E-Mail Policy

Government of Democratic Socialist Republic of Sri Lanka

Ministry of Technology

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
- ***NICI***: National Information and Communication Infrastructure
- ***ICT4D***: ICT for Development
- ***IC Act***: Information and Communication Act
- ***MoT***: Ministry of Technology
- ***LAN***: Local Area Network
- ***MDAs***: Ministries, Departments and Agencies
- ***E-Mail***: Electronic Mail
- ***Mailbox***: Email Account (Electronic E-Mail Account Mailbox)
- ***PS***: Permanent Secretary
- ***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. Introduction

The Government of Sri Lanka relies on email as a primary communication tool to enhance efficiency and responsiveness with its stakeholders and citizens. The Government E-mail service, hereafter called “GovMail,” is available to state employees and officials to support government operations and provide effective service to the public, other institutions, and relevant stakeholders. Users are responsible for utilizing this service purposefully and in accordance with the code of conduct, as well as legal and ethical standards.

Due to the importance of email for its speed and convenience, it is crucial to minimize risks from both intentional and unintentional misuse. This policy offers guidelines to ensure that GovMail use does not infringe on the rights of government employees and citizens, is not employed for purposes prohibited by government laws, rules, and regulations, and does not legally compromise the Government of the Democratic Socialist Republic of Sri Lanka.

3. Scope

This E-mail policy applies to all government institutions using the GovMail email service under the (gov.lk) domain. This includes all government organizations, such as Ministries, Government Departments, Provincial Councils, District Secretariats, Divisional Secretariats, Local Authorities, Government Corporations, Statutory Bodies, Companies fully owned by the Government, Local Governor Offices, and Embassies and High Commissions of Sri Lanka. All these entities are required to adopt this policy.

Only the email services provided by the Government of Sri Lanka shall be used for official communications by the aforementioned government organizations. Email services from other providers shall not be used for any official communication. This email policy applies to all government institutions using the government email platform under the (gov.lk) domain and is applicable to the following entities:

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 Government of Sri Lanka working outside the country in Embassies, Higher Commissioners and Consulates provided with an Email Account from the government email platform.

IV. All employees of Government of Sri Lanka provided with an Email Account from the government email platform.

V. All employees of Government of Sri Lanka 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, applications, and services

IX. Any committee, working group, technical team, Audit Team or institution established in the future to maintain, manage and audit the government email platform on behalf of the government.

X. All third party individuals, groups, corporate bodies, organizations, or institutions managing the government email platform or providing services to the government email platform.

4. Objective

The overall objective of this Email Policy is to ensure formalized, standardized, effective, efficient, reliable, and secure official electronic communications. The policy also aims to enhance ownership, transparency, and accountability in the management of government or public records, in particular electronics or digital records.

This policy is also to provide a robust framework that articulates standardized and formalized electronic communications guidelines for the government of Sri Lanka. The guidelines spell out the requirements for intra and inter government electronic communications guidelines as well as instructions on the electronic communications with its development partners. The e-mail policy will therefore help ensure the following:

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 institutions to the official email platform by the end of December 2026.

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 email records.

IX. To enhance trust and confidence in government email system and services.

X. To promote transparency and accountability in email communication within Government.

5. Policy Statement

Ministry of Technology on behalf of Government of Sri Lanka 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 when manual correspondence is inconvenient.
- ✓ 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 intra and inter government email communication.

Additionally, this email policy has been established to ensure the following:

1. Users comply with all the usage principles and guidelines set forth in this policy.
2. Email maintenance, management, and usage are monitored to ensure compliance.
3. All institutions or their representatives sign the policy to indicate their agreement to comply with it.
4. All institutions sign a Service Level Agreement (SLA) with the Email Service Provider to ensure quality of service and business continuity.
5. The Email Implementing Entity is responsible for implementing the policy within its areas of responsibility.
6. This policy is approved and supported by the Cabinet.

6. 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:

- **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: [Ex: min.tec@dpt.gov.lk]
- **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.
- **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.
- **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.
- **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.
- **External Email Accounts**: These are either private or third party 'Email Accounts' that are integrated with the Government Email Platform under the (. gov.lk) domain for the purpose of forwarding an official email from a private email account to official to an official email account.
- **Government Email Platform:** This refers to as the Government Email platform and associated services setup, configured and deployed by Government of Sri Lanka, under the management of MoT, providing free email services to Government employees for their official email communication.
- **(. gov.lk) 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.
- **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.
- **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.
- **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.

- **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.
- **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.
- **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.
- **Users:** This refers to all users of the Government Email platform.
- **Civil Service:** This refers to as the distinct body of staff within public sector of the Sri Lanka.
- **Civil Servant:** This refers to as an employee of the public sector in accordance with the Civil Service Law.
- **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.
- **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.
- **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.
- **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.
- **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.
- **Policy Implementing Entity:** Is the Institutions entrusted to implement this policy.
- **User Institution:** Is any Institution using the Government Email Platform.
- **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.
- **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 Sri Lanka 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

7. 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:

Ministry of Technology (MoT) in collaboration with other Government and Private stakeholders 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 everyone using the government email platform under the (. gov.lk) domain.
- ✓ To constitute an Email committee, technical team 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.
- ✓ To educate users about the policy, including security measures, acceptable use guidelines, and data privacy practices.
- ✓ To ensure technical safeguards are in place, such as strong password management systems, spam filters, and potentially Data Loss Prevention (DLP) solutions.

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:

Ministry of Technology (MoT) 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 Ministry of Technology (MoT). 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 including of minimum of 2 DR drills annually.
- ✓ Vulnerability Assessment and Penetration testing (VAPT) should be performed annually.
- ✓ Make sure the Government Email platform is available 24/7 for use by all users under the (.gov.lk) 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.
- ✓ Establish Call Center where users can log queries related to the use of the government email platform including 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 breaches to authorities and ensure timely fixes or solutions 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 encryption and multi-factor authentication, 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 unauthorized 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 including complying with all relevant data protection & privacy regulations.
- ✓ Ensure data sovereignty by maintaining strict control over data in processing, data in transit, and data at rest. This includes complying with Sri Lankan data protection laws, implementing robust encryption for data transfers, and ensuring secure storage with measures to prevent unauthorized access and breaches.

- ✓ 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 communication.
- ✓ 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.lk) domain, which is to:

- ✓ Make sure all Government employees requiring an official email account to perform their duties under its Institution are provided with an Email Account under the (. gov.lk) domain.
- ✓ Identify and trained someone to be responsible for managing the institution info email including receiving, sending, and forwarding emails and as well as 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.lk) 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.

- ✓ Ensure all Government employees under its Institution only use 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 use the Government Email Platform for email communication only.
- ✓ Report any security breach, hack, 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 audit of 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.lk) domain:

- ✓ The 'User' shall request from its Institution to be provided with an Email Account under the (. gov.lk) 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.lk) domain.
- ✓ In the case a 'User' is transferred from its previous Institution to a new Institution with an existing Email account under the (. gov.lk) 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 always ensure safe and secure usage of its Email Account under the (. gov.lk) 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 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 should not share their official email account with any other.
- ✓ The User should enable multi factor authentication for their official email account if they send and receive government sensitive data.
- ✓ The User should refrain from logging into their official email account from untrusted or unverified networks.
- ✓ The user should strictly follow the password guideline.
- ✓ 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 Email Policy.

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

9. E-Mail Account Creation

The Email Service Provider (Ministry of Technology (MoT)) or its representative, shall create all Email Accounts under the (. gov.lk) 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 Ministry of Technology (MoT) for the case of Specific Non-employees where necessary.
- ✓ Email Accounts shall be created, hosted, maintained, and managed for all eligible Users by Ministry of Technology (MoT) 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:

A. E-mail Naming Convention

a. The Official Organisation E-mail domain shall be @<Agency Abbreviation>.gov.lk

   i. Examples of Government Organisation E-Mail Domains:

Government Organisation	E-Mail Domain
Ministry of Education	@*edu*.gov.lk
Department of Postal	@*postal*.gov.lk
Ceylon Electricity Board	@*ceb*.gov.lk

b. The naming convention for the Office and Employee Account shall observe the following rules:

   i. The general syntax for Division or non-personnel (to include distribution lists and shared mailboxes) e-mail accounts shall include the name of the division / section / unit / project of the Organisation followed by the domain @< Organisation Abbreviation>.gov.lk

Example:

Component or Division	E-Mail Address Name
Records	records@*<Organisation Abbreviation>*.gov.lk
HR	hr@*< Organisation Abbreviation>*.gov.lk
Support	support@*< Organisation Abbreviation>*.gov.lk

   ii. E-Mail accounts shall follow the following guidelines:

      i. The general syntax for all Employee E-Mail accounts shall include the employee's first name followed by a period (.) and the last name,

followed by the domain name of the Agency.

Syntax: **firstname.lastname@<Organisation Abbreviation>.gov.lk**

Example:

Employee Name	Employee Email Address
Sampath Ekanayake	sampath.ekanayake@*<Organisation Abbreviation>*.gov.lk

iii. In the event an employee has the same first and last name of an existing account, the new employee account shall follow the following guidelines:

i. The new e-mail account shall include the employee's first name, followed by a period (.), the employee's middle initial, followed by a period (.) and then the last name, followed by the domain name of the Agency.

Syntax: **firstname.middleinitial.lastname@<Organisation Abbreviation>.gov.lk**

Example:

Employee Name	E-Mail Address Name
Sampath Kaushal Ekanayake	sampath.k.ekanayake@*<Organisation Abbreviation>*.gov.lk

- ✓ Default password of all newly created Email Accounts shall be determined by Ministry of Technology (MoT) and at first sign-in, Users shall be notified to change their default passwords.
- ✓ Ministry of Technology (MoT) will create and maintain only one Email Account and Email address per User, however, may support additional Email aliases, one forwarding to the other.
- ✓ Ministry of Technology (MoT) will create and maintain two email addresses for the Email Administrators, one for administrative duties and the other for routine tasks, and will create and maintain an Administrative Account for each IT / ICT Unit of various MDAs for email accounts management under their purview.
- ✓ Ministry of Technology (MoT) will create and maintain service account with a lower-level administrative privileges for testing.

10. 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 Signature:

All eligible users with an Email Account using the Government Email Platform, under the (. gov.lk) 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)]*

B. Email Disclaimers:

All institutions likewise their employees using the Government Email Platform under the (. gov.lk) 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 Sri Lanka, 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……..

C. 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), (.ppt), (.pptx), (.xls), (.xlsx), (.txt), (.avi), (.mp4/mpeg-4), (.mov), (.wmv), (.flv), (. webm), (. kvm) and (.jpg/jpeg/jpe/jfif/png/gif/bmp/tif/tiff/heic).
- Size Limit: Will be determined by the respective email administrator.
- 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 accessed 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).

D. 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 opens a spam email or clicks on a spam link or downloads a spam attachment, as a result, the User's devicestarted 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 Ministry of Technology (MoT) 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.

E. 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.lk) 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 informed 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.

11. Email Account Deactivation

The following procedure 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.
- ✓ 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 resigned, 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.

12. 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:

A. Acceptable Use:

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

- ✓ Send, forward and reply 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 and related 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.

B. 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 reply emails for non-official communication purpose.
- ✓ Use private email accounts 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.
- ✓ 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 sent fraud or forgery related messages 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.
- ✓ 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.
- ✓ Use of official email to 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.
- ✓ 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.

13. 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 Email 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:

A. 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 (12) characters, with the combination of special symbols, 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.
- ✓ 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.
- ✓ Deploy email security authentication methods; Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC).
- ✓ 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.
- ✓ 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 have 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.
- ✓ All sensitive information must be identified and classified according to its level of sensitivity (e.g., public, internal, confidential, restricted). Data classification must be reviewed regularly and updated as necessary.
- ✓ Deploy a Data Loss Prevention (DLP) solution to prevent unauthorized access, transmission, or destruction of sensitive data.

B. 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 the 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 forwarding 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 peaked at for any reason whatsoever.

C. Confidentiality:

Emails are not considered to offer the highest form of confidentiality due to limitations 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 PDF file, word file or any other common filing format and share the passwords or decryption keys or unlock keys 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 these policy confidentiality principles.

D. Archival

- ✓ All public bodies must employ email archiving to maintain a tamper-proof copy of the emails.
- ✓ The email archiving solution must be approved by the Ministry of Technology.
- ✓ Note that this email archive solution is also important in defining email retention policies.
- ✓ Archived emails must be stored in a secure and accessible manner.
- ✓ 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.

E. Data Retention and Disposal

- ✓ Data Retention Period: All email data must be retained for a minimum of seven years to comply with legal and regulatory requirements. After this period, data retention should be reviewed, and only necessary data should be retained longer, subject to specific legal requirements.
- ✓ Data Review and Archiving: Email data older than seven years must be reviewed annually. Relevant data may be archived securely, while non-essential data should be earmarked for disposal following review by authorized personnel.
- ✓ Data Disposal: When email data is no longer needed, it must be disposed of securely and permanently. Disposal methods must ensure that data cannot be reconstructed or retrieved, including using data wiping or physical destruction of storage media.
- ✓ Compliance and Monitoring: Compliance with data retention and disposal policies must be monitored regularly. Audits should be conducted to ensure adherence to the policy, and any breaches or anomalies must be reported and addressed

promptly.

- ✓ User Notification: Users must be informed about the data retention and disposal policies, including their rights and responsibilities regarding email data. Clear guidelines on data handling and storage must be provided to all users.
- ✓ Legal Hold: In the event of litigation or legal investigations, relevant email data must be preserved and exempt from the standard disposal process until the hold is lifted by authorized legal personnel.
- ✓ Data Backup: Regular backups of email data must be conducted to prevent data loss. Backup data should be stored securely and be subject to the same retention and disposal policies as primary data.

14. Policy Compliance

A. Compliance Measure

The Ministry of Technology will verify compliance to this policy through various methods, including but not limited to periodic reviews and site inspections, video monitoring, business tool reports, internal and external audits and inspections, and feedback from any and all other sources.

B. Non-Compliance

Any user found to have violated this policy may have his/her privileges revoked and may be subject to disciplinary and/or legal action. The unauthorized use of any form of hacking programs or tools within the confines of the Government networked device is strictly prohibited. Any violations will be considered a cyber-incident or cyber breach and will be prosecuted to the fullest extent of the laws of the territory of Sri Lanka.

15. Review

This policy shall be reviewed and updated every three (3) years, by Ministry of Technology (MoT) 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 Ministry of Technology (MoT) 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	2024	First Final Policy Document
-----	--------	2027	First Reviewed & Updated Policy Document