E-mail Policy
# of the
Government of Sri Lanka

ICTA
ideas actioned
Information and Communication Technology Agency

Information and Communication Technology Agency of Sri Lanka

Version History

Version	Date	Comment
1.0	05.04.2024	Review of the Initial Draft

List of Acronyms

E-mail	Electronic Mail
GoSL	Government of Sri Lanka
MFA	Multi Factor Authentication
SLAs	Service Level Agreements

Table of Contents

1 Introduction

1.1 Vision

Strengthening secure and efficient communication for GoSL officers through effective use of e-mail facility.

1.2 Background

a. The Government of Sri Lanka recognizes Electronic Mail (e-mail) as the prime official communication[1] channel for both internal[2] and external[3] communication.

b. This policy outlines the framework and acts as the basis for the use of e-mail service within public service.

c. All government officials are encouraged to comply with the policy ensuring effective, efficient, and productive use of e-mail communication.

1.3 Purpose and Scope

a. The document outlines the policy framework for the governance, usage and adoption of the e-mail facility for the Government organizations in Sri Lanka.

b. Upon implementation, this policy supersedes all other guidelines and directives, if any, followed by the Government organizations/officers pertaining to the usage of an e-mail facility.

c. This policy is subject to updates and revisions as necessary, by the Implementing Agency, on a periodic basis to ensure its applicability and relevance.

1.4 Recognition and Applicability

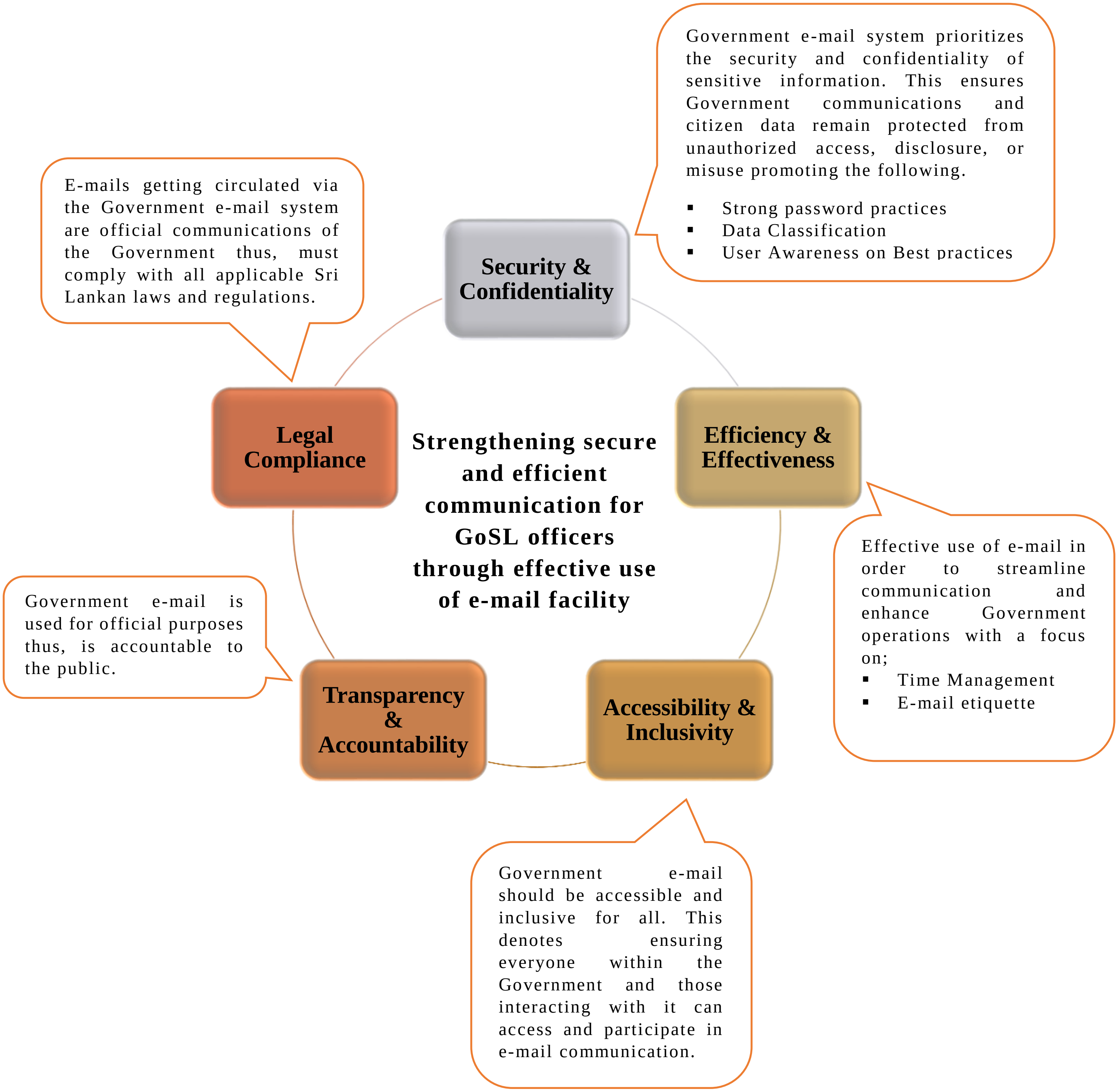
a. The policy applies to all Government organizations and officers as defined in the applicable legislation to Government service.

[1] Communication denotes data owned by the Government of Sri Lanka that gets exchanged via e-mail transactions between domicile and non-domicile users who access the Government e-mail service.

[2] Communication between different departments of a Government organization and different Government organizations.

[3] Communication with citizens and businesses

2 Policy Principles


Security & Confidentiality
Legal Compliance
Efficiency & Effectiveness
Transparency & Accountability
Accessibility & Inclusivity

Strengthening secure and efficient communication for GoSL officers through effective use of e-mail facility

Government e-mail system prioritizes the security and confidentiality of sensitive information. This ensures Government communications and citizen data remain protected from unauthorized access, disclosure, or misuse promoting the following.

- Strong password practices
- Data Classification
- User Awareness on Best practices

E-mails getting circulated via the Government e-mail system are official communications of the Government thus, must comply with all applicable Sri Lankan laws and regulations.

Effective use of e-mail in order to streamline communication and enhance Government operations with a focus on;

- Time Management
- E-mail etiquette

Government e-mail is used for official purposes thus, is accountable to the public.

Government e-mail should be accessible and inclusive for all. This denotes ensuring everyone within the Government and those interacting with it can access and participate in e-mail communication.

Figure 1 : Policy Principles

3 Policy Objectives

The following are the key objectives for implementing an e-mail policy for the Government of Sri Lanka.

3.1 **Enhance Secure Communication:** Establishing safeguards to protect sensitive Government information and citizen data[4]. It would outline practices like strong password requirements, encryption protocols for specific e-mail content, and limitations on what types of data can be sent via e-mail.

3.2 **Optimize Efficiency and Workflow:** Effective use of e-mail to streamline communication and improve Government services and operations. This objective also attempts to promote a professional and respectful e-mail communication, emphasizing proper e-mail etiquette, discouraging inflammatory language, and ensuring a clear distinction between personal and government e-mail usage.

3.3 **Ensure Accessibility and Inclusivity:** Making Government e-mail communication accessible to everyone within the Government and those interacting with the Government. In achieving the objective, special focus needs to be paid on trilingual e-mail access and availability, considering accessibility features for users with disabilities, and providing alternative communication channels for those without e-mail access.

3.4 **Promote Transparency and Public Trust:** Ensure that the e-mail service used by the Government is reliable and promotes public trust. It upholds guidelines for recordkeeping of e-mail communication, procedures for handling public information requests submitted via e-mail, and protocols for using e-mail for public announcements.

3.5 **Ensure Compliance with the Legal Domain:** The policy prioritizes ensuring all electronic communications adhere to the legal landscape of the country. This denotes that all e-mail communications must comply with data privacy regulations, intellectual property laws, and any other relevant legislation, in order to safeguard sensitive Government information, protect Government copyrights and licenses, and ensures all e-mail communications take place within the boundaries of Sri Lankan law.

[4] This objective adheres the policy guidelines on data classification recognized by the Cloud Policy for the Government of Sri Lanka

4 Policy Statements

4.1 Governance

Policy Principle 1 – Security and Confidentiality

Objective 1 – Enhance Secure Communication

Policy Statement 1.1

The users of the Government e-mail facility are required to create a strong password for e-mail access in alignment of the following.

- *The minimum password length should be 8 characters, with at least one uppercase letter (A-Z), lowercase letter (a-z), a digit (0-9), and a special character (e.g. !@#$%^&*).*
- *Auto-saving of the password shall not be permitted.*

Policy Statement 1.2

Industry standards on encryption protocols, for both data at rest and in transit, to be adhered in order to guarantee that sensitive Government information remains secure during transmission and storage.

Policy Statement 1.3

Government organizations are responsible for classifying the data owned by them based on the Sri Lanka Government Information Classification Framework (SLGICF) and implementing necessary access controls will be implemented to restrict access to sensitive e-mails only to authorized personnel with a legitimate need to know.

Policy Statement 1.4

Enforce a comprehensive security incident management plan to ensure prompt detection, control, and recovery in case of data/system breaches.

Policy Statement 1.5

All Government officials should refrain from sharing the e-mail password or any information in an official e-mail with anyone.

Policy Principle 2 – Legal Compliance

Objective 2 – Ensure Compliance with Legal Domain

Policy Statement 2.1

Materials and resources accessible through the Government e-mail facility are subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets, or other proprietary information. Users shall not use the e-mail facility in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

Policy Statement 2.2

All e-mails circulated via Government e-mail facility should be archived in accordance to the prescribed archival timelines by law, following a transparent record keeping mechanism, ensuring that archived information is securely stored and easily accessible.

Policy Statement 2.3

All communications via the Government e-mail facility shall be the property of the Sri Lanka Government.

4.2 Usage

Policy Principle 3 – Efficiency and Effectiveness

Objective 3 – Optimize Efficiency and Workflow

Policy Statement 3.1

All Government employees are expected to respond to the e-mails received within a reasonable timeframe, as determined by the urgency and importance of the communication.

Policy Statement 3.2

All e-mail communications through the Government e-mail facility, should be supported by a clear and concise subject line, accurately summarizing the content of the message.

Policy Statement 3.3

E-mail communication should contain plain language, in order to ensure clear and concise messages that are readily understandable by a wider audience with varying levels of literacy.

Policy Principle 4 – Transparency and Accountability

Objective 4 – Promote Transparency and Public Trust

Policy Statement 4.1

Government officials must clearly disclose the official capacity in e-mail communication. This includes providing the designation, organization, contact information to ensure accountability and facilitate the recipient to verify the authenticity of the communication.

Policy Statement 4.2

Government officials are discouraged from using personal e-mail accounts for official communication purposes.

Policy Statement 4.3

Audit logs to be enabled to track e-mail activity, including sending, receiving, forwarding, and deletion. These logs will be maintained for a defined period to ensure accountability and facilitate investigations in case of suspected misuse.

Policy Statement 4.4

Introduce a clear mechanism for reporting suspected e-mail policy violations.

4.3 Adoption

Policy Principle 5 – Accessibility and Inclusivity

Objective 5 – Ensure Accessibility and Inclusivity

Policy Statement 5.1

The design of the e-mail solution i.e. interface and features should ensure accessibility and inclusivity.

Policy Statement 5.2

Implementing agency to offer support for all three official languages in the country, to ensure that everybody, including the citizens, can effectively use the e-mail facility regardless of their language proficiency.

Policy Statement 5.3

The implementation agency should ensure a feedback mechanism is available for users to report accessibility issues or provide suggestions for improvement.

Policy Statement 5.4

Raise awareness among Government officers and citizens about the importance of using the Government e-mail facility, focusing on awareness campaigns, workshops, and educational material highlighting the benefits of an accessible and inclusive e-mail solution for all users.

5 Responsibilities and Authority

5.1 Responsibilities of Government Organizations

a. Disseminate the e-mail policy among the staff and facilitate the effective, efficient, and ethical usage of Government e-mail facility[5]. The policy document must be shared with all new recruits as a part of the orientation program.

b. All Government user organizations must ensure that they are compliant to the e-mail policy and remove all possible impediments to its successful implementation.

c. Publish e-mail contact details of the staff on their official websites, enabling citizens to engage in user-friendly communication to obtain government services.

d. Appoint one or more administration officers for the management of the e-mail solution from the organization's end[6].

e. Ensure that the end devices are equipped with a licensed Operating System with a next-generation security solution approved by the Implementation Agency.

f. Define and share the format of the organizational e-mail signatures for the staff.

g. Provide necessary assistance to the implementation agency to create awareness among the users and train them in making the delivery a success.

h. Maintain a procedure to pre-identify the user movements including transfers, promotions, retirements, and resignations with an adequate time period to off-board the user and close (discontinue) the e-mail account properly[7].

[5] Once the e-mail facility is technically made available by the implementation agency, all Government organizations must commence using it within a reasonable pre-agreed period, between the implementation agency and organization, from the launch. They must ensure that no other alternative e-mail facility is used for official communication.

[6] These officers are called 'e-mail administrators' in this policy.

[7] Once a user movement is identified, it is the responsibility of the e-mail administrators to close the account upon taking the back-ups.

i. Define proper procedures to take action against staff who breach standard e-mail usage practices specified in this document. Implementation Agency will assist the government client organizations in this process by providing guidance and evidence to such breaches.

5.2 Responsibilities of the Users

a. Ensure that the Government e-mail facility is used only for official communication purposes[8].

b. Refrain from re-directing official e-mails to any other e-mail service provider[9]. Such re-direction will be treated as a breach of security.

c. Refrain from deleting highly sensitive official e-mails received to his/her account. If such deletion takes place, it is treated as a breach of security.

d. The official e-mail address should not be used to register for any unauthorized online services[10].

e. Users, who take their laptops/mobile devices outside office premises, must ensure that the e-mail facility is not accessible by a third party. A user will be held responsible for all the activities that happens, within or outside the office premises, via the client assigned to him/her.

f. Refrain from logging-in to the e-mail system from untrusted or unverified wireless or wired networks (such as public internet kiosks).

g. If a device, used to access the e-mail facility is lost or stolen, e-mail administrators must be duly notified.

h. If the e-mail account appears to be compromised and/or automatic e-mails are being generated from the e-mail address, e-mail administrators must be immediately notified to take appropriate remedial action.

i. Strictly follow the password guidelines in creating/maintaining the passwords.

j. Refrain from revealing the password to a third party.

[8] E-mail facility is provided as a professional resource in fulfilling the official duties.

[9] This implies that users should not provide their official e-mail account details to private e-mail service providers.

[10] Unauthorized online services in this context would encompass any online service which is not related to official work.

k. If advised, make use of 2-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) to further secure the e-mail account.

l. Maintain all e-mails confidential unless there is a genuine need to share the same for information and necessary actions. No e-mail should be shared with a third party who does not have a genuine and official need to possess such information. Any deviation from this will be treated as a breach of security as information security is a shared responsibility.

m. Be careful when using ‘Distribution Lists’ to reduce the risk of sending e-mails to unintended recipients. ‘Distribution Lists’ should be kept up-to-date.

5.3 Responsibilities of the Implementation Agency

a. Serve as a single point of contact for all aspects of the e-mail solution lifecycle. This includes planning, design, and implementation, ensuring a smooth transition to a robust, secure, and user-friendly e-mail system for Government organizations.

b. Maintain an effectual relationship with each Government organization to successfully carry out e-mail infrastructure implementation and obtain its full use.

c. Collaborate with e-mail administrators and users of Government organizations to deliver seamless system support while maintaining robust security measures.

d. Enter into Service Level Agreements (SLAs) with each Government organization, to define clear expectations for service delivery timelines and quality [11].

e. Planning, designing, creating, and maintaining the e-mail infrastructure. All issues related to managing infrastructure are the responsibilities of the implementation agency.

f. Decide the format of the e-mail address, in liaison with the Government organizations, focusing on the maximum attachment(s), size per e-mail, and maximum storage for a user. The implementation agency must;

  - Decide the parameters specified above in consideration of the practical aspects of the system usage. They should not, in any way, prevent a user from effectively and efficiently using the e-mail facility.

[11] SLAs must be first discussed in detail with the Government organizations. A standard SLA format should be developed and offered to all Government organizations that on-boards to the e-mail solution.

- Consider the nature of the operations and requirements of each Government organization in deciding these parameters.

- Incorporate a feedback mechanism to gather feedback on areas for further improvement.

g. Maintaining back-ups of the e-mails.

h. Suspend/deactivate the user account(s), in consultation of the respective Government organization, in case of incidents identified as a 'Breach of Security'.

i. Conducting awareness and training sessions for the users with the support of the Government organizations.