DIGITAL DOCUMENT MANAGEMENT POLICY

DRAFT 1.9

ICTA
ideas actioned

INFORMATION AND COMMUNICATION TECHNOLOGY AGENCY OF SRI LANKA

LIST OF ABBREVIATIONS

AWS	Amazon Web Services
BYOD	Buy Your Own Device
CD	Compact Disc
DLP	Data Loss Prevention
DVD	Digital Video Disc/Digital Versatile Disc
ICTA	Information and Communication Technology Agency of Sri Lanka
ISO	International Organization for Standardization
IT	Information Technology
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology (a unit of the U.S. Commerce Department)
PDF	Portable Document Format
USB	Universal Serial Bus

TABLE OF CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

Many government organizations, largely depend on the use of paper as the most preferred medium for documentation purposes. The presence of paper is inevitable in almost every sphere of the government sector and this has automatically generated a 'paper-driven' culture in the public service of the country. This has not only led to a 'paper-filled' environment in government organizations which eventually leads to consequences such as the decaying of important documents, lack of storage space, lack of a mechanism to retrieve important documents in time, and financial loss to create storage space. Simultaneously it creates inefficiencies, inaccuracies, delays, and waste of time which diminishes productivity and efficiency in public service delivery.

On the other hand, as a result of the rapid advancement in technology; citizens and businesses have become more accustomed to the digital means of fulfilling their needs and expectations. They expect the same level of efficiency and delivery from the government as well. The public sector cannot meet the expectations of the citizens while still being paper-dependent.

1.2 NEED

The Government of Sri Lanka, under its National Policy Framework, has recognized the importance of becoming 'digital' in every spectrum to ensure an efficient and productive service delivery. One significant area where government focus is high in terms of ensuring its digital transformation is the document management by the government organizations, taking a shift from the paper-driven culture towards digital documents.

Document management in the government sector reflects the accountability, transparency and adherence to the legislative obligations by the government organizations in delivering their services to the public. It is the source of proof and evidence that bind government organizations towards their prime duty of ensuring citizens' expectations.

It is the responsibility of government organizations as well as officers who create, receive, and maintain public records to ensure their safekeeping and availability; upholding efficiency, productivity, accountability, interoperability, service delivery and more importantly the citizens' expectations.

In order to facilitate this requirement, the need for a proper digital document management system is of utmost importance.

1.3 PURPOSE AND SCOPE

The purpose of the policy is to provide the government organizations with an understanding of how electronic records are created, maintained, disseminated, and destroyed in a manner that achieves efficiency, productivity, transparency, and accountability expected from government organizations.

All government staff is expected to follow the guidelines given in the policy document in their efforts in creating, maintaining, and preserving digital records which carry national and citizen data and information.

These guidelines uphold the recognition of recordkeeping requirements for the management of digital records whilst maintaining the best practice standards to ensure its security.

1.4 RATIONALE

In a national context, documents carry evidence of services provided by government organizations. Documents can be in any form, including digital. Digital documents are records created, communicated, and maintained using computer technology. They may be born digital or converted into digital form from their original format.

Digital documents can be created in many forms such as word-processed documents, spreadsheets, presentations, e-mail, websites, and online transactions. Digital records can be found in many systems throughout an organization, including databases and business information systems, shared folders, hard drives, etc. These records are subject to the same legal weightage as records on paper.

A digital document;

- contains information that is, and continues to be, an accurate reflection of what occurred at a particular time;
- can be placed in context so that the circumstances of its creation and use can be understood together with its content; and
- can be reconstructed electronically when required so that each version is brought together as a whole and presented logically.

The best way to preserve the content, context and structure of digital documents, is to manage the same through a proper digital document management system.

1.5 APPLICATION

The policy applies to all government officers, in active service, creating or handling documents on behalf of the government organizations.

The policy applies to but is not limited to, documents created, generated, sent, communicated, received, or stored by electronic means.

1.6 IMPLEMENTATION, MONITORING, AND EVALUATION

Any policy should be followed comprehensively and effectively by a strategy. The document specifies different strategies to achieve its expected objectives. It is the responsibility and accountability of the relevant stakeholders to initiate the strategies at the ground level. Although the document does not assign time-bound goals associated with responsibilities and accountabilities, it does create the organizational framework to achieve the outcomes.

A detailed Monitoring and Evaluation framework has already been agreed upon with the M&E division of the Information and Communication Technology Agency (ICTA) to evaluate the implementation of the strategies. Accordingly, partial evaluations will happen every year and the first complete evaluation is due in three years. The document is due for changes every year, if necessary, with the agreement of the stakeholders involved.

2 OBJECTIVES

The policy expects to achieve the following objectives.

1. Efficacy and efficiency in government service ensuring that document related activities are carried out within a minimum time frame, providing a faster and satisfied service delivery to the public.
2. Reduce loss and misappropriation of documents guaranteeing faster search, retrieval, and security of documents.

3 DEFINITIONS

3.1 WHAT IS A DOCUMENT?

As per Britannica Dictionary[1], a document denotes;

- An official paper that gives information about something or that is used as proof of something,
- A computer file that contains text that you have written

Computer Document

A file created by a computer application that includes spreadsheets, word processing (text), audio, presentations, video, images, or other kinds of data.

3.2 WHAT IS A RECORD?

As per Britannica Dictionary[2], also describes a record as;

- An official written document that gives proof of something or tells about past events.

The Cambridge Dictionary[3] defines a record as;

- A piece of information or a description of an event that is written on paper or stored on a computer.

3.3 DIFFERENCE BETWEEN A DOCUMENT AND A RECORD

The main distinction between a document and a record is depicted below.

Document	Record
Can be revised and edited	Cannot be revised or edited
Do not act as evidence	Acts as evidence
Usually saved for a short time	Saved for a long time

[1] https://www.britannica.com/dictionary/document
[2] https://www.britannica.com/dictionary/record
[3] https://dictionary.cambridge.org/dictionary/english/record

4 POLICY PRINCIPLES, STATEMENTS AND GOALS

4.1 DOCUMENT MANAGEMENT SYSTEM SOFTWARE

Government organizations must minimize the creation, sharing, and storage of physical documents and move toward an electronic or digital document management mechanism.

Achieving this necessitates:

a. Having a Document Management System (which is essentially an electronic filing cabinet) for every government organization which can use as a foundation for organizing all digital and paper documents.

b. Choosing the right document management system after accurately assessing the need of each government organization. (One of the first choices to make is whether the organization needs an on-premises or cloud-based solution[4]. Each type of system offers almost the same functionality, but there are several key differences in the way maintenance is performed and data is stored[5].)

c. Uploading the soft-converted hard copies of documents directly into the document management system. (Often, document management systems allow users to enter metadata and tags that can be used to organize all stored files. Most document management systems also have a built-in search engine, allowing users to quickly navigate even the most expansive document libraries to access the appropriate file. For storing sensitive information most document management systems have permission settings, ensuring that only the appropriate personnel can access privileged information.)

4.2 LOGICAL AND STANDARDIZED FOLDER STRUCTURE

The document management facility should be adequately flexible to provide an allocated virtual filing space for every division in the organization. A logical and standardized folder structure is essential for this.

Achieving this necessitates:

a. Having a document management software, that allows creating multiple virtual file folders to store documents of different divisions in the organization such as finance, procurement, human resources, IT, Legal and audit, etc.

[4] Refer Annexure 1 – Advantages and disadvantages of On-Premise and Cloud based solutions

[5] Refer Annexure 2 – Essential features of a document management system

b. Having an individual virtual file folder for each division in the organization facilitates a paperless environment throughout the organization and also allows ease of reference by providing access only to the required virtual folder.

c. Naming virtual file folders coherently within an appropriate and meaningful subject area.

d. Developing and introducing a pre-defined naming convention within the organization

e. Avoiding the use of individual names and number sequences in naming virtual file folders.

f. Restricting the folder structure to a maximum of six sub-folder levels.

g. Assigning the access levels depending on the necessity to access the documents contained within the folder.

h. Developing a user access matrix and ensuring compliance to the same.

4.3 DOCUMENT NAMING CONVENTIONS

Government organizations must maintain consistency in naming digital document folders as well as document names. They should avoid naming files in an ad hoc manner, which leads to inefficiencies and delays.

Achieving this necessitates:

a. Having a document management software that provides the facility to include templates for the names of documents that are expected to find in each folder. These are called pre-defined document names. These pre-defined document names create a way to remain consistent in the way that the documents are named as the files are stored away.

b. Having a system that provides the customizability in the pre-defined document names. Suggested pre-defined names should be ideally given with the template structures in the document management software, which can be modified at any time. The pre-defined document names can even include a formula that will provide the current date to be included in the document name.

c. Citing the date at the beginning of the document name, so that all files will be in chronological order when looking in the folders.

4.4 ACCESS AND PERMISSIONS

Government organizations must ensure the confidentiality of documents by taking appropriate measures to minimize potential threats to confidential information from both external and internal sources, such as documents of personal information, financial information, organizational records, etc.

Achieving this necessitates:

a. Setting up role-based security within the document management software in a manner where user groups and individual users are created with pre-defined access rights. It allows system administrators to determine what kind of access each user will have, including what file folders they can access and what type of access they have for documents in them.

    - The system administrator should maintain an updated user access matrix in line with the organizational structure/divisions and related functions.
    - The system administrator role should be clearly defined detailing the permissions associated with the role.

b. Implementing role-based security in the document management software for every layer in the system i.e. virtual file cabinet, drawer, folder, and document. This enables system administrators to grant user access only for the required layer with the required type of access rights.

c. Providing system access subject to the following.

    - Access requests to the system should be supported with a valid justification.
    - Access should not be granted to folders/documents which are not related to the work scope of the requester. In the event, that such access is needed, the same should be supported with an approved justification from the management.

d. Applying the changes made to the documents in the system only upon formal validation and approval from the respective line manager.

e. Ensuring mobile accessibility. This should include permission to view, edit and share files from anywhere.

f. Seeking further advice from Information and Communication Technology Agency (ICTA) if government organizations are unable to provide properly supervised access to digital documents.

4.5 DOCUMENT RETENTION

Government organizations should adhere to the document retention rules and regulations as applicable at the time.

Achieving this necessitates:

a. Ensuring that the following data retention timelines, as specified in Part III Section 7 (3) of the Right to Information Act No.16 of 2016 are adhered to.

   - Data (Documents) in existence on the date of coming into operation of the act, for not less than ten years (10) from the date of enforcement of the act
   - Data (Documents) created after the enforcement of the act, for not less than twelve (12) years from the date on which same is created

b. Having a document management system that supports a document retention module that allows government organizations to set the retention rules/conditions on all documents stored in the system.

c. Having a system that provides a document encryption facility that prevents modification or deletion of documents until the maturity date is reached.

d. Providing the system administrator with the permission to determine what action will be taken on each file at the time of setting up the retention rules/conditions. These options include purging, moving (archiving), and copying the files.

e. Taking regular and comprehensive system backups (at a pre-defined frequency depending on the criticality and timeliness of documents).

f. Providing secure storage facilities for digital devices, including fire and water-resistant housings and appropriate environmental controls.

g. Making high standards of systems security available to prevent digital documents from being unlawfully altered or destroyed and be safe against computer viruses.

h. Classifying digital document/information/records according to information classification policy[6]

[6] Refer Annexure 3 – Information Classification Policy

4.6 DOCUMENT PROTECTION

Government organizations should ensure document protection, upholding the guidelines prescribed by Personal Data Protection Act No. 09 of 2022, specifically in its Part I on Processing of Personal Data (Documents), at all times when information is shared with external parties using reliable mechanisms for data (document) sharing purposes.

Achieving this necessitates:

a. Handling personal documents in compliance with the obligations specified under the Act

b. Using a document management system that supports online client portals for transferring information to clients, vendors, and officers.

c. Allowing the system to transfer files speedily and securely while supporting encryption.

4.7 DOCUMENTS IN TRANSIT

When documents are in transit, Government organizations should ensure that they cannot be accessed, manipulated, and deleted due to the lack of security that is in place on the file structure created.

Achieving this necessitates:

a. Deploying a document management system that provides automatic encryption according to the international standards (ISO/NIST) when the files are stored and being transferred from the computer to the server, where files are being stored.

b. Prohibiting access to the files stored in the system via the operating system folder structure.

c. Having a system backup that offers high security features to ensure information is protected at all times, even if it is stored in a cloud[7].

[7] Government organizations should strictly adhere to the guidelines prescribed in Part III of the Personal Data Protection Act, No. 19 of 2022 when transferring data to a cloud located outside Sri Lanka.

4.8 DIGITAL SIGNATURE AND DIGITAL CERTIFICATES

The Government has recognized the importance of introducing Digital Signatures and Digital Certificates as enablers that elevate its information and service delivery. A Government Organization that intends to introduce a system that recognizes Digital Signatures and Digital Certificates should obtain services from a Certificate Service Provider (CSP).

Achieving this necessitates:

a. Obtaining the services from Lanka Clear (Pvt) Ltd (LCPL), owned by a consortium led by the Central Bank of Sri Lanka (CBSL) and a group of commercial banks, for the use of Digital Signatures and Digital Certificates, as it is the only authorized CSP in Sri Lanka.[8]

4.9 AUDIT TRAIL AND COMPLIANCE

Government organizations should strictly be compliant with record retention rules, which ensures that all actions within the organization's document management system such as viewing documents, editing files, and deleting or purging documents are accurately tracked.

Achieving this necessitates:

a. Having a document management system that facilitates an audit trail to run reports on actions that are taking place within the system.

  - The system should be capable enough to run an audit trail on an individual document or across the entire system.
  - The audit trail should track all activities executed through the system, providing a document filtering facility to search through the records in the audit trail.
  - A file structure that provides consistency and easy reference to files/documents that are necessary to perform audit activities must be maintained.
  - Deletions or modifications of the audit trail should be prohibited.
  - A proper version control must be available for every document available in the system

[8] The standard operation procedure with related to Digital Signatures and Digital Certificates are available at https://www.icta.lk/digital-signature

4.10 MANAGING UNSTRUCTURED DOCUMENTS

Government organizations should have a mechanism to handle documents that have been and remain completely unmanaged such as e-mails, MS Office documents, pictures, etc.

Achieving this necessitates:

a. Having document management software to manage all active working documents that are normally stored in a desktop, laptop, or 'My Documents folder.

b. Ensuring that the organization is working on the current version of the document, not the version that was created years ago.

4.11 ELIMINATING DUAL ENTRY ERRORS

Government organizations should minimize duplication of documents due to the use of a wide variety of different software solutions and avoid inconsistencies in similar information captured by multiple programs.

Achieving this necessitates:

a. Having document management software that provides integration with different software solutions to help eliminate dual entry and errors (can be either an on-premises application or a cloud-based system).

b. Avoiding duplicate copies or wrong/outdated versions.

4.12 DIGITAL DOCUMENTS CLASSIFICATION

Proper document classification is an essential element in ensuring that documents are maintained in a manner that promotes document integrity, document confidentiality, compliance with legal/regulatory principles and requirements and ease of access.

Achieving this necessitates:

a. Ensuring strict adherence to the guidelines prescribed in the Information Classification Policy [9]

[9] Refer Annexure 3 – Information Classification Policy

4.13 SECURITY OF DOCUMENTS

Government organizations should ensure that the documents created and stored in the document management system are secure from unauthorized access, modification and deletion of documents and records.

Achieving this necessitates:

a. Limiting access to the system and the documents only to authorized personnel to protect its integrity and prevent unlawful access, alteration, or destruction of documents.

b. Having periodic attestation of access rights by the heads of departments to ensure proper access control is maintained when employees leave the organization or changes take place in the assigned system role.

c. Establishing network security systems, such as firewalls, to protect against unauthorized access to document management system that is accessible through external connections, such as the internet.

d. Installing appropriate gateway filter software to ensure that filter definitions are regularly updated to protect against spam, computer viruses, etc.

e. Implementing measures to ensure secure transmission of digital records to external parties.

f. Maintaining finalized and approved digital documents in 'Locked' mode to prevent subsequent alterations or accidental destruction.

   - Finalized documents should always be stored in PDF mode.

g. Using digital signatures[10] to authenticate digital documents and provide security and confidence in authorship.

h. Storing important digital documents either offline or on systems without external links.

i. Establishing appropriate system backup procedures and disaster recovery strategies to protect against loss of digital documents.

[10] Government organizations should adhere to the policy directives enshrined in Digital Signature Policy

j. Restricting transferring or copying of digital documents to USB or external drivers.

k. Developing and implementing audit trails to detect;

- Who can access the system and what are the user rights and access permissions assigned to them (as per a defined and approved user access matrix)
- Changes made to the documents such as creation, modification and deletion
- Adherence to prescribed security procedures
- The occurrence of fraud or unauthorized acts

l. Reviewing security practices (at a pre-defined time interval) and examining system log files (if any) to identify potential attempts to breach system security as well as previously undetected breaches.

m. Classifying digital documents according to the information security classification policy for the organization.

n. Having a next-generation endpoint security system with ransomware protection.

o. Implementing Data Loss Prevention (DLP) tools in the endpoint devices, IT networks and other ICT systems which contain sensitive data. The DLP tools should monitor the endpoint devices, networks and ICT systems for possible data loss, alert the users on potentially risky user actions which might result in data loss, and detect and prevent any unauthorized data transfers.

p. Ensuring strict adherence by staff members to security policies of the organization and taking necessary actions, where deviations are observed.

q. Arranging regular training on Information security for the staff members.

r. Formulating a set of guidelines to address the following and ensure the safety of data/information

- Accessing the system and documents via external networks
- Data encryption for transferring purposes
- Employee awareness on handling a situation of suspicion if the user account has been hacked.

s. Implementing a Mobile Device Management (MDM) Solution by the government organizations that provides BYOD[11] (Bring Your Own Device) policy for staff, to ensure the security of the organization's digital documents and restrict offline data downloading and processing.

4.14 DISASTER RECOVERY

Documents on digital storage devices are more prone to damage from disaster (i.e. natural disasters, technological disasters, accidental human errors, etc.) than other document formats hence, necessary proactive measures should be in place to address the unexpected.

Achieving this necessitates:

a. Having a disaster recovery mechanism/plan.

b. Ensuring the availability of regular and comprehensive system backups.

c. Having all digital documents of high importance duplicated and dispersed.

d. Ensuring that the devices facilitating storage are secure from potential natural and environmental hazards

e. Preserving system and application documentation passwords in a secure manner.

f. Maintaining system security at a high level to prevent digital documents from being subject to unlawful access, alteration, virus attacks, etc.

g. Making arrangements for data integrity checking to ensure completeness of saved digital documents.

h. Enabling timely re-establishment of vital computer systems and critical data, along with a disaster recovery plan, disaster recovery exercises and regular recovery tests on back-ups.

i. Formulating a dedicated internal team to provide advice on recommended handling procedures and preservation techniques for damaged digital documents.

[11] Bring Your Own Device (BYOD) Policy facilitates employees in an organization with the option of using a personal machine (i.e. laptop) for official use or purchasing a device and getting its cost reimbursed via the organization.

4.15 AUTHENTICITY OF DIGITAL DOCUMENTS

Digital documents carry evidence of the activities of government organizations. In order to ensure their evidential value and legal admissibility, systems and processes must prevent unauthorized alteration of digital documents and ensure authenticity.

Achieving this necessitates:

a. Ensuring that the document management system is capable of capturing the modifications made to the documents.

b. Ensuring reliability of software applications used by the digital document management system

c. Having a version control for every digital document

d. Restricting access to digital records only to authorized persons or applications

e. Introducing security mechanisms to prevent unauthorized persons or applications from accessing the digital documents

f. Having audit trails to verify that the digital documents have not been accessed inappropriately/illegally or altered without permission.

4.16 DISPOSITION OF DOCUMENTS

All digital documents must be subject to disposition at the end of the defined retention period.

Achieving this necessitates:

a. Destroying all electronic records and documentation as per applicable laws, as well as the prescribed guidelines in the policy.

b. Ensuring that an electronic record scheduled for disposition is disposed of in a manner that guarantees the protection of confidential information.

4.17 SELECTION AND MAINTENANCE OF STORAGE MEDIA

Government organizations should ensure that storage devices and systems for storing digital documents are capable, throughout their lifecycle, to meet the following requirements.

Achieving this necessitates:

a. Allowing easy retrieval on time

b. Retaining the records in an accessible format until the disposition date as per the records retention schedule.

4.18 STORAGE OF DIGITAL RECORDS

Storage of data provides evidential weight to the work carried out by the government organizations thus, secure data and information storage is of prime importance to every government organization.

Achieving this necessitates:

a. Storing digital records/documents either in online, offline, or nearline modes.

- Online

Online records can be contained on any storage device that is available for immediate retrieval and access. Records stored online are active digital records i.e. records that are regularly required for official purposes.

- Offline

Digital records stored offline are not immediately available for use. Offline digital records are contained on a system or storage device that is not directly accessible through the organization's network. Thus, it requires human intervention to make it accessible to users. These records are usually retained on removable digital storage media such as magnetic tape, CD, or DVD and are generally inactive digital records not regularly required for official purposes.

Government organizations must monitor and guard against environmental degradation and changes in technology that may adversely affect the storage media.

- Nearline

Nearline storage of digital records depicts that the records are contained on removable digital storage media but remain relatively accessible through automated systems connected to the network. These digital records are technically considered to be offline.

b. Storing digital records as online records initially and, as the immediate need to refer to them diminishes over time, they can be moved to either nearline or offline storage, depending upon the technology available to the government organization, the ongoing relevance and value of the records and their retention requirements.

c. Deciding the storage type of digital records based on the need, relevancy and age.

d. Storing the following types of digital documents in online mode.

- Digital records of vital significance to a government organization
- Digital records that need to be retained in the organization for a long term
- Digital records of archival value

e. Adhering to the following guidelines, irrespective of the storing method, in selecting a storage device.

- How frequently the digital records be accessed
- The capacity of the storage device to accommodate the size, number, and complexity of digital records planned to be stored
- The reliability and durability of the storage device to meet the required retention periods for the digital records.
- Technical standards associated with the storage device technology. It is recommended to be open-source since proprietary formats are less widespread and thus, hardly be sustained and supported over time.
- Special physical and environmental storage requirements of the storage device
- Cost/benefit impact of the storage device against the needs of the government organization. Costs include migrating records, the storage device and associated hardware, and any training that may be required.

4.19 TRAINING AND AWARENESS

Government organizations should ensure that their staff possesses the right knowledge and skills to handle and maintain digital documents.

Achieving this necessitates:

a. Educating staff attached to all levels on the importance of maintaining digital records and ensuring that they are thorough with handling the same (increase staff awareness).

b. Developing and delivering training by staff with the responsibility of digital recordkeeping to educate other staff on appropriate procedures for creating, managing, and preserving digital records.

c. Designing staff training programs in a manner that covers the following topics, inter alia.

- Document Management Systems – Characteristics and usage
- Importance of the security/protection of records
- Characteristics of digital documents and records
- Digital document/record backup, storage, and archiving
- Responsibility of the officers in maintaining the security of documents
- Best practices for capturing digital documents/records into the system
- Security aspects for digital records

5 DOCUMENT LIFECYCLE

All documents, in any form, are subject to a lifecycle during their useful life and finally get archived for later use or destroyed when no more useful. It is vital to understand the lifecycle and its different stages when creating and handling documents to ensure that they are managed effectively.

Achieving this necessitates:

a. Educating government staff and enhancing awareness on the importance of maintaining a digital document lifecycle[12]

b. Building capacity within each government organization, achieving the continuity of the digital documents

c. Complying with regulatory requirements of retention and maintenance of digital documents

[12] Refer Annexure 4 – Lifecycle of a Document

6 LEGAL ADMISSIBILITY OF DIGITAL DOCUMENTS

Sri Lankan legal framework has recognized the validity and admissibility of electronic documents, promoting their use for official purposes. Electronic Transactions Act, No. 19 of 2006 as amended by the Electronic Transactions (Amendment) Act No. 25 of 2017 are the main legal enactments that provide legal admissibility and recognition to digital records and documents in Sri Lanka. The presidential circulars No. SP/SB/01/13[13] and No. CTF 01/2021[14] have also been issued to further promote and uplift the importance of the usage of electronic records, documents, and communication within the public sector.

The Electronic Transactions Act, No. 19 of 2006 in its Chapter II on Recognition of Data Messages and Other Communications in Electronic Form stipulates as follows.

a. Electronic data messages, electronic documents, electronic record, or other communication shall not be denied their legal recognition, validity, and enforceability.

b. Although certain laws require documents to be in written form, such requirement can be satisfied by electronic documents provided information in such electronic documents can subsequently be referred to.

c. Where certain laws require information to be retained in original form, the same can be satisfied by electronic documents if their integrity is assured and information in electronic documents can subsequently be referred to.

d. Where certain laws make it mandatory to authenticate information communication by affixing a signature, the same can be fulfilled by electronic documents and communication by using an electronic signature for authentication purposes.

e. If any act or enactment requires particular information to be published in the gazette, such requirement can be fulfilled by publishing said information in the electronic gazette.

[13] Refer Annexure 5 – Presidential circular No. SP/SB/01/13

[14] Refer Annexure 6 – Presidential circular No. CTF 01/2021

7 POLICY IMPLEMENTATION

7.1 RESPONSIBILITY OF GOVERNMENT ORGANIZATIONS

It is the responsibility of the government organizations to follow the policy directives and take all efforts to ensure that digital records, data and information are maintained in a manner that upholds their safety and authenticity.

Achieving this necessitates:

a. Managing all digital records for which the organization is responsible, in an integrated manner as per their importance as corporate assets.

b. Creating complete and accurate digital records and capturing them into systems with recordkeeping functionality.

c. Storing digital records in proper conditions to ensure continued and uninterrupted accessibility.

d. Providing security and authentication controls to ensure that digital records are safe from malicious damage and unauthorized altering.

e. Implementing adequate business continuity plans for digital records. Frequent backups (frequency depends on the type and criticality of the information)

f. Maintaining digital records in accessible formats for as long as they are required.

g. Providing access to digital records for permitted employees.

h. Securely destroying digital records as per legal requirements in a manner that they cannot be reconstructed.

i. Transferring digital records of archival value, and information about them, to the National Archives.

j. Managing digital records following recordkeeping requirements

7.2 MONITORING AND EVALUATION

Monitoring and evaluation enable government organizations to analyze the progress of achieving the intended outcomes of having a document management system and determine its efficiency, effectiveness and sustainability.

Achieving this necessitates:

a. Carrying out effective monitoring and evaluation by all government organizations, ensuring the system functionality, data integrity and proper adherence to the policy by its subjects through the rightful implementation of M&E frameworks and indicators.

b. Reviewing the approaches and strategies followed in deploying the document management system in response to the changing circumstances in a manner not to lose the overall direction.

c. Introducing measures to improve and enhance efficiency, productivity, and sustainability in the long run.

ANNEX 1 – ADVANTAGES AND DISADVANTAGES OF ON-PREMISE AND CLOUD-BASED DOCUMENT MANAGEMENT SYSTEMS

The selection of a document management system leads to two options i.e. on-premises system or a cloud-based system. Both options have advantages as well as disadvantages thus, the final decision should be made in consideration of the same to deploy the best for the organization.

On-premises Document Management System

An on-premises document management system denotes a physically available system within the organizational premises. Accordingly, it requires the organization to;

- Be in direct control of the system
- Have its own servers and storage
- Perform the system maintenance activities on their own
- Be responsible for the security of the documents available in the system
- Ensure the availability of a backup process for document retention
- Have a dedicated team/resource pool to monitor and overlook the system functionality

An on-premises system involves both positive and negative features. In terms of the positive aspects, the main benefit is that since the organization is in control of the system, there is very minimal or no dependency (on third parties or the internet) for system functionality.

Similarly, the main negative aspect associated with an on-premises system is the cost, for the initial deployment as well as subsequent system upgrades/updates. At the same time, unless an organization has a backup process in place, the security and retention of the documents are threatened.

Cloud-Based Document Management System

A cloud-based system is provided by a system vendor whose system is hosted in a cloud and system access enabled via the internet. Cloud-based systems incur a monthly or annual fee including maintenance and software update costs.

The main advantage of having a cloud-based system is that there is no upfront cost attached to it. Similarly, there is no need to have an in-house dedicated team to monitor and overlook system functionality. Furthermore, the system can be accessed by the users from anywhere with the support of an internet connection and no backup process is required since documents get automatically saved in the cloud.

In terms of the disadvantages of having a cloud-based system the fact that system functionality solely depends on the system provider takes precedence over the rest. Thus, accessibility, functionality, and security of the system lie with the vendor, and issues from the vendor's end would prevent the users from enjoying these rights. Moreover, issues in the internet connection would also prevent the users from accessing the documents in the system.

ANNEX 2 – ESSENTIAL FEATURES OF A DOCUMENT MANAGEMENT SYSTEM

These are some of the most important document management system features.

a. Document storage

The most basic and critical function of a document management system is the ability to store the documents safely and in an easily searchable manner.

b. Keyword search

A sound document management system contains a broad keyword search option that facilitates easy access to any document based on specific keywords. Some systems include metadata and tags that make recalling a document or group of documents simpler.

c. Permissioned access to certain documents

Having tiered permissions enable access provisioning to specific documents only to permitted employees and prevents others from viewing or editing them.

d. Document access monitoring tools

These tools enable to monitor who is accessing what documents. This is an essential security feature to ensure the confidentiality of the documents.

e. Document edit history and restoration

A document management system should have an edit history and restoration options to view who has edited a given document. Versioning allows to recall older versions of documents that have been revised and to track which changes were made at what time by which users.

f. Auto-delete on outdated documents

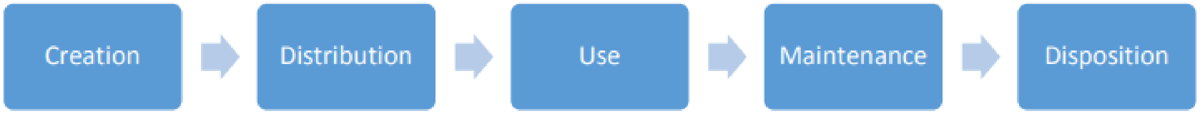
Document management systems come with regulation controls for automatic saves and deletion to free up storage space.

g. Mobile device access

Mobile accessibility of the system is a key feature that enables capabilities including document viewing, editing and sharing.

ANNEX 3 – LIFECYCLE OF A DOCUMENT

The lifecycle of a document would take the following form.



- **CREATION**

a. This is the creation or origination point of the document which can take either manual form or digital form.

b. Documents that carry information on government data should be well designed from the point of creation, using relevant naming conventions and document templates where necessary (incorporating relevant data fields that need to be captured).

c. Government officers must act responsibly, lawfully, and professionally when creating documents relating to government activities in government systems.

d. Created documents should be stored in an allocated location in a manner where their security is ensured.

- **DISTRIBUTION**

a. Upon the completion of drafting, editing, and obtaining signatures the document is ready for circulation and distribution.

b. If the document is published and distributed as an upgrade to a previous version, it should be ensured that the intended updates have been properly incorporated. So that the responsible parties can share the document further, depending on its type and intended purpose.

- **USE**

a. Use takes place after a document has been distributed internally, where it can be used to arrive at decisions, further actions, or serve any other organizational purpose.

b. This phase defines how users access and use a document and its contents.

c. Access can be permanent or temporary. Content can be retrieved repeatedly and read, write and release access can also be stored.

d. Changes to the document can also occur during this phase, subject to the defined security guidelines, access permissions and approvals.

- **MAINTENANCE**

a. The maintenance phase signifies the importance of accurate maintenance of a document in active status, making it available for reference purposes.

- **DISPOSITION**

a. Once a document has aged and lost its usefulness, it leads to disposition or archival.

b. It is the process of removing a document in a way that renders it unreadable (for paper records) or irretrievable (for digital records).

ANNEX 4 – INFORMATION CLASSIFICATION POLICY

1 INTRODUCTION

Information is an essential resource that must be protected throughout its life cycle. However, not all pieces of information an organization holds have the same value and do not require the same level of protection. The categorization of information assets in information security is a process allowing the organization to assess the degree of sensitivity of its information and to determine the level of protection concerning the risks incurred in terms of availability, integrity, and confidentiality.

An organization will thus be able to take into account the degree of sensitivity determined to put in place measures enabling it to comply with its legal obligations, avoid financial losses as well as reputational risks and achieve its objectives with regard to its level of services and to increase the confidence of citizens and businesses in public services.

1.1 IMPACT LEVELS RELATED TO INFORMATION ASSETS OF AN ORGANIZATION

The level of impact reflects the significance of the consequences that a breach in the security of an information asset can have on the organization and its customers or other organizations. These consequences can result in the organization's inability to:

- Fulfill its mission;
- Comply with laws, regulations, and contractual obligations;
- Preserve its brand image and that of the government;
- Maintain or enhance the confidence of customers and partners in the services offered;
- Respect the fundamental rights of individuals to the protection of personal information concerning them and their private life;
- Respect the protection of confidential information shared by the business entities concerning their business presence and competitive advantage;
- Contribute towards the functioning of third-party organizations that depend on its services.

The table below describes the levels of impact that public bodies can adapt to their context.

Impact Level	Description

1	Low (negligible)	▪ Affects a line of business, i.e. a specific service/facility provided, in the organization.
2	Medium (moderate)	▪ Affects several areas of activity of the organization
3	High (severe)	▪ Significantly affects the quality of services essential to the population. ▪ Affects the image of the organization. ▪ Affects the activities of one or more other organizations. ▪ Affects respect for the fundamental rights of individuals to the protection of personal information concerning them and of their privacy, without harming the health, life, or well-being of these individuals. ▪ Affects respect for the confidentiality of the information shared by the business entities to the protection of their business presence and competitive advantage.
4	Very High (very serious)	▪ One or more services essential to the population cannot be provided. ▪ Endanger the health, life, or well-being of persons. ▪ Affects respect for the fundamental rights of individuals to the protection of personal information concerning them and their privacy and, as a result, endangers the health, life, or well-being of these individuals. ▪ Affects the government's branding, with or without publicity.

In addition, the impact levels expressed in terms of availability, integrity, and confidentiality are described in the table below.

Security Criteria	**Impact Levels**

	Level 1 (Low)	**Level 2 (Medium)**	**Level 3 (High)**	Level 4 (Very High)
Availability	The disruption of access to or use of information assets has a negligible impact on the organization.	The disruption of access to or use of the information asset has a moderate impact on the organization.	The disruption of access to or use of information assets has a serious impact on the organization.	The disruption of access to or use of information assets has a very serious impact on the organization.
Integrity	The unauthorized modification or destruction of the information asset has a negligible impact on the organization.	Unauthorized modification or destruction of information assets has a moderate impact on the organization.	Unauthorized modification or destruction of information assets has a serious impact on the organization.	The unauthorized modification or destruction of information assets has a very serious impact on the organization.
Confidentiality	Unauthorized access or disclosure of information assets has a negligible impact on the organization.	Unauthorized access or disclosure of information assets has a moderate impact on the organization.	Unauthorized access or disclosure of information assets has a serious impact on the organization.	The unauthorized access or disclosure of information assets has a very serious impact on the organization.

2 INFORMATION CLASSIFICATION

Information Classification is system encompassing principles, methodology, tools, and framework for designating different categories of Information based on impact and value. There are numerous different definitions of

Information Classification; however, all of these views have the following principles in common.

- It applies to all information assets across the organization (any type or size);
- It provides a basis for data sharing and accessibility policies across the organization;
- It supports Confidentiality, Integrity, and Availability (CIA) principles of Information Security;
- The classification should be done according to sensitivity and value of the information (but not limited to);
- The Framework should be simple to understand and administer;
- The value of information changes with time, regulatory requirements, and changing business environment;
- The classification should not be dependent or open to interpretation by different people; but rather a set of governing rules;
- Such classification needs to be done over the entire lifecycle of information;
- The Information Classification should include extended organization - department, business partners, contractors, other organizations, and citizens;
- Classification is not ownership of a single individual and impacts everyone; and
- The classification rules are dynamic and need a constant upgrade.

2.1 ASSIGNING INFORMATION CLASSIFICATION

Every government client organization is responsible for ensuring that information assets have a classification that is authorized by the information owner and that a custodian who is responsible for implementing and maintaining information assets according to the rules set by the owner has been assigned.

Information assets should be classified by the information owner or delegated at the earliest possible opportunity and as soon as the originator or owner is aware of the sensitivity of the information asset.

In case of information assets that are externally generated, and not otherwise classified, the organizational officer who receives them should ensure that an owner and custodian are assigned and that the asset is incorporated into the organization's information asset registers as appropriate.

2.2 ALTERING INFORMATION CLASSIFICATION

Fundamentally, the security classification of any information may be altered only by the organization which has originally assigned the classification to that information (owner organization).

Security classification thought to be inappropriate should be queried with the organization which has initially assigned the classification or the organization now responsible. If the organization is abolished or merged, the organization assuming the former organization's responsibilities may alter the classification. For information that has been transferred into the custody of the Government Archive of Sri Lanka, it is a good practice if such information is also stored and handled by the security classification assigned to that information.

2.3 DURATION OF THE SECURITY CLASSIFICATION

Duration of security classification means the period up till which the information shall be deemed to be sensitive and should be handled and stored by the security classification assigned.

When an information asset is classified, it may be possible to determine a specific date or event, after which the consequences of compromise might change. An event may trigger an increase in the sensitivity of the information, for example, a human resource form may become 'Confidential' when complete or filled.

The duration of security classification can be specified in the following ways:

- The organization owning the information or assigning the security classification to information may settle a specific date or event for declassification based on an assessment of the duration of the information's sensitivity. On reaching the date or event the information should be automatically declassified;

- Declassification period of information can also be assigned in terms of a set period after the last action on an asset (e.g. six months after last use);

- If the organization assigning the security classification cannot decide a specific date or event for declassification, information should be marked for declassification at a pre-defined period as per applicable Government norms like 10 years from the date of the original classification;

- Organization assigning the security classification may extend the duration of security classification, change the security classification, or reclassify specific information only as per the protocols and guidelines for security classifying information;

- Information may be marked for an indefinite duration of security classification as well, and Cabinet documents are not included in such arrangements

2.4 LEVELS OF SECURITY CLASSIFICATION

Broadly, five levels (four classification levels plus ―Unclassified) of security classification have been defined as

- Unclassified (White)
- Public **(Green)**
- Limited Sharing **(Amber)**
- Confidential **(Red)** and
- Secret **(Scarlet)**

2.4.1 UNCLASSIFIED

All Government information, until such time they are evaluated and classified, must be allocated to the interim classification status ―**Unclassified**. Any unclassified information should be treated similarly or higher to information classified as ―Limited sharing. Prior authorization must be obtained from the information owner to release **unclassified** material to the public (which is in effect changing the classification of the information).

2.4.2 PUBLIC

Any information which is easily available to the public, Government employees, organizations, regulators, project managers, support staff, and contractors including information deemed public by legislation or through a policy of routine disclosure can be classified as **"Public"**. This type of information requires minimal or no protection from disclosure. Examples of public information include:

- Government acts and policies;
- Organization contact persons;
- Information on public services provided to citizens by Government;
- Weather Information; and
- Advertisement for job postings

Note:

While Public information assets have no confidentiality requirements it is still important to ensure their accuracy and completeness (integrity) prior to release. For example, information published on a website must be protected from being tampered with or changed. Information Classification Framework does not discuss controls that ensure the integrity and availability of public information, and steps must be taken by organizations to ensure Public information assets remain available within business needs and are not tampered with.

Some information assets intended for public consumption may have confidentiality requirements before their release (for example, budget papers). In this case, the point at which the information asset will be reclassified to the Public must also be indicated.

Information assets must be specifically classified as public before their release. Public information should at all times be approved as such by the information owner. Where information assets have not yet been classified, they should be treated as unclassified and not as public.

2.4.3 LIMITED SHARING

Information is security classified as **"Limited Sharing"** when compromise of information may lead to minor probability of causing limited damage to the Government of Sri Lanka, commercial entities, or members of the public. Unauthorized disclosure of this information will cause negligible or no damage to internal security, Sri Lankan forces, or Sri Lanka's foreign relations. Examples of Limited sharing information are:

- Organization processes and information;

- Personal information[15] of citizens;
- Confidential information of business entities;
- Minutes of meetings and file notes of Organizations;
- Government evaluation of a company's products; and
- Inventory data.

2.4.4 CONFIDENTIAL

Information is classified as **"Confidential"** when compromise of information may lead to a high probability of causing damage to national security, internal stability, national infrastructure, forces, commercial entities, or members of the public.

In the case of material marked 'CONFIDENTIAL,' the information asset is subject to disclosure which may be limited or prohibited.

Examples of Confidential information are:

- Personal case files such as benefits, program files, or personnel files;
- Tax returns or financial health of the organization;
- Sharing of personal health information of individual;
- Trade secrets; and
- Salary information

2.4.5 SECRET

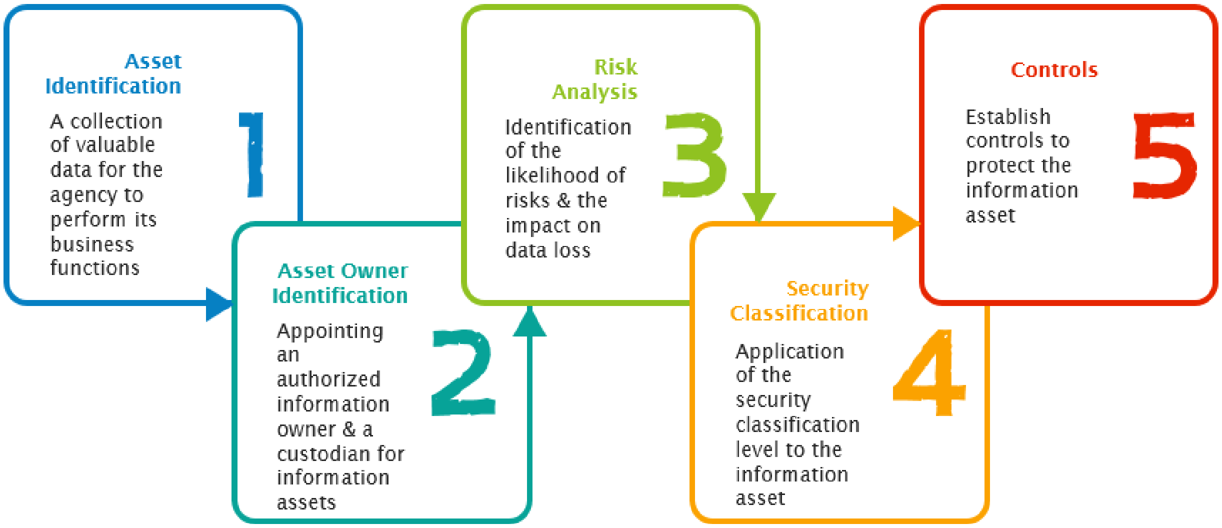
Information is classified as **"Secret"** when compromised could cause serious damage to national security, Government, nationally important economic and commercial interests or threaten life. It could also raise international tension and seriously damage relations with other governments, shut down or substantially disrupt significant national infrastructure and seriously damage the internal stability of Sri Lanka or other countries. Examples of Secret information are:

- Details of sex offenders and victims;
- Criminal investigations for major crime;
- Data related to foreign affairs;
- Cabinet documents; and
- Provincial Budget prior to public release

3 THE INFORMATION CLASSIFICATION PROCESS

[15] Personal information is governed by the Data Protection Act

It is necessary to ensure that the process is understood to be an organic process, that is, that information classifications need to be periodically and regularly reassessed, and that the application of this process on a 'one-off' basis will not provide the required protection of information.


Asset Identification
A collection of valuable data for the agency to perform its business functions
1
Asset Owner Identification
Appointing an authorized information owner & a custodian for information assets
2
Risk Analysis
Identification of the likelihood of risks & the impact on data loss
3
Security Classification
Application of the security classification level to the information asset
4
Controls
Establish controls to protect the information asset
5

3.1 STEP1: IDENTIFY INFORMATION ASSETS

Information assets are defined as an identifiable collection of data, stored in any manner and recognized as having value for enabling an agency to perform its business functions, thereby satisfying a recognized agency requirement.

Examples of information assets include, but are not limited to:

- Records
- Documents
- Electronic messages
- Rows in a database
- Tables or figures within a document
- Database tables
- Collections of data objects about a single logical entity or concept such as 'customer'
- Content identified through - Uniform Resource Locators (URLs) or Uniform Resource Identifiers (URIs)
- Metadata about other information assets.

Information spanning multiple media types or formats must ensure classification requirements are applied to all types of formats, to ensure overarching classification control is maintained.

If any information assets exist that are not stored in paper-based or electronic formats (such as photographs or test samples), they should still be classified using the Information Security Classification but will require additional agency policies to ensure consistent evaluation and application.

'Information asset' is not used to refer to the technology used to store, process, access, and manipulate information, which is more properly described as Information and Communication Technology (ICT) assets. ICT assets that are not considered as information assets include:

- Software including application and system software, development tools and utilities, and the associated licenses
- Physical assets such as computing equipment, storage media (CDs, DVDs, tapes, and disks), power supplies, air conditioners, and other technical equipment which may impact the confidentiality, availability, or integrity of information resources.

3.2 STEP 2: IDENTIFY THE OWNER OF THE INFORMATION ASSETS

Each organization is responsible for ensuring that information assets have a security classification that is authorized by the information owner and that a custodian who is responsible for implementing and maintaining information assets, according to the rules set by the owner, has been assigned. Information assets should be classified by the information owner or delegate at the earliest possible opportunity, and as soon as the originator or owner is aware of the sensitivity of the information asset.

In the case of information assets that are externally generated, and not otherwise classified, the agency officer who receives them should ensure that an owner and custodian are assigned and that the asset is incorporated into agency information asset registers as appropriate.

Note:

Information owners define the policy which governs the information assets of an organization, for example determining the classification of information assets. An owner will often delegate the operational responsibility for information assets to a custodian, who applies controls that reflect the owner's expectations and instructions such as ensuring proper quality, security, integrity, correctness, consistency, privacy, confidentiality, and accessibility of the information assets.

3.3 STEP 3: IMPACT ASSESSMENT OF INFORMATION ASSETS FOR THE RISK ANALYSIS

The purpose of the assessment is to identify the probability or likelihood of the threat is and what the impact would be if there was a loss to the integrity, availability, confidentiality, or the value of information assets. Risk assessments are undertaken to properly identify risks.

When determining the correct information security classification level for an information asset or domain, a range of considerations needs to be taken into account. Where information assets can be security classified according to legislation, regulation, policy, contractual, or other pre-determined means, it should be so classified. For example, breach of proper undertakings to maintain the confidentiality of information provided by third parties and breach of statutory restrictions on the management and disclosure of information need to be considered, and these may influence the final security classification level.

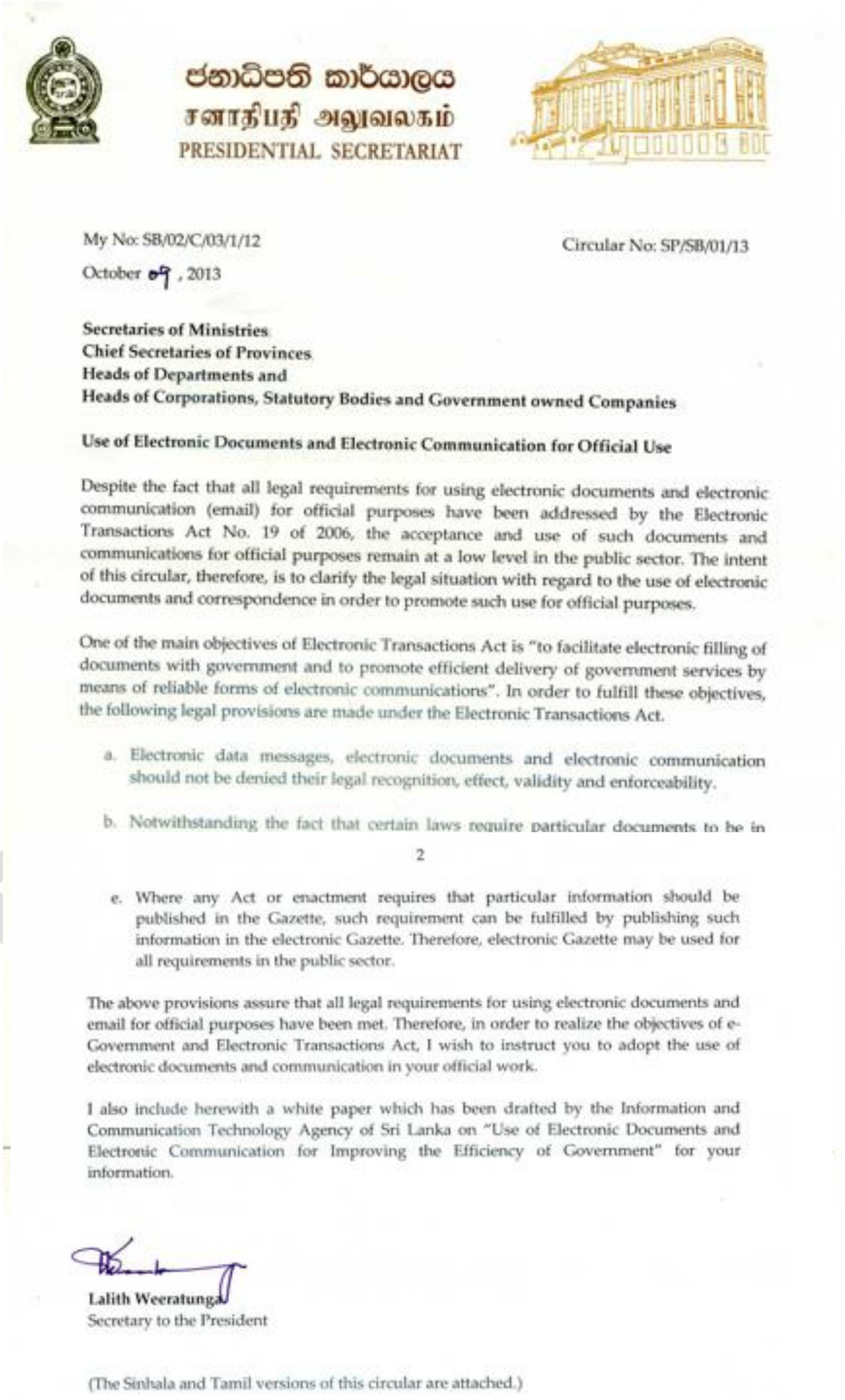
3.4 STEP 4: DETERMINE THE SECURITY CLASSIFICATION OF THE INFORMATION ASSET

The highest security classification level determined by the impact assessment must be applied to that asset.

3.5 STEP 5: APPLY CONTROLS BASED ON SECURITY CLASSIFICATION

Appropriate controls, as prescribed in the 'National Data Sharing Policy', must be applied to ensure that protection is given to information assets commensurate with the security classification level that has been determined.

ANNEX 5 – PRESIDENTIAL CIRCULAR NO. SP/SB/01/13



ජනාධිපති කාර්යාලය
சனாதிபதி அலுவலகம்
PRESIDENTIAL SECRETARIAT

My No: SB/02/C/03/1/12

Circular No: SP/SB/01/13

October 09 , 2013

Secretaries of Ministries
Chief Secretaries of Provinces
Heads of Departments and
Heads of Corporations, Statutory Bodies and Government owned Companies

Use of Electronic Documents and Electronic Communication for Official Use

Despite the fact that all legal requirements for using electronic documents and electronic communication (email) for official purposes have been addressed by the Electronic Transactions Act No. 19 of 2006, the acceptance and use of such documents and communications for official purposes remain at a low level in the public sector. The intent of this circular, therefore, is to clarify the legal situation with regard to the use of electronic documents and correspondence in order to promote such use for official purposes.

One of the main objectives of Electronic Transactions Act is "to facilitate electronic filling of documents with government and to promote efficient delivery of government services by means of reliable forms of electronic communications". In order to fulfill these objectives, the following legal provisions are made under the Electronic Transactions Act.

a. Electronic data messages, electronic documents and electronic communication should not be denied their legal recognition, effect, validity and enforceability.

b. Notwithstanding the fact that certain laws require particular documents to be in

2

e. Where any Act or enactment requires that particular information should be published in the Gazette, such requirement can be fulfilled by publishing such information in the electronic Gazette. Therefore, electronic Gazette may be used for all requirements in the public sector.

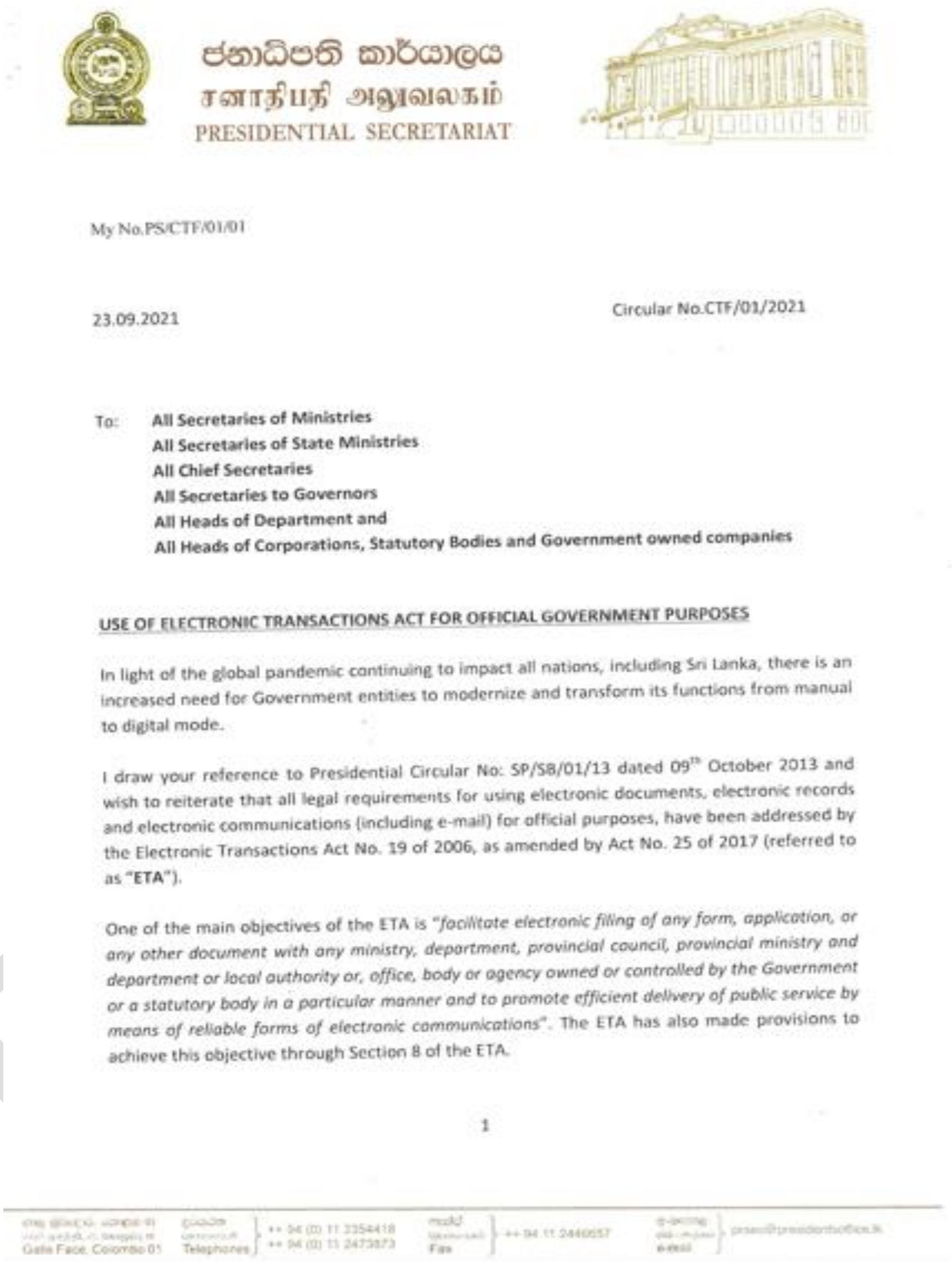
The above provisions assure that all legal requirements for using electronic documents and email for official purposes have been met. Therefore, in order to realize the objectives of e-Government and Electronic Transactions Act, I wish to instruct you to adopt the use of electronic documents and communication in your official work.

I also include herewith a white paper which has been drafted by the Information and Communication Technology Agency of Sri Lanka on "Use of Electronic Documents and Electronic Communication for Improving the Efficiency of Government" for your information.

Lalith Weeratunga
Secretary to the President

(The Sinhala and Tamil versions of this circular are attached.)

ANNEX 6 – PRESIDENTIAL CIRCULAR NO. CTF 01/2021



ජනාධිපති කාර්යාලය
சனாதிபதி அலுவலகம்
PRESIDENTIAL SECRETARIAT

My No.PS/CTF/01/01

23.09.2021

Circular No.CTF/01/2021

To:
All Secretaries of Ministries
All Secretaries of State Ministries
All Chief Secretaries
All Secretaries to Governors
All Heads of Department and
All Heads of Corporations, Statutory Bodies and Government owned companies

USE OF ELECTRONIC TRANSACTIONS ACT FOR OFFICIAL GOVERNMENT PURPOSES

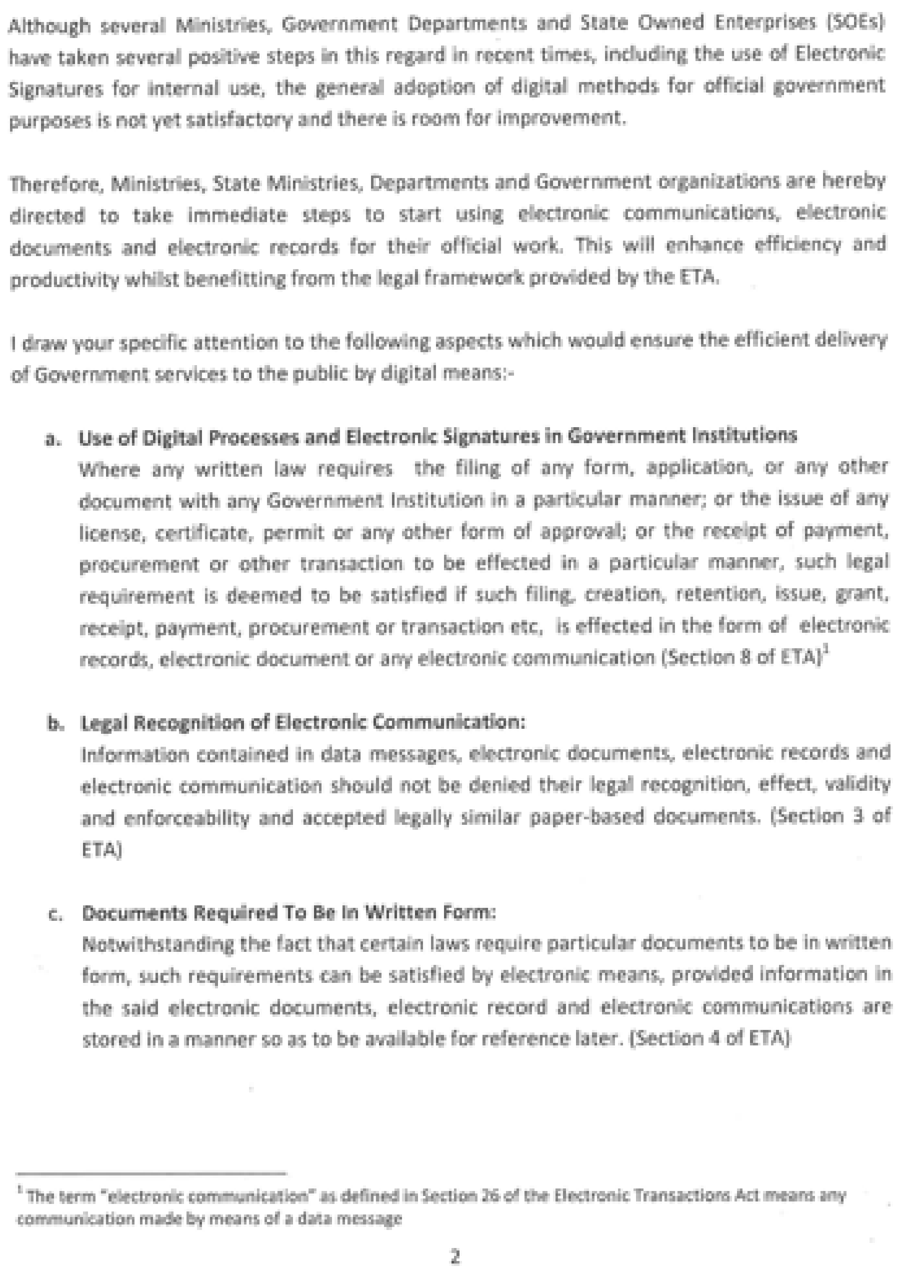
In light of the global pandemic continuing to impact all nations, including Sri Lanka, there is an increased need for Government entities to modernize and transform its functions from manual to digital mode.

I draw your reference to Presidential Circular No: SP/SB/01/13 dated 09th October 2013 and wish to reiterate that all legal requirements for using electronic documents, electronic records and electronic communications (including e-mail) for official purposes, have been addressed by the Electronic Transactions Act No. 19 of 2006, as amended by Act No. 25 of 2017 (referred to as "**ETA**").

One of the main objectives of the ETA is *"facilitate electronic filing of any form, application, or any other document with any ministry, department, provincial council, provincial ministry and department or local authority or, office, body or agency owned or controlled by the Government or a statutory body in a particular manner and to promote efficient delivery of public service by means of reliable forms of electronic communications"*. The ETA has also made provisions to achieve this objective through Section 8 of the ETA.

1

[illegible]
Galle Face, Colombo 01
[illegible] Telephones ++ 94 (0) 11 2354418 ++ 94 (0) 11 2473873
[illegible] Fax ++ 94 11 2440657
[illegible] e-mail presec@presidentsoffice.lk



Although several Ministries, Government Departments and State Owned Enterprises (SOEs) have taken several positive steps in this regard in recent times, including the use of Electronic Signatures for internal use, the general adoption of digital methods for official government purposes is not yet satisfactory and there is room for improvement.

Therefore, Ministries, State Ministries, Departments and Government organizations are hereby directed to take immediate steps to start using electronic communications, electronic documents and electronic records for their official work. This will enhance efficiency and productivity whilst benefitting from the legal framework provided by the ETA.

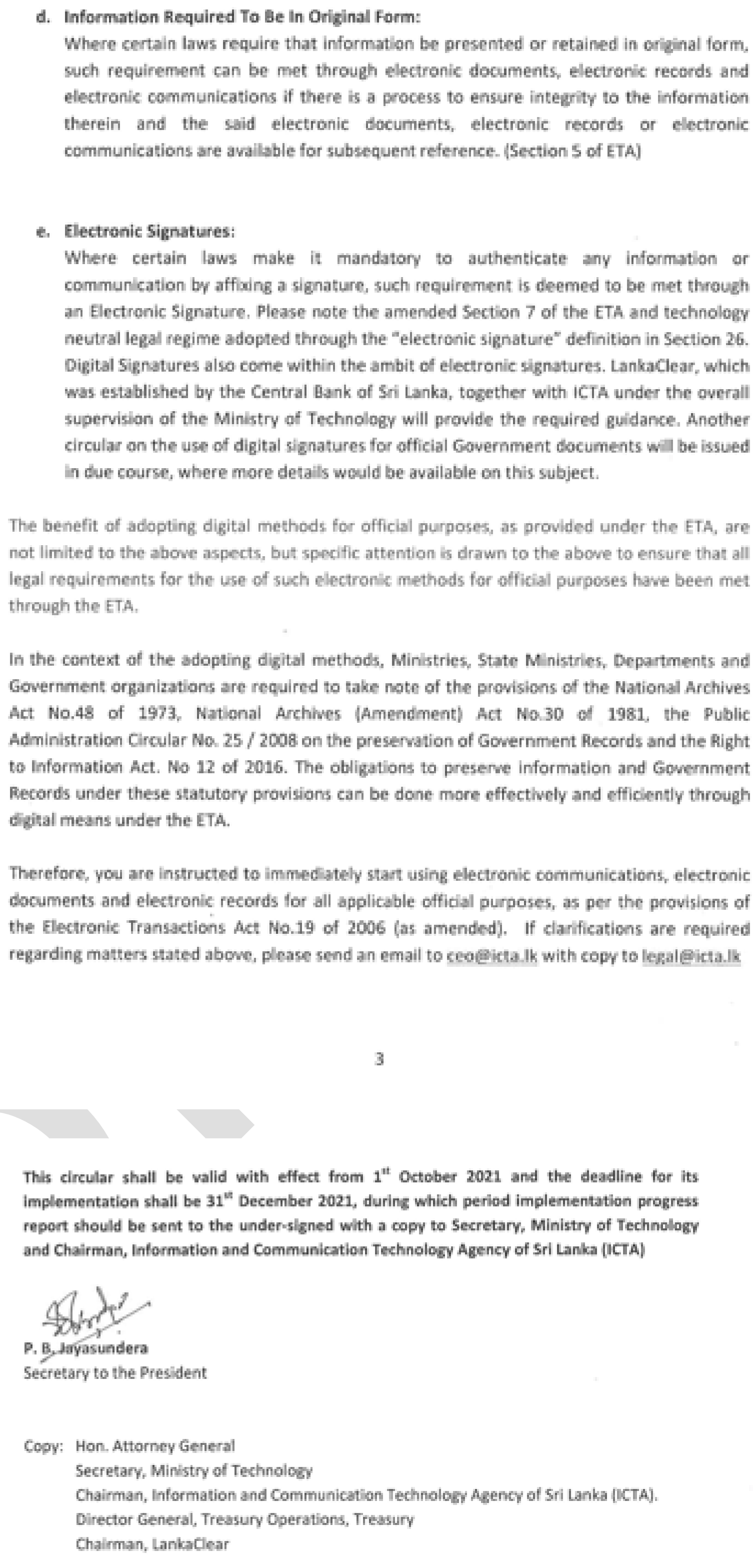
I draw your specific attention to the following aspects which would ensure the efficient delivery of Government services to the public by digital means:-

a. **Use of Digital Processes and Electronic Signatures in Government Institutions**
Where any written law requires the filing of any form, application, or any other document with any Government Institution in a particular manner; or the issue of any license, certificate, permit or any other form of approval; or the receipt of payment, procurement or other transaction to be effected in a particular manner, such legal requirement is deemed to be satisfied if such filing, creation, retention, issue, grant, receipt, payment, procurement or transaction etc, is effected in the form of electronic records, electronic document or any electronic communication (Section 8 of ETA)[1]

b. **Legal Recognition of Electronic Communication:**
Information contained in data messages, electronic documents, electronic records and electronic communication should not be denied their legal recognition, effect, validity and enforceability and accepted legally similar paper-based documents. (Section 3 of ETA)

c. **Documents Required To Be In Written Form:**
Notwithstanding the fact that certain laws require particular documents to be in written form, such requirements can be satisfied by electronic means, provided information in the said electronic documents, electronic record and electronic communications are stored in a manner so as to be available for reference later. (Section 4 of ETA)

[1] The term "electronic communication" as defined in Section 26 of the Electronic Transactions Act means any communication made by means of a data message



d. **Information Required To Be In Original Form:**

Where certain laws require that information be presented or retained in original form, such requirement can be met through electronic documents, electronic records and electronic communications if there is a process to ensure integrity to the information therein and the said electronic documents, electronic records or electronic communications are available for subsequent reference. (Section 5 of ETA)

e. **Electronic Signatures:**

Where certain laws make it mandatory to authenticate any information or communication by affixing a signature, such requirement is deemed to be met through an Electronic Signature. Please note the amended Section 7 of the ETA and technology neutral legal regime adopted through the "electronic signature" definition in Section 26. Digital Signatures also come within the ambit of electronic signatures. LankaClear, which was established by the Central Bank of Sri Lanka, together with ICTA under the overall supervision of the Ministry of Technology will provide the required guidance. Another circular on the use of digital signatures for official Government documents will be issued in due course, where more details would be available on this subject.

The benefit of adopting digital methods for official purposes, as provided under the ETA, are not limited to the above aspects, but specific attention is drawn to the above to ensure that all legal requirements for the use of such electronic methods for official purposes have been met through the ETA.

In the context of the adopting digital methods, Ministries, State Ministries, Departments and Government organizations are required to take note of the provisions of the National Archives Act No.48 of 1973, National Archives (Amendment) Act No.30 of 1981, the Public Administration Circular No. 25 / 2008 on the preservation of Government Records and the Right to Information Act. No 12 of 2016. The obligations to preserve information and Government Records under these statutory provisions can be done more effectively and efficiently through digital means under the ETA.

Therefore, you are instructed to immediately start using electronic communications, electronic documents and electronic records for all applicable official purposes, as per the provisions of the Electronic Transactions Act No.19 of 2006 (as amended). If clarifications are required regarding matters stated above, please send an email to ceo@icta.lk with copy to legal@icta.lk

3

This circular shall be valid with effect from 1st October 2021 and the deadline for its implementation shall be 31st December 2021, during which period implementation progress report should be sent to the under-signed with a copy to Secretary, Ministry of Technology and Chairman, Information and Communication Technology Agency of Sri Lanka (ICTA)

P. B. Jayasundera
Secretary to the President

Copy: Hon. Attorney General
Secretary, Ministry of Technology
Chairman, Information and Communication Technology Agency of Sri Lanka (ICTA).
Director General, Treasury Operations, Treasury
Chairman, LankaClear