The Republic of The Gambia

Government Email Policy

[2020–2024]

ZERO DRAFT

MINISTRY OF INFORMATION AND COMMUNCATION INFRASTRUCTURE
MOICI | GRTS BUILDING, MDI ROAD, KANIFING

Table of Contents

1. Preamble

Communications 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 communications, from within and/or one end to another. With time though, generations relatively improved, in terms of efficiency in communication compared to their preceding generations. This upgrade can be attributed to constant development and innovations in ICTs especially in terms of infrastructure.

In today's generation, often referred to as the knowledge & information generation or, the generation of ICTs as influenced by the confluence of technologies, systems, platforms, applications, standards, protocols and people working together in a coordinated way to enable communication and sharing of information seamlessly.

Evidence is increasingly pointing to ICTs as the surest means for communication, sharing of information and socio-economic transformation. The adoption, usage and integration of ICTs not only in our daily activities, but most importantly the recognition and priority it has been given by most countries around the world, as a critical driver and partner for accelerated-and-sustained socio-economic growth and development continue to reinforce the need for countries like the Gambia to place ICT on top of the national development discourse.

In addition to the recognition given to ICTs or the recognition it deserves, through investments, R&D and innovation, followed by robust policies, strategies, action plans and regulations formulated, geared towards the enhancement and/or development of the global ICT industries, yielded a dividend of approximately $30 Trillion returns to the global economy in 2019.

The GoTG, as a key player and member of the global societies has also recognized the great potentials and benefits that ICTs can proffer to socio-economic-and-socio-political development and, as a result, invested in ICT infrastructure, access, services, policies, strategies and regulations so as to enhance the development of its ICT sector/industry.

Notably, in terms of ICT infrastructure, GoTG has deployed the ECOWAN & NBN national fiber optic internet backbone and contributed in the deployment of the ACE international fiber optic internet backbone plus formulation of various policies/strategies/legislation such as NICI/ICT4D policy, National Broadband Policy & Strategy, National Cyber Security Policy & Strategy, Data Protection and Privacy Policy & Strategy, e-Government Program and IC Act of 2009.

In the E-Government Program, an E-Government Data Center was deployed, which is hosting electronic government of platforms, systems, applications and services including importantly the Government E-Mail system. This mailing platform is acting as a secure means for day-to-day communications of all Government employees. However, since the inception of the E-Mail system, there has never been a policy guiding its usage. This E-Mail Policy, will spell out the purpose, objective and as well as set the basis and guidelines for the usage of the GOTG official email

2. Introduction

The Internet and Electronic/Digital Communication has virtually transformed all activities of human life in all sectors of life; from the way we do business, have meetings, interact, travel, conduct payments and communicate etc., as such, in the domain of communication, particularly online communication powered by the Internet, it is highly paramount for Government or public institutions to have policies that help employees or staff understand how they should use or not use their available mediums of communication such as an official email system.

At its best, an official email system provides efficiency, effectiveness and productivity in services delivery and also better-informed workforce. On the flip-side, the misuse of such mediums of communication such as an email system, can create; issues that distract from and undermine the mission of an institution, risks of legal liabilities, reputational damages financial loss and security breaches amongst other host of issues.

MOICI, understanding the needs for Internet Infrastructure, internet access and the use of electronic/digital communication for information exchange and service delivery, continue to deploy various ICT infrastructures, applications and e-services on behalf of the GoTG. Such as LAN in all MDAs & Fiber to MDAs for internet connectivity and the E-Government Data Center hosting Web Portals for various MDAs, Government Information Systems and most importantly the Government E-Mail system for information exchange and service delivery.

Since the day it was deployed in 2010, the Government E-Mail system under the custodian of MOICI, has been serving its purpose as a platform for information exchange and service delivery for all employees of MDAs, although some glitches and service interruptions were encountered over the years, the reliability of the official email has significant improved after tireless efforts to remedy the bottlenecks. As such, MOICI deems it necessary to have a policy that would lay the foundation and set forth guidelines for its usage.

Moreover, MOICI recognizes that principles of freedom of speech, data protection & privacy, confidentiality and integrity of information have implications on the use of the Government E-Mail system and has set forth certain pillars or guidelines in this policy that will ensure individuals' fundamental human rights are protect as stipulated in the 1997 constitution.

This E-Mail policy set forth the guidelines for using the Government email services, which is a highly recognizable medium of communication for GoTG, so as to ensure all official communication including information/data exchange between users within Government, inside and/or outside the country are done in an acceptable way informed by this policy.

2.1. Policy Formulation Process & Life Cycle

For every policy formulation process, there are methods or procedures to follow and different policies may have different scope and requirements, but methods or procedures of formulation can sometimes be the same, similar or different. In this policy, the following methods are employed from pre-formulation, during-formulation and post formulation.

Firstly, immediately after the directive for the formulation of this policy was given by MOICI management, a benchmarking approach was devised, which looked into; existing tools or guidelines for email policy formulation, existing email policies in developed/developing countries formulated based on international best practices and existing email policies in the sub-Saharan African region.

The policy benchmarking process looked into the great details of the structure of those existing email policies and their associated content, then come up with a well-organized and standardized table of content of this policy, 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 E-Mail system.

Secondly, since a standard policy formulation process is usually done through a stakeholder consultative process, similarly for this policy, an email policy survey questionnaire was developed, carefully reviewed internally and adopted by MOICI, which was then floated to all relevant MDAs to collect the basic data needed as an input for the basis of the formulation of this policy and collate the collected basic data as an indicators report for this policy.

Accordingly, after collecting the data using the email questionnaire, it was an evident that (X) institutions out of (Y) institutions have their own private email system, in which, in total, they're paying a minimum amount of GMDXXXX annually for operation and maintenance of their private email systems/services, which is very costly and unsustainable.

It was also an evident from the survey that (X%) of MDAs employees are using their private emails for official communications while (Y%) usually perform unacceptable or unprofessional acts on their official email accounts. Notably, (B%) of MDAs staff never use the Government email system, (R%) of institutions use their private email for official communication, (K%) of institutions show interest in using the Government email system and (J%) interchangeably use their private email system and the Government E-Mail system.

Considering the minimum amount of GMDXXX to be saved if all MDAs use the Government E-Mail system and reduction/elimination of risks and unacceptable use of the Government E-Mail system for official communication is a strong indication or justification for the formulation of this policy.

Upon completion of the policy formulation process, this policy; was shared for internal review within MOICI, shared online on the MOICI website for all MDAs to review and send in their comments/suggestions.

After incorporating all the relevant comments/suggestions from MDAs, a validation workshop was organized to validate the policy and the validated policy document was sent to Cabinet for adoption and enforcement.

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

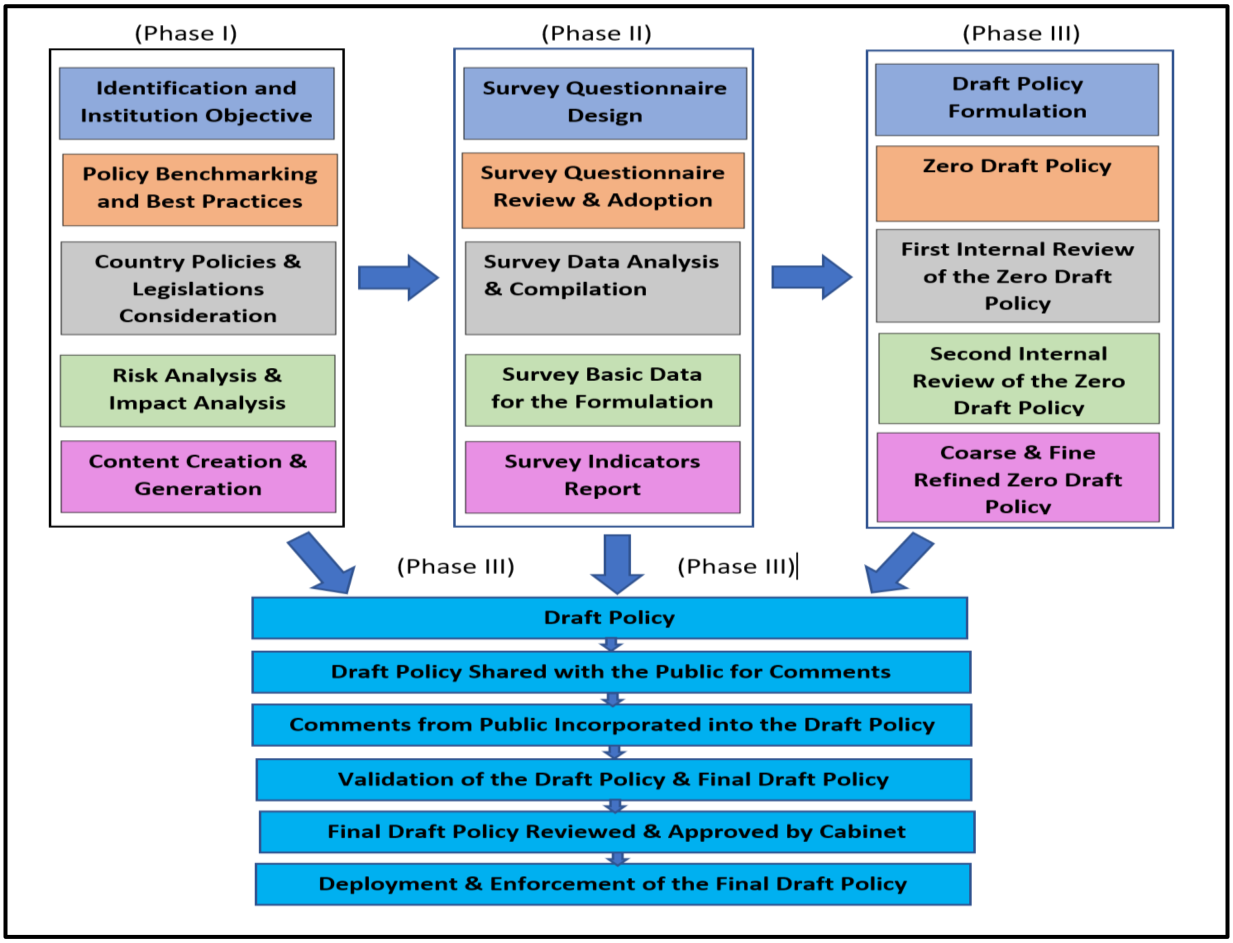
(Phase I)
Identification and Institution Objective
Policy Benchmarking and Best Practices
Country Policies & Legislations Consideration
Risk Analysis & Impact Analysis
Content Creation & Generation
(Phase II)
Survey Questionnaire Design
Survey Questionnaire Review & Adoption
Survey Data Analysis & Compilation
Survey Basic Data for the Formulation
Survey Indicators Report
(Phase III)
Draft Policy Formulation
Zero Draft Policy
First Internal Review of the Zero Draft Policy
Second Internal Review of the Zero Draft Policy
Coarse & Fine Refined Zero Draft Policy
(Phase III)
(Phase III)
Draft Policy
Draft Policy Shared with the Public for Comments
Comments from Public Incorporated into the Draft Policy
Validation of the Draft Policy & Final Draft Policy
Final Draft Policy Reviewed & Approved by Cabinet
Deployment & Enforcement of the Final Draft Policy

Figure (1): Policy Formulation Process

The formulation process of the E-Mail Policy was done based on the above procedures in three (3) different phases. This policy formulation process is based on a standard policy formulation process with a life cycle, in which upon enforcement, the policy life cycle will continue through regular reviews and updates with series of versions.

2.2. Vision & Mission Statement

This Government E-Mail Policy is inspired by and based on the following vision & mission statements:

Vision Statement: A secure, robust, reliable and available E-Mail system for government Service that ensures effective communication for all employees and promotes efficiency in service delivery.

Mission Statement: To provide a platform of E-Mail communication that is highly reliable and scalable to respond to all electronic/digital communication needs of Government and also achieve 100% usage of the Government E-Mail system by the entire Civil Service for all their official communications.

2.3. Purpose

Effective and efficient communication is a desired goal for any company, corporate body, organization, institution or government including the Government of the Gambia. The purpose of this policy is as follows:

I. To create and provide E-Mail Accounts to all eligible employees of Government.
II. To facilitate effective and efficient E-Mail communication in all MDAs.
III. To define rules or procedures on how Government employees should send, receive and manage their official E-Mail Account.
IV. To highly mitigate or where possible totally eliminate the risks associated with the usage of official E-Mail Accounts for official communication.

2.4. Scope

For the purpose of this policy, considering international best practices and standards, there is an extent at which this E-Mail Policy is applicable both at institution and/or users' level and also there're limitation where it does stop. This E-Mail Policy is applicable or covers the following:

I. All employees of the GoTG provided with an E-Mail Account by MOICI under the (. gov.gm) domain.
II. All employees of the GoTG sending, receiving, retaining and processing email messages with associated contents/attachments, through the Government E-Mail system under the (. gov.gm) domain.
III. All interns, consultants and any other third party (being it individual, group, corporate body, organization/institution) created/assigned with an E-Mail Account under the (. gov.gm) domain.
IV. All Government employees managing the Government E-Mail system or those employees entrusted to perform email audit on the (. gov.gm) E-Mail Accounts.

2.5. Objectives

As stated in the Vision & Mission Statement of this policy, on the wishes and aspirations of GoTG through MOICI in enhancing its E-Mail system in terms of security, reliability and availability and ensure its usage by all employees of Government, followed by specified purpose and scope of usage. The following are the main objectives of this E-Mail Policy:

I. To enforce the use of the Government E-Mail system by all government employees for official communication.
II. To ensure that all Government employees from now on and the future will be provided with an E-Mail Account under the (. gov.gm) domain and given access to the Government E-Mail service.
III. To ensure continue access of the Government E-Mail service by all its 'Users' in an effective, efficient and secure manner.
IV. To ensure effective, efficient, reliable, lawful, ethical, sustainable and cost-effective 'E-Mail Communication' within the 'Civil Service'.
V. To ensure all employees of Government using the Government E-Mail system abide by all the rules or guidelines of usage set forth in this policy.
VI. To ensure effective monitoring and compliance on the usage of the Government E-Mail system/services through periodic/random E-Mail Accounts Audits.

2.6. Definitions

This E-Mail Policy intends to follow standard E-Mail Policy principles and for it to be achieved, certain terms and keywords must be clearly defined. The following terms/keywords are deemed as relevant and necessary to be defined:

a) **Email/E-Mail**: Any message either in plain text, html format or image(s), sent or received by electronic means between networked computer users 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 account service provider with a username and password to enable access to email account, to send and receive emails.
c) **Email Account Creation:** Is the process of creating an email account by an email account service provider following a definite set(s) of rules and/or requirements or requirements provided or requested by a user, institution, organization, or corporate body.
d) **Email Account Transfer:** An email account transfer is the process of transferring or moving an entire email account from one domain or sub-domain to another.
e) **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.

f) **External Email Accounts:** These are either private or third party 'Email Accounts' that are integrated with the Government Email system under the (. gov.gm) domain for the purpose of email forwarding for either personal or official communication.

g) **Government E-Mail system**: This refer to as the E-Mail system setup, configured and deployed by GoTG, under the governorship of MOICI providing free email services to Government employees for their official email communication.

h) **(. gov.gm) domain:** This refer 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.

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

j) **Email Attachment:** This's 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.

k) **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.

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

m) **E-Mail Communication:** This refer 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.

n) **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, that must be followed.

o) **Users:** This refers to all users of the Government E-Mail system.

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

q) **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.

r) **Password:** It is a secret word, phrase or string of characters assigned by default by the email account provider or set by the user to gain access to an email account.

s) **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.

t) **E-Mail Account Service Provider:** In this policy, MOICI is always referred to as the E-Mail Account Service Provider, providing/managing the Government E-Mail system.

3. Policy Statement

MOICI on behalf of GoTG encourages and promotes the idea that all Government employees can achieve a recognizable level of productivity and efficiency in service delivery in the public sector, through the use of the available computing and electronic/digital communications facilities it is providing, especially the Government E-Mail system.

This E-Mail Policy has been established to; ascertain that the Government E-Mail system is an appropriate medium for official communication for Government employees, make sure all Government employees use the Government E-Mail system for their official email communication including recordkeeping requirements for email at all times, based on legal and ethical requirements set and detailed in this policy document, and ensure fluid and consistent email communication within Government.

4. Roles and Responsibilities

The following responsibilities are specified for all the entities providing or using the Government E-Mail system/services:

A. Responsibility of Policy Implementing Agency:

MOICI, GICTA, Cabinet or Other (any identified entity) are entrusted with the responsibility of implementing this E-Mail Policy. As such, the following are their 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
- To constitute an E-Mail Audit team within Government or outsource to a third party.
- To monitor compliance and levy sanctions or penalties for violation of usage rules
- To maintain and be updating this policy regularly when needed
- To ensure adequate budget/funds are allocated to the Government E-Mail system.

B. Responsibility of E-Mail Account Service Provider:

MOICI will be responsible for the role of E-Mail Account Service Provider for Government, even in the case that the role of the E-Mail Account Service Provider is outsourced or subcontracted to a third party, the third party shall be acting on behalf of MOICI. The following are the responsibilities of the E-Mail Account Service Provider:

- To identify and delegate trusted team of ICT Officers/Technicians as administrator(s) to manage the Government E-Mail system.
- To make sure the Government E-Mail system is available for use by all MDAs 24/7
- To ensure the Government E-Mail system is highly secure and reliable for use at all times.
- To ensure the privacy and confidentiality of users' email data are safeguarded.
- To give E-Mail Auditors required access needed to access the Government E-Mail system.

- To manage E-Mail Accounts of all ‘Users’ including; responding to E-Mail Accounts request, creating E-Mail Accounts, deactivating E-Mail Accounts, E-Mail Accounts transfers, regular Email Accounts backup and resolving E-Mail Accounts issues.
- To create a unique email address where users can send in their email accounts creation, deactivation, transfers, issues relating to their accounts and password changes requests.
- To report any system failures and malfunctions in relation to the Government E-Mail system/services and incidents including security breach, to management and ensure fixes/solutions to the failures, malfunctions or incidents.
- To conduct trainings were needed to ‘Users’ of the Government E-Mail services for usage or any other relevant purpose upon request by their host institutions.
- To sensitize government employees as well as their institutions on the importance and benefits of using the Government E-Mail system as a medium of official communications.

C. Responsibility of User Institutions:

The following are the responsibilities of the User Institutions:

- To make sure all Government employees ‘Users’ under their Institution are provided with an E-Mail Account under the (. gov.gm) domain.
- To request for a new E-Mail Account under the (. gov.gm) domain, for newly recruited Government employee under their Institution.
- To request for an E-Mail Account transfer, of a Government employee who had been transferred from another Institution to its Institution.
- To provide both internet and/or computer to Government employees under their Institution to be able to access the Government E-Mail service.
- To ensure all Government employees under its Institution only uses the Government E-Mail service for their official communication.
- To make sure all Government employees under its Institution abide by all the rules set forth in this policy.
- To ensure all Government employees under its Institution uses the Government E-Mail service for legal, legitimate and ethical purpose only.
- To report any security breach, hacks or other related incident from any Government employee under its Institution to the E-Mail Account Service Provider.
- To report any unappropriated, illegal, illegitimate and unethical behavior of any Government employee towards the usage of the Government E-Mail service and ensure their sanctions or penalization.
- To notify the E-Mail Account Service provider of email deactivation, when an employee service is terminated or no more active for any other reason.
- To give E-Mail Auditors required access needed, when conducting E-Mail Accounts audit of Government employees under their Institutions/Organizations.

D. Responsibility of Users:

The following are the responsibilities of the Users:

- If not given, the 'User' should request from its Institution to be provided with an E-Mail Account under the (. gov.gm) domain.
- In the case a 'User' is transferred from its previous Institution to a new Institution with an existing E-Mail account under the (. gov.gm) domain, the 'User' should request from its Institution for the transfer of its E-Mail Account.
- If not provided, the User should request from its Institution to be provided with an access to internet and computer, so as to gain access to Government E-Mail service.
- If not done, the User should request from its Institution to deactivate its official E-Mail Account after retirement, resignation and when going for secondment.
- To ensure at all times, safe usage of its E-Mail Account under the (. gov.gm) domain.
- To report any security breach, hacks or other related incident associated with its Government E-Mail Account to its Institution.
- To give E-Mail Auditors the required access needed from them during E-Mail Accounts audit periods.
- To comply with any directive issued by the Authority dealing with investigations, sanctions or penalties due to violation of usage rules or related, of the Government E-Mail service.

5. Service Level Agreement

For both User Institutions and Users to carry out their responsibilities successfully on the usage of the Government E-Mail services, the E-Mail Account Service Provider, in this context, MOICI, shall provide the email services based on an SLA between itself and User Institutions.

This SLA shall be initiated and formulated by MOICI or representative of MOICI, reviewed and accepted by all User Institutions. Upon acceptance of the SLA, MOICI, the E-Mail Account Service Provider or its representative shall sign its part of the SLA and provide a copy of the SLA to all User Institutions for their signature. This SLA shall immediately come to effect once it's signed.

The purpose of the SLA is to make sure that E-Mail Account Service Provider (MOICI), will at all times ensure that email services are functioning normally and smoothly without interruption of services. If this SLA is breached by the E-Mail Service Provider beyond the agreed terms of the SLA, User Institutions shall have the liberty to use their private E-Mail services or allow its Users to use their Private E-Mails for official communication.

6. Policy Pillars

The SLA recommended in this policy will act as a check for the E-Mail Account Service Provider (MOICI), in normal circumstances, to be providing the required email services to all Users in all MDAs. Likewise, this E-Mail Policy is shouldered by twelve (12) standard policy pillars, set as canopy of rules or guidelines for the usage of the Government E-Mail service.

These twelve (12) E-Mail Policy Pillars, were extracted from; benchmarking of international, regional E-Mail policies/ best practices and the responses of the Government E-Mail policy survey questionnaires received from MDAs during the survey exercise, as stated in the policy formulation process section of this document. As it stands, the following are the Pillars of the Government E-Mail policy with its underline principles:

6.1. Eligibility

For eligibility purpose, the Users of the Government E-Mail Policy shall include:

- ✓ All employees of Government working in the Civil and Public Service of the country.
- ✓ All Cabinet Ministers working in Government
- ✓ The Presidency
- ✓ Specific non-employees as deemed necessary and approved by MOICI 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 E-Mail Accounts created under the (. gov.gm) domain. But, the E-Mail Account Service Provider (MOICI), may choose to offer a treatment of urgency to any of the eligible user, either based on their request or MOICI establishing it.

6.2. E-Mail Account Creation

The E-Mail Account Service Provider (MOICI) or its representative, shall create all E-Mall Accounts under the domain of the Government E-Mail system. The following are the E-Mail Account Creation process:

- ✓ E-Mail Accounts shall be created based on request from the User Institutions or initiated by MOICI for the case of Specific Non-employees where necessary.
- ✓ E-Mail Accounts are created and maintained for all eligible Users by MOICI at its Data Center housing its E-Mail system.
- ✓ E-mail address of all newly created E-Mail Accounts shall bear the following format: firstname-initial+middlename-Initial-IfAny+surname@Institution-short-name.gov.gm
- ✓ Default password of all newly created E-Mail Accounts shall be determined by MOICI and at first sign-in, Users shall be notified/advised to change their default passwords.
- ✓ MOICI will create and maintain only one E-Mail Account and E-Mail address per User, but may support additional E-Mail aliases, one forwarding to the other.

6.3. Ownership

Once eligible users are created or assigned with an E-Mail Account, they're privileged at will and given the liberty to user their E-Mail Accounts legally, legitimately and ethically for all their official communication, but the ownership of the E-Mail Account shall remain to be Government property and everything it contains, 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 E-Mail 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 the User Institution.

6.4. Email Specific Procedures

Upon being eligible and creating an E-Mail Account for a User, the User is privileged to send and receive emails related to its official communication.

As a matter of principle, the specified structure of an E-Mail Account and the procedures of sending, receiving, forwarding and checking Emails using the Government E-Mail services, are stated as follows:

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.

- ❖ **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 should be short, clear, precise and informative.

b) Email Signature:

All eligible users with an Email Account using the Government E-Mail services, under the (. gov.gm) domain, shall use Email Signature with the following format while sending 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]*

c) Email Disclaimers:

All institutions likewise their employees using the Government E-Mail system under the (. gov.gm) domain, must manually include the following email disclaimer into the settings of their E-Mail Accounts or reach out to the E-Mail Account 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/forwarding emails with an attachment using the Government E-Mail service, the user should consider the attachment to have the following properties:

- Formats: (.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.

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 solely for official communication
- Email to be send, must possess all the listed email formats in section 6.4 dealing with Email Specific Procedures.
- Email to be send, must be carefully composed, addressed and send only to the intended recipients.
- Email to be send, must be appropriate, legal, legitimate and ethical under the context of this policy.
- Email to be send, if containing attachments, must be in harmony with all the attachment properties listed under the Email Attachments subsection (d) of section 6.4.
- If an Email with sensitive information, has been sent mistakenly to a wrong and unknown recipient, the sender should immediately inform its institution of the incident, but if it has been mistakenly sent to a known recipient, the recipient should be contacted immediately by the User or its Institution, for the email to be deleted immediately.
- Auto send/reply must be configured by the User when going on leave or vacation or being sick, indicating the reason for the auto send/reply.
- Indicate where necessary that the Email you are sending and its associated attachments should be printed and given to the institution’s records office for recordkeeping or archived in case of digital recordkeeping.
- If valid Email sent to recipient(s) bounced back, it should be re-sent for the second time, but if bounced back again, the recipient(s) must be informed.

f) Email Spams:

The Users of the Government E-Mail service and E-Mail Account 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 be immediately be labeled as a spam, marked as junk 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 or deleting them.
- Users may choose to report spam emails to the E-Mail Account Service Provider for them to be filtered.
- In the case that a User mistakenly labelled, marked as junk or deleted a relevant email, when realized, the email should immediately be restored.
- E-Mail Account Service Provider shall provide or implement, where necessary a spam filter on the Government E-Mail system to minimize incoming spams.

- ❖ In the case that a spam filter is implemented by the E-Mail Account Service Provider, it should be ensured that the filter rules are not too high to be filtering relevant emails.
- ❖ In the case that a relevant email has been filtered by the spam filter implemented by the E-Mail Account Service Provider, when realized, 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 email started automatically sending or distributing unwanted email(s) to other Users, the User should immediately alert IT/ICT Officer/Technician at its institution or MOIC for support.

g) Receiving Email:

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

- ❖ When necessary, the User should respond to the received email(s), by relying to all email addresses if more than one or to single email or copy other new email address.
- ❖ If an email is received with attachments, the User should be cautious when opening the attachments and scan them were necessary.
- ❖ Auto reply may be configured by the User in the User E-Mail Account settings where necessary, to convey the arrival of the sender email.
- ❖ Auto reply is encouraged to be configured by the User in the User E-Mail Account settings during leave, sick period or vacations or out of office or during meetings, to inform senders.
- ❖ Print email messages and associated attachments if any and hand them to the institution records office/unit where recordkeeping is needed.
- ❖ Received an Email mistakenly sent to a User email address, the User should inform the sender if known and delete it or immediately delete it if not known.
- ❖ If an Email received on behalf of the institution is mistakenly deleted permanently by the User, the User must notify the institution about it.

h) Forwarding Email:

All Users and/or institutions must consider the following when receiving 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, relevant or intended recipients.
- ❖ Email to be forwarded, must be appropriate, legal, legitimate and ethical under the context of this policy.
- ❖ If Email to be forwarded with associated attachments is suspected to contain virus or malwares or other malicious activities, the User should notify the recipient(s) if known.

- If an Email with sensitive information is mistakenly forward to another known user, the recipient should be alerted to deleted such Email, but in the case that it is forwarded to an unknown user, the institution should be informed.
- Indicate where necessary that the Email you are forwarding and its associated attachments should be printed and given to the institution's records office for recordkeeping or archived in case of digital records keeping.
- If valid Email sent to recipient(s) bounced back, it should be re-sent for the second time, but if bounced back again, the recipient(s) must be informed.

i) Checking Email:

All Users and/or 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/login functions on their accounts when signing-in or login using their person/official computers.
- Users may choose to configure their personal smart phones, tablets and handheld devices for them to be able to access the Government Email system with auto sign-in/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/logout from their Government E-Mail Accounts upon accessing them using a shared or public computer.
- Limit or minimize the number of tries or password/usernames guesses, should in case they forget their passwords/usernames, they should immediately contact IT/ICT Officers/technicians at their Institutions or reach out to MOICI for password reset or username details.

j) Group Mailbox:

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

- All Group Mailbox(es) shall be created, used for purpose of official communication only.
- Any Eligible Government employee with an E-Mail Account can create a Group Mailbox(es) for legitimate purpose, only if the need arises.
- Institutions may or can assign their employees to create a Group Mailbox for any specific legitimate purpose related to the Institution work.
- MOICI, upon request as technical support, from Users or Users Institutions/Organizations, may or can create a Group Mailbox for them.
- For any Group Mailbox created, there must 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.
- If spam/junk email is sent to the Group Mailbox, the administrator(s) should carefully examine it and delete it immediately if confirmed to be a spam/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 an email, for official communication or not has been sent to the Group Mailbox mistakenly, the sender if known, must be inform prior to deleting it or delete immediately otherwise.
- If any of the members of the Group Mailbox mistakenly added email address of another person (third party) and send an email relating to the Group Mailbox to that third party, the third party must be contacted if known to delete that email immediately or report the incident.

k) Mailbox Capacity Limit:

Each eligible User, Institution or Group Mailbox User, using the Government E-Mail system, shall be provided by the E-Mail Account Service Provider (MOICI), with the following Mailbox Capacity Limits by default:

- Capacity Limit for Individual Users Mailbox: **60 Megabyte**
- Capacity Limit for Institution/Organization Mailbox: **70 Megabyte**
- Capacity Limit for Senior Government Official Mailbox: **70 Megabyte**
- Capacity Limit for Group Mailbox: **60 Megabyte**

The above capacity limits may be adjusted by the E-Mail Account Service Provider (MOICI) based on needs, strong justifications and availability of space at the MOICI Data Center. In any case, all users guided by this policy, shall make sure that they judiciously utilize the way they use their E-Mail Accounts when sending, forwarding, receiving and replying emails.

The E-Mail Account Service Provider (MOICI) or its representative, must at all times ensure that there is enough storage capacity for Mailboxes under the Government E-Mail system. 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.

6.5. Email Account Transfer

All eligible Email Accounts holders of the Government E-Mail system, 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 case a User is moved or transferred to a new institution, a new Email Account shall be created for the User, holding the user’s institution subdomain.
- ✓ All the content of the User Previous Email Account, will be migrated to new one, based upon the User request through its institution.
- ✓ Prior to migrating the User Previous Email Account, the User has the right to request from the E-Mail Account Service Provider (MOICI) or its representative through the User institution, for its previous Email Account to be re-directed to the new one, until User Email Account migration fully completed.
- ✓ All Email Specific Procedures in section 6.4 and all others for the purpose of this policy, shall be applicable to the new Email Account of the User.
- ✓ 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.

6.6. Email Account Deactivation

For the same legitimate purpose new Email Accounts are created, applies to deactivating an existing Email Account under the Government E-Mail system. Email Accounts Deactivation follow the following processes:

- ✓ All institution that signs the SLA recommended under this policy, shall inform the E-Mail Account Service Provider of any employee, who resigns, retired, died, on secondment or sacked/fired from job.
- ✓ Email Accounts of any Government employee who resigns, retired, died, on secondment or sacked/fired from job, shall be deactivated either upon request by the User or the User institution, from the Email Account Service Provider and should be restored upon return.
- ✓ Email Account Service Provider will be at will or liberty to deactivate Email Accounts of Government employee who resigns, retired, died, on secondment or sacked/fired from job, if notification is not given for a period of 6 months if known.
- ✓ In case of security threat to the Government E-Mail system, the E-Mail Account 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 it has been fixed.
- ✓ In the case of security threat, subsequent to deactivation, the concerned user or competent institution shall be informed.
- ✓ Before/after deactivating an Email Account, the User might choose to migrate any folder created in the Email Account for personal purpose only, to its Private/External Email Account.

6.7. External Email Accounts

The following procedures shall govern the usage of External Email Accounts that are linked or integrated in one way or the other with the Email Account of a User using the Government Email system under the (. gov.gm) domain:

- ✓ Users of the Government E-Mail system, must create a special folder where all inbound emails from its Private or External Email Account(s) are moved or archived, in the case of email forwarding or re-direction.
- ✓ Inbound emails that are Non-official in nature, forwarded or re-directed from Users Private or External Email Accounts, can be forwarded or send further by Users, to any other email address for purpose of personal use if legal and/or legitimate.
- ✓ Inbound emails that are official in nature, forwarded or re-directed from Users Private or External Email Accounts, can be forwarded or send further by Users, to any other email address for the purpose of official communication only.

6.8. Acceptable & Unacceptable Use

The E-Mail Account Service Provider is the custodian of the Government E-Mail system, that is providing email services to all employees of the GoTG for official communication purpose only. As such, there are acceptable and unacceptable usage of the Government Email system and its associated services, as stated below:

Acceptable Use:

All Government employees (Users), are allowed to use their Government E-Mail Accounts under the (. gov.gm) domain without limitation, but guided by the following acceptable use principles, employees can user their emails to:

- ✓ Send, forward and received emails for official communication.
- ✓ Send or forward emails that are legal, legitimate and ethical in nature to other Users or email addresses for work related purpose.
- ✓ Communicate with partners, businesses and citizens.
- ✓ Dispatch or receive official correspondence or letters on behalf of their institutions.
- ✓ Embed them in websites contact or registration forms or use it as contact info 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 and related corporate events, for work related purpose.
- ✓ Purchase software or other products/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:

Besides the acceptable use, there are also unacceptable use principles or scenarios when utilizing or using the Government Email system. The following are unacceptable to be done by any user when using the Government Email system and its associated services:

- ✓ Send, forward and received emails for Non-official communication purpose.
- ✓ Use private or External Email Accounts for official communication while the SLA is valid.
- ✓ Link or integrate Private/External Email Account without creating a specific folder where personal emails would be moved or archived.
- ✓ 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 6.4 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 or antimalware 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 addresses deliberately.
- ✓ 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.

6.9. Personal Use

The Government E-Mail system is meant for official communication purpose only, although modest personal use of the Email services is allowed. The Users of the Government Email services can user their email addresses to;

- ✓ Send emails to families, friends and businesses, as far as it is in harmony with the acceptable use principles and put in a separate email folder created in the Email Account.
- ✓ Download ebooks, guides and other relevant contents that is legal, safe and appropriate for use for personal purpose.
- ✓ Purchase products and services as far as they are legal, safe and appropriate for use for personal purpose and do not interfere with official communication and work of the user institution.
- ✓ Register for Non-Official or Non-work-related conferences, workshops, symposiums, trainings, trade fairs, career fairs and related corporate events.
- ✓ Register or login to participate to a Non-Official or non-work-related video conference platform for meeting or video conferencing purpose.

6.10. Security, Privacy & Confidentiality

All Users of the Government Email services and as well as the Email Account Service Provider, must consider the issues of Email Security, Data Privacy and Confidentiality when using their Email Accounts or the Government Email System/services and its associated equipment.

Emails Systems or Accounts are the most commonly targeted mediums by hackers through attacks, confidentially breaches, stolen data, viruses and malwares. These issues can damage reputation, credibility and compromise legality and security of equipment. As such, the following are the set guidelines under this policy:

Security:

For the purpose of Email security, the users and administrators of the Government Email system/services must:

- Select strong passwords at least eight (8) character, with the combination of special symbols, capital letters, random characters and numbers, that are not easily guessable.
- Change passwords frequently
- Avoid writing down passwords openly in plaintext 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.
- Scan attachments with an appropriate licensed antivirus or antimalware software before opening 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 at acceptable level to filter email spams only.

Privacy:

The privacy of Users using the Government Email services are as important as the security of Email Accounts of Users and the Government Email system itself. For privacy purposes, the Users of the Government Email services as well as the Administrators, must ensure:

- All official emails should be carefully looked, 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 being used 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 looked at for any reason whatsoever.

Confidentiality:

Emails are not considered confidential in nature 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 the purpose of email confidentiality, Users and Administrators of the Government Email system/services, must ensure:

- Someone on an email is Blind Copied, so that other recipients in the “To’ field and “Cc” filed will not be able to see that the person who was blind copied received the email.
- Confidentiality message is added to the sender Email Signature, for recipients to know the email contains confidential information.
- Send/forward confidential information in a password encrypted attachment, locked PDF file, 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.
- Consultants, contractors and entity or people(s) hired by institution or E-Mail Account Service Provider must conform to this policy security/privacy/confidentiality guideline.

6.11. Retention, Archiving and Deletion

As per the IC Act of 2009 under MOICI, Emails are acceptable means of communication and can be used as an electronic evidence. The Data Protection and Privacy Policy&Strategy/Act, under MOICI, likewise the (National Records Service Act 1999) under NRS all clearly spelt out how electronic records should be processed, retained, archived and deleted or disposed.

This Email Policy complemented by the above existing Acts and Policy, under this section, set forth the following guidelines on Email Retention, Archiving and Deletion when using the Government Email system/services:

Retention:

As specified under section 6.3 of this policy, that all E-Mail Accounts with their associated contents under the Government Email system, are properties of GoTG. For that reason, the following are the guidelines for preserving or retaining Official E-Mail Accounts:

- ✓ All Government employees must ensure that emails with continuing values are preserved or retained at all times.
- ✓ All E-Mail Accounts of Government employees must be kept as evidence and where appropriate captured under the institution records management system(s).
- ✓ Email Account Service Provider (MOICI), must ensure that all Official Email Accounts of Government employee who resigned, retired, died or sacked are retained/preserved for a period of time required by law, before they are archived or migrated for storage for longer term retention/preservation purpose.
- ✓ Retention decisions should take into account; official, operational, business needs, legal and regulatory requirements, accountability and transparency expectations.
- ✓ Official emails relating to complaints, appeals, disputes and grievances should be retained as long as there is a need to preserve an audit trail.
- ✓ Email Accounts of Non-Official staff such as Interns, Consultants, Contractors, Researchers or Others must also be persevered or retained for a period of time required by law.

Archiving:

Hence all Email Accounts of Government employees under the (. gov.gm) domain are properties of GoTG, it is of high importance to retain or preserve the Email Accounts as long as necessary and possible. The following are the guidelines for Archiving Official Email Accounts:

- ✓ For the case of resigned, retired, dead or sacked User, after the Email Account of the User is retained or preserved for a period of one (1) year, the Email Account with all its associated contents must be archived by the Email Account Service Provider.
- ✓ Email Accounts of Government employee shall not be archived while they are still active in service.

- ✓ All archived Email Accounts must be stored properly in either of forms; external hard drives, local data centers with DR sites capable of live replications, Government/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 from one 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 and sacked User into employment service.

Deletion:

Upon retaining, preserving or archiving Email Accounts with their associated contents, there are instances or scenarios were Email Accounts of Users or institutions under the (. gov.gm) domain, can be deleted or not deleted. The following are the guidelines for deletion of Official Email Accounts:

- ✓ 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 record and have their Email Accounts archived for a period of five (5) years, the Email Account Service Provider upon consultation with the Authority, may choose to delete their Email Accounts.
- ✓ Users may immediately choose to delete all emails both (person and official) with no continuing value from their Email Accounts.
- ✓ 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, 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 its contents are not yet migrated to the new Email Account.
- ✓ In the case where the SLA recommend by 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 shall never be deleted under any circumstance.
- ✓ Group Mailbox(es) created and being used for illegal, illegitimate and unethical use shall be deleted by the Email Account 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.

6.12. Exceptions

All the guidelines and principles set forth here in this policy, must definitely be observed, adhered to and/or respected or the User or User Institution will face sanctions/penalties, but in every rule, there are exception sometimes. 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.
- ✓ 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, the Email Account Service Provider or the User host institution shall not be held responsible.
- ✓ In the case of extremely urgent and justifiable situations triggered by extremely rare emergency cases, the User might choose to use their External/Private Emails for Official Communication.
- ✓ In the case of extremely urgent and justifiable situations triggered by extremely rare emergency cases, the User might choose to ignore some parts of the Email Specific Procedures in section 6.4 under this policy.
- ✓ In the case of extremely urgent and justifiable situations triggered by extremely rare emergency cases, Users may choose to give their email credentials to other trusted Government employees to login, access and send/forward emails on their behalves.
- ✓ In the case of extremely urgent and justifiable situations triggered by extremely rare emergency cases, Users may choose to send/forward and received emails from a computer or device that is not secure or not in line with privacy/confidentiality principles.
- ✓ Email Account Service Provider may deliberately reset Users Email password, login into Users Email Account or Check contents of Users Email Account as a result of Court directive or Email Auditors, for the purpose of investigation, but should not misuse it.
- ✓ In a justifiable situation, Users Institutions may choose to request for the deactivation of a particular employee Email Account or Non-Official staff, but the request must be sent to MOICI formally before deactivation can take place.
- ✓ The SLA recommended by this policy shall not be applicable during major repair, maintenance, upgrade and migration.
- ✓ Email Account Service provider does not need the consent/permission of the user during Email Account backups, migration where necessary, but when archiving Email Accounts, permission is needed from MOICI management and section 6.10, shall be applicable.
- ✓ Email Auditors has the power under this policy, for the purpose of monitoring and compliance may give a directive for an Email Account of a particular user to be suspended or deactivated.
- ✓ National Security Agencies, Embassies/Related are the only institutions allowed; to have their own Email Servers providing email services to its staff or they may choose to use the Government email system, but in any case, shall be Govern by this Email Policy.

7. Monitoring & Compliance

To ensure the guidelines, particularly those in this policy pillars are followed, adhered and respected by all users of the Government E-Mail system/services, there is need for regular monitoring of email usage and email activities, so as to ensure compliance.

A group of Email Auditors shall be constituted by the Policy Implementing Agency and in some instances the Email Account Service Provider shall be responsible in monitoring all email activities of the Government email system/services so as to ensure compliance and may have access to all information or data held in all Email Accounts under the (. gov.gm) domain and also reserves the right to access the following and under the following circumstances:

- ✓ Any employee Email Account with its associated contents in suspicious situations of unacceptable usage.
- ✓ To check whether a particular User or Institution is complying with this policy.
- ✓ To establish the existence of facts relevant to work or official communication.
- ✓ In an emergency situation.
- ✓ In connection with criminal investigation or court order or legal/statutory requirements.
- ✓ 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 the Email Account Service Provider for the purpose of an investigation.
- ✓ In a situation of prolong absence of an employee where access is needed to ensure business continuity of work for a particular institution.
- ✓ Email Account Service Provider may be requested by the Email Auditors or the Authority where necessary, available and possible, to install an automated email monitoring tool or system for effective monitoring purpose, but must be limited to monitoring purpose only.
- ✓ If the case of refusal to comply by the User, Email Auditors or the Authority can order the application or usage of legal interception systems where necessary, appropriate and possible to email services of that particular User.
- ✓ Monitoring & Compliance report must be constituted after periodic Email Audits and forwarded or shared with; the Email Policy Implementing Agency for sanctions or penalties enforcement purpose and Users institutions for recordkeeping purpose.

8. Violations & Consequences

The monitoring and compliance report and any other evidence-based detection of unacceptable usage of the Government Email system/services by; the Email Account Service Provider, Users or Users Institutions or an automated tool, shall determine violations and their corresponding consequences.

The Policy Implementing Agency shall review the report of the Email Auditors and the ones from the Email Account Service Provider either by itself or automated tools on case-by-case basis. If any Government employee is found liable, the following are but not limited to the list of possible consequences, sanctions or penalties under this policy, that must be enforced against any employee found wanting:

- ✓ Suspension, restriction of access and termination of employment in the worst case for the case of an individual user.
- ✓ Suspension and restriction of access for a period determined by the Policy Implementing Agency for the case of an Institution.
- ✓ Non-Official Staff, Interns, Consultants, Contractors, Researchers or Others, may have contracts or privileges terminated or legal action taken against them.
- ✓ Employee or institution may be taken to court, in cases of serious financial, material or reputational damages with possible heavy fines to be determined by the court.
- ✓ For lesser serious cases, an employee may be given a period of time to remedy the situation.
- ✓ If the employee or institution believes not to be guilty of the violations, the employee or institution will be given a single chance to appeal against the charges with concrete evidences to prove innocent and if found innocent the sanctions will be lifted immediately, otherwise maintained.
- ✓ An employee found guilty with lesser serious case under suspension or restriction can be exonerated by an executive directive in a situation of state or public interest.

9. Review

This policy shall be reviewed and updated every four (4) years, by MOICI in collaboration with GICTA, Cabinet and all other relevant stakeholders, to keep up with the pace of evolution of technology and its underlying policies. Minor review may also be done annually by MOICI internal staff or more frequently if the need arises.

MODIFICATION HISTORY:

Version	Document	Date	Changes
1.0	Government Email Policy	2020	First Final Draft
-----	--------	2024	First Review & Updated Draft
-----	--------	------	----------------------

10. Acronyms

The following are the list of 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
- ***MOICI***: Ministry of Information and Communication Infrastructure
- ***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 Mail Box)
- ***PS***: Permanent Secretary
- ***PSC***: Public Service Commission
- ***GICTA***: Gambia ICT Agency
- ***SLA***: Service Level Agreement
- ***IT***: Information Technology
- ***ebook***: Electronic Book (Electronic Book Format)
- ***SSL***: Secure Socket Layer
- ***PGP***: Pretty Good Privacy
- ***Cc***: Carbon Copy (Email Carbon copy)
- ***PDF***: Portable Document Format
- ***NRS***: National Records Service
- ***DR***: Disaster Recovery (Disaster Recovery Site)

11.Policy Adoption

DECLERATION:

The Cabinet of the Government of The Gambia has thoroughly read, reviewed and understood the provisions of this Policy pertaining to the usage of the Government Email system and its accompanying services.

Concurrently, Cabinet therefore acknowledges and approves its usage by all Government employees. Cabinet also equally recognizes the use of the Government Email system and its accompanying services as an accepted mode of official communication. Thus, all government employees are urged to abide by all the guidelines, procedures and principles set forth is this policy.

Also, for the purpose of enforcement, the Policy Implementation Agency recommended by this policy shall be immediately constituted by MOICI to enforce this policy.

Approved ____ **Date** ________________

Secretary General and Head of the Civil Service

Approved ____ **Date** _______________

Secretary to Cabinet

Approved ____ **Date** _______________

Hon. Minister of Information and Communication Infrastructure

Effective Date: ____