

DRAFT 4.2

Please do not quote.

National Digital Government/Governance Policy for Sri Lanka

Ministry of Technology

and

Information and Communication Technology Agency of Sri Lanka

June 2022

TABLE OF CONTENTS

1	INTRODUCTION	3
1.1	Background	3
1.2	Need	4
1.3	Purpose and context	4
1.3.1	Digital Economy	4
1.3.2	Digital Government	5
1.3.3	Digital Laws.....	6
1.3.4	Policy Direction	6
1.4	Rationale.....	7
1.4.1	Overarching Principles.....	7
2	DIGITAL GOVERNMENT FOR GOOD GOVERNANCE	9
3	POLICY PRINCIPLES, STATEMENTS AND GOALS	11
3.1	POLICY PRINCIPLES, STATEMENTS AND GOALS # 1	12
3.2	POLICY PRINCIPLES, STATEMENTS AND GOALS # 2	16
3.3	POLICY PRINCIPLES, STATEMENTS AND GOALS # 3	18
3.4	POLICY PRINCIPLES, STATEMENTS AND GOALS # 4	20
3.5	POLICY PRINCIPLES, STATEMENTS AND GOALS # 5	23
3.6	POLICY PRINCIPLES, STATEMENTS AND GOALS # 6	27
	Annexure I. Presidential Secretariat circular PS/GPA/Circular/01/2020	32
	Annexure II. Linkage of Digital Government Ambitions to Associating Good Governance Principles Council of Europe ELoGE model.....	34
	Annexure III. Information and Communication Technology Agency (ICTA).....	41
	Annexure IV. ICTA's Approach to Digital Government as per the Digital Government Transformation Roadmap Approved by the Cabinet	43
	Annexure V. Digital Government Policy Journey	46
	Annexure VI. Lanka Interoperability Framework (LIFe)	49

List of Abbreviations

CDIO	Chief Digital Information Officer
CINTEC	Computer and Information Technology Council of Sri Lanka
COMPOL	National Computer Policy
ICTA	Information and Communication Technology Agency
ICT	Information Communication Technology
GIC	Government Information Centre
GoSL	Government of Sri Lanka
HR	Human Resource
LGC	Lanka Government Cloud
LGN	Lanka Government Network
LIFe	Lanka Interoperability Framework
LOB	Line of Business
MVP	Minimum Viable Product
NARESA	Natural Resources, Energy and Science Authority of Sri Lanka
NDX	National Data Exchange
NSDI	National Spatial Data Infrastructure
POC	Proof of Concept
PSC	Project Steering Committee
RSS	Really Simple Syndication
SLCERT	Sri Lanka Computer Emergency Readiness Team
SLUDI	Sri Lanka Unique Digital Identification
SSO	Single-Sign-On
ROI	Return on Investment
RTI	Right to Information
TCO	Total Cost of Ownership

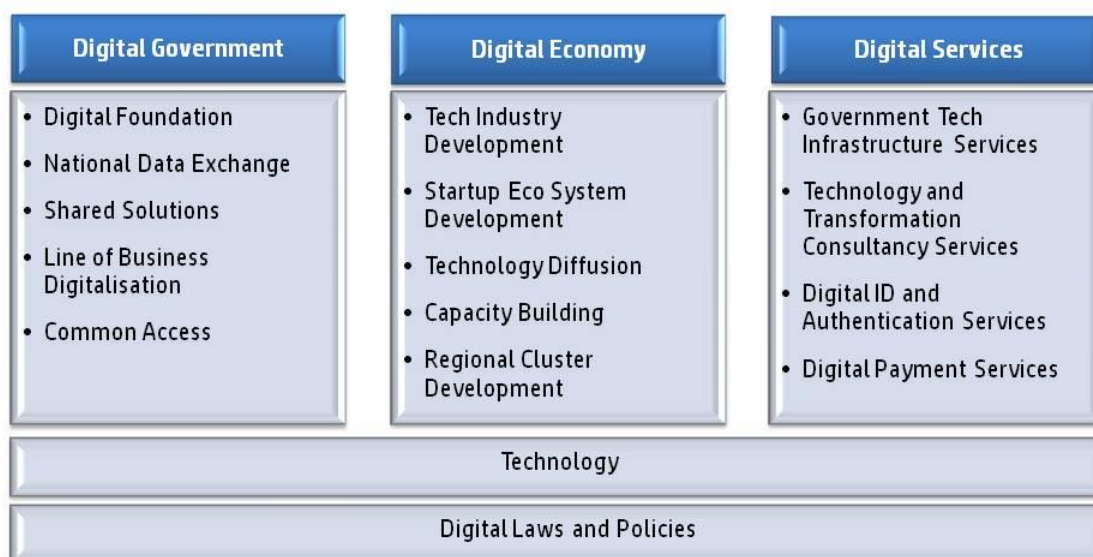
1 INTRODUCTION

1.1 Background

The government of Sri Lanka has presented its policy framework titled ‘Vistas of Prosperity and Splendour’. This National Policy Framework of the government constitutes nine key policies aimed at achieving the fourfold outcomes of a productive citizenry, a contented family, a disciplined and just society, and a prosperous nation. The nine key policies, giving due consideration to socio, economic, environmental, and political aspects are:

1. Priority to National Security;
2. Friendly, Non-aligned, Foreign Policy;
3. An Administration free from Corruption;
4. New Constitution that fulfills the People’s Wishes;
5. Productive Citizenry and a vibrant Human Resource;
6. People Centric Economic Development;
7. Technology Based Society;
8. Development of Physical Resources;
9. Sustainable Environmental Management and Disciplined, Law Abiding and values based society

Under the National Policy Framework, His Excellency the President and the Cabinet have approved the Digital Transformation Policy/Strategy framework with three main pillars (Digital Government, Digital Economy, and Digital Services) and sub-pillars as highlighted below. Digital Laws and Policies with Technology act as cross-cutting components of this framework.



1.2 Need

The aim of creating a digital ideology for Sri Lanka has at its roots, the empowerment of its people. The objective of this policy is to develop an indispensable medium where individuals can live out their relations, according to a social structure that encourages novel ideas, norms, and values.

Done well, a digital ideology can inspire our society to become more efficient and results-oriented, building connected communities with new technology and better control over their lives. That will be a medium that would help us understand how we can localize and culturally fine-tune our systems and government into affecting lives positively.

Digital Government, a subject area mandated to the Ministry of Technology, would empower the citizens of Sri Lanka, allowing easy access to information, provision of participation through public consultations in policy/decision making, allow automated services for public welfare and streamline government functions while ensuring transparency.

This policy is in alignment of Sri Lanka digital government roadmap, a previous version of the digital government policy was approved in 2009 and this version supersedes the same.

1.3 Purpose and context

1.3.1 Digital Economy

Digital economy is a key pivot for the digital transformation of the country which brings efficiency. Thus the policy would act as the catalyst that drives Sri Lanka's digital economy, which will facilitate industry expansion and increased foreign direct investment while creating opportunities for start-up innovation and entrepreneurship through capacity building and tech diffusion. Preferred business and employment opportunities would open up for local companies and the country's technology industry would move steadily towards the goal of becoming a USD 3 billion export earner by 2024. Further, building an efficient and effective Digital Government will result in Sri Lanka ranking high in doing business indices and increase the demand by international investors selecting the country as an investment destination.

Building Digital Government is identified as one of the three essential pillars in creating "A Better Living Conditions for Citizens" by transforming Sri Lanka into a sustainable sovereign nation that is safe and secure, prosperous, knowledge-based, and inclusive by 2024.

1.3.2 Digital Government

Digital Government is gradually re-inventing the way a government establishes and maintains its relationships with the public, offering its services more meaningfully and efficiently. It also redefines the roles of government and the citizen actively bringing the latter to the centre of the government sphere with increased openness and dynamic participation. Going far beyond just offering public goods, the governments, through Digital Government, now create vibrant democracies with inclusiveness and transparency, safeguarding citizen rights. Further, Digital Government solutions will bring together multiple government organizations in diverse areas such as Agriculture, Manufacturing, National Security, Law and Order, etc. The implementation of Sri Lanka Unique Digital Identity (SLUDI) and Digital Signatures are two such initiatives introduced by the Information and Communication Technology Agency of Sri Lanka to drive the country towards a technology-based society.

This transformation has been made possible by digital technology developments and augmented usage by the population, which has become almost a universal phenomenon in recent years. For instance, as at March 2022 the statistical overview of the telecommunication sector in the country has been as follows¹ and these numbers are significant for a country with about a 22 million² population.

Category	Count
Total fixed line subscriptions	3.8 Million
Total fixed broadband subscriptions	2.6 Million
Total fixed line voice and data subscriptions	1.8 Million
Total fixed line data only subscriptions	1 Million
Total mobile telephone subscriptions	31 Million
Total mobile broadband subscriptions (3G and 4G)	19 Million
Total mobile voice and data subscriptions	21 Million

(Telecommunications Regulatory Commission of Sri Lanka)

¹ https://www.trc.gov.lk/images/pdf/Statics_2022_May.pdf

² Central Bank of Sri Lanka – Annual Report 2021
https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/publications/annual_report/2021/en/16_S_Appendix.pdf

1.3.3 Digital Laws

Digital laws play a major role in the use of ICT, as it provides the necessary legal framework for using electronic data and digital documents for official as well as personnel purposes and carrying out electronic transactions. The relevant legislation for use of ICT in government and the establishment of Digital Government services is the Electronic Transactions Act No. 19 of 2006. The use of Electronic Signatures through technologies such as “Digital Certificates” enables users to achieve confidentiality and integrity using the public key cryptosystem and hash function. The Computer Crimes Act No. 24 of 2007 provides for the identification of computer crimes and stipulates the procedure for the investigation and enforcement of such crimes. The Data Protection Act No.19 of 2022 provides for the regulation of the processing of personal data. The Cyber Security Act, once implemented, has provision for the setting up of a Cyber Security Agency which shall be the apex and executive body for all matters relating to cyber security policy in Sri Lanka and shall be responsible for the implementation of the National Cyber Security Strategy of Sri Lanka.

Influenced by their digital experiences with businesses, citizens' expectations of public services are rising. They now expect public administration to adapt to their ways of doing things, not the other way around. This creates serious challenges to governments as now they must transform themselves using digital technology to bring services to the doorsteps of citizens.

1.3.4 Policy Direction

This document, taking the same direction, provides the policy direction to the Sri Lanka government on the implementation of a Digital Government, under the provisions given by the Information and Communication Technology Act, No.27 of 2003 (Incorporating Amendment Act No. 33 of 2008) to provide guidance and facilitate the implementation of Information and Communication Technology programs and strategies to government. It is further expected to promote the ‘Whole of Government’ concept emphasizing the need for greater collaboration and coordination across government organizations to eliminate duplication, optimize resources, create synergies among agencies and deliver seamless services to the citizens and businesses of the country. Whilst adhering to and applying this policy as the baseline, government organizations should similarly adhere to other policies introduced to promote Digital Government.

1.4 Rationale

1.4.1 Overarching Principles

When formulating the Digital Government policy, the following overarching principles have been considered. They should be incorporated, as appropriate, into the implementation of Digital Government solutions.

- Specific guidelines and frameworks issued by the Presidential Secretariat, Ministry of Technology, ICTA³, Sri Lanka Telecommunication Regulatory Commission, and SL-CERT related to Digital Government procedures.
- Provisions in Data Protection and Cyber Security legislation
- Data Classification Framework, Data Sharing Policies, Digital Maturity Model, and Digital Competency Framework compiled by ICTA
- Respective Government strategies (application development and support/maintenance) for Line of Business Solutions
- Security by Design: Products and capabilities have been designed to be foundationally secure.
- Privacy by Design: Ensure protection for the privacy of citizens during the development of products, services, practices, guidelines, physical infrastructures, etc.
- Accessibility by Design: Product or service can be used by everyone—however they encounter it. (Emphasis on minorities, marginalized and differently-abled categories)
- Mobile First by Design: Approach in which web designers start product design for mobile devices first.
- Trilingual by Design: Availability of data and information in any of the three official languages i.e. Sinhala, Tamil, and English⁴, also adhering to National Language Policy⁵.
- Achievement of sustainability, cost-effectiveness, and productivity

³ Refer Annexure III – Information and Communication Technology Agency (ICTA)

⁴ All government organizations must use Sinhala and Tamil Unicode for all computing work (such as creating documents, web sites, software systems, and in the electronic transmission of information). Sri Lanka Standard Institution has standardized Sinhala and Tamil Unicode key board layout and input methods under the standards respectively SLS 1134 : 2004, including Part 1 thereof and SLS 1326: 2008.

⁵ Department of Official Languages

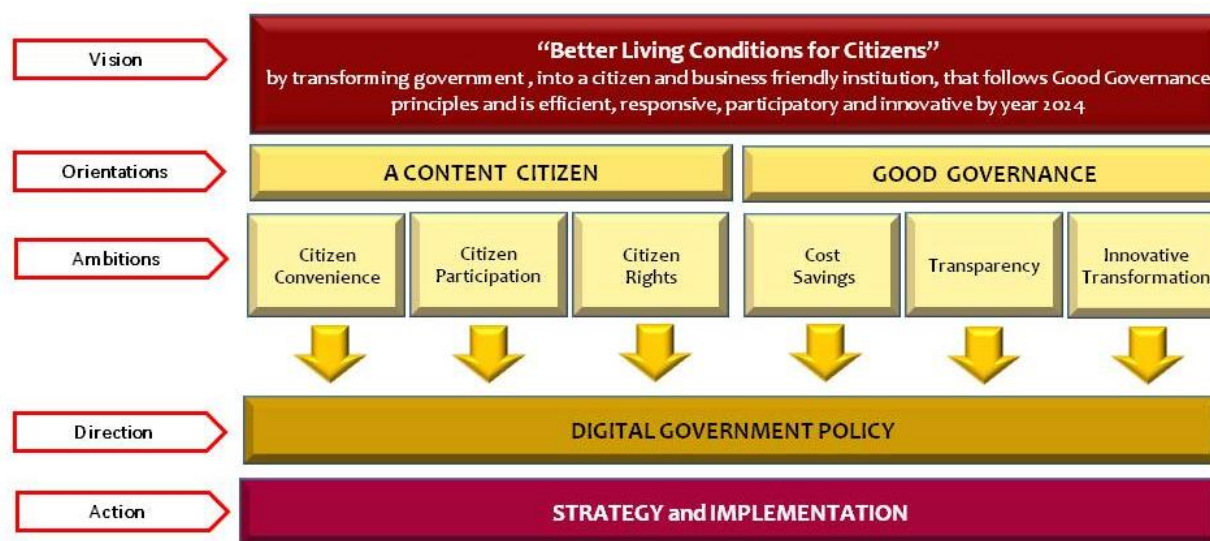
https://www.languagesdept.gov.lk/web/index.php?option=com_content&view=article&id=38:official-languages-policy&catid=2:uncategorised&lang=en&Itemid=163

The Digital Government Policy further mandates government organizations to follow the directives of the Presidential Secretariat Circular PS/GPA/Circular/01/2020 dated January 13, 2020, which positions the Information and Communication Technology Agency (ICTA) specifically in its Point (b), to drive national digital initiatives of the Government of Sri Lanka, for a cohesive, coordinated approach, to build a whole of government framework where data should be shared across systems for providing citizen-centric services effectively and efficiently⁶.

⁶ Refer Annexure I - Presidential Secretariat Circular PS/GPA/Circular/01/2020

2 DIGITAL GOVERNMENT FOR GOOD GOVERNANCE

The vision of Sri Lanka's Digital Government is "A Better Living Conditions for Citizens: by transforming government into a citizen-friendly institution following Good Governance principles and that is efficient, responsive, participatory and innovative".



Under two orientations of a Content Citizen and Good Governance, the six (06) goals are articulated as:

1. Citizen is central and paramount to Digital Governance. All e-government services, be them informational or transactional, will be devised for **Citizen Convenience** – be them individuals or businesses.
2. Active **Citizen Participation** in Digital Governance will make the solutions more inclusive. Citizens' needs for information and services are respected and delivered to the best of their expectations.
3. Digital Government guarantees the Protection of **Citizens' Rights** by the implementation of strong legal frameworks.
4. Digital Governance is aimed at substantial **Cost Savings** in producing meaningful outcomes for the society, in terms of finance, time, and environment, by proactively re-engineering the processes for efficacy and efficiency.
5. Digital Government will make a Society free from bribery and corruption achieved with **Transparency**, Openness, and Responsiveness.

6. Digital Governance is a means for change, not an end goal in itself. It is a continuous **Innovative Transformation** that continuously researches for and implements advanced end-to-end technological solutions in making society a more cultured, enlightened, compassionate, healthier, and sustainable place to live.

All these parameters stem from Good Governance principles, the fundamental governance building block of modern society. Therefore these six goals of Digital Government must be strictly aligned with the latter. This is done by aligning each Digital Government goal to two principles of the Council of Europe 12 Principles of Good Governance⁷.

⁷ Refer Annexure II - Linkage of Digital Government Ambitions to Associating Good Governance Principles Council of Europe ELoGE Model

3 POLICY PRINCIPLES, STATEMENTS AND GOALS

This page is intentionally left blank.

3.1 POLICY PRINCIPLES, STATEMENTS AND GOALS # 1

“Citizen is central and paramount to Digital Government. All Digital Government services, be them informational or transactional, will be devised for Citizen Convenience – be them individuals or businesses.”

People are at the heart of any successful digital transformation, well before technology. It is for this reason that the Digital Government places citizens at the centre of the transformation.

Digital Government offers faster and intuitive digital services to simplify the lives of citizens through a smoother circulation of information; be more proactive in its relations with citizens and reach citizens faster and more efficiently as well as effectively by designing public services that are easy to use. This is done through innovative solutions unlocking the full potential of emerging technologies. Citizen convenience is the paramount factor in the process. Digital Government services, be them informational or transactional, will reach all citizens in a manner convenient for each either free of charge or at affordable costs.

Digital Government solutions must further facilitate the ‘Improved Quality of Life of Citizens’ irrespective of their socio-economic levels or geographical locations.

Achievement of these necessitates:

1. Publishing by government institutes all relevant information required by the general public, with frequent and regular updates in multiple channels by:
 - a. Presenting their government services through the government services aggregator www.gov.lk, always on a trilingual basis (mandatory)
 - b. Using, in addition to the above, all other available digital channels, including social media, to share more dynamic information with the public initiating effective dialogues with them on all matters related to them in an appropriate medium. Social media profiles utilized for this purpose need to include;
 - i. Verified profile statuses for social media accounts of organizations and leadership
 - ii. Governing policies related to social media handling
 - c. Developing internal mechanisms to compile, collect, translate and provide such information for publishing always assuring they are relevant and updated

- d. Taking necessary steps, in line with Right to Information principles, to proactively disclose all information relevant to the public on time, while adhering to the Data Protection Act No.19 of 2022⁸, in a language they readily understand
 - e. Making all forms, guidelines, circulars and any other artifacts relevant to the citizens, available across all channels, in digital format for download.
2. Be responsive and interactive to satisfy citizens' expectations by:
- a. All government organizations providing e-mail and collaboration facilities to staff, as required by each department.
 - b. Executing, by public officials, high-quality decisions and processes on time, supported by data and automation, subject to the provisions of automated decision making within the stipulated legal provisions on data protection.
 - c. Making online services available on a 24x7 basis, for efficient and faster Digital Government services.
 - d. Connecting and collaborating seamlessly with other parties in the state mechanism (through digital means), so that the client's expectations are met the soonest.
 - e. Public officers responding to electronic inquiries made by the citizens in a meaningful and timely manner through e-mail or alternative means; ensuring that the response is made through the same means that the inquiry was made.
 - f. Government organizations, following a collaborative approach, agree jointly to follow a "no door is closed" policy, i.e. responding to citizen inquiries, through any channel by any agency a citizen selects to access government
 - g. Offering, whenever appropriate trilingual helplines for citizens, who face usage issues in accessing government services, preferably on a 24x7 basis; with minimum operational time during working hours.
3. Establish Digital Government service delivery standards across institutions for winning the trust of the public by:
- a. Setting up benchmarks for quick, meaningful, and responsive delivery for multiple channels including, but not limited to, multipurpose kiosks, e-mail, web, voice, SMS, mobile apps, e-services, etc. to be adhered to by practitioners in their public service interactions

⁸ https://www.icta.lk/icta-assets/uploads/2022/03/09-2022_E.pdf

- b. Continuously monitoring, by administrators, of the digital delivery quality regarding availability, capability, quality of the offering, and responsiveness across all government institutes for determining public satisfaction
 - c. Letting the public regularly evaluate and respond to the service quality through the same channels they receive services
 - d. Making the service quality figures of each organization public on a regular basis for them to benchmark against similar services to make further improvements.
 - e. Ensure that the internal processes/principles are in alignment with the legal and legislative directives on data protection and cyber security as of date.
4. Ensure that ICT based service delivery mechanisms are inclusive by devising specific mechanisms to provide multi-channel services to accommodate the segments who are differently-abled, digitally marginalized, lack IT know-how, etc.
5. Adopt “Mobile First” strategies, i.e. prioritize offering Digital Government services through smartphones, in addition to the manual counters; as the most utilized user device, by:
- a. Simplifying existing and new Digital Government services so that even a user with only a mobile handset known as a ‘feature phone’ (for convenience and affordability reasons) can effectively obtain them
 - b. Offering separately designed solutions for each category of user devices (PC, tab, smart phone) that take features of each into account⁹ following responsive web design techniques
 - c. Following ‘Progressive Advancement’ (i.e. building a solution to work on a lower browser and add advanced features for higher versions) than ‘Graceful Degradation’ designing, where the process is reversed so that lower browser users find only a cut-down version
 - d. Customizing solutions for different types of mobile handsets such as a smartphone, a feature phone, or a basic phone, depending on their capabilities
 - e. Promoting the use of smartphones by the public for use of Digital Government services with sufficient media coverage to create awareness
6. Ensure the ‘User Journey First’ approach in all new developments initiated by government organizations.

⁹ For example, smartphone screen size is smaller than that of a PC screen; it may be difficult for a smartphone user to take a print

7. Recognize the standards for digital identification as per the legislation on electronic/digital communication and transactions as appropriate by the date and acceptance by authorities of digital signatures and digital certificates.
8. Allow citizens to Single-Sign-On (SSO) to any Government Information System using the unique digital ID, provided through SLUDI, and avail of required services.
9. Encourage digital payment options for receiving Digital Government services by:
 - a. Researching and experimenting with different transaction options, for the best-suited ones in delivering Digital Government services by each channel
 - b. Providing an extensive range of digital payment solutions to pay for Digital Government Services
 - c. Gradually discouraging the public from using government services through traditional means by offering more value-added services in Digital Government services whenever possible
 - d. Ensuring that the facilitation of digital payment options is subjected to the approved methods by relevant legislation and regulations governing the same.
10. Maintain records of citizens' complaints, grievances, and suggestions related to Digital Government Services systematically and take appropriate actions to improve the services
11. Continuously improve Digital Government services based on active monitoring and evaluation of the quality of service and citizen/business satisfaction on multiple channels

3.2 POLICY PRINCIPLES, STATEMENTS AND GOALS # 2

“Active Citizen Participation in Digital Governance will make the solutions more inclusive. Citizens’ needs for information and services are respected and delivered to the best of their expectations.”

Inclusion can be financial or social. Financial inclusion is when individuals and businesses have access to useful and affordable financial products and services that meet their needs – transactions, payments, savings, credit, and insurance – delivered responsibly and sustainably¹⁰. Social inclusion, on the other hand, is the process of improving the terms for individuals and groups to take part in society; the ability, opportunity, and dignity of those disadvantaged based on their identity to take part in society.¹¹ A better Digital Government meets both these requirements simultaneously.

In addition, with dynamic and constant citizen participation; Digital Government offers transparency, which is essential to meet good governance standards.

Achievement of these necessitates:

1. Obtain public opinion, as deemed as required, when devising legislation, government policies, and other aspects of governance by:
 - a. Providing, by every government entity, means for obtaining citizens’ grievances, complaints, ideas, opinions, comments, and observations to ensure active citizen participation/contribution before initiating any service
 - b. Facilitating citizen interaction through multiple channels such as kiosks with interactive electronic interfaces, mobile handsets, websites, e-mail, blogs, online discussion forums, and social media to obtain wider public participation, as necessary and required, when devising national legislation, policies, regulations, plans, and budgets.
2. Take corrective/follow up actions visible to citizens through electronic means wherever possible and authorized by:
 - a. Having a key person or a unit to review and take appropriate actions with regards to grievances, complaints, ideas, opinions, comments, observations, etc. obtained from citizens
 - b. Using the same citizen-engagement mechanisms, informing citizens of the results of citizen engagement.

¹⁰ <https://www.worldbank.org/en/topic/financialinclusion/overview>

¹¹ <https://www.worldbank.org/en/topic/social-inclusion>

3. Comply with Right to Information (RTI) requirements guaranteeing the ability of people to receive information under the Right to Information Act, No. 12 of 2016, while adhering to the provisions of the Data Protection legislation by:
 - a. Establishing an enabling environment for people to have access to information which are significant for them
 - b. Creating multiple channels for the purpose as appropriate
 - c. Appointing and empowering, by Heads of Institutions, Information Officers responsible for releasing information to the public
 - d. Ensuring proactive disclosure of information always, effectively reducing the number of queries
 - e. Establishing differently-able-friendly electronic means for the benefit of that community

3.3 POLICY PRINCIPLES, STATEMENTS AND GOALS # 3

“Digital Government guarantees the Protection of Citizens’ Rights by the implementation of strong legal frameworks.”

In the domain of delivering government services to the public, says UN-OHCHR, good governance reforms advance human rights when they improve the state’s capacity to fulfill its responsibility to provide public goods which are essential for the protection of a number of human rights, such as the right to primary and secondary education, health and food. It further states reform initiatives may include mechanisms of accountability and transparency, culturally sensitive policy tools to ensure that services are accessible and acceptable to all, and paths for public participation in decision-making.¹²

Achievement of these necessitates:

1. Having, each practitioner organization, an overview of what data it handles, what the data signify, what they can be used for, what processes they are part of, and who can use them.
2. Formulate and adopt by each practitioner organization, an organizational Information Security Procedures¹³ by:
 - a. Retaining personal data and information using an appropriate mechanism for as long as it is required as per laws, regulations, and rules governing such data and information¹⁴; so that such data and information be divulged only as per rules and regulations governing such release
 - b. Maintaining electronic records in such a manner to ensure confidentiality and prevent unauthorized access, modification, alteration, transmission, or deletion/removal.¹⁵
 - c. Documenting and implementing acceptable use of information and assets associated with information systems.¹⁶

¹² United Nations Human Rights Office of the High Commissioner, Undated, Good Governance and Human Rights, <https://www.ohchr.org/EN/Issues/Development/GoodGovernance/Pages/GoodGovernanceIndex.aspx>

¹³ This should align with Information and Cyber Security Strategy of Sri Lanka <https://www.cert.gov.lk/Downloads/NCSSStrategy.pdf>

¹⁴ Data Protection Act No. 19 of 2022

¹⁵ The directives articulated in the Digital Document Management Policy by ICTA, which is in its development stage, should be considered as the primary source of guidance upon it getting published.

¹⁶ This should be in alignment with the strategies and policies on information security and cyber security developed by Sri Lanka CERT.

- d. Carrying out data storage devices disposal/repairs according to accepted information security standards in the organizational information security policy
 - e. Selecting the right storage media considering the possible period of preservation against technological advancements that makes the former outdated/obsolete¹⁷
 - f. Periodically checking media used for taking regular backups against their possible obsolescence due to technological advancements. In such cases, older sets of backups must be transferred fully to a new medium¹⁸.
3. Design, while ensuring individual data privacy, Digital Government solutions and implement them:
 - a. Collecting all necessary data that assist decision making of the digital transformation process
 - b. Analyzing the maturity of the transformation of respective organizations¹⁹
 - c. Improving the entire Digital Economy to create a citizen-centric business-focused culture/society
4. Design Digital Government solutions, in addition to the above, ensure security by design, mobility by design, and data by design; whilst adhering to the legal principles enshrined in legislation on data protection, cyber security as well as computer crimes, for timely and quality delivery of services.
 - a. Government organizations need to cooperate to deliver an integrated service to citizens through the National Data Exchange (NDX)

¹⁷ Adherence to the National IT Policy and the Cloud First approach by ICTA are essential.

¹⁸ Deployment of cloud services via developing tenants to ensure backup

¹⁹ The Digital Maturity Model for Government of Sri Lanka, developed by Information and Communication Technology Agency with the assistance of other stakeholders can be used for this purpose.

3.4 POLICY PRINCIPLES, STATEMENTS AND GOALS # 4

“Digital Governance is aimed at substantial Cost Savings while producing meaningful outcomes for the society, in terms of finance, time and environment, by proactively re-engineering the processes for efficacy and efficiency.”

A widespread myth is re-engineering makes e-government services cost more. Multiple studies have found evidence for the opposite.

The economy is just one aspect. Digital Government brings savings also in terms of time and environment. It leads to less fossil fuel consumption and lets citizens and businesses use the time saved in traveling for more productive activities.

Achievement of these necessitates:

1. Improve all practitioner organizations, of their processes by employing process re-engineering principles wherever necessary and implementing Digital Government solutions to offer citizen centric services by:
 - a. Evaluating their service delivery standards and identifying challenging areas and processes contributing to the problem
 - b. Iteratively re-engineering the existing processes to improve the service delivery
 - c. Continuously reviewing and updating organizations' user manuals to incorporate changes/improvements of re-engineered processes
2. Attempt, as much as possible, to design new solutions with a single sign-on, a single window for all Digital Government services
3. Define, for each citizen, a single digital identity²⁰ to be based on Sri Lanka Unique Digital Identification (SLUDI) standards that can be used over all government systems seamlessly, without each system demanding identification, and which can be used by state sector organizations to build workflows across them, establishing an interoperable data model that will allow disparate and independent Digital Government services to independently innovate yet; remain interoperable in order to facilitate collaborative and shared operation.
4. Implementation of information systems by government organizations be carried out in a phased out and incremental manner by embracing agile project management practices.

²⁰ A digital identity is a set of identifiers, such as a username, e-mail address, mobile number or a biometric that uniquely describes and entity and its relationships with other entities. To prove the ownership of the digital identity the owner has to prove that he or she possesses the corresponding authentication factors. Given the increasing risk of digital sabotage, the verification of the ownership is done by multiple factors.

- a. A phase or an implementation increment/cycle should be completed within 6 months unless otherwise there is a valid and justifiable reason to exceed this timeline.
 - b. Phase-1 should be a ‘Minimum Viable Product’ (MVP) with the most essential features, and subsequent phases may include the other good-to-have features.
 - c. If the project carries significant risks, a ‘Proof of Concept’ (POC) phase is required to be implemented before the MVP.
 - d. Each phase of increment should be rolled out for live usage, and learnings from each phase should be incorporated into the development of subsequent phases/releases.
5. All practitioner organizations to consult ICTA before implementation to ensure that the new solutions comprise reusable components as much as possible.
 - a. Practitioner organizations should get their technological decisions vetted by ICTA before implementation.
 - b. It is mandatory to ensure that all new solutions are in adherence to the sectorial digital transformation roadmaps of ICTA.
6. Exposing by, all solutions implemented, service Application Programming Interfaces (APIs) for other third-party organizations and in specific cases, by private entities, to consume data through the National Data Exchange (NDX)²¹
7. Take by government organizations, all measures to ensure resource optimization and productivity of the IT resources i.e. technical resources, and human resources; in a manner where the maximum use is gained without letting them be in idle mode.
8. Avoid duplication of work by every practitioner organization, before implementing a new solution, by checking the availability and suitability of ICT solutions already available with other government organizations²²
 - a. Consultation with ICTA is mandatory in arriving at a feasible decision.
9. Use of shared cluster applications, provided by the GoSL, by cluster members for avoiding duplication of effort and guaranteeing increased efficiency. A strong justification is mandatory to use anything contradictory.
 - a. Use common ICT infrastructure and facilities, including but not limited to National Data Exchange (NDX), National Spatial Data Infrastructure (NSDI), Lanka Government Network (LGN, to share data and information among government organizations), middleware infrastructure, Lanka Government Cloud (LGC, for

²¹ Proposed to be implemented

²² Applications such as Integrated Human Resources Management System, Financial Management System and Inventory and Asset Management System developed by Public Services Commission, Ministry of Finance etc. are already available for the use. ICTA or the line ministry can coordinate the application components sharing measures.

cloud-based software services), Mobile Portal, GovSMS, Lanka Government Payment Service (to process electronic payments) and Government Information Centre (GIC, for citizen services for providing service-related information to the public) in providing citizen services

10. Re-use, as much as possible, information already collected within the organization or in the particular service domain by:

- a. Practitioner organizations creating their data sets in formats ready for sharing
- b. Deciding on the data owners with inter-organization consultation and consensus
- c. Signing MoUs with data owners of the hubs for obtaining such information
- d. Ensuring the uniqueness of each data record of the hubs, the unique IDs such as Sri Lanka Unique Digital Identity (SLUDI), Company Registration Number, Land Identification Number, etc. are used. The organizations that intend to obtain data from hubs should, therefore, use the data standards of those unique IDs in their systems for data interoperability.
- e. Allowing any user to subscribe for notifications if data accessed earlier has undergone any transformation to ensure that all systems are in synchronization
- f. Developing schema for each piece of data available, in consultation with the data custodians, that conform to and adopt interoperability standards, so that others who wish to consume data can adapt these published data to their internal data architectures

11. Have detailed and effective e-waste disposal programs for the computer and peripheral equipment used by organizations, in par with the environmental requirements of the country.

²³

12. Allow no used digital equipment/machinery to be re-introduced for the government organizations' use.

²³ Electronic Waste or E-waste includes obsolete or broken electrical or electronic devices. In Sri Lanka the Hazardous Waste (Scheduled Waste) Management rules were first announced under the National Environmental Act in 2008. As per this regulation, E – Waste has been categorized as a scheduled waste and every generator, collector, stores, transporter, recover, recycler and disposer should obtain a license from the Central Environmental Authority (CEA) for the disposal. The CEA in collaboration with the other stakeholder companies has initiated a program to collect and discard all electronic items, by introducing e-waste collection points island-wide. The CEA has mandated that the E – Waste should be given only to authorized collectors. At the time any E-waste is being disposed the government organizations should take all measures to ensure that the regulatory requirements stipulated by the CEA are duly followed.

3.5 POLICY PRINCIPLES, STATEMENTS AND GOALS # 5

“Digital Government will create a transparent framework for a society free from bribery and corruption achieved with openness and responsiveness.”

Trust between citizens and government is based on the transparent use of public resources that optimize government spending leaving more funds for development activities. That also creates more organized societies with citizens benefitting from the protection of citizens’ rights and lowering service costs.

Achievement of these necessitates:

1. Create and proactively update, all practitioner organizations, new legal frameworks, regulations, and procedures to guarantee openness and transparency of activities by:
 - a. Designing internal protocols through the integrated use of data and digital technologies
 - b. Reviewing and making amendments to the existing legislation to allow effective, efficient, and meaningful services to the public in a productive manner and introducing new legislature where necessary to support Digital Government solutions with openness and transparency.
 - c. Ensuring that information is available to the public in a simple and an understandable manner
 - d. Releasing information affiliated to different personnel upon a due request, subject to exceptions such as state secrets, as defined by the Right to Information Act, No. 12 of 2016
2. Maintain data in electronic form (preparation and formulation, storage, retention, migration, and archiving) following the Electronic Transactions Act No. 19 of 2006 which specifies how government organizations should use electronic documents, electronic records, or other communication in electronic form by:
 - a. Enabling Government Information Systems to capture, store, process, and transmit data in any of the three official languages, i.e. Sinhala, Tamil, and English, following standards for internal and government audit requirements and with the relevant provisions of the National Archives Act no. 48 of 1973, and any amendments also with National Audit Act - 2018.
 - b. Transliterating/translating and storing data originally captured in Sinhala/Tamil in English to maintain the completeness of the data sets

- c. Converting paper-based and legacy data systems to digital form after cleaning and updating them
 - d. Ensuring privacy and security always by government systems that have legitimate needs to collect citizen data, in doing so.
 - i. Data protection and cyber security rules and regulations, as defined by the Data Protection Act No.19 of 2022 and the proposed Cyber Security Act, should be adhered to at the point of implementation.
 - e. Not accessing and not sharing such collected data without a legitimate reason (proper approval from data owners/in line with governing legislation on data protection, cyber security, computer crimes)
 - f. Taking all necessary precautions during the design process to prevent data misuse.
3. Make such data and information available through multiple channels to meet the requirements of citizens and businesses by:
- a. Publishing all such information in the central platform www.gov.lk
 - b. Creating means such as organizational websites, which are accessible by any device, giving priority to ones like smart devices that have become the most popularly used method to reach Digital Government services
 - c. Offering voice-based services using appropriate channels including Government Information Centre – 1919 services to communicate and offer assistance on new changes or updates
 - d. Using 1919, as much as possible, as the central voice service for all government organizations to make it more convenient for citizens to remember. However, government organizations can have their own contact centre numbers if needed.
 - e. Introducing new features to GIC-1919 to support differently-abled citizens²⁴
 - f. Providing information through social networks, web syndication technologies such as RSS forums, and other suitable social media as appropriate
 - g. Evaluating bi-annually each channel for the effectiveness in providing Digital Government services through the integration of social CRM services.
4. Offer citizen-centric government services electronically through multiple channels and in any one or more of three languages i.e. Sinhala, Tamil, or English as appropriate, required by the law and regulations, treating citizens' needs the utmost priority, observing inclusiveness, and on a 24x7 basis whenever possible by:

²⁴ This is to be managed by ICTA

- a. Creating the services to cover key functional areas of each public service entity
 - b. Devising different approaches for multiple channels such as unified front office (One-Stop-Shop), multipurpose kiosks, e-mail, web, voice, SMS, mobile services
 - c. Planning infrastructure facilities with availability, reliability, and scalability to ensure adequate bandwidth availability for users to reach government services and websites at all times²⁵
 - d. Adhering to as provisions of Electronic Transactions. Act, No. 19 of 2006, with amendments, for delivery of transactional services. (Electronic payments can be accepted by government organizations for the services offered).
 - e. Preparing standard procedure handbooks/process manuals for all digitally enabled services for all stakeholders in three languages i.e. Sinhala, Tamils, and English as appropriate
 - f. Providing information on the type of services provided, costs for such services, delivery time, etc are displayed in every service providing institution.
5. Collaborate with other institutions, state or non-state, local or international, for providing ‘connected government services’ for seamless client-centric service delivery by:
 - a. Participating organizations sharing data and working collaboratively on agreed governance and data sharing policy frameworks²⁶
 - b. Developing the necessary back-end and front-end applications for ensuring the availability of data and services required for providing seamless client-centric services
 - c. Providing raw data and/or data services to others as open data, in accordance with a data format such as ‘metadata’, which would not; breach national security, and organizational policies, violate privacy, be identifiable (persons, specific locations, etc) and breach any constitutional or legal requirements, adhering to the Open Data principles mutually agreed.
 6. Implement open and interoperability standards defined by National Data Exchange (NDX) and Lanka Interoperability Framework (LIFe)²⁷ to offer joined-up service delivery (citizen-friendly and seamless) by:

²⁵ ICTA is in the progression of transforming to a ‘Cloud First’ approach

²⁶ In order to facilitate this requirement, data owners should provide basic data to other government organizations for authentication as well as providing services based on mutual understanding. Privacy and confidentiality of such data should be maintained by the receiver.

²⁷ Refer Annexure VI – Lanka Interoperability Framework (LIFe)

- a. All government organizations using open standards to ensure interoperability, vendor neutrality, and flexibility in the development of Digital Government systems, purchasing IT products, and preservation of records²⁸
7. All government organizations must follow the open data policy and share their own with the other government organizations, and even with the private sector, as appropriate and following the available legislation at the moment²⁹.

²⁸ All government organizations must identify the information domains that they belong to and adopt and implement interoperability standards accordingly conforming to the standards specified in National Data Exchange (NDX) and Lanka Interoperability Framework (LIFe).

²⁹ Data Protection Act No.19 of 2022, in particular.

3.6 POLICY PRINCIPLES, STATEMENTS AND GOALS # 6

“Digital Governance is a means for change, not an end goal in itself. It is a continuous Innovative Transformation that continuously researches for and implements advanced end-to-end technological solutions in making the society a more cultured, enlightened, compassionate, healthier and sustainable place to live.”

Digital Government develops incessantly, with the public always aspiring for higher service quality. This calls for continuous review, development, and update of solutions with time. Innovation is the action to innovate, i.e. to constantly improve the existing, in contrast to the invention, which aims to create new. For this, it is essential to maintain a strong workforce of ICT professionals within the government continuously nurturing them. It also follows that all fresh activities are supported by research and development.

Achievement of these necessitates:

1. Appoint, by each Head of the organization, as defined by the Digital Transformation Roadmap of the organization, a Chief Digital Information Officer (CDIO) who will be the organization’s focal point for its Digital Government transformation process.
2. Make CDIO a role that brings together the experience and skills-set of the Chief Information Officer and the Chief Digital Officer responsible for leading all aspects of IT and digital strategy, as an evangelist and facilitator, with hands-on experience of a competent and positive individual; in par with the government digital competency framework.
3. Promote and develop ICT activities within the organization, by the CDIO, as the interface for ICT programs and projects, interconnecting the government organizations with other state and private organizations by:
 - a. Researching and determining the Digital Government requirements within the organization
 - b. Bringing the ICT development requirements to the notice of the higher management
 - c. Liaising on the organization’s implementation of Digital Government with the designated officer at ICTA³⁰ at least once in every three months or as and when necessary
 - d. Providing technical direction to the organization by identifying the current level of Digital Government maturity and improving the same

³⁰ Refer Annexure III – Information and Communication Technology Agency of Sri Lanka (ICTA)

- e. Be overall responsible for the information and communication technological operations of the organization, for outsourced ICT projects, and be responsible for managing the implementation life-cycle of such projects.
4. Implement and maintain a proper information systems governance framework for all Digital Government solutions by:
 - a. Drafting and implementing, under the leadership of each CDIO, an annual and a short-term ICT plan which enunciates how ICT is to be used in realizing the vision and mission of the organization while considering the development costs of such applications.
 - b. Allocating adequate funds, in conjunction with ICTA³¹ (to avoid duplication), in its annual budget for ICT procurements and sufficient funds for the maintenance of existing equipment, systems, and networks
 - c. Formulating and establishing a Project Steering Committee (PSC) whenever a Digital Government project is implemented, by each head of the department to ensure stakeholders' commitment, participation, assistance, and collaboration
 - d. Adopting, implementing, and maintaining a proper information systems governance framework to ensure successful implementation of Digital Government solutions.
 - e. Taking necessary steps to ensure continuity of projects when employees involved in ICT projects are transferred/retired either within or between organizations
 - f. Assigning a “shadow” officer – an officer who would be aware of all aspects of the ICT system for each officer involved in a Digital Government project for all officers whose skills are critical to the successful implementation of a project, to be used in case the latter is transferred, leaves, or is promoted
 - g. Ensuring that there is a period of handing over of duties when an officer-involved in an ICT project is transferred
 - h. Developing and implementing a plan to ensure continuity of ICT projects and to ensure the availability of information at the required level and the required time
5. Adhere to correct procurement policies, guidelines, and practices as stipulated by Treasury and further by:
 - a. Implementing software and hardware development for government by the external vendor(s) only after entering into contractual agreements
 - b. Consulting ICTA³² before embarking on any major ICT project (total estimated cost over Rs.10 million), to;

³¹ Refer Annexure III – Information and Communication Technology Agency of Sri Lanka (ICTA)

- i. ensure that they conform with general standards applicable to all government organizations, especially concerning interoperability and localization requirements, and
- ii. ensure that such projects can be fully integrated into the government wide ICT system.

If a government organization deems that ICTA advice is necessary for any project, even of less than Rs.10 million, they can refer the same to ICTA.

- c. Referring to standard technical specifications presented by ICTA, at its website www.icta.lk when procuring hardware items such as desktop computers, laptop computers, printers, etc.
- d. Carrying out procurement of information systems, ICT equipment, software, software development, and consulting services, as per the applicable ‘Procurement Manual and Guidelines’ of the Procurement Division of the Department of Public Finance, Ministry of Finance, or any successor thereto, and in accordance with other related regulations³³
- e. Facilitating the submission of open source based proposals for Digital Government projects, as appropriate, as open-source software, many a time, offers more cost-effective software application options for government. Such facilitation should meet the following criteria. In the event of not meeting them, fully or partially, the approach should always be toward the financially competitive market solutions, to ensure total cost-effectiveness and sustainability.
 - i. Return on Investment (ROI) and Total Cost of Ownership (TCO) are favorable for the government
 - ii. Implementability is easier when compared with other solutions
 - iii. International security standards are met

However, it is the sole discretion of the government organization to decide the most suitable mechanism i.e. open source or market solutions, in consideration of the aforementioned aspects.

- f. Evaluating ROI for 3-7 years, depending upon the size and the nature of the project, to assess the cost-effectiveness of proposals

³² Refer Annexure III – Information and Communication Technology Agency of Sri Lanka (ICTA)

³³ Guidance from ICTA could be obtained in relation to the operational aspects of procurement. In major (total estimated cost over LKR 10 million, enterprise level solutions) ICT projects, the Procurement Committee could include one person nominated by ICTA.

- g. Entertaining project proposals that proposes only licensed software either proprietary or open-source³⁴
 - h. Ensuring the transfer of ownership of Intellectual Property Rights to the government, whenever possible, in software development for the government
 - i. Installing software on desktops, only by a systems administrator or authorized persons to do so, without violating intellectual property rights
 - j. Following the periodic regulations issued by the relevant ministries including the Ministry of Finance
6. Ensure the usage and security of the Internet and intranet by adopting adequate management and security policies by:
- a. Implementing Internet/Intranet usage policies to guide users on Internet/Intranet usage complying with the policies and codes of conduct of the organization
 - b. Maintaining organizational information security adhering to the Information and Cyber Security Policy for Government Organizations published by SLCERT.
 - c. Creating LAN and e-mail accounts only after clearance by the organization's management and disabling them on the same day of an employee's departure from the organization
 - d. Defining standard formats for the LAN accounts and the names of the PCs and servers in the network
 - e. Providing adequate backup facilities to ensure that all essential information and software can be recovered following a disaster or a media failure
 - f. Using LGN facilities (mandatory option for all government organizations to provide Internet for staff) appropriately
 - g. Adhering to LGN policies on Internet and Intranet usage; particularly in assigning, controlling, and monitoring Internet access
7. Implement necessary HR development plans to ensure successful Digital Government implementation by:
- a. Assessing the human resource capacity building needed for all levels of staff, by effectively deploying the 'Digital Competency Framework', to address organizational requirements for Digital Transformation on an annual basis.

³⁴ Use of software without a valid license or making modifications and carrying out customizations to licensed software without adhering to the license conditions would be contrary to the Intellectual Property Act of 2003 and would result in legal penalties (both criminal and civil liability)

- b. Incorporating a substantial component for Digital Transformation related to human resource capacity building into the organizational HR plan
 - c. All officers, including senior management and middle management staff in Government organizations, be competent in the use of ICT in their daily work, and necessary awareness and training be provided to achieve this competency
 - d. Implementing, by senior management, suitable incentive schemes for staff who are proficient in ICT and/or obtain relevant qualifications in ICT
 - e. Encouraging, by senior management, all staff in government organizations to obtain government approved computer qualifications
 - f. Ensuring that Chief Digital Information Officers (CDIOs) gain sufficient knowledge in Digital Government and ICT, particularly on emerging technologies
 - g. Guaranteeing continuous development of government staff of all emerging technologies and trends
8. Carry out by government organizations a Risk Assessment exercise for every Digital Government project.
9. Carry out effective monitoring and evaluation by all government organizations, for the outputs and outcomes of their Digital Government projects, on appropriate M&E frameworks and indicators as discussed and agreed with ICTA.
10. Formulate and implement by each government organization, a communication plan for disseminating Digital Government information to all stakeholders, assisting users of Digital Government services; building the trust and confidence of users of Digital Government services, and assessing the satisfaction levels of users.
11. Encourage, by government organizations and government officers, the support and promotion of the national digital transformation process, contributing to positively embrace the same towards a conducive environment.

Annexure I. Presidential Secretariat circular PS/GPA/Circular/01/2020

ජනාධිපති කාර්යාලය
சனாதிபதி அலுவலகம்
PRESIDENTIAL SECRETARIAT



My No: PS/GPA/Circular/01/2020
 January 13, 2020

To: All Secretaries of Ministries
All Secretaries of State Ministries
All Chief Secretaries
All Secretaries to Governors
All Heads of Departments
All Heads of Statutory Organizations

Positioning the Information and Communication Technology Agency (ICTA) of Sri Lanka to drive National Digital Initiatives of the Government

It has been observed that many government agencies are implementing information technology based solutions in isolation and in a compartmentalized culture of service delivery. This, in addition, has resulted in a lack of a cohesive, coordinated approach to build a whole-of-government framework where data should be shared across systems for providing citizen-centric services effectively and efficiently.


Furthermore, despite such initiatives outcomes have not been efficient, cost effective and public centric. Instead, due to the demand for extra employees, buildings and logistic facilities, service delivery cost has risen. It has also led to wasteful public expenditure programmes in the national budget. This compartmentalized strategy has also tapped foreign funding from different sources, engaged consultants and project management teams, and created wasteful expenditure on non-compatible systems and equipment.

In this background, His Excellency the President has directed that all ICT/digital solutions having an impact on citizen service delivery should be implemented under the overall management and supervision of the Information and Communication Technology Agency (ICTA) of Sri Lanka to ensure the following:

- Provide public service delivery to the people in a cost-effective and people-friendly manner.
- Ensure full compliance with the National Digital Policy and strategies of the government adopted by the Cabinet of Ministers from time to time.
- Ensure optimal use of national-level ICT infrastructure (Lanka Government Cloud, Lanka Government Network, Payment Gateway, SMS gateway etc) as defined by the ICTA from time to time.
- Ensure compliance with the technical and data architecture and standards formulated by the ICTA and approved by the Cabinet of Ministers from time to time.
- Ensure compliance with digital law requirements such as the Electronic Transactions Act and data protection legislation.
- Eliminate duplication of IT related work by several agencies and minimize the cost of repeated data collection and data entry efforts.
- Enforce digital identity sharing to avoid inconvenience to citizens who transact online.

1/2

Please convey the above instructions to all organizations and Project Directors under your purview and instruct to transfer such projects and programmes, including financial provision to the ICTA in a suitable manner in consultation with the Treasury regarding transfer of funding procedure. Any queries in the above regard may be directed to Chief Executive Officer of ICTA (email: ceo@icta.lk) with copy to Chairman, ICTA (email: chairman@icta.lk).


P B Jayasundera
Secretary to the President

CC: Secretary to the Prime Minister
Secretary to the Cabinet of Ministers
Secretary to the Treasury
Auditor General
Chairman, Information and Communication Technology Agency (ICTA) of Sri Lanka

Annexure II. Linkage of Digital Government Ambitions to Associating Good Governance Principles Council of Europe ELoGE model

No.	Title	Digital Government Ambition	Associating Good Governance Principles (out of the 12, as specified by the Council of Europe ELoGE model ³⁵)
1	Citizen Convenience	Citizen is central and paramount to Digital Governance. All e-government services, be them informational or transactional, will be devised for Citizen Convenience – be them individuals or businesses.	<p>Principle 2: Responsiveness</p> <p>Objectives, rules, structures, and procedures are adapted to the legitimate expectations and needs of citizens.</p> <p>Public services are delivered, and requests and complaints are responded to within a reasonable timeframe.</p>
			<p>Principle 3: Efficiency and Effectiveness</p> <p>Results meet the agreed objectives.</p> <p>The best possible use is made of the resources available.</p> <p>Performance management systems make it possible to evaluate and enhance the efficiency and effectiveness of services.</p> <p>Audits are carried out at regular intervals to assess and improve performance.</p>
2	Cost Savings	Digital Governance is aimed at substantial Cost Savings in producing meaningful outcomes for the society, in terms of finance, time, and	<p>Principle 7: Competence and Capacity</p> <p>The professional skills of those who deliver governance are continuously maintained and</p>

³⁵ <https://www.coe.int/en/web/good-governance/12-principles-and-elope>

No.	Title	Digital Government Ambition	Associating Good Governance Principles (out of the 12, as specified by the Council of Europe ELoGE model ³⁵)
		environment, by proactively re-engineering the processes for efficacy and efficiency.	<p>strengthened to improve their output and impact.</p> <p>Public officials are motivated to continuously improve their performance.</p> <p>Practical methods and procedures are created and used to transform skills into capacity and to produce better results.</p> <hr/> <p>Principle 10: Sound Financial Management</p> <p>Charges do not exceed the cost of services provided and do not reduce demand excessively, particularly in the case of important public services.</p> <p>Prudence is observed in financial management, including in the contracting and use of loans, in the estimation of resources, revenues, and reserves, and in the use of exceptional revenue.</p> <p>Multi-annual budget plans are prepared, with the consultation of the public.</p> <p>Risks are properly estimated and managed, including by the publication of consolidated accounts and, in the case of public-private partnerships, by sharing the risks realistically.</p> <p>The local authority takes part in</p>

No.	Title	Digital Government Ambition	Associating Good Governance Principles (out of the 12, as specified by the Council of Europe ELoGE model ³⁵)
			arrangements for inter-municipal solidarity, fair sharing of burdens and benefits, and reduction of risks (equalization systems, inter-municipal cooperation, mutualization of risks...).
3	Citizen Participation	Active Citizen Participation in Digital Governance will make the solutions more inclusive. Citizens' needs for information and services are respected and delivered to the best of their expectations.	<p>Principle 1: Fair Conduct of Elections, Representation, and Participation</p> <p>Local elections are conducted freely and fairly, according to international standards and national legislation, and without any fraud.</p> <p>Citizens are at the centre of public activity and they are involved in clearly defined ways in public life at the local level.</p> <p>All men and women can have a voice in decision-making, either directly or through legitimate intermediate bodies that represent their interests. Such broad participation is built on the freedoms of expression, assembly, and association.</p> <p>All voices, including those of the less privileged and most vulnerable, are heard and taken into account in decision-making, including over the allocation of resources.</p> <p>There is always an honest attempt to mediate between various legitimate interests and to reach a</p>

No.	Title	Digital Government Ambition	Associating Good Governance Principles (out of the 12, as specified by the Council of Europe ELoGE model ³⁵)
			<p>broad consensus on what is in the best interest of the whole community and how this can be achieved</p> <p>Decisions are taken according to the will of the many, while the rights and legitimate interests of the few are respected.</p> <hr/> <p>Principle 4: Openness and Transparency</p> <p>Decisions are taken and enforced as per rules and regulations.</p> <p>There is public access to all information that is not classified for well-specified reasons as provided for by law (such as the protection of privacy or ensuring the fairness of procurement procedures).</p> <p>Information on decisions, implementation of policies, and results are made available to the public in such a way as to enable it to effectively follow and contribute to the work of the local authority.</p>
4	Organized Society	Digital Government will make an Organized Society, free from bribery and corruption achieved with openness and responsiveness.	<p>Principle 5: The Rule of Law</p> <p>The local authorities abide by the law and judicial decisions.</p> <p>Rules and regulations are adopted following the procedures provided for by law and are enforced impartially.</p>

No.	Title	Digital Government Ambition	Associating Good Governance Principles (out of the 12, as specified by the Council of Europe ELoGE model ³⁵)
			<p>Principle 11: Human rights, Cultural Diversity and Social Cohesion</p> <p>Within the local authority's sphere of influence, human rights are respected, protected, and implemented, and discrimination on any grounds is combated.</p> <p>Cultural diversity is treated as an asset, and continuous efforts are made to ensure that all have a stake in the local community, identify with it, and do not feel excluded.</p> <p>Social cohesion and the integration of disadvantaged areas are promoted.</p> <p>Access to essential services is preserved, in particular for the most disadvantaged sections of the population.</p>
5	Protection of Citizens' Rights	Digital Government guarantees the Protection of Citizens' Rights by the implementation of strong legal frameworks.	<p>Principle 6: Ethical Conduct</p> <p>The public good is placed before individual interests.</p> <p>There are effective measures to prevent and combat all forms of corruption.</p> <p>Conflicts of interest are declared on time and persons involved must abstain from taking part in relevant decisions.</p> <p>Principle 12: Accountability</p>

No.	Title	Digital Government Ambition	Associating Good Governance Principles (out of the 12, as specified by the Council of Europe ELoGE model ³⁵)
			<p>All decision-makers, collective and individual, take responsibility for their decisions.</p> <p>Decisions are reported on, explained, and can be sanctioned.</p> <p>There are effective remedies against maladministration and against actions of local authorities which infringe civil rights.</p>
6	Innovative Transformation	Digital Governance is a means for change, not an end goal in itself. It is a continuous Innovative Transformation that continuously researches for and implements advanced end-to-end technological solutions in making society a more cultured, enlightened, compassionate, healthier, and sustainable place to live.	<p>Principle 8: Innovation and Openness to Change</p> <p>New and efficient solutions to problems are sought and advantage is taken of modern methods of service provision.</p> <p>There is a readiness to pilot and experiment with new programs and to learn from the experience of others.</p> <p>A climate favorable to change is created in the interest of achieving better results.</p>
			<p>Principle 9: Sustainability and Long-term Orientation</p> <p>The needs of future generations are taken into account in current policies.</p> <p>The sustainability of the community is constantly taken into account.</p> <p>Decisions strive to internalize all</p>

No.	Title	Digital Government Ambition	Associating Good Governance Principles (out of the 12, as specified by the Council of Europe ELoGE model³⁵)
			<p>costs and not to transfer problems and tensions, be they environmental, structural, financial, economic, or social, to future generations.</p> <p>There is a broad and long-term perspective on the future of the local community along with a sense of what is needed for such development.</p> <p>There is an understanding of the historical, cultural, and social complexities in which this perspective is grounded.</p>

Annexure III. Information and Communication Technology Agency (ICTA)

Information and Communication Technology Agency of Sri Lanka (ICTA) as the implementation agency of Digital Government policy has been entrusted with implementing a detailed road map in line with the vision of the government to establish a digitally inclusive Sri Lanka, with a citizen-centric Digital Government for the convenience of every Sri Lankan.

This has made ICTA a high-level entity for providing National Level Guidance and Co-ordination for National Priorities including providing efficient and citizen-centric services with the simplification of market processes and state mechanisms; expanding Digital Governance using Information Technology as a knowledge exchange tool; establishing of international e-commerce and e-payment systems and designing new laws and organizational frameworks Data Protection, Cyber Security and Intellectual Property Rights.

Information and Communication Technology Agency of Sri Lanka (ICTA) was established in July 2003 and according to Information and Communication Technology Act No. 27 of 2003, (ICT Act), ICTA was identified as the legal successor to CINTEC and became the apex ICT institution of the Government, presently functioning within the purview of the Ministry of Technology.

Under the ICT Act No. 27 of 2003 ICTA was empowered to formulate and implement strategies and programs in both the Government and the private sector and pursuant thereto ICTA prepared programs and strategies on Information and Communication Technology, which are presently embodied in the “e-Sri Lanka Development Project”.

The “e-Sri Lanka Development Project”, formulated during the period 2002-2005, is aimed at taking the dividends of ICT to all segments of Sri Lankan society and furthering the socio-economic development of the nation. Through the implementation of this multi-donor funded project an enabling environment is being created, where government works in partnership with stakeholders to create the necessary infrastructure and establish e-government services.

In October 2004 the Cabinet of Ministers identified the “e-Sri Lanka Development Project” as the National Information Technology Action Plan of the Government, and further strengthened ICTA's legal mandate in the following manner:

- Specific authorization and mandate for ICTA to implement all the components of the e-Sri Lanka Development Project;
- Authorize ICTA to recommend to the Cabinet of Ministers the appropriate policy and regulatory framework required for the implementation of the e-Sri Lanka development project and to support ICT development in Sri Lanka; and
- Authorize ICTA to periodically review the above program components and make such modifications as may be required from time to time in keeping with the Policy as approved by the government.

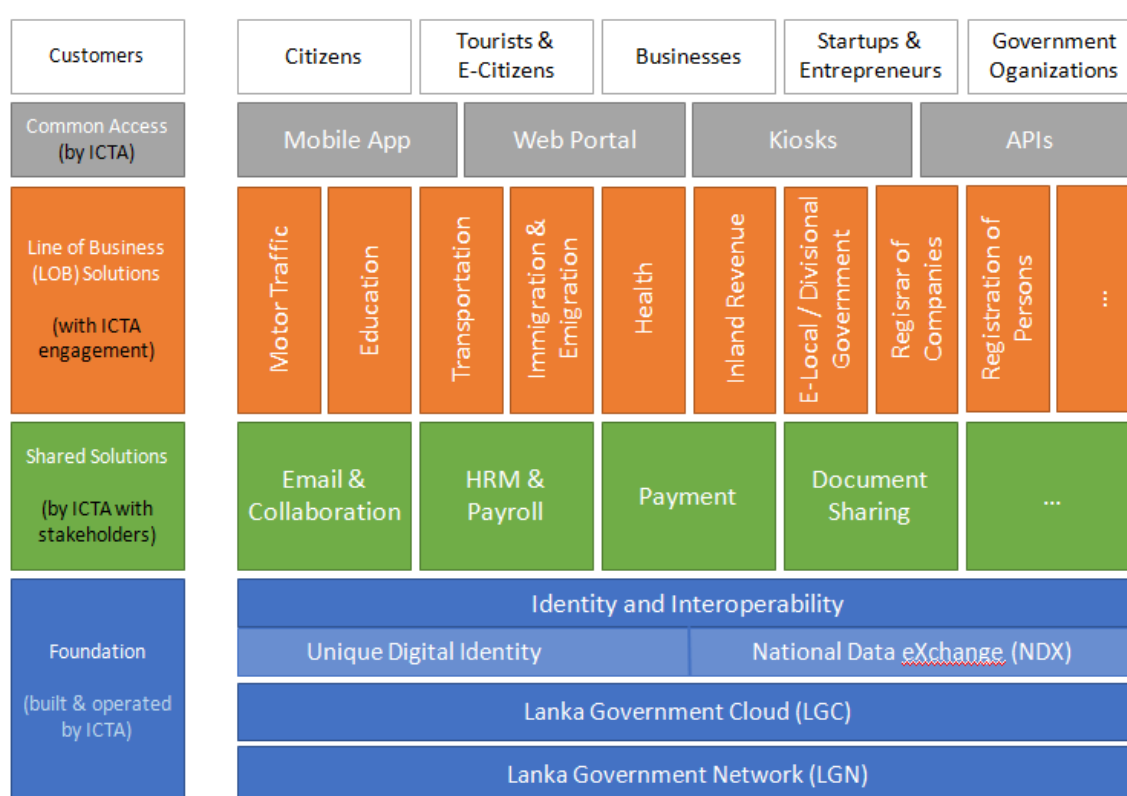
Subsequently, the Information and Communication Technology (Amendment) Act, No. 33 of 2008 Act has empowered ICTA to submit recommendations to the Inter-Ministerial Committee for formulating the National ICT Policy Framework for submission to the Cabinet of Ministers for their approval.

Currently, ICTA is under the Ministry of Technology, with HE the President himself as the Minister.

Annexure IV. ICTA's Approach to Digital Government as per the Digital Government Transformation Roadmap Approved by the Cabinet

One of ICTA's key directives, Digital Government, is the transformation process of state organizations, to make them more efficient, effective, profitable, and sustainable. The digital transformation, which is being planned and will be executed by ICTA, would increase the adaptability and connectivity of state entities, helping them to easily integrate with other systems.

ICTA has already drawn up the digital governance architecture, which has several layers i.e. foundation, shared solutions, Line of Business solutions, common access, and users. While the Foundation layer is the ICT Agency's sole responsibility, they will work with various partners in implementing other layers. The foundation layer is now in process with the setup of the Lanka Government Network and the Lanka Government Cloud where solutions for all state organizations would be stored. ICTA is now developing the Identity and Interoperability Platform and National Spatial system which will complete the foundation layer of digital governance.



Once this is developed, state organizations will be able to collaborate and share key information to carry out their functions. For example, someone needing an identity card or passport in the

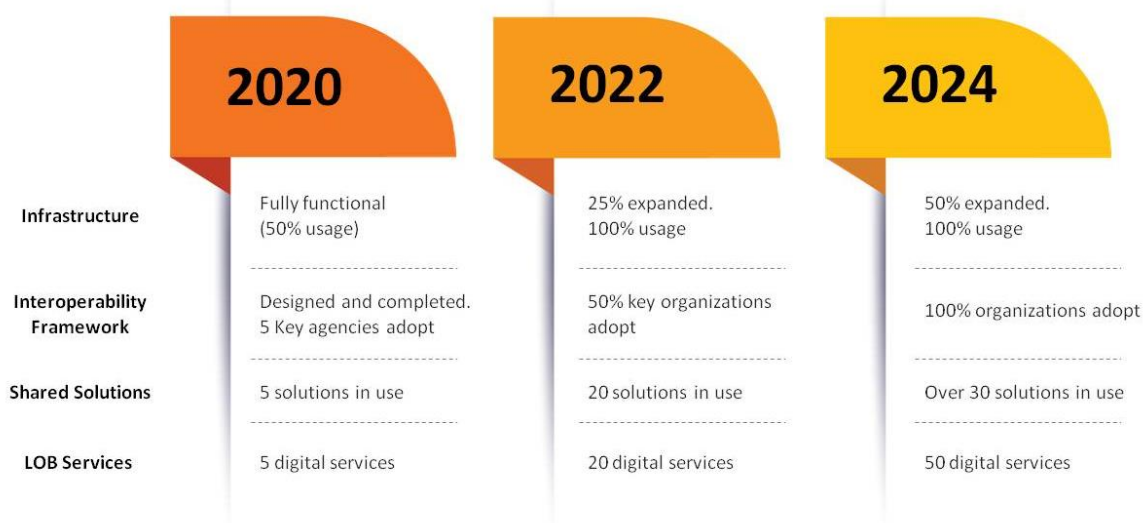
current scenario has to go to several government institutions i.e. the ‘grama-niladhari’, passport office, registrar’s office, back to the grama-niladhari, etc., to get the job done. With National Data Exchange (NDX), the issuing department would be able to access all relevant information, even data owned by other state departments to handle the task at hand.

The National Spatial Data Infrastructure (NSDI) is another key platform that facilitates interoperability, collaboration, and consistency amongst government organizations for the achievement of efficiency and effectiveness in government. It enables spatial data standardization; avoiding data duplication, improving data quality as well as transparency in data sharing across government organizations, and providing a technological platform for developing spatial data decision support tools. The effective utilization of the NSDI by the government organizations would uphold and promote the digital transformation process within the government.

The Identity Interoperability Platform, the foundation for all digital solutions, helps to digitally establish and validate the identity of persons. For example, if a citizen wants a driver’s license, the application is filled online and the relevant government organization will access all necessary data to confirm the applicant’s identity and eligibility i.e. birth, health, and other information from the relevant organizations, to process the application.

Shared Solutions is the next layer in ICTA’s digital transformation strategy and it covers all the solutions used by most state organizations for their day-to-day operations, such as email collaboration, payroll, human resources management, and payments. While the agency will design and develop some of these solutions, they will also use different service providers. The Line of Business (LOB) solutions layer is another key area in digital government that deals with government processes. ICTA will initially select ten to twelve areas to spearhead high-impact projects, to execute on a turnkey basis. While the design and architecture of these projects will be the agency’s responsibility they will outsource development, implementation, and maintenance.

In selecting partners to develop shared and LOB solutions, the ICT agency plans to work with local private companies instead of engaging foreign partners. They will encourage Sri Lankan companies to develop solutions for motor traffic, education, transportation, health, and other sectors. In the event local expertise and capacity are not available within one entity, ICTA says they will encourage local enterprises to form consortiums to bid for developing solutions for the agency. ICTA will give priority to consortiums who work with startups and regional companies.



Once these solutions are developed by local organizations, they can be packaged, productized, and sold overseas, similar to the solution developed by a Sri Lankan company for the Colombo Stock Exchange. The company replicated and sold it to several stock exchanges across the world, including the London Stock Exchange. This is a model ICTA will emulate, to open up new opportunities for software companies that will have a tremendous impact on the local economy.

ICTA's vision is to deliver digital governance services to every citizen, and this is where the common access layer will play a role. It will be the interface between users and services provided via different solutions. For citizens who do not own a computer or are not tech-savvy, kiosks and communication centres will be set up in villages to assist them.

In order to ensure the achievement of planned/desired results under different Digital Government program components, it is essential to establish a comprehensive Results-Based Monitoring and Evaluation system across all program components. As part of this system, Digital Government projects require gathering diverse data with broad coverage first to establish baselines and then to measure outcomes and impact. To identify a holistic picture of the effort, the data requirements, responsibilities, methodologies, and frequencies will be developed for each project. To ensure the ownership, proper responsibilities, and accountability-related aspects, these will be validated with the key stakeholders through a participatory process.

Annexure V. Digital Government Policy Journey

The Government of Sri Lanka first recognized the need for the development of ICT through the National Computer Policy (COMPOL) of 1983. This first attempt was taken by the Natural Resources, Energy and Science Authority of Sri Lanka (NARESA) under the instructions of the then President. A committee appointed by NARESA produced the National Computer Policy.

The acceptance of COMPOL by the government gave rise to the establishment of the Computer and Information Technology Council of Sri Lanka (CINTEC), -later termed the Council for Information Technology - by a Parliamentary Act No. 10 of 1984, to function directly under the then President.

The first e-Government policy of Sri Lanka was approved by the Cabinet of Ministers in December 2009 to be adopted and implemented by all government organizations from 2010 through 2012. ICTA which was given the mandate by the Cabinet of Ministers to monitor the implementation, review the policy, and revise as necessary, conducted a series of conferences and workshops around the country involving government managers to create awareness of the content of the policy and approaches for implementation and review.

ICTA carried out annual reviews of the implementation of e-Government policy in 2010, 2011, 2012, and 2013. Regrettably, the rate of successful implementation of e-Government policy by government organizations has been extremely low, despite the efforts made by ICTA as well as participating organizations.

Having analyzed the reasons for low implementation, the following decisions were made by ICTA with the involvement of key stakeholders.

- The e-Government policy contained very complex policy requirements
- The policy was too extensive. It had 29 policy statements and 177 policy guidelines which should be implemented by all government organizations regardless of different e-Government maturity levels they are at.
- There was no clear identification of responsibilities with regard to the implementation of the policy.
- Chief Digital Information Officers (CDIOs) who are generally responsible for the implementation of the policy had no clear idea of how to do that. Moreover, CIOs had no authority to implement those.
- It was also not clear to the government why they should implement the policy. (Policy objectives were not clear)

The Digital Government Policy Review Committee

In order to draft the revised version of the policy, the then Chairman of ICTA appointed a Digital Government Policy Review Committee.

The policy review committee embarked on a journey to address the above issues while revising and updating the policy as and when necessary. In order to compile the policy statements and guidelines, the committees studied such requirements documented in other countries and the requirements included in the first version of the policy.

The committee agreed on a new theme for the policy and drafted 10 policy objectives under which the 32 policy statements were identified.

The committee appointed a Working Committee in order to draft the policy guidelines. The e-Government Policy Working Committee drafted policy guidelines, and identifies the responsibilities of the implementation of the policy by using the RACI (Responsible, Accountable, Consulted and Informed) matrix.

The Working Committee also identified a convenient approach for government organizations to implement the policy requirements and identify the e-Government maturity stage of their organizations.

Input from Consultative Process

Once the policy was drafted it was presented to government CIOs, Senior Managers of the government, ICT-based, and non-ICT-based private sector managers, academia, and civil society members for receiving a wider consultation. Moreover, a public consultation was requested and received for improving the policy by using public media.

The input of that consultative process went to two documents; one more internal, relatively more detailed and serves as an implementation guide for the public sector. The second, a relatively short document, with the same input, presents Digital Government to a more external audience, not necessarily constituting only the public sector, but still key stakeholders. So both are useful, but for two different audiences. This document also aligns itself with the National Digital Transformation Policy for Sri Lanka 2020-2024 of the Information and Communication Technology Agency of Sri Lanka that provides the high-level principles and conceptual framework for Sri Lanka to achieve sustained digital economic development and growth, through the creation of an Innovative Economy and an Effective Government.

More recently, the Policy document was reviewed for a second time to ensure its alignment with the new policy environment and the latest Information and Communication Technology developments by the following review committee.

1. Mr. Chandana Rodrigo – Additional Secretary, Ministry of Technology
2. Mr. A.K.R. Alawatta – Additional Secretary (Admin.), Ministry of Technology

3. Mr. Thushara Suraweera – Additional Secretary (Reforms), Ministry of Justice
4. Mr. T.R. Waruna Sri Dhanapala – Additional Secretary (Regional Administration Reforms), State Ministry of Home Affairs
5. Mr. Udesch Senevirathna – Senior Assistant Secretary, Prime Minister’s Office
6. Mr. Hiranya Samarasekara – Principal Advisor, Ministry of Technology
7. Mr. B.K. Prabath Chandrakeerthi – Commissioner General of Labor Department of Sri Lanka
8. Mr. Kancahana Thudugala – Chief Digital Government Officer, ICTA
9. Mr. Sameera Jayawardena – Associate Chief Digital Economy Officer, ICTA
10. Mr. Chanuka Wattegama – Director Policy, ICTA
11. Mr. Sanjee Balasuriya – Director Information Security, ICTA
12. Mr. Gavashkar Subramaniam – Director, Government Engagement, ICTA
13. Mr. M.C.M Farook – Director IT, TRCSL
14. Ms. Madhavi N. Gunawardana – Director, Administration and Corporate Affairs, TRCSL
15. Mr. Ranjan Marasinghe – Director Planning and ICT, Department of Wildlife Conservation
16. Mr. Lalith Waduge – Director ICT, Ministry of Education - Higher Education Division
17. Mr. Aloka Bandara – Director Public Administration
18. Ms. Samanthi Sennanayaka – Senior Lecturer, SLIDA
19. Ms. Shiranthi Ratnayake – Additional Director General, National Policy Planning

Annexure VI. Lanka Interoperability Framework (LIFe)

The Government of Sri Lanka is committed towards the achievement of a technology based society as articulated in the National Policy Framework. In order to succeed in that, it is of prime importance to establish a connected network of government services, government organizations, citizens and businesses. The said connectivity can be only achieved by way of establishing an interoperable framework which enables diverse information systems from different government organizations to seamlessly work in unison. This is where Lanka Interoperability Framework (LIFe) comes into life facilitating interoperability between different government platforms, entities and systems. ICTA drives the project on LIFe as the implementation agency.

It is a set of open standards to ensure the highest degree of operability and provide all government services through a single window. Presently, LIFe comprises of the following domains.

- Personal Domain
- Land Domain
- Vehicle Domain
- Project Coordination Domain

The development of health and education domains are currently ongoing in liaison with the respective domain ministries, leaving the following areas for future developments.

- Agriculture
- Transport
- Judicial
- Trade