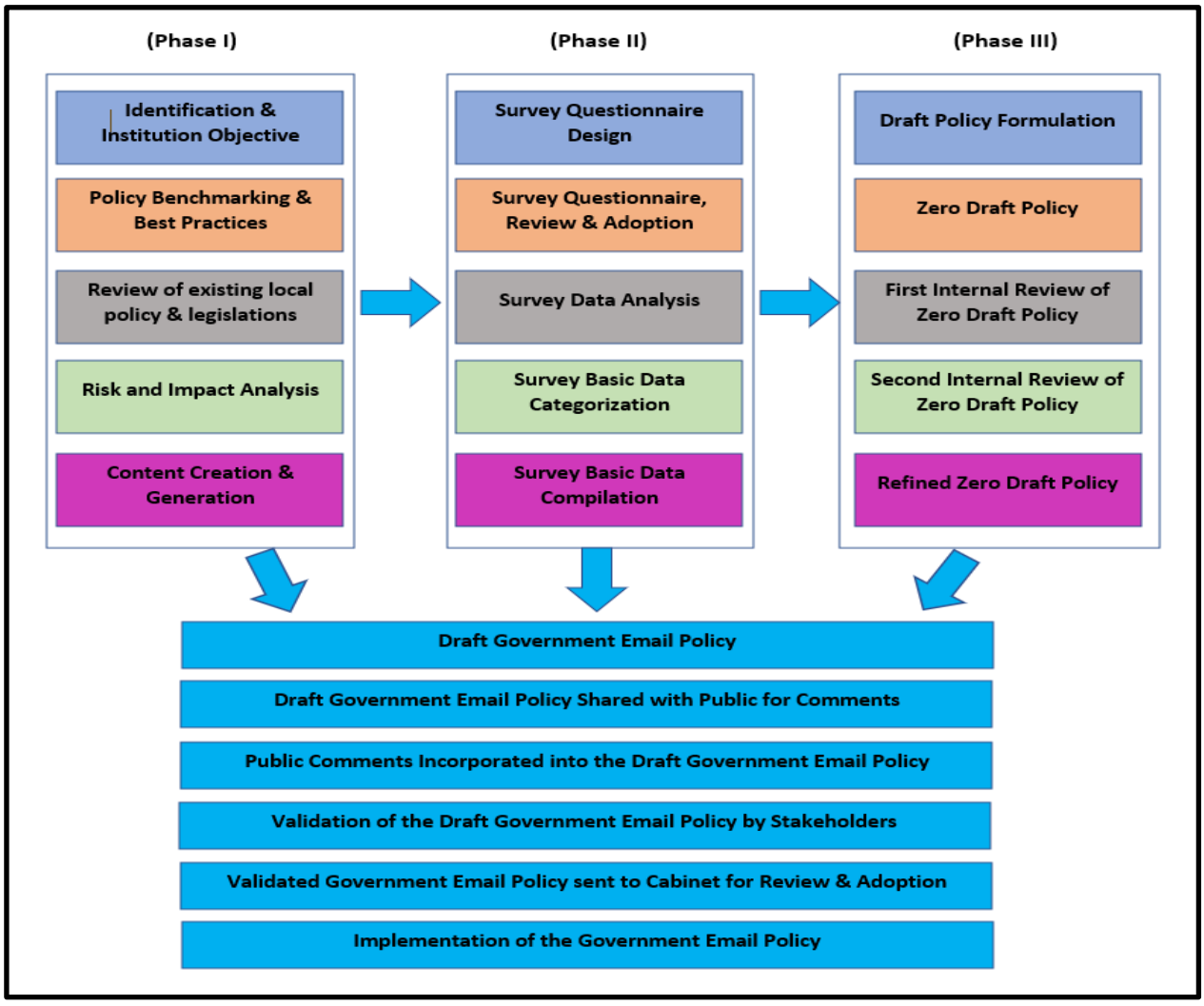

Figure (1): Policy Formulation Process

The formulation process of the E-Mail Policy passes through the above three (3) different phases as indicated in figure (1). Once the last stage of the third phase of the formulation process is completed, which is implementation phase, it will be followed by series of annual and midterm reviews of the policy to ensure is always up to date and up to standard.

3.2. Purpose

The general purpose of this policy is to provide a robust framework that articulates standardized and formalized electronic communications guidelines for the government of the Gambia. The guidelines spell out the requirements for intra and inter government electronic communications guidelines as well as instructions on the GOTG's electronic communications with its development partners. The email policy will therefore help ensure the following:

I. To ensure the availability of email accounts to all eligible employees of Government.
II. To ensure effective and efficient email communication within Government.
III. To ensure email communication is an acceptable means of official correspondence.
IV. To provide guidelines on how Government employees should send, receive, and manage their official email accounts.
V. To provide guidelines on risk mitigation for the government email system and email communication within government.
VI. To outline the acceptable use of government email platform.
VII. To ensure the security and confidentiality of government email communication and information.
VIII. To ensure the proper management, preservation, retention and archiving of government emails records.
IX. To enhance trust and confidence in government email system and services.
X. To promote transparency and accountability in email communication within Government.

3.3. Scope

The scope of this email policy covers all government institutions using the government email platform under the (. gov.gm) domain and it is applicable to the following:

I. All government institutions using the government email platform.
II. All Local Governor Offices, Embassies, Higher Commissioners and Consulates using the government email platform.
III. All employees of GoTG working outside the country in Embassies, Higher Commissioners and Consulates provided with an Email Account from the government email platform.
IV. All employees of GoTG provided with an Email Account from the government email platform.
V. All employees of GoTG sending, receiving, retaining, and processing email messages with associated contents or attachments, through the government email platform.
VI. All interns, consultants and any other third party including individual, group, corporate body, organization, or institution using the government email platform.
VII. All government employees managing the government email platform.
VIII. All government email infrastructure including computers, equipment, devices, application, and services.
IX. All entities or individuals performing email audit on official email accounts.

The scope does not include local chief offices, municipalities, local government agencies and independent public institutions or entities established by an act of parliament or individuals working for such public institutions or entities that are not using the government email platform or provided with an email account under the (. gov.gm) domain.

3.4. Objectives

The overall objective of this Email Policy is to ensure formalized, standardized, effective, efficient, reliable, and secure electronic communications within Government as well as between government and its relevant partners. The policy also aims to enhance ownership, transparency, and accountability in the management of government or public records, in particular electronics or digital records. The following are the specific objectives of the Government Email Policy:

I. To ensure government email communication serves as an adequate replacement for official correspondence or an acceptable concurrent alternative within the next 4 years.
II. To ensure the onboarding of all Government to the official email platform by the end of December 2023
III. To ensure all government institutions and employees uses official government email for all their official electronic communications by the end of December 2023.
IV. To ensure 99% availability and reliability as well as enhanced secure access of the Government Email Platform starting from June 2023
V. To ensure effective, efficient, lawful, ethical, and sustainable email communication within government.
VI. To ensure 100% compliance to the email policy usage principles by all users all by the end of Q4 2023
VII. To ensure effective quarterly monitoring and auditing on the usage of the Government Email system and associated services through automated, periodic, or other systemic methods.

3.5. Definitions

This Email Policy contains certain technical terms and keywords that should be clearly defined to avoid ambiguities for non-technical users of the government platform. The terms or keywords in this policy are defined as follows:

a) **Email/E-Mail**: Any message either in plain text, html format or image(s), distributed by electronic means from one computer user to one or more recipients via a network using the following sender or recipient address format: [something@domainname.something].
b) **Email/E-Mail Account**: Is a virtual address and container for email messages provided to an

individual by an email service provider with a username and password to enable access to email account, to send and receive emails.

a) **Email Account Creation:** Is the process of creating an email account by an email service provider following a definite set(s) of rules or requirements based on a requirement provided by a particular user or entity.

b) **Email Account Transfer:** An email account transfer is the process of transferring or moving an entire email account and/or its associated content from one domain or sub-domain to another.

c) **Email Account Deactivation:** It is the process of changing the state of an email account from its active state to an inactive state, that can be restored back anytime it's need again without deleting any of its associated content.

d) **External Email Accounts:** These are either private or third party 'Email Accounts' that are integrated with the Government Email Platform under the (. gov.gm) domain for the purpose of forwarding an official email from a private email account to official to an official email account.

e) **Government Email Platform**: This refers to as the Government Email platform and associated services setup, configured and deployed by GoTG, under the management of MOCDE, providing free email services to Government employees for their official email communication.

f) **(. gov.gm) domain:** This refers to as the legal and officially registered, recognized and acceptable assigned identifiable IP address translated into a unique name, that allows users to connect to the Government centralized server where website and email account data of MDAs and Government employees resides.

g) **Email Signature:** This refers to as a characterized and personalized signature block, often called an email footer, which provides an email recipient with the sender's name, designation, institution name, email addresses and phone numbers.

h) **Email Attachment:** This is computer file(s) attached to an email message to be sent to one or more email recipients, either in text document format, image, video, or zipped folder.

i) **Disclaimer:** An email disclaimer is a block of text that is added to an outgoing email to limit liability, often appear at the bottom of an email message, after an email signature.

j) **Spams:** Any irrelevant or unsolicited bulk Emails sent to an email address(es) for the purpose of advertisement, phishing and spreading malware, are here referred to as spams.

k) **Email Communication:** This refers to as the sending and receiving of messages in the format of plain text, html, images or documents over networked computers or devices using uniquely identified email addresses.

l) **Official Communication:** This is a form of formal communication from Government employee or institution that stems from authority, accountability, and responsibility of a job guided systematic procedures, certain set rules and orders set for the civil service, which must be followed.

m) **Users:** This refers to all users of the Government Email platform.

n) **Civil Service:** This refers to as the distinct body of staff within public sector of the Gambia.

o) **Civil Servant:** This refers to as an employee of the public sector appointed by the decision of the Gambia PSC in accordance with the Civil Service Law.
p) **Password:** It is a secret word, phrase or string of characters assigned by default by the email service provider or set by the user to gain access to an email account.
q) **Virus:** An infective piece of code or computer program that is capable of copying or replicating itself by modifying or interrupting other computer programs or services.
r) **Email Service Provider:** It is the government entity entrusted of establishing, operating, maintaining, and managing the Government Email Platform and also providing email services to all eligible government employees.
s) **e-Discovery / E-Discovery**: Is short for electronic discovery, which is defined as the process of discovery in civil litigation that is carried out in electronic formats.
t) **External Hard Drive**: Is an external hard drive is a portable storage device that can be attached to a computer through a USB or FireWire connection, or wirelessly.
u) **Policy Implementing Entity**: Is the Institutions entrusted to implement this policy.
v) **User Institution**: Is any Institution using the Government Email Platform.
w) **Carbon Copy (Email Carbon copy):** Email sent to individual(s) other than the main recipient(s), for the purpose of the individual(s) copied to be informed or aware of the message or email conveyed or being conveyed.
x) **Blind Carbon Copy**: Blind carbon copy allows the sender, responder, or forwarder of an email to conceal the person entered in the Bcc field from the other recipients, the electronic version of confidential files.

In an event one or all of the above definitions contradicts in part or in whole a definition that exists in other national laws or regulations, more so the laws or regulations governing the ICT sector of the Gambia including data protection and privacy, national records management and or any other related, the definition in those laws or regulations shall prevail, unless otherwise if the definitions set forth is this email policy are more complete in nature, meaning the definitions in other national laws or regulations is subset of the definitions in this policy.

4. Policy Statement

MoCDE on behalf of GoTG encourages and promotes the idea that all government employees can achieve a recognizable degree of productivity and efficiency in service delivery by leveraging on the available computing or digital communications systems and services it is providing, especially the Government Email platform. Consequently, this Email Policy has been designed, developed, and formulated to ascertain that:

- Government Email platform is an appropriate and acceptable medium and means of official communication.
- Government Email System and Service can act as a permanent replacement for manual correspondence (hard-copy letters and documents) or act as an alternative in the absence of the Government Email System and Service.
- Government Email System and Service is used by all Government Employees and Institutions for their official communication. including records management requirements for emails.

- Government Email and Service ensures fluid, consistent, and effective email communication within government.

In addition, this email policy has been established to ensure that; it users comply with all the usage principles and guidelines set forth is this policy, email maintenance, management and usage is monitored to ensure compliance, all institutions or its representatives sign the policy to indicate agreement to comply with it, all institutions to sign an SLA with the Email Service Provider to ensure quality of service and business continuity, Email Implementing Entity is responsible for implementing the policy within its areas of responsibility and this policy is approved and supported by Cabinet.

5. Roles and Responsibilities

The following responsibilities are specified for all the entities providing or using the Government Email Platform:

A. Responsibility of Policy Implementing Entity:

MOCDE in collaboration with MOPS, PMO, PSC and/or any other identified entity by Government is entrusted with the responsibility of implementing this Email Policy. As such, the following are its core responsibilities:

- To make available both the soft and hard copy of this policy document to all MDAs.
- To enforce this policy and make sure it is applicable to all MDAs and employees of government using the government email platform under the (. gov.gm) domain.
- To constitute an Email committee or working group to spearhead matters relating to the Government email platform and its associated activities.
- To constitute an Email Audit Team within government, may be from Internal Audit or National Audit Office or outsource to a third party to carry out Email Audits with reports and give instruction for an automated audit system or tool to be installed by the E-Mail Service Provider to perform automated audit functions on the government email system and service.
- To monitor compliance and carry out action for violation of acceptable usage principles set forth in this policy.
- To maintain and be updating this policy regularly when needed
- To ensure adequate budget or funds are allocated for the sustainability of the email platform.

In carrying out this responsibility, the policy implementing entity should collaborate and consult with all key stakeholders to ensure this Email Policy is implemented according to standards and keeping in view the issues of transparency, accountability, and the rights of Users.

B. Responsibility of Email Service Provider:

MoCDE will be responsible for the role of Email Service Provider for the government email platform, even in case this role is outsourced or subcontracted to a third party in the future, the third party shall be acting on behalf of MoCDE. The following are the core responsibilities of the Email Service Provider, which is to:

- Identify and delegate trusted team of technicians as administrator(s) to manage the government email platform including regular backups and disaster recovery planning.

- Make sure the Government Email platform is available 24/7 for use by all MDAs and users under the (. gov.gm) domain.
- Manage Email Accounts of all 'Users' including responding to email accounts creation request, user verification, creating email accounts, testing email accounts, configuring email accounts, deactivating email accounts, email Accounts transfers, email accounts audits, regular email accounts backup and resolving email accounts issues.
- Create a unique email address where users can send in their email accounts creation, deactivation and transfer requests, and issues relating to their accounts and password change requests.
- Report any system failures and malfunctions in relation to the Government Email Platform and incidents including security breach to authorities and ensure timely fix or solution to the failures, malfunctions, or incidents.
- Ensure the Government Email Platform including email accounts and passwords is highly secure and reliable at all times.
- Use appropriate security measures including email encryption, to protect sensitive or confidential information.
- Install or deploy where possible, an automated account management system that will create and alert the system administrator regarding changes to the system or abnormal activities.
- Ensure the privacy and confidentiality of users' email data are safeguarded.
- Comply with all laws, regulations, and policies related to the use of government email platform and other electronic communications including complying with all relevant data protection & privacy regulations.
- Comply with all national records preservation, retention, archiving and management requirements and all principles set forth under this email policy.
- Avoid using the government email for any illegal, immoral, or unethical activities.
- Conduct trainings were needed to 'Users' of the Government Email Platform for usage or any other relevant purpose upon request by their host institutions.
- Sensitize government employees as well as their institutions on the importance and benefits of using the Government Email Platform as a medium of official communications.
- Provide technical support and assistance to employees and authorized users in the event of any issue or concern with the Government Email Platform.
- Act as the point of contact for any issue or concern relating to the Government Email Platform and notify Users and Institutions on Email Accounts matters.
- Give Email Auditors required access needed to access the Government Email Platform.

The responsibility of the Email Service Provider is not limited to only ensuring the Government Email Platform is properly functioning or providing acceptable services to its users, also the Email Service Provider should ensure that the underlying Infrastructure for the Email Platform is regularly enhanced and improved at all times and the people managing the Email Platform are equipped with the right tools and their capacity regularly updated.

C. Responsibility of User Institution:

The following are the responsibilities of the User Institution (MDA) using the Government Email Platform under the (. gov.gm) domain, which is to:

- Make sure all Government employees under its Institution are provided with an Email Account under the (. gov.gm) domain.
- Identify and trained someone to be responsible for managing the institution info email including receiving, sending, and forwarding emails and as well printing emails and associated contents for the records if need be.
- Identify a focal person or point of contact responsible for all activities related to the Government Email Platform and associated activities.
- Request for a new Email Account under the (. gov.gm) domain from the Email Service Provider, for newly recruited Government employees under its Institution including personal information such as full name and contact.
- Request for an Email Account transfer from the Email Service Provider, of a government employee who had been transferred from another Institution to its Institution including personal information such as full name, email, and contact.
- Provide both internet and computers to Government employees under their Institutions to be able to access the Government Email Platform and make sure the devices being used to access the email are secure.
- Ensure all Government employees under its Institution only uses the Government Email Platform for official communication.
- Make sure all Government employees under its Institution adhere to the government email acceptable, unacceptable usage and other policy principles set forth in this policy.
- Ensure all Government employees under its Institution uses the Government Email Platform for email communication only.
- Report any security breach, hacks, or other related incident from any Government employee under its Institution to the Email Service Provider.
- Report any activity or behavior of any Government employee that goes against the government email acceptable and unacceptable usage principles set forth in this policy and ensure actions are taken against violations.
- Notify the Email Service provider to deactivate email account of an employee, when his/her service is terminated or no more active for any other reason.
- Request for training of its staff on how to use the Government Email Platform from the Email Service Provider.
- Give Email Auditors required access needed, when conducting Email Accounts auditof Government employees under its Institution in case of non-automated email auditing.
- Comply with all principles set forth under this email policy.

D. Responsibility of Users:

The following are the responsibilities of the Users using the Government Email Platform under the (. gov.gm) domain:

- The 'User' shall request from its Institution to be provided with an Email Account under the (. gov.gm) domain in case it is not provided.
- The 'User' shall provide personal details including full name and contact details to its Institution when requesting for an email account under the (. gov.gm) domain.

- In the case a 'User' is transferred from its previous Institution to a new Institution with an existing Email account under the (. gov.gm) domain, the 'User' shall request from its Institution for the transfer of the contents its previous Email Account to the new one.
- The User shall request from its Institution to be provided with an access to internet and computer, to gain access to Government Email Platform in case it is not provided.
- The User shall request from its Institution to deactivate its official Email Account after retirement, resignation and when going for secondment in case it is not done.
- The User shall always ensure safe and secure usage of its Email Account under the (. gov.gm) domain.
- The User shall regularly check and respond to emails in a timely manner either through enabling email notification or manually.
- The User shall report any security breach, hacks, or other related incident associated with its Government Email Account to its Institution or Email Service Provider.
- The User shall abide by all laws, regulations, and policies related to the use of government email and other electronic communications including data protection and privacy requirements.
- The User shall comply with all the acceptable and unacceptable policy usage principles set forth in this policy.
- The User shall comply with all national records preservation, retention, archiving and management requirements.
- The User shall request for training on how to use the government email system if not provided.
- The User shall give Email Auditors the required access needed during Email Accounts audits.
- The User shall comply with any directive issued by the policy implementing entity dealing with e-Discovery or actions taken against him/her due to violation of the government email acceptable usage principles set forth in this policy.

The User at all times, aside the above responsibilities shall ensure responsible and secure use of the Government Email Platform and also comply with all national laws and regulations, more so the laws and regulations in the ICT sector or related including data protection & privacy and national records management requirements as per the Nation Records Service Act.

6. Service Level Agreement

To compel the Email Service Provider to provide well-functioning and uninterrupted services and manage expectations of all users of the Government Email Platform while at the same time ensure trust and confidence in using it and also set principles for instances where users are not liable for not using the Government Email Platform due to service outages and performance issues, a Service Level Agreement (SLA) is needed to serve as a contract between the Email Service Provider and User Institutions.

This SLA shall be initiated, formulated by MoCDE or representative of MoCDE, reviewed and accepted and signed by all User Institutions using the Government Email Platform under the (. gov.gm) domain and this SLA shall immediately come to effect once it's signed and institutionalized and may be reviewed periodically when the need arises.

7. Policy Pillars

In ensuring effective and efficient Email communications within government there is a need for a secure, stable, and reliable Email communication platform and also a set of policy guidelines on how the Email communication platform should be used and how email exchanges should be done between users of the platform.

Consequently, this email policy set forth the following ten (10) standard policy pillars with its underline principles for the usage of the Government Email Platform:

7.4. Eligibility

For eligibility purpose, the Users of the Government Email Policy shall include:

- ✓ The Presidency
- ✓ The Vice President and all Cabinet Ministers working in Government.
- ✓ All employees of Government working in the civil and public service including those working outside the country in diplomatic missions.
- ✓ Specific non-employees as deemed necessary and approved by MOCDE management including Contract Staffs, Interns, Researchers, Consultants, Volunteers and Partners.

All those that are deemed eligible, shall become eligible after starting work and worked for at least five (5) working days before having their Email Accounts created under the (. gov.gm) domain. However, the Email Service Provider (MOCDE), may choose to offer a treatment of urgency to any of the eligible user, either based on their request or MoCDE establishing it.

7.5. E-Mail Account Creation

The Email Service Provider (MoCDE) or its representative, shall create all Email Accounts under the (. gov.gm) domain of the Government Email Platform and the following are the Email Account creation process:

- ✓ Email Accounts shall be created by institutions or based on request from the User Institution or initiated by MOCDE for the case of Specific Non-employees where necessary.
- ✓ Email Accounts shall be created, hosted, maintained, and managed for all eligible Users by MOCDE at its Data Center or elsewhere hosting the Government Email Platform.
- ✓ Email Account creation process in normal situation shall not take more than 24 hours.
- ✓ Email address of all newly created Email Accounts shall bear the following format: (firstname-initial)and(middlename-Initial-IfAny)and(surname/surnamePlusANumber)@Institution-subdomain.gov.gm
- ✓ Email address for the President, Vice President, First Lady(ies) and First Gentleman shall bear the following formats respectively: President@op.gov.gm & HE@op.gov.gm , VP@ovp.gov.gm , firstladyOrfirstlady1/2@op.gov.gm and FG@op.gov.gm.
- ✓ Email address of all Ministers, Secretary General, Secretary to Cabinet, Chief Protocol

Officer, Permanent Secretaries shall bear the following formats respectively: Minister@institution-subdomain.gov.gm,SG@institution-subdomain.gov.gm, SC@institution-subdomain.gov.gm,CPO@institution-subdomain.gov.gm,and PS@institution-subdomain.gov.gm or PS1/2@institution-subdomain.gov.gm.

- ✓ Email address of all Governors, Embassies, Consulates, Higher Commissioners shall bear the following formats respectively: RegionName@molgl.gov.gm and ResidingCountryTopLevelDomain@mofa.gov.gm.
- ✓ Default password of all newly created Email Accounts shall be determined by MOCDE and at first sign-in, Users shall be notified to change their default passwords.
- ✓ MOCDE will create and maintain only one Email Account and Email address per User, however, may support additional Email aliases, one forwarding to the other.
- ✓ MoCDE will create and maintain two email addresses for the Email Administrators, one for administrative duties and for routine tasks, and will create and maintain an Administrative Account for each IT / ICT Units of various MDAs for email account management of various email accounts under their MDAs.
- ✓ MoCDE will create and maintain service account with a lower-level administrative privileges should be created for testing.

7.6. Ownership

Once eligible users are created or assigned with an Email Account, they are privileged at will and given the liberty to user their Email Accounts and Email Addresses for all their official communication in line with the acceptable and unacceptable usage principles set forth in this policy, however, the ownership of the Email Account and its associated information or contents shall remain to be Government property, including the following:

- ✓ All messages including plaintext, html, images, videos, text documents, files, and zipped folders, meant for official communication sent from or received in the User Email Account.
- ✓ All distributed or group email(s) containing messages including plaintext, html, images, videos, text documents, files, and zipped folders, in which the User email address was copied, meant for official communication.
- ✓ All advertisements, promotional materials, special offers or related, send to the User email address for the purpose of business or related, sent from an entity or partner of theUser Institution.

Since all Email Accounts for all Users registered in the Government Email Platform with a domain or subdomain name under the (.gov.gm) domain belongs to the Government, the User must at all times not personalized its Email Account and shall ensure proper safeguards for its Email Account and all its associated content from leakages, damages and lost.

7.7. Email Specific Procedures

The User, upon eligible and acquiring a valid official government Email Account, is privileged to send and receive emails related to official communication only. In light of this email policy, the following are the specified structure and format of an official Email Account and the procedures for sending, receiving, carbon-copying, forwarding, and checking Emails using the Government Email Platform.:

a) Email Formats:

The standard and accepted format of sending an Email message must contain the following: Subject Line, Salutation, Body of the Email, Signature and Disclaimer, as detailed below:

- **Subject Line**: The subject line should have the following attributes: Short, Specific, Simple,Informative and contain markers like; *Important*, *Urgent*, *Notice*, *Re*, *Reply* and *Fwd*.
- **Salutation**: The salutation should be formal in nature, for example, for unfamiliar people,use '*To Who It May Concern'*, '*Dear Sir/Madam*', or '*Dear*'. For Senior Officials, use their designation only or followed by their names, '*Hon. Minister/HM*', '*Permanent Secretary/PS*' etc.
- **Body of the Email**: The body of the Email should be formatted using grammatical structures such as sentence and paragraphs with punctuations, bold, underline or bullet points were necessary. It should also be simple, clear, understandable, and readable.
- **Signature**: The email signature must contain the name of the sender, designation, name of institution, email address of sender and contact details of sender.
- **Disclaimer**: The email disclaimer(s) should always last after the signature block, it shouldbe short, clear, precise, and informative.

b) Email Signature:

All eligible users with an Email Account using the Government Email Platform, under the (. gov.gm) domain, shall use Email Signature with the following format while sending and receiving emails:

- *[Full Name of the User]*
- *[Designation/Job Title]*
- *[Specific Job Role (Optional)]*
- *[Name of Institution]*
- *[Department/Unit/Directorate - (Optional)]*
- *[Telephone Number(s)]*
- *[Social Media App Number(s)] - (Optional)]*
- *[Email Addresses]*
- *[Institution Website / Official social media Page(s) – Optional]*
- *[Professional Social Media Accounts/Handles – (Optional)]*

c) Email Disclaimers:

All institutions likewise their employees using the Government Email Platform under the (. gov.gm) domain, must manually include the following email disclaimer into the settings of their Email Accounts or reach out to the Email Service Provider to support them include it.

DISCLAIMER STARTS

All the attachments, messages and/or contents associated with this email, are strictly considered to be property of the Government of The Gambia, unless the content clearly indicates otherwise. All the attachments, messages and/or contents associated with this email, are considered strictly confidential, intended for the addressee only and solely for the purpose of official communication. If you are sure that you are not the intended addressee and you might have mistakenly received this email, please do not disclose, or use any information associated with this email for any reason good or otherwise, rather kindly notify the sender and delete this email immediately. In addition, the views, ideas, and opinions expressed in this email, are those of the sender/forwarder, unless otherwise clearly stated to be those of the institution. In the case of any loss or damages incurred as a result of using this email and all its attachments, messages and/or contents, the institution shall not be liable for it. The institution does not, in any case, warrant the integrity of this email, nor that it's free from errors, viruses, interception and/or interference.

DISCLAIMER ENDS

d) Email Attachments:

For the purpose of sending or forwarding emails with an attachment using the Government Email Platform, the user should consider Email the attachment to have the following properties:

- Formats: (.pdf), (.zip), (.rar), (.doc), (.docx), (.txt), (.avi), (.mp4/mpeg-4), (.mov), (.wmv), (.flv),(. webm), (. kvm) and (.jpg/jpeg/jpe/jfif/png/gif/bmp/tif/tiff/heic).
- Size Limit: 10 MB
- Link(s): In case it is above 10 MB, to send as a link sitting on a cloud.
- Indicative: All attachments should be indicated in the body of the email as attachments.

Additionally, the following should be considered by a User when sending, receiving, and forwarding an email with an attachment using the Government Email Platform:

- The attachment shall be scanned for viruses, malware or related before sending.
- The attachment shall not be corrupt or damaged prior to sending it to any User.
- The attachment shall be in a common file format such as the one above that can be easily opened or access by any User.
- The attachment shall be compressed if it is large in size to reduce transmission time and storage space and shall not be above maximum attachment size limit.
- The attachment shall be labeled appropriately and have a clear and descriptive file name.
- The attachment shall be encrypted if it contains sensitive or confidential information.
- The attachment shall be sent using a secure method, such as S/MIME or PGP, if possible.
- The attachment shall not contain any prohibited content, such as copyrighted materials or harmful software or application(s).

e) Sending Email:

All Users and/or institutions must consider the following when sending email(s) related to official communication:

- Email to be send, must be professional in nature and solely for official communication.
- Email to be send, must possess all the listed email formats in section 7.7 dealing with Email Specific Procedures.
- Email to be send, must be carefully composed, addressed, and send only to the intended and correct recipient(s).
- Email should be professional and free from offensive or inappropriate language and content.
- Email to be send, if containing attachments, must be in harmony with all the attachment properties and principles listed under the Email Attachments subsection (d) of section 7.7 and shall be relevant to the content of the email.
- Email to be send, if sensitive or confidential, shall be labelled as sensitive or confidential, encrypted where possible and send through a secure means.
- Email to be send, shall not be for the purpose of spam, unwanted or unsolicited messages.
- An Email with sensitive information that has been sent mistakenly to an unintended recipient, the sender should immediately inform its institution of the incident, however, in the case that it hasbeen mistakenly sent to a known recipient, the recipient should be contacted immediately by the User or its Institution, for it to be deleted immediately.
- Auto send/reply must be configured by the User when going on leave or vacation or beingsick, indicating the reason for the auto send/reply.
- Email and associated attachments being sent that requires to be printed and handover to the recipient records office for records, must be labeled as such when being sent.
- A valid Email sent to recipient(s) that has bounced back for whatsoever reason, it should be re-sent for the second time, but if bounced back again, the recipient(s) must be informed for an alternative.
- Users shall comply with all relevant laws, regulations, and policies of GoTG including data protection & privacy and national records management requirements when sending emails.
- Users shall comply with all principles set forth in this email policy when sending emails.

f) Email Spams:

The Users of the Government Email Platform and the Email Service Provider must consider the following when dealing with received spam emails or in the case spams are automatically send from the User Email Account either due to virus, malware, or others:

- Spams received either as email message, links or attachments should immediately be labeled as a spam, marked as junk and/or deleted.
- Users should carefully examine whether the received email is a spam email or not

prior to labeling them as spam, marking them as junk and/or deleting them.

- Users may choose to report spam emails to the Email Service Provider for them to be filtered.
- In the case that a User mistakenly labelled, marked as junk, or deleted a relevant email with a thought that it is a spam email, when detected, the email should immediately be restored where possible.
- Email Service Provider shall provide or implement, where necessary a spam filter on the Government Email Platform to minimize incoming spams.
- In the case that a spam filter is implemented by the Email Service Provider, it should be ensured that the filter rules are not too high to be filtering relevant or real emails.
- In the case that a relevant or real email has been filtered by the spam filter implemented by the Email Service Provider, when detected, the email should immediately be restored.
- In the case that the User mistakenly open a spam email or click on a spam link or download a spam attachment, as a result, the User computer started behaving abnormally or its email started automatically sending or distributing unwanted email(s) to other Users, the User shall immediately inform the Email Service Provider or MOCDE or its institution for support in addressing such issues.
- In the case that the spam filter if any, installed by the Email Service Provider is no more working, the Email Service Provider shall inform all users and also come up with an alternative as a temporal fix until the filter is fully restored.

g) Receiving Email:

All Users and/or Institutions must consider the following when receiving any email related to official communication:

- A User shall check the sender information, subject line, and content of a received email, to determine whether the email is legitimate, relevant, and intended for the recipient.
- A User, upon receiving an email that is confidential or sensitive, must ensure that the received email is handled appropriately according to the principles set forth in this policy.
- When necessary, the User should respond to the received email(s), by relying to all email addresses in the email loop if any or put in copy other new email address(es).
- A User should be cautious when opening a received email with an attachment and ensure such an attachment is scanned where necessary and is safe to open before it is opened.
- Auto reply may be configured by the User in the User Email Account settings where necessary, to convey delivery notification of email to the intended recipient.
- Auto reply shall be configured by the User, indicating status of leave, sick period, vacations, out of office or long meetings to other Users or Email Senders.
- An Email received mistakenly by a User, the User shall inform the sender if known and delete it or immediately delete it if not known.

- ❖ Print received email messages and associated attachments and hand it over to the records unit or office for records keeping, in the case where the email system is not integrated with both government records management system (EMRS) and/or archives management system. However, email attachments that are too bulky needs not to be printed and shall be maintained in the email account of the user or forwarded if need be.
- ❖ An Email received on behalf of an institution that has been mistakenly deleted permanently by a User, the User must have to inform its institution of the incident.
- ❖ Users shall comply with all relevant laws, regulations, and policies of GoTG including data protection & privacy and national records management requirements when receiving emails.
- ❖ Users shall comply with all principles set forth in this policy when receiving emails.

h) Forwarding Email:

All Users and/or institutions must consider the following when forwarding any email related to official communication:

- ❖ Email to be forward should be forwarded only for the purpose of official communication.
- ❖ Email to be forwarded should be forwarded to the right or intended recipients.
- ❖ Email to be forwarded, must be professional and appropriate in nature.
- ❖ Email with associated content forwarded to a recipient that is suspected to contain virus, malwares or other malicious activities, the User that forwarded the email shall immediately notify the recipient(s) when detected.
- ❖ Email with sensitive information mistakenly forward to another known user, the recipient should be alerted to delete such Email, however in the case that it is forwarded to an unknown user, the institution should be informed.
- ❖ Email and associated attachments being forwarded that requires to be printed and handover to the recipient records office for records, must be labeled as such when being forwarded.
- ❖ A valid official Email forwarded to recipient(s) that has bounced back for whatsoever reason, it should be re-sent for the second time, however if bounced back again, the recipient(s) must be informed for an alternative.
- ❖ Users shall comply with all relevant laws, regulations, and policies of GoTG including data protection & privacy and national records management requirements when forwarding emails.
- ❖ Users shall comply with all principles set forth in this policy when forwarding emails.

i) Checking Email:

All Users and institutions must consider the following when checking their Email Accounts:

- ❖ Sign-in or login to their Email Accounts using their Username and Password
- ❖ Users may choose to use auto sign-in or login functions on their accounts when signing-in or login using their person or official computers.

- User shall check email account regularly during working hours and respond to important and urgent messages in a timely manner.
- Users may choose to configure their personal smart phones, tablets, and handheld devices for them to be able to access the Government Email Platform with auto sign-in or login functions.
- Users may choose to configure email notification on their personal or officially assigned computers where possible and necessary.
- Users must immediately sign-out or logout from their Government Email Accounts upon accessing them using a shared or public computer.
- Users shall limit or minimize the number of tries on password or usernames guesses, in case of forgotten passwords or usernames, and should immediately reach out to Email Service Provider for password reset or username details.
- Users shall comply with all relevant laws, regulations, and policies of GoTG including data protection & privacy and national records management requirements when checking email account.
- Users shall comply with all principles set forth in this email policy when checking emails.

j) Group Mailbox:

All Users and/or institutions must consider the following when setting up a group mailbox or participating as a group member in a group mailbox:

- All Group Mailbox(es) shall be created, used for purpose of official communication only.
- Any Eligible Government employee with an Email Account can create Group Mailbox(es) if need be.
- A User creating a Group Mailbox must first ensure that the group mailbox is necessary for official communication and that it aligns with the Institution's objectives and goals.
- Institutions may or can assign their employees to create a Group Mailbox for any specific purpose related to the Institution work.
- The Email Service Provider shall create Group Mailbox(es) for Users or Institutions based on their request.
- All members of the Group Mailbox shall be eligible and have an official email address under the (. gov.gm) domain.
- For any Group Mailbox created, there must be a group leader or administrator to coordinate email activities related to the group.
- For any Group Mailbox created, the group leader or administrator may choose to assign to other group members as group leaders or administrators.
- Spam or junk email that is sent to a Group Mailbox, the administrator(s) of the Mailbox shall carefully examine it and delete it immediately if confirmed to be a spam or junk email.
- Group Mailbox administrator(s) may choose to add in new group members or remove existing members if the need arises, upon consulting other group members if need be.
- An email, for official communication or not that has been sent to the Group Mailbox mistakenly, the sender if known, must be inform prior to deleting it or delete immediately otherwise.

- ❖ A third-party email address that has been mistakenly added to a Group Mailbox by a member of the Group, resulting to an email sent to that third party, the third party must be contacted for the email to be immediately deleted or the incident shall be reported to the authorities.
- ❖ All Group Mailbox members shall ensure the protection of the Group Mailbox from unauthorized access and also carefully handle sensitive and confidential information communicated via the group in line with the security and confidentiality information set forth under this email policy.
- ❖ All members of the Group Mailbox shall comply with all relevant laws, regulations, and policies of the Government including data protection & privacy and national records management requirements.
- ❖ All Group Mailbox members shall comply with all the principles set forth under this email policy.

k) Mailbox Capacity Limit:

Each eligible User, Institution or Group Mailbox User, using the Government Email Platform shall be provided with the following Mailbox Capacity Limits by default by the Email Service Provider:

- ❖ Capacity Limit for Individual Users Mailbox: **25 GB**
- ❖ Capacity Limit for Institution/Organization Mailbox: **50 GB**
- ❖ Capacity Limit for Senior Government Official Mailbox: **35 GB**
- ❖ Capacity Limit for Group Mailbox: **40 GB**

The above capacity limits may be adjusted by the Email Service Provider (MOCDE) based on needs, justifications, and availability of space at the MOCDE Data Center or MoCDE Email Hosting Platform. In any case, shall make sure judicious utilization of their official Email Accounts when sending, forwarding, receiving, and replying to emails. The Email Service Provider (MOCDE) or its representative, must at all times ensure that there is enough storage capacity for Mailboxes under the Government Email Platform. In addition,growth rate capacity needs of the Mailboxes should be well calculated so as to forecast for the future capacity needs of the Mailboxes and prepare for future expansion.

7.8. Email Account Transfer

All eligible Email Account holders of the Government Email Platform, who are moved or transferred from one institution to another, the following will be the procedure regarding previous Email Account Transfers, considering the User previous and present institution:

- ✓ In the event that a User is transferred from one Institution to another, its previous email account still stays with him/her, while the email account of the person concerned will be moved to its new institution subdomain to act as his/her default email account and the old email account deactivated, not deleted.
- ✓ A transferred User willing to transfer its email account from its previous institution,

must submit a written request for transfer of email account to the Email Service provider via its current institution including name, email address, phone number (optional), name of both previous and current institution.

- ✓ All the content of the User Previous Email Account shall be archived first by user previous institution, then migrated to the user new Email Account bearing it current institution subdomain.
- ✓ Once an email account of a User is fully transferred, the User reserved the right to receive Emails from its old or previous email account by default through email forwarding or similar techniques, unless the User do not want to receive emails from its old or previous email account.
- ✓ All Email Specific Procedures in section 7.7 and all other Email Policy Pillars, shall be applicable to the new Email Account of the User bearing it current institution subdomain.
- ✓ Credentials (Password) of the previous and new Email Account of the User must not be the same again when changing the default password of the new Email Account bearing its current institution sub-domain.
- ✓ In an event the User or its current institution do not receive any notification request for Email Account Transfer, the User or its Institution must follow up to ensure it is done appropriately in a timely manner.
- ✓ Email Service Provider, Email Administrators, User Institutions and Users shall comply with all principles set forth in this policy and as well all laws and regulations including data protection and privacy and national records management requirements when processing email account transfers.

7.9. Email Account Deactivation

The following procedures applies to deactivating an existing Email Account under the Government Email Platform:

- ✓ Prior to deactivating any Email Account (User, Institution or Group Email Account), the entire Email Account and all its associated contents must first be archived.
- ✓ A User who is no more in service, must submit a written request or its Institution must submit a written request on behalf of that User to the Email Service provider including the name, email address, phone number (optional) of the User Email Account to be deactivated or the Email Administrator of the institution with the administrative privileges if any, shall immediately disable the User Email Account and reactivated when the User comes back, however the Email Service Provider must be notified.
- ✓ All institution that signs the SLA as indicated in section 6 of this policy, shall notify the Email Service Provider of any employee, who officially resigns, retired, died, on secondment or sacked or fired from job for its Email Account to be deactivated within 24 hours, however in the case of death, the notification process can be prolonged.
- ✓ Email Accounts of any Government employee who resigns, retired, died, on secondment or sacked or fired from job, shall be deactivated either upon request by the User or the User institution within 24 hours, from the Email Account Service Provider

and shall be restored upon return of the employee within 24 hours.

- ✓ Email Service Provider will be at will or liberty to immediately deactivate Email Accounts of Government employee who resigns, retired, died, on secondment or sacked or fired from job, if notification is not given any time after 24 hours of detection.
- ✓ In case of security threat to the Government Email Platform, the Email Service Provider will be at will or liberty to suspend or deactivate the Email Account posing the security threat immediately and should be restored after the threat has been resolved.
- ✓ In the case of security threat, subsequent to deactivation, the concerned user or competent institution shall be informed.
- ✓ In case a request for deactivation has not been done by Email Service Provider in the required timeframe, the Institution of the User must contact the Email Service Provider to follow up on the request to make sure the deactivation is done immediately.
- ✓ Email Service Provider, Email Administrators, User Institutions and Users shall comply with all principles set forth in this policy and as well all laws and regulations including data protection and privacy and national records management requirements when deactivating email accounts.

7.10. External Email Accounts

The following are the principles set forth regarding the usage of and interaction with an External Email Accounts of a User while using the Government Email Platform under the (. gov.gm) domain:

- ✓ An official correspondence received by a User through a Social Media Platform or an External Email Account must be immediately forwarded to the User Official Government Email Address while copying some senior management staff of its institution when forwarding correspondence.
- ✓ An official email with all its associated contents received by a User in his/her External Email Account (Private Email Account) must be immediately forwarded to the User Official Government Email Address while copying some senior management staff of its institution when forwarding such email.
- ✓ Users must take or apply the appropriate security measures to protect sensitize or confidential information when using or interacting with External Email Accounts including encrypting emails where possible and the use of VPNs for email communication.
- ✓ Users shall avoid taking snapshot of official communication from their official email accounts using their mobile phones or social media platforms and forward it to their external email accounts.
- ✓ Users shall comply with all relevant laws, regulations, and policies of GoTG including data protection & privacy and national records management requirements when dealing with external email accounts.
- ✓ Users shall comply with all principles set forth under this email policy when dealing with External Email Accounts.

These policy principles related to external email accounts are carved out as safeguards with the assumption that prior to institutionalizing or implementing this Government Email Policy, there were Government Employees or Institutions with an official email accounts, as a result people or entities who

had their private emails or had contacts with them before would obviously or may send emails or documents related to official communications to their private emails and, in this policy document when an official email or correspondence is sent to the User or Institution private email account, the User or Institution must forward the received official email or correspondence to their official email accounts for records keeping, email preservation and archiving purpose.

7.11. Acceptable and Unacceptable Use

The Email Service Provider is the custodian of the Government Email Platform, that is providing email services to Government Institutions and Employees using it. To use the Government Email Platform for official Email Communication, the following are the set of principles for acceptable and unacceptable usage of the Government Email Platform:

Acceptable Use:

All Government employees or institutions are allowed to use their Government Email Accounts under the (. gov.gm) domain without limitation, however guided by the following acceptable use principles:

- ✓ Send, forward and receive emails for official communication to or from a government employee, public institutions or third parties through their official email accounts.
- ✓ Send, reply, or forward emails that are legal, legitimate, and ethical in nature to other Users or email addresses for work related purpose.
- ✓ Send, reply, forward or receive emails for financial approvals with attachments and assignment of tasks.
- ✓ Communicate with partners, businesses, and citizens.
- ✓ Send, receive, or respond to official correspondence or letters using scanned document format or plaintext.
- ✓ Copy relevant Users and institution info email address when sending, forwarding, and receiving emails for official communication.
- ✓ Embed official email addresses in websites contact or registration forms or use it as contact info email address.
- ✓ Participate in Group Mailbox(es) for official communication purpose.
- ✓ Register or login to a video conference platform for official communication purpose,either as a participant or organize and send meeting email notifications to users.
- ✓ Register for conferences, workshops, symposiums, trainings, trade fairs, career fairs andrelated corporate events, for work related purpose.
- ✓ Purchase software or other products or services online on behalf of its institution.
- ✓ Share their email with other people during conferences, workshops, and other related events for work related purpose.

Unacceptable Use:

Aside the acceptable use, there are also unacceptable use principles or scenarios when using the Government Email Platform. The following are unacceptable activities or behaviors from any user when using the Government Email Platform:

- ✓ Send, forward and received emails for non-official communication purpose.
- ✓ Use private for official communication while the SLA is still valid.
- ✓ Link or integrate External Email Account without adhering to the conditions of using an external email account.
- ✓ Send or forward illegal, illegitimate, and unethical emails to other users or email addresses for whatever purpose.
- ✓ Send an email that is not in harmony with section 7.7 of this policy.
- ✓ Delete email(s) meant for official communication.
- ✓ Send insulting, provoking, bullying, trolling, hate, racial and discriminatory messages and contents.
- ✓ Send unauthorized and classified institutional information.
- ✓ Send or request to be send fraud or forgery related message or contents.
- ✓ Send an email from other people or users account without their authorization.
- ✓ Participate in any illegal or unauthorized hacking activity including but not limited to, Email Spoofing, Email Flooding, Email Bombing, Snooping, Packet Sniffing or Eavesdropping.
- ✓ Send data that violates copyrights or intellectual property rights.
- ✓ Share login credentials with a third party.
- ✓ Share other user's login credentials with a third party either through the user email account or any other means or bridge their security, privacy, and confidentiality.
- ✓ Send other people's confidential and/or personal information.
- ✓ Login on a computer without appropriate or unlicensed antivirus software.
- ✓ Login on a public computer without logout or enabling auto-login.
- ✓ Send spam or junk emails or viruses and/or malwares to other users or email addressesdeliberately.
- ✓ Send unsolicited personal, commercial advertisements, promotion or promotional materials to other users or email addresses.
- ✓ Register or login at unsafe or suspected websites or services.
- ✓ Request for Email Account while not eligible or create an Email Account for ineligible Users.
- ✓ Filter relevant email(s) without notifying the User or the Authority.
- ✓ Refuse to comply during email audits.
- ✓ Illegally deactivating Email Account of any User.
- ✓ Reset User password or login into a User E-Mail Account without their consent.

7.12. Security, Privacy & Confidentiality

All Users of the Government Email Platform and as well as the Email Service Provider, must consider the issues of Email Security, Data Privacy and Confidentiality when using their Email Accounts or the Government Email Platform.

Considering the criticality of Emails Platforms or Accounts and their vulnerability to cyber-attacks, more so email platforms hosting sensitive government data, there is a need for security, privacy, and confidentiality of such critical or sensitive platforms and its associated data. As such, the following principles are set forth in this policy to ensure security and provide safeguards on privacy and confidentiality of Government data in the Government Email Platform:

Security:

Considering the security of all Government Email and all its associated contents, the users and administrators of the Government Email Platform must ensure the following:

- Select strong passwords at least eight (8) character, with the combination of specialsymbols, capital letters, random characters, and numbers, that are not easily guessable when creating passwords.
- Update passwords regularly to protect the email account from unauthorized access.
- Avoid writing down passwords openly in plain text manner.
- Safeguard username and passwords to restrict access to their accounts and Email Servers.
- Install and use licensed operating systems, licensed antiviruses and licensed software &apps, Installed & configure application firewalls at all times on Users computers where the Government Email Platform is accessible.
- Scan attachments with an appropriate licensed antivirus or antimalware software beforeopening them.
- Avoid opening spam contents or clicking spam or virus suspicions links or attachments.
- Configure and use valid and licensed SSL certificates on Email Servers at all times.
- Install and use licensed operating systems, licensed antiviruses and licensed software &applications on the Servers hosting the Email services.
- Setup, install, configure, and use firewalls appliances/equipment on both the Network and Email Servers.
- Install and use Email Spam filters on the Email Servers where necessary, configured atacceptable level to filter email spams only.
- Use multi-factor authentication, where possible, to provide an extra layer of security for email accounts.
- Regularly review and update access controls and permissions for email accounts and the email system to ensure that only authorized users can access sensitive or confidential information.
- Limit access to sensitive or confidential information to only those who has the right to access it.
- Ensure that all emails and attachments containing sensitive or confidential information are encrypted to protect against unauthorized access.

- Ensure Email Backups, Disaster Recovery Plans for the Email Platform and Redundancy for all equipment, devices and systems associated with Government Email Platform.

Privacy:

The privacy of Users using the Government Email Platform are as important as the security of Email Accounts of Users and the Government Email Platform itself. For purpose of privacy, the Users of the Government Email Platform as well as the Administrators, must ensure the following:

- All official emails should be carefully verified, particularly those containing personal, critical, and sensitive information of users and ensure their safety and security before sending or forwarded them to other users or email addresses.
- Computers, computing resources and network elements are safe and secure before beingused to send and receive emails.
- Encryption methods and PGPs are used when sending/forwarding emails personal, critical,and sensitive information of users.
- Sensitive and privacy related information or data of users filtered by the spam filter installed on the Email Servers, are not opened, or peaked at for any reason whatsoever.

Confidentiality:

Emails are not considered to offer the highest form confidentiality due to limitation in technology and user errors. However, there are several steps that can be taken to ensure and increase confidentiality of emails. For email confidentiality purpose, Users and Administrators of the Government Email Platform, must ensure the following:

- Not to breach confidential information or emails of other users when using the Government Email Platform.
- In an event of a confidential information that has to be sent using an Email, in which the sender does not want Users in an email loop to know the other Users in the same email loop, the Blind Carbon Copy (Bcc) function shall be used where appropriate.
- Confidentiality message is added to the sender Email Signature, for recipients to know the email contains confidential information.
- Send or forward confidential information in a password encrypted attachment, locked PDFfile, word file or any other common filing format and share the passwords or the encrypted or locked document using different mode of communication.
- Not use tools, software, applications or devices on the end users' computers, institution network and email servers that can limit or eliminate confidentiality of emails.
- Third party entities or people hired by institution or Email Service Provider using the Government Email Platform, must conform to this policy confidentiality principles.

7.13. Retention, Archiving and Deletion:

In the context of the GoTG, the IC Act of 2009 stipulated that Emails are acceptable means of communication and can be used as electronic evidence and the Data Protection and Privacy Policy & Strategy set guidelines on how data should be processed and exchanged. Similarly, the National Records Service Act of 1993 provides guidelines on how to manage government or public records from creation to destruction or permanent preservation as archives.

However, the use of electronic communications such as an email for official communication is somewhat nascent and in the absence of a comprehensive Government E-Mail Policy, managing email communication and considering E-Mail as acceptable official means of communication will be impossible or make managing of email contents as public records difficult, although emails are considered as public records in NRS Act of 1993, therefore its retention, Archiving and deletion should be tied broadly with the provisions of the NRS Act.

The NRS Act gives the responsibility of creation or retention schedules to institutions; thus section 6.10 of this Act can be considered as the Retention Schedule for email policies and as such, this Email Policy set forth the following principles on Email Retention, Archiving and Deletion when using the Government Email Platform:

Retention:

As specified under section 7.6 of this email policy, that all Email Accounts with their associated contents under the Government Email Platform, are properties of GoTG. For that reason, the following are the set principles for preserving or retaining Official Email Accounts:

- ✓ All Government employees must ensure that official emails with continuing values are preservedor always retained.
- ✓ All Email Accounts of Government employees and its associated contents must be kept as evidence and where appropriate and possible captured under institutions records management system(s).
- ✓ Email Service Provider (MoCDE), must ensure that all Official Email Accounts of Government employee who resigned, retired, died, or sacked are retained or preserved for the required period, before they are archived or migrated for storage for longer term retention or preservation purpose.
- ✓ Retention decisions for Official Email Accounts and its associated contents should consider; official, operational, business needs, legal and regulatory requirements, accountability, and transparency expectations.
- ✓ Official emails relating to complaints, appeals, disputes, and grievances should be retained if there is a need to preserve them for an audit trail.
- ✓ Email Accounts of Non-Official staff such as Interns, Consultants, Contractors, Researchers or Others must also be persevered or retained for the required period.
- ✓ All Government official emails shall be preserved for a period required by law (NRS Act).

Archiving:

Hence all Email Accounts of Government employees under the (. gov.gm) domain are properties ofGoTG, it is of high importance to retain or preserve the Email Accounts as long as necessary and possible. The following are the set principles for Archiving Official Email Accounts and its associated contents for longer term retention and preservation purpose:

- ✓ All Government Email accounts with its Users still in service, must be automatically archived temporary by the Email system on weekly basis or manually by the User itself every six (6) months if automated archiving is not possible.
- ✓ For the case of resigned, retired, dead or sacked User, after the Email Account of the Useris retained or preserved for a period of six (6) months, the Email Account with all its associated contents must be archived automatically by the Email System or manually by the Email Service Provider.
- ✓ Email Accounts of Government employee shall not be archived permanently while they are still active in service, however, shall be archived permanently at the national archives or national archives management system when no more permanently in service.
- ✓ All archived Email Accounts must be stored properly in either form, external hard drives, local data centers with DR sites capable of live replications, Government or local private clouds, and any other acceptable, safe, and secure storage medium.
- ✓ Archived Email Accounts stored in the above forms may be migrated or re-archived fromone location to another or one form to another.
- ✓ Archived Email Accounts may be restored for the purpose of investigation, research or returned of the resigned, retired, secondment and sacked User into employment service.
- ✓ All Email Accounts to be archived, shall be achieved in compliance with national laws including data protection & privacy and National Records Service Act of 1993.

Deletion:

As the same principles for retaining, preserving, or archiving Email Accounts and its associated contents, there are also principles set to be followed when deleting an Email and its associated contents under the Government Email service, which are as follows:

- ✓ All illegal, illegitimate, and unethical emails for any purpose must be immediately deleted or ordered to be deleted upon detection.
- ✓ All Government employees who retired permanently or died without any criminal recordand have their Email Accounts archived for a period of ten (10) years, the Email Account Service Provider upon consultation with the MOPS, NRS or other stakeholders, may choose to delete their Email Accounts and its associated contents.
- ✓ Users may immediately choose to delete all emails with no continuing value from their Email Accounts such as junks, spams, or emails of similar nature.
- ✓ Emails with viruses, malwares, and other malicious codes, either embedded in the email contents, links, or attachments, should be immediately deleted.

- ✓ All retained or persevered Email Accounts of Non-Official staff, Consultants, Contractors,Researchers or Others, after serving their retained or preserved period, must be deleted.
- ✓ In the case of Email Account Transfer, once new Email Accounts are created for newly transferred employees and contents migrated and archived, the Email Account Service Provider should immediately delete the old Email Account.
- ✓ In the case of Email Account Transfer, the old Email of the User must not be deleted, if itscontents are not yet archived or migrated to the new Email Account.
- ✓ In the case where the SLA stipulated in this policy is no more applicable, official emails shall never be deleted under any circumstance.
- ✓ Email Accounts of Users who are on Secondment, Sick Leave or Leave Without Salary shallnever be deleted under any circumstance.
- ✓ Email Account of a User or an Institution must be deleted when it no longer required to be retained, as determined by relevant laws and regulations and method of deletion shall ensure secure and confidential destruction of sensitive information.
- ✓ Group Mailbox(es) created and being used for illegal, illegitimate, and unethical use shallbe deleted by the Email Service Provider immediately upon detected or User institution may order the Group Mailbox Administrators delete them immediately or request its deletion from the Email Account Service Provider.

7.14. Exceptions

All the principles set forth here in this policy, must be observed, adhered to and/or respected or the User or User Institution will face possible punitive actions, however, there are exception and the exception in this policy mostly associated with the policy pillars, are as follows:

- ✓ Irrespective of eligibility criteria, an Email Account may be created for any User under the(. gov.gm) domain based on an executive directive or request and even in such case, the created email shall be used in accordance with all principles set forth in this email policy.
- ✓ In the case that an Email Account has been created based on an executive directive, any consequence or issues created by the User of that Email Account that goes against the email policy, the Email Service Provider shall not be held responsible.
- ✓ In emergency situations, the retention, archiving, and deletion principles set forth in this email policy may be temporarily suspended to ensure that important and time-sensitive information is communicated and acted upon as quickly as possible.
- ✓ In emergency situations, the User may choose to use their External or Private Emails for official communication.
- ✓ In emergency situations, the User may choose to ignore some parts of the Email Specific Procedures in section 7.7 under this policy, when sending, receiving, or forwarding an email, however the user shall cc their official email address only during the process.
- ✓ In emergency situations, Users may choose to give their email credentials to other trusted Government employees to login, access, and send or forward emails on their behalf's.

- ✓ In emergency situations, Users may choose to send, forward, or received emails from a computer or device that is not secure or not in line with privacy or confidentiality principles set forth in this policy.
- ✓ Email Account Service Provider may deliberately reset Users Email password, login into Users Email Account or Check contents of Users Email Account due to directive from court or Email Auditors, for the purpose of investigation.
- ✓ In a justifiable situation, Users Institutions may choose to request for the deactivation ofa particular employee Email Account or Non-Official staff, but the request must be sent to MOCDE formally before deactivation can take place.
- ✓ The SLA set forth in this policy shall not be applicable during major repair, maintenance, upgrade, and migration.
- ✓ Email Service provider does not need the consent or permission of the user during Email Account backups, migration where necessary, but when archiving Email Accounts,permission is needed from MOCDE management and principles in section 6.10, shall be applicable.
- ✓ In E-discovery situations, the retention, archiving, and deletion principles set forth in this email policy may be temporarily suspended to comply with legal requirements.
- ✓ In events of a system failure, the retention, archiving, and deletion principles set forth in this email policy may be temporarily suspended to ensure the recovery of important data and the continuity of government operations.
- ✓ Email Auditors, for the purpose of monitoring and compliance may give a directive for an Email Account of a particular user to be suspended or deactivated.
- ✓ Email Accounts and its associated contents are contained information or data that are classified or labelled as classified, must never be accessed by Email Auditors, Email Service Provider, or the Government Email Platform Administrators and needs special safeguards if to be archived at the nation archive(s).
- ✓ Government institutions operating under sensitive national security domains are the only institutions excluded; to have their own Email Servers providing email services to its employees.
- ✓ Government institutions operating under sensitive national security domains using the Government Email Platform under the (. gov.gm) domain, are exempted from the policy principles set forth in this email policy in the situation where Email Communication involves classified or highly classified information or data.

The exceptions listed above are limited and should not be used as a means to circumvent the principles set forth in this email policy. They shall only be used in exceptional, reasonable, and/or justifiable circumstances and authorities shall be informed, or it shall be thoroughly documented, where possible whenever it is used. Also, Users exercising these exceptions shall comply at all times, with the relevant national laws and regulations including data protection & privacy and national records management requirements, and also should be done in accordance with the principles of due process, transparency, and accountability.

8. Monitoring & Compliance

To ensure the principles, particularly those in this policy pillars are followed and respected by all users of the Government Email Platform, there is need for regular monitoring of all Users email activities, so as to ensure compliance to the principles of this email policy.

Additionally, a team of Email Auditors may be constituted by the Policy Implementing Entity to monitor all Users email activities, Email Administrators and the Government Email Platform and ensure compliance by all Users and Administrators to all the principles set forth in this email policy.

Alternatively, in some instances where necessary, the Email Service Provider shall monitor all Users email activities through an automated means or otherwise to ensure compliance. The Email Service Provider may have access to all information or data held in all Email Accounts under the (. gov.gm) domain when necessary and reserves the right to access the following and under the following circumstances:

- ✓ Any employee Email Account with its associated contents in suspicious situations ofunacceptable usage.
- ✓ To monitor whether a particular User or Institution is complying with this email policy.
- ✓ To establish the existence of facts relevant to work or official communication.
- ✓ For the purpose of e-Discovery.
- ✓ Demand or request for encryption keys, email account credentials to gain access to an employee Email Account with its associated contents either directly from the employee or through the Email Service Provider for the purpose of an investigation or audit.
- ✓ Email content, attachments, metadata, and other related information stored in Users email accounts.
- ✓ Email logs and system logs to detect any security incidents or unauthorized access to Users email accounts.
- ✓ In a situation of prolong absence of an employee where access is needed to ensure business continuity of work for a particular institution.
- ✓ Email Service Provider may be requested by the Email Auditors where necessary, available, and possible, to install an automated email monitoring tool or system for effective monitoring purpose only.
- ✓ In case of refusal to comply by the User, Email Auditors or the Policy Implementing Entity can order the Email Administrators to reset or change the password of the User where possible or order for the application or usage of legal interception systems where necessary, appropriate, and possible to the E-Mail account of that User.
- ✓ Monitoring & Compliance report shall be constituted after periodic Email Audits and forwarded or shared with; the Email Policy Implementing Entities for enforcement of punitive action.
- ✓ Enforcement actions due from the monitoring & compliance report constituted by Email Auditors shall be shared with the institution of the sanctioned User for record keeping.

The monitoring of Users Email activities shall be done in a manner that respects privacy and data protection laws, and in accordance with the principles of transparency, accountability, and due process.

9. Violations & Consequences

The monitoring and compliance report from Email Auditors or through automated system means or any other evidence-based detection of unacceptable usage of the Government Email Platform, can be used by the Policy Implementing Entity or any other delegated entity acting as an oversight to determine violations and their corresponding consequences.

In the case of violation of the Government Email acceptable & unacceptable usage principles, the following are the range of possible consequences:

- ✓ Suspension, restriction of access and even for the worst case, termination of employment for the case of an individual user.
- ✓ Suspension and restriction of access for a period determined by the Policy Implementing Entity for the case of an Institution.
- ✓ For the case of Non-Official Staff, Interns, Consultants, Contractors, Researchers or Others, may have contracts or privileges terminated or more serious punitive action taken against them.
- ✓ More serious punitive action may be levied against Users or institutions in cases of serious financial, material, or reputational damages.
- ✓ For lesser serious violations, an employee may be warned or given a period to rectify or remedy the violation.
- ✓ Users or Institutions can appeal against any punitive action levied against them, however, an administrative sanction can be lifted for the case of reasonable appeal or maintained otherwise.
- ✓ A liable User or Institution under punitive action with a lesser serious violation, can have their punitive action lifted by an executive directive or through an appeal process administered by the E-Mail Implementing Entity.

The consequences may not be limited to the ones above, rather the ones above are set of possible range of consequence, and it is up to the decision of the Policy Implementing Entity to decide what is the most appropriate measure for any form of violation regarding the acceptable and unacceptable usage of the Government Email Platform and all other principles set forth in this email policy.

10.Review

This policy shall be reviewed and updated every four (4) years, by MOCDE in collaboration with relevant stakeholders, to keep up with the pace of evolution of technology and its underlying usage. Periodic or midterm review may be done annually by MOCDE and/or stakeholders or when need arises. The following table indicates the modification history of the Email Policy:

Version	Document	Date	Changes
1.0	Government Email Policy	2023	First Final Policy Document
-----	--------	2027	First Reviewed & Updated Policy Document