Please do not quote

Draft Ver. 2.9

E-Mail Policy for Government Organizations

(Design, Implementation, Management, Administration, User Training and Usage)

September, 2022

Information and Communication Technology Agency of Sri Lanka

Table of Contents

List of Abbreviations

BCC	Blind Carbon Copy
CC	Carbon Copy
CERC	Contingent Emergency Response Component
E-mail	Electronic Mail
HR	Human Resource
HTML	Hypertext Markup Language
ICTA	Information and Communication Technology Agency
IMAP	Internet Message Access Protocol
MFA	Multi-Factor Authentication
GoSL	Government of Sri Lanka
PC	Personal Computer
SLAs	Service Level Agreements
SMTP	Simple Mail Transfer Protocol
URL	Uniform Resource Locator
2FA	2-Factor

1 Introduction

1.1 Background

Government of Sri Lanka has identified Electronic Mail (E-Mail) as one of the key communication medium not only among intra and inter-departmental messaging but for correspondence with the citizens and businesses as well. All government officers are encouraged to use E-Mails effectively, efficiently and productively in their communication. In that exercise, they are directed to follow the standard guidelines of E-Mail usage. This document act as the basis for the acceptable E-Mail usage within government organizations.

1.2 Need

a) The key requirements of this policy document includes creating the policy platform enabling the users to utilize the E-Mail facility in an efficient, effective, productive, lawful, and ethical manner. It also intends to build the standards for E-Mail use, so that the entire system functions smoothly irrespective of the number of users and complexity of the network.

b) This policy is mandatory for all officers and government institutions that are provided with E-Mail facility[1] by the government. The scope remains dynamic and expands following the spreading of the program.

1.3 Purpose and Context

a) This document outlines the policy framework for the provision and usage of the E-Mail facility for the government organizations in Sri Lanka.

b) Information and Communication Technology Agency (ICTA) is recognized as the Implementation Agency of the project on behalf of the Government of Sri Lanka (GoSL).

c) This document is dynamic. Further changes to the same, as deemed necessary, will be made by the Implementation Agency periodically.

d) Guidelines or instructions on E-Mail usage, previously issued by ICTA, under the e-Government Policy of 2009 will be superseded by this policy.

[1] Initially 100,000 E-Mail accounts would be provided

1.4 Rationale

This policy provides the direction for the establishment of an official communication mechanism for the government organizations which is efficient, secure, systematic, convenient and productive; with a focus on safeguarding the information security, reputational damage of government organizations/officers, and security breaches whilst promoting citizen convenience.

The following definitions have been followed throughout the policy document as the basis of devising the policy.

a) **E-mail**, or in full **Electronic-mail** stands for messages transmitted and received by digital computers through a network. An E-Mail system allows computer users on a network to send text, graphics, sounds, and animated images to other users.[2]

b) E-Mail uses multiple protocols within the TCP/IP suite. For example, SMTP is used to send messages, while the POP or IMAP protocols are used to retrieve messages from a mail server. The original E-Mail standard only supported plain text messages. Eventually, E-Mail evolved to support rich text with custom formatting. Today, E-Mail supports HTML, which allows E-Mails to be formatted the same way as websites. HTML E-Mail messages can include images, links, and CSS layouts. One can also send files or "E-Mail attachments" along with messages.

[2] https://www.britannica.com/technology/e-mail

2 Recognition

a) All government client organizations must recognize E-Mail as one of the key media for communication among both internal and external clients (including citizens and businesses). Given its speed, effectiveness, and convenience; they must further recognize it as the most preferred mode of internal and external communication in most instances.

b) According to the Electronic Transactions Act, No. 19 of 2006, no data message, electronic document, electronic record or other communication shall be denied legal recognition, effect, validity, or enforceability on the ground that it is in electronic form.

c) All government client organizations must recognize the government's E-Mail infrastructure as official. All official E-Mail communication must happen through that. Any similar facilities offered by other E-Mail providers, local or international, should not be used in official communications. Any such possible use will not necessarily have the status to be treated as official communication.

3 Policy Principles, Statements and Goals

When composing an E-Mail message, it is important to use good netiquette. The following sections discuss some key practices which upholds such good netiquette.

a) Users shall include a subject to the E-mail which summarizes the content. The body of the content shall start with the recipient's name and conclude with one’s name or "Signature". A typical signature includes name, E-Mail address, and/or website URL. A professional signature may include the company name and title as well. Most E-Mail programs allow one to save multiple signatures, which one can insert at the bottom of an E-Mail.

b) If one wants to send an E-Mail to multiple recipients, one should add each E-Mail address to the "To" field. However, if the E-Mail is primarily intended for one person, one should place the additional addresses in the "CC" (carbon copy) field. If one is sending an E-Mail to multiple people that don't know each other, it is best to use the "Bcc" (blind carbon copy) field. This hides the E-Mail addresses of each recipient, which helps prevent spam.

c) The following can be treated as inappropriate use of official E-Mail facility which can lead the organization to financial or reputational risk. Users may also get charged for offenses under relevant laws.

    - Creation and exchange of E-Mails that could be seen as harassing, obscene or threatening and/or consists of any sexual content in any form.

    - Exchange of classified information or any other privileged, confidential, or sensitive information with parties not privy to such information.

    - Spamming: Distribution of unsolicited E-Mails to groups of users with or without the intention of promotion. This also includes the creation and exchange of advertisements, solicitations, chain letters, and other unofficial, unsolicited E-Mail.

    - Misrepresentation of the identity of the sender of an E-Mail.

d) Users should at all times comply with the guidelines prescribed in the policy as well as applicable laws in a manner which would not lead to misconduct as specified, but not limited to, below. Identified misconduct would lead to disciplinary actions punishable under relevant laws.

    - Creation and exchange of information in violation of any laws such as;

        - Computer Crime Act No. 24 of 2007 (Computer Crime Act);
        - Electronic Transactions Act No.19 of 2006 (Electronic Transactions Act);

- Right to Information Act No. 12 of 2016 (RTI Act);
- Intellectual Property Act No. 36 of 2003 (Intellectual Property Act)

- Willful transmission of an E-Mail containing a computer virus.

- Use or attempt to use the E-Mail accounts of others without their permission.

- Transmission of E-Mails involving language derogatory to any particular community including but not limited to a religious or ethnic group.

- Sending E-Mails which can be treated as sexual harassment.

e) The E-mail should be supported with an information classification note at the end of it. One such example is as follows;

“This message and any attachment included may contain information that is privileged or otherwise protected from disclosure. The sender of this electronic mail message does not waive any applicable privilege or protection from disclosure.

If you are not the intended recipient or received the message by mistake, you must not copy this message or attachment or disclose the contents in any way. Notify the sender and delete the E-Mail immediately.”

4 Applicability

The policy applies to all government organizations and government officers as defined in the applicable legislation[3] to government service, regardless of time of the day, location and method of access. Upon implementation, it supersedes all other guidelines and directives, if any, followed by the government organizations/officers pertaining to the usage of an E-Mail facility during the course of executing the assigned duties and responsibilities.

[3] One such reference would be the Right to Information Act No. 12 of 2016

5 Eligibility of a User

a) It is the responsibility of each government client organization to decide the officers eligible to use E-Mail facilities, based on the guidelines and discussions with the Implementation Agency, but at their discretion. They must take into account the work functions and responsibilities of a user, position in the organization structure, and ability of the organization to provide the necessary resources before this decision. As a thumb rule, it is advised to provide E-Mail facilities to officers in both executive and non-executive categories. Even non-executive officers can be provided with the facility depending upon the need and the available resources. There is no specific number of E-Mail accounts provided for any organization. As highlighted above, that must be decided purely on the organizational requirements.

b) An officer provided with the E-Mail facility is called “an E-Mail user” in this document.

c) Only government officers in active service will be eligible for an E-Mail account. The E-Mail account gets discontinued, immediately on the effective date, upon cessation of the position either through a transfer, promotion, retirement, or resignation from government service. However, the users can ‘carry forward’ the same E-Mail accounts if the transfer/promotion happens within the same department. E-Mail addresses change with the movement to another department.

d) In special circumstances, allocating E-Mail accounts for those outside, active, and permanent government services is within the discretion of the Implementation Agency.

6 E-Mail Setup

a) Typically an E-Mail user is given one official account, personally to him/her under the official designation/position of the user (called “Positional Account” henceforth) with an alias to his/her name. A user can use either depending on the circumstances.

b) The objectives of creating E-Mail addresses for designation/position is to offer credibility in citizen communication and to maintain continuity in the case of an officer being transferred, promoted, retired, or left the organization.

c) E-Mails to all “Positional Accounts” are redirected to the personal account of the officer who holds the position on any given date. This redirection ends immediately in case of a transfer, promotion, retirement, or leave of the position. In such cases, the E-Mail Administrators must facilitate a new redirection. Such changes should be handled using a change management methodology. E.g., A form submission to track changes

d) At all times a “Positional Account” must be linked to a “Personal Account” ensuring every E-Mail sent will be received and read.

e) “Positional Account E-Mail Addresses” must indicate the position of the user.
E.g. secterary@abc.gov.lk, sas@abc.gov.lk

f) If there are more users under the same designation/position, a numeral after the designation/position will distinguish one from another.

g) “Positional Accounts” must be decided in consultation with the Government Client Organizations. There should also be a standard format for doing this.

h) For Personal Accounts, the following format is used for the creation of E-Mail addresses.

<initials – maximum 3><surname>@<Organization domain name>
E.g. hmpbandara@abc.gov.lk, rtdesilva@abc.gov.lk

i) Only small case Roman letters (26 letters) and Arabic numerals (10 numerals) must be used in E-Mail addresses. No other characters are allowed. Particularly no special characters such as periods and underscores are allowed. E-Mail addresses cannot be created in local languages. (Sinhala and Tamil.) The objective is to maintain standards in the creation of E-Mail addresses.

7 Password Policy

a) The policy recognizes the password related guidelines prescribed in the Information and Cyber Security Policy for government organizations at all times thus, users are expected to comply with the same whilst adhering to this policy.

b) When using passwords for authentication, all users are required to use a unique password. It is essential to create a strong password as per the guidelines discussed below. A strong password will make it difficult, if not improbable, for a bad actor to guess a password through either manual or automated means.

c) The minimum password length should be 8-characters long, with at least one uppercase letter (A-Z), lowercase letter (a-z), a digit (0-9), and a special character (e.g. !@#$%^&*). It is recommended to consider passwords that provide enhanced security.

d) Passwords used must be changed at least every three months. (System settings should be configured to prompt the change of password as specified)

e) Use of previously used passwords is restricted.

f) Passwords must not be based on personal information such as names of family, friends, relations, colleagues, etc. Examples for passwords that must not be used is available at;

https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10k-most-common.txt

8 Security of the E-Mail System

a) Use of a personal Smartphone (or a device such as a Tab) for accessing official E-Mail is allowed with the discretion of the management of each Government Client Organization. However, this facility is provided only to a device with a SIM card registered to the same user name. Such devices and SIM cards will be whitelisted. Using the Government E-Mail facility with a non-whitelisted third party owned device or SIM card is treated as a breach of security.

b) If deemed necessary, Implementation Agency will introduce additional security measures in sending E-Mails categorized classified and sensitive. The client organization and users must strictly follow such guidelines issues when sending E-Mails in that category.

c) All document sharing must be treated according to the updated Information Classification Policy[4] defined by the ICT Agency of Sri Lanka. Anyone who breaches the standard by sharing classified documents with an unauthorized set of users by E-Mail will be subjected to the immediate cancellation of the E-Mail account and other disciplinary procedures decided by the respective client organizations.

d) There should not be any provision to re-direct any E-Mail addressed to a user with a de-activated/deleted account to another E-Mail service provider.

[4] Refer Annexure I – Information Classification Policy

9 Security Incident Management Process

a) A security incident is defined as any adverse event that has an impact on the availability, integrity, confidentiality, and authority of Government data. Security incidents can be due to various factors like malware, phishing, loss of a device, compromise of an E-Mail ID, etc.

b) It shall be within the right of the Implementation Agency to deactivate or remove any feature of the E-Mail service if it is deemed as a threat and can lead to a compromise of the service.

c) Any security incident, noticed or identified by a user must immediately be brought to the notice of the E-Mail administrators who either attend to it on their own or if not, bring that to the notice of the Implementation Agency immediately.

10 Intellectual Property Rights

a) Materials and resources accessible through the official government E-Mail service 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 service in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

b) All E-Mail messages within the Government E-mail systems shall be the property of the Sri Lanka Government.

11 Policy Implementation

11.1 Strategies

It is the responsibility of the implementation agency, government client organizations, E-Mail administrators and users to strictly follow the policies and guidelines in this document. Implementation agency, with the assistance of government client organizations should devise a strategic plan to implement the policies given in this document.

11.2 Responsibilities and Authority

11.2.1 Responsibilities of Implementation Agency

a) Information and Communication Technology Agency, as the Implementation Agency, is responsible for planning, designing, implementing the solution, and finally engaging in a hand-holding period to provide effective, quick, and secure trouble-free E-Mail services for the client government organizations.

b) The Implementation Agency is expected to maintain an effectual relationship with each Government Client Organization to successfully carry out the E-Mail infrastructure implementation and obtain the full use of it.

c) For the implementation and the support phases, Implementation Agency must appoint responsible officers and inform their names, positions, and contact numbers to the government client organizations. A regular follow-up is essential as government officers may face regular transfers etc.

d) The Implementation Agency is also responsible for providing support to the administrators and the users continuously and also responsible for the security of the system.

e) The Implementation Agency should be ready to enter into Service Level Agreements (SLAs) with each Government Client Organization, individually, for speedy and effective support. Service Level Agreements must be first discussed in detail with the Government Client Organizations. A standard SLA format should be developed for this purpose and offered to all client organizations that on-boards the E-Mail service. This will enable standardized and simplified operations management.

f) In other words, the Implementation Agency plans, designs, creates, and maintains the entire E-Mail infrastructure. All issues related to managing infrastructure are the responsibilities of the Implementation Agency. It can be treated, for convenience, as the E-Mail solution provider.

g) If Implementation Agency deviates from the standard procedure of implementation and managing of E-Mail services, depending upon any special requirements of a certain government client (e.g. Maybe some communications need additional security measures) the said organization must fully support the procedure.

h) Implementation Agency will decide, among other things, the format of the E-Mail address (in liaison with the government organizations), maximum attachment(s), size per E-Mail, and maximum storage for a user. Implementation Agency must decide these parameters considering purely the practical aspects of the usage. They should, in any way, not prevent a user from effectively and efficiently using E-Mail facilities. Implementation Agency must consider the nature of the business and requirements of the client organization in deciding these parameters. At the same time, the implementation agency should also incorporate a feedback mechanism to gather feedback on areas for further improvement.

i) Implementation Agency is responsible for taking and maintaining back-ups of the E-Mails, with or without the assistance of the Government Client Organizations. The task can be outsourced or delegated but the prime responsibility and accountability for data storage rest with the Implementation Agency.

j) In case of an incident identified as a “Breach of Security,” the Implementation Agency has the authority to immediately suspend/deactivate the user account(s). Further actions will be taken with the consultation of the respective Government Client Organization.

k) Implementation Agency is responsible for conducting awareness and training sessions for the users with the support of the Government Client Organizations. The types of awareness/training sessions, participants, and intervals at which such sessions are carried out, etc. should be decided at the discretion of the Implementation Agency, upon having consultations with Government Client Organizations.

11.2.2 Responsibilities of Government Client Organizations

a) Government Client Organizations must ensure they follow the E-Mail policy and guidelines, remove all possible impediments to the implementation and operations, encourage and monitor that their staff attend the training sessions for administrators and users, and use E-Mail facility following the given guidelines.

b) Government Client Organizations are responsible for facilitating the effective, efficient, and ethical usage of E-Mail. They should open the facility only to officers relevant, selected at their discretion.

c) It is the responsibility of the Government Client Organizations to productively use GoSL E-Mail facilities for their activities. Advantages of E-Mail over other traditional communication channels, such as speed, effectiveness, low cost, security, etc. must be fully exploited for the benefit of the organization, users, and citizens. Productive use of E-Mail includes but is not limited to effective internal communication, sending invitations for meetings and events, event organization (e.g. workshops) and information sharing, integration with other collaboration tools, and ensuring information security.

d) Government Client Organizations must publish E-Mail contact details of their staff on websites etc., enabling citizens to engage in user-friendly communication with them. (E-mail harvesting tools may use for spam) The contacts made available to citizens could be official E-Mails of government staff or the contact details of a specific service provider for the service provided.

e) Each Government Client Organization must develop a culture to guarantee every E-Mail that it receives must be read and meaningfully responded to within a realistic time period. E-Mail services should be handled with the understanding that it is an easy and effective channel opened for citizens to communicate with government agencies.

f) Each Government Client Organization is expected to maintain an effective relationship with the Implementation Agency to successfully carry out the implementation of the E-Mail facility and obtain its full use.

g) Each Government Client Organization must appoint one or more administration officers for the management of the solution from the client's side. (They are called "E-Mail Administrators" in this document.) The number of administrators and whether they should work full-time or part-time depends on the type of the organization and the complexity of the operation.

h) Government Client Organizations must ensure, whenever necessary, the end devices are equipped with a licensed Operating System with a next-generation security solution approved by the Implementation Agency.

i) Government client organizations must define and share the format of the organizational E-Mail 'signatures' for their staff.

j) Once the E-Mail facility is technically made available by the implementation agency, including the former content migration, all government client organizations must commence using it within a reasonable pre-agreed period, between the implementation agency and client organization, from the launch. They must not use any other E-Mail facility, particularly any public E-Mail facility for official communication.

k) Government Client Organizations must ensure that there will not be any alternative E-Mail facility for its users.

l) Government Client Organizations must provide the necessary assistance to the Implementation Agency to create awareness among the users and train them in making the delivery a success.

m) Each Government Client Organization must have 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 down" (discontinue) the E-Mail accounts properly. Once a user movement is identified, it is the responsibility of the E-Mail Administrators to "close down" the account after taking the back-ups.

n) All Government Client Organizations must take steps to guarantee the confidentiality of the data. The users must be instructed on this. Government client organizations should immediately bring to the notice of the Implementation Agency any possible risks/threats.

o) Government Client Organizations are responsible for the dissemination of the E-Mail policy document among its prospective E-Mail users. The E-Mail Policy document must be shared with all new recruits as a part of the Orientation program.

p) Government Client organizations must have pre-defined procedures to take action against those 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.

11.2.3 Responsibilities of E-Mail Administrators

a) E-Mail Administrators must be appointed by the Government Client Organizations.

b) The E-Mail Administrators must be responsible for the management of the E-Mail systems of their organizations, according to the specified guidelines provided by the implementation agency.

c) E-Mail Administrators must be responsible for the on-boarding and off-boarding of E-Mail users depending upon the HR changes in government client organizations.

d) Each E-Mail Administrator will be given access to a “Delegated Admin Console”, which must be used for the E-Mail account management rights. They will be able to create or “closedown” accounts, onboard or off-board users, and reset passwords under the domain allocated to them, as and when necessary, without routing the request through Implementation Agency.

e) E-Mail Administrators must take the responsibility to have Anti-Virus software installed in user workstations. Also, they should ensure the virus signatures are up-to-date and are the latest available version.

f) E-mail administrators must put in place an incident reporting framework to report misuse of E-Mail systems.

11.2.4 Responsibilities of Users

a) E-Mail facility is provided to users as a professional resource in fulfilling their official duties. Users must ensure the E-Mail facility is used only for official work.

b) Users must be aware of the security classification of information[5], when handling and composing E-Mail messages and should not use the E-Mail system to transmit messages and information that are beyond confidential or secret.

c) Users must not redirect official E-Mails from their official system to any other E-Mail service provider. (This also implies that users should not provide their official E-Mail account details to private E-Mail service providers.) Such redirection will be treated as a breach of security. However, this is not applicable in the case of personal subscriptions.

d) A user must not delete any meaningful official message received to his/her account. If any meaningful official messages are deleted by the users, it is treated as a breach of security.

e) The official E-Mail address should not be used to register for any unauthorized online services. Unauthorized online services in this context would encompass any online service which is not related to the official work of the respective government officer or institution.

f) Users, who take their laptops/mobile devices outside office premises, must ensure that the E-Mail facility is not accessible to any other party (e.g. a family member). A user will be held responsible for any E-Mail related activity that happens within or outside office premises using the client assigned to him/her.

g) Users must not log in to the E-Mail system from untrusted or unverified wireless or wired networks. (E.g. from public internet kiosks).

h) Users must take due care to ensure the physical security of their PCs, mobile phones, tablet PCs, etc. If a device is lost or stolen, E-Mail Administrators must be duly notified.

i) Digital devices (PCs, mobile phones) used by users must not be shared with co-workers or any third parties.

[5] Annexure I – Classification of Information Policy

j) If a user's E-Mail account appears to be compromised and/or automatic E-Mails are being generated from an E-Mail address, E-Mail administrators must be immediately notified to take appropriate remedial action.

k) Users must strictly follow the given Password Policy in creating/maintaining their passwords.

l) It is the responsibility of an E-Mail user not to reveal his/her password to another party. Here the "other party" includes a superior officer, unless special permission via delegation of mailbox/calendar is given. A password should be treated as personal and the user must always be responsible for its use.

m) E-Mail users must not inadvertently reveal E-Mail/password to other parties by having them written in possible open space. A user is expected to memorize the password.

n) Where advised, a user must make use of 2-Factor (2FA) or Multi-Factor Authentication (MFA) to further secure their E-Mail accounts.

o) Users must keep their E-Mails confidential unless there is a genuine need to share them for information and actions. While Implementation Authority takes all possible steps to ensure the confidentiality of data, users are expected to take similar steps from their end. No E-Mail should be shared with a party that does not have a genuine and official need to possess that data. Any deviation from this will be treated as a breach of security as Information security is a shared responsibility.

p) Users must be careful when using 'distribution lists' to reduce the risk of sending E-Mails to unintended recipients. Owners of 'distribution lists' should ensure their lists are kept up to date.

q) Users are responsible and liable for all actions performed by using their user ID(s) and password(s).

r) Users are further responsible and liable for any activity they perform using their E-Mail account user parameters for login on to any other system.

11.3 Monitoring

a) During the implementation and after, the overall monitoring of the E-Mail solution is the responsibility of the Implementation Agency, which must devise the procedures and processes for the same.

b) The Implementation Agency, with the consent of the client organizations, must list the team that has the permission for monitoring the E-Mail system and make it available to the client organizations along with information on the monitoring activities.

c) Notwithstanding any clauses in this document, the disclosure of logs/E-Mails to law enforcement agencies by the Implementation Agency will be done only within the legal framework of Sri Lanka.

d) The Implementation Agency will not entertain any requests from any other organization, apart from what is stated in the above clause 6 (b) and (c) for scrutiny of E-Mails or release of logs.

e) Implementation Agency is responsible for maintaining the content and the logs for twelve years as per the requirements of the Right to Information Act No. 12 of 2016.

f) It is the responsibility of the Implementation Agency to periodically audit the E-Mail systems at Government Client Organizations with the consent and cooperation of the latter. Implementation Agency has the discretion to outsource this task to a party it finds suitable.