Policy and Procedures for ICT Usage in Government
(e-Government Policy)

2009-12-02

Information and Communication Technology Agency of Sri Lanka (ICTA)
160/24, Kirimandala Mawatha, Colombo 00500, Sri Lanka
Phone +94 11 2369099, 2369100, Fax: +94 11 2369091
Email: GovICTPolicy@icta.lk
www.icta.lk

Table of Contents

(A) Introduction

A.1. Vision

The Government of Sri Lanka has developed the following vision for leveraging Information and Communication Technology (ICT) for the development of the government sector,

> *"To adopt ICT in all its aspects to make government more efficient and effective, improve access to government services, and create a more citizen centric government"*

A.2. Background

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) on 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 Information and Communication Technology Agency of Sri Lanka (ICTA) was established in July 2003 and pursuant 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 Presidential Secretariat.

Under the ICT Act No. 27 of 2003 ICTA was empowered to formulate and implement strategies and programmes 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 to further 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;

- Authorize ICTA to periodically review the above programme 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.

This document has been formulated consequent to the above mandates given to ICTA by the Cabinet in various forms as described above.

A.3. Objectives

This document is to serve as a set of policies and procedures for the government sector in using ICTs to achieve overall development within organizations and in delivery of government services. It will assist in benchmarking each organization’s activities against the Policy, which will enable organizations to identify the areas which need attention and where rectification needs to be carried out. It will also ensure consistency in ICT activities and practices. The Policy articulates the minimum requirements expected of government organizations, and government organizations could add on to this and create their own organizational ICT policies and procedures, within this Policy framework. Thus, the Policy is mandatory for providing a unified approach in implementing e-government services and achieving the following;

- Improved efficiency and effectiveness of government organizations in Sri Lanka thereby making each government organization’s budget go further.
- Ease and accessibility of government information and services for citizens, and other government organizations.
- Promote good governance.
- Develop ICT competence among government employees.
- Manage ICT resources in sustainable manner.

(B) Operational Framework

B.1. Timeframe

The implementation time frame is three years, commencing January 2009 and shall be extended from time to time, as determined by the government, with appropriate modifications. All government organizations should adopt the policy and procedures within the assigned time frame. The policies and procedures envisaged under this document will not be a static. It will be updated as frequently as required, taking into account changing trends in the environment, in technology, and changes in business processes.

B.2. Responsibility and ownership

ICTA is responsible for the formulation, maintenance and updating of the policies and procedures. Individual government organizations are responsible for adopting and implementation of the policies and procedures. ICTA is responsible for monitoring the implementation of the policies and procedures.

B.3. Scope

These policies and procedures should be followed by all government organizations; Ministries, government Departments, Provincial Councils, District Secretariats, and Divisional Secretariats and Local Authorities, government Corporations, Statutory Bodies, and Companies fully owned by government. This document should be adopted by each government organization and customized if necessary.

B.4. Process

The ICT Agency of Sri Lanka set up an ICT Policy Committee in November 2004 to formulate the first draft of policies and procedures for use of ICT in government.

After an internal review, the initial draft was presented in February 2005 to a representative gathering of stakeholders mainly comprising members of the ICTA Focus Groups and Working Groups. There was an extensive discussion on the policy and the views of the participants were taken into account and the policy was further modified. This document was later presented to approximately 150 Chief Innovation Officers (CIOs) of the Western Province on 2005-03-10 and to a group of CIOs and Re-engineering Government Focus Group members on 2008-07-22. The document was made available to the Public, on www.icta.lk in order to ascertain the views of a wider audience.

ICTA published advertisements in the newspapers inviting the views of the public and interested parties on the draft document. The views received as a consequence was considered by ICTA before finalizing and deploying this document. Comments were received from several government organizations, private organizations, citizens, associations, health personnel, etc. All comments were reviewed and discussed and the draft of this document was amended incorporating relevant recommendations.

(C) Enabling Legal Environment

The issue of formulating and incorporating into the country’s legal system suitable measures relating to ICT, so as to promote the development of ICT, and to create a facilitating legal environment is presently being addressed by ICTA. In this regard, ICTA is carrying forward the work originally undertaken by CINTEC, consequent to specific mandates given to ICTA by the Cabinet of Ministers.

C.1. Electronic Transactions Act

The most relevant legislation for use of ICT in government and establishment of e-government services is the Electronic Transactions Act No. 19 of 2006. The drafting of Electronic Transactions legislation was enabled through a joint Cabinet Memorandum of the Prime Minister, the Minister of Trade and Commerce and the Minister of Science and Technology. Consequently, on 22nd September 2004 the Cabinet of Ministers decided that legislation on Electronic Transactions should be prepared through the Legal Draftsman's Department in conjunction with ICTA. The legislation was prepared by the Legal Draftsman with legal and policy inputs from ICTA and presented to Parliament on 7th March 2006. The Electronic Transactions Act was brought into operation with effect from 1st October 2007 (vide Gazette Extraordinary No. 1516/25 of 27th September 2007).

The Electronic Transactions Act No. 19 of 2006 is based on the standards established by United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) and Model Law on Electronic Signatures (2001).

The objectives of the Act as are as follows

1. to facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty;
2. to encourage the use of reliable forms of electronic commerce;
3. to facilitate electronic filing of documents with government and to promote efficient delivery of government services by means of reliable forms of electronic communications; and
4. to promote public confidence in the authenticity, integrity and reliability of data messages and electronic communications. This has ensured that electronic communication is officially and legally accepted as a proper means of communication (emphasis added).

Based on this Act steps could now be taken by government organizations to provide services by electronic means as well as to retain data and information in electronic form.

As a follow-up to the enactment of the Electronic Transactions Act, Sri Lanka became one of the first three countries in the Asian Region (and first country in South Asia) to sign the *United Nations Convention on the Use of Electronic Communications in International Contracts* (commonly known as the e-Contracting convention). This was consequent to a Cabinet decision initiated by the Ministry of Science and Technology.

The Convention aims to enhance legal certainty and commercial predictability where electronic communications are used in relation to international contracts. It addresses the determination of a party's location in an electronic environment; the time and place of dispatch and receipt of electronic communications; the use of automated message systems for contract formation; and the criteria to be used for establishing functional equivalence between electronic communications and paper documents – including "original" paper documents – as well as between electronic authentication methods and hand-written signatures.

As another necessary follow up action, ICTA is in the process of setting up a Certifying Authority for issuing digital signatures for Sri Lankan government organizations and citizens to ensure the authenticity and Non-repudiation.

C.2. Computer Crimes

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 Bill was presented in Parliament and debated on 23rd August 2005 and thereafter extensively revised by the Parliamentary Standing Committee “B”. It was enacted as legislation in May 2007 and certified by the Speaker of Parliament on 9th July 2007.

The basis of the Computer Crimes Act No. 24 of 2007 is to criminalise attempts at unauthorised access to a computer, computer programme, data or information. It also contains a provision to deal with unauthorised use of computers regardless of whether the offender had authority to access the computer.

The Act creates offences for unauthorised modification, alteration or deletion of information and denial of access, which makes it an offence for any person to program the computer in such a manner so as to prevent authorised persons from obtaining access. Other offences sought to be created under the proposed Act include causing damage or harm to the computer by the introduction of viruses and logic bombs etc, unauthorised copying of information, unauthorised use of computer service and interception of a computer programme, data or information while it is been transmitted from one computer to another.

The Act introduces a new regime for the investigation of offences. Provisions have been made in the Act to designate a panel of ‘Experts’ to assist the Police in the investigation of computer crime offences.

C.3. Data Protection

Data protection rules have become an increasingly important legal regime in an information age where personal data has become a significant asset of many companies, especially those operating over the Internet. However, in a connected global economy, national data protection rules can be easily circumvented and protections granted to the citizens lost as data is transferred out of the jurisdiction. In an attempt to prevent such circumvention, the EU data protection regime contains provisions controlling the transfer of personal data to non-EU countries, such as Sri Lanka.

At present the Government is pursuing a policy based on the adoption of a Data Protection Code of Practice, encompassing the private sector, with the possibility of the code being placed on a statutory footing through regulations issued under the Information and Communication Technology Act of 2003. As such, this approach can be seen as self- or co-regulatory approach. (Refer section 0103)

C.4. Intellectual Property Rights (IPR)

As regards the protection of intellectual property rights (IPR), the Intellectual Property Act no. 36 of 2003 replaced the Code of Intellectual Property Act no. 52 of 1979. The IP Act of 2003 contains several new features in relation to the protection of software, trade secrets and integrated circuits. (Refer Sections 0204 and 0205 of this document for detail)

Section 1: ICT Management

0101: ICT Governance

The organization's senior management, structures and processes shall ensure that the organization's ICT supports, sustains and extends the organization's goals, objectives and strategies.

010101: ICT Unit: Each government organization should set up an ICT Unit within the organization. The size and structure of the ICT Unit may vary, depending on the ICT requirements of the organization and the extent to which ICT activities/projects are outsourced.

010102: Roles and Responsibilities within the ICT Unit: The ICT Unit should be 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.

010103: Central ICT Support Unit: Government has set up a central data center under Lanka Government Network, comprising staff who are proficient in ICT, to provide technical advice and support (e.g. hardware, software, networking and communications) to government organizations, as required.

010104: Appointment of CIO: Each government organization should appoint a Chief Innovation Officer (CIO). The CIO should be the organization's focal point for ICTA's Re-engineering Government programme. He/she should be an officer at the second level of the hierarchy in the organization and report to the Head of the organization, or to the Secretary, in respect of a Ministry. He/she should be the Head of the ICT Unit, with of the core business of the organization and with at least minimum level of ICT knowledge.

010105: Responsibilities of CIO: The CIO shall be responsible for the promotion and development of ICT within the organization, and shall be the interface in respect of ICT related programmes and projects on which the government organization is interconnected with other organizations. CIOs should liaise on the organization's implementation of e-government with the designated person at ICTA at least once every three (3) months or as and when necessary. The following teams should report to the ICT Unit Head: Technical operations, Project Management and Outsourcing, Planning and ICT Policies, Business Operations, and Outsourced vendors who provide services to implement and operate ICT systems. The CIO should be responsible for the implementation of this policy by the year 2011.

010106: Each government organization should draft and implement an annual ICT plan which enunciates the way in which ICT is to be used in realizing the vision and mission of the organization. The plan should include the annual plan for ICT procurements. The ICT plan could be part of the main business plan of the organization. The plans should be made available, as far as possible, to other government organizations, to minimize the risk of overlap and to maximize the reuse of ICT solutions. The CIO should be responsible for drafting and implementing the ICT Plan for the organization (also refer section 0203).

0102: Information Lifecycle Management

The Government organization shall be committed to complying with relevant record keeping laws, regulations, and standards, which will apply to all records regardless of format, including paper and electronic records.

010201: Government Information Systems should be able to capture and store data in any of the three languages, i.e. Sinhala, Tamil and English. Furthermore all Government Information Systems should be able to produce correspondence to its clientele in their preferred language out of the above mentioned languages.

010202: In order to achieve the completeness of the data set, all such data should be transliterated and translated to English language and stored in English Language, regardless of the data input and capture language. (For details on Transliteration visit www.icta.lk/technology/transliterator).

010203: The Multilingual Data of Government Information Systems should be maintained in all three languages.

010204: Migration into electronic format: Data available in participating government organizations to be collected, inspected, updated, structured in the required format, and cleansed and its integrity ensured before being migrated into electronic format.

010205: Retention of records: The information created and stored by the organization's information systems must be retained, stored and archived, in conformity with the relevant provisions of the National Archives Act No. 48 of 1973, any amendments thereto, and with Section 15 of the Information technology, Security techniques - Code of Practice for information security management, ISO/IEC 17799. (Refer Annex 1). The relevant guidelines of the International Council of Archives (ICA) pertaining electronic storage of documents adopted from time to time by the National Archives Department shall also be complied with.

010206: Electronic records should be retained in such a manner so as to retain their accessibility and usability, integrity and authenticity, and their legal admissibility and evidential weight.

010207: Electronic records should be maintained in such a manner to ensure confidentiality and prevent unauthorized access, modification, alteration or deletion / removal.

010208: Electronic records should be maintained in such a manner to ensure that they are complete in content and contains the related information necessary for the organization's business and transactions.

010209: Information systems should meet with available standards for internal and government audit requirements and with the relevant provisions of the National Archives Act no. 48 of 1973, and any amendments thereto.

010210: Data migration between platforms: Organizations should develop a preservation strategy that ensures accessibility and scalability to ensure seamless migration of existing records between technological platforms as software and hardware get replaced. Use of open standards, (refer Annex 3) where the specifications are public and without restrictions in their access or in implementation, for preservation is recommended.

010211: Meta data standards: Information should be retained to ensure maximum consistency of metadata across government organizations.

010212: Representation of dates and time in documents: Dates, time and time zone should be specified as in ISO 8601 – the international standard for representation of dates and time. The international standard date notation is; YYYY-MM-DD, where YYYY is the year in the Gregorian calendar, MM is the month of the year and DD is the day of the month. The international standard notation for the time of day is hh:mm:ss.

010213: The government organization shall ensure all staff is aware of the organizations' electronic record-keeping requirements; and required training for staff shall be provided.

010214: Requirements for retention/ preservation of records in electronic form as well as requirements for originality in the context of electronic documents are prescribed under Section 5 and 6 of the Electronic Transactions Act No. 19 of 2006.

010215: Electronic records shall be deleted/destroyed only under the normal administrative practices of the organization, and in compliance with the applicable laws and regulations.

0103: Protection of personal data

The Government organization should handle personal information on citizens in conformance to the relevant laws, codes of practice, regulations, and standards.

010301: Personal data and information should be retained in the manner and for as long as it is required as per laws, regulations and rules governing such data and information. Such data and information should be divulged only in accordance with rules and regulations governing such release. (The Data Protection Code of Practice when available, would provide appropriate guidelines).

010302: Email addresses of citizens gathered from government web sites should not be divulged, made available or sold to third parties.

010303: Personally identifiable information obtained through government web sites shall not be kept for longer than is necessary for the purpose for which it was obtained.

0104: Standards

Standards will be used in government organizations for the improvement of interoperability and efficiency of the government organization.

010401: The Sri Lanka Standards Institution (SLSI), established under Act No. 6 of 1984, will be responsible for introducing relevant standards to government organizations and also to ensure easy and prompt accessibility of standards to users and developers.

010402: Government organizations should use standards as adopted by SLSI in order to ensure full interoperability, and participation of all stakeholders.

010403: Government organizations should conform to latest versions of the Lanka Interoperability Framework (LIFe) and Addendums made by ICTA from time to time in collaboration with the government organizations, as published in www.life.gov.lk.

010404: It is recommended that government organizations use solutions that meet the characteristics of open standards. (Refer Annex 3).

010405: All government organizations must conform to SLS 1134 : 2004, including Part 1 thereof, for all ICT use with respect to Sinhala, such as for Sinhala documents, web sites, software systems, and in the electronic transmission of information.

010406: All government organizations must conform to SLS 1326: 2008, for all ICT use with respect to Tamil, such as for Tamil documents, web sites, software systems, and in the electronic transmission of information.

010407 In a Memorandum submitted to the Cabinet of Ministers by the President on the ***"Re-engineering Government Program"*** and approved on 13th September 2006, all government agencies are required to consult ICTA before embarking on any major ICT Project (over Rs 2 Million), in order to (a) ensure that they are in conformity with general standards applicable to all government agencies specially in relation to interoperability and localization requirements, and (b) to ensure that such projects can be fully integrated to the government wide ICT system.

0105: Data Administration – Hubs

Data administration will be carried out to ensure the confidentiality, quality and integrity of the data, and to ensure the necessary infrastructure for availability to those authorised access.

010501: Ownership: The data owner of each hub should be as follows: the data owner for the land registry hub and the population registry hub should be the Registrar General; the data owner for the Company Registry should be the Registrar of Companies.

010502: Responsibility: The data owner of each hub should be responsible for the accuracy, confidentiality and integrity of data, access rules, regulations and data updates.

0106: Network, Application and Data Architectures

010601: Data, applications and network architectures of ICT systems of government organizations should comply with the Addendum to the NEA Guidelines on Standards Document (Version 1.0, September 2007), for government information systems and ICT solutions .

0107: ICT Audit

Government organizations should carry out ICT audits to ensure that the organization's information systems safeguard information assets, maintains data integrity, and is operating to maximize the value received from the organization's ICT functions.

010701: Each government organization and the Auditor General's Department should ensure that ICT Audits are carried out if and only if the staff of government organizations and the Auditor General's Department who are to carry out ICT Audits are trained and capable of carrying out ICT Audits.

010702: Each Ministry should take charge of ICT Audits in the organizations under its purview. The heads of the organizations are responsible for carrying out of ICT Audits and follow up work.

010703: Capacity building should be carried out within the Audit Sections of Ministries so that the staff is able to carry out ICT Audits.

010704: Capacity building should be carried out within the Auditors General's Department, to ensure that staff is able to carry out ICT Audits.

0108: Accessibility and Service Delivery

Government organizations shall improve citizen accessibility to government services, extending service provision beyond traditional means while complying with relevant standards, as given in 0104.

010801: Heads of government organizations and CIOs should ensure that government information and services are delivered using all possible channels of service delivery, and should also extend towards delivery of services through mobile devices.

010802: All such services which are provided through electronic or mobile platforms should be channelled through the Country Portal of Lanka Gate project which is the gateway for all eGovernment services in Sri Lanka. Lanka Gate is the middleware infrastructure of the government which provides an integrating platform, payment gateways and the Country Portal to provide all eGovernment services.

010803: All Government organizations should attempt to provide as much as information and services through mobile platforms. The mobile information and service gateway built as a part of Lanka Gate by ICTA to use the common, short telephone code "1919" should be used by all government organizations for delivery of such information and services.

010804: Government organizations should work towards information and ICT enabled services being available 24 / 7 and not restricted to normal office hours.

010805: Government organizations should ensure that citizens and businesses should not have to rely on any specific technology to access government services.

010806: Each government organization should provide relevant content to the Government Information Centre (GIC).

0109: Contracts and Information Assets Management

Government organizations' employees, consultants, contractors and other third parties should understand their roles and responsibilities. Appropriate protection for organizational assets should be implemented and maintained.

010901: Employees, consultants, contractors and third party users should agree and sign the terms and conditions of their contracts which should state theirs and the organizations responsibilities which should include, but not be limited to;

- requirement to sign a non-disclosure agreement prior to being given access to the organization's information and information processing facilities.
- employees, consultants, contractors and other users legal responsibilities and rights.
- responsibilities of the employee, consultant, contractor, or third party user with regard
  to handling of information received from other organizations or external parties.
- responsibilities of the organization in handling personal information.
- responsibilities that are extended outside the organization's premises and outside working hours.
- actions to be taken if the employee, consultant, contractor, or third party, disregards the organization's contractual obligations, policies and procedures. (also refer section 0203)

010902: Government organizations should document and implement a policy for the acceptable use of information and assets associated with information processing facilities.

(refer sections 7 and 8 of the international standard, Information Technology, security techniques – code of practice for information security management – ISO/IEC 17799, and also the model information security policy for government. See Annex 1).

0110: ICT Project Continuity

Government organizations shall manage its human resources, systems and funds to ensure project continuity.

011001: Government organizations should develop and implement a plan to ensure continuity of ICT projects and to ensure the availability of information at the required level and the required time (also refer section 10, government information security policy. See Annex 1).

011002: Government organizations should take necessary steps to ensure continuity of projects when employees involved in ICT projects are transferred, either within or between organizations.

011003: Shadow Concept: Officers in charge of key projects should be assigned a "shadow" officer – an officer who would be aware of all aspects of the ICT system. If an employee with a skill critical to the successful implementation of a project is transferred out / leaves an organization, or is promoted, then he/she should be replaced by a officer with similar skills, if possible with the "shadow" officer.

011004: Handing Over Duties: When an officer involved in an ICT project is transferred, there should be a period of handing over duties, ranging from 1 to 3 weeks.

Section 2: Procurement and Contractual issues

0201: Procurement Procedure

020101: Procurement of information systems (IS), ICT equipment, software, and software development, and consulting services, shall be carried out in accordance with the applicable "*Procurement Manual and Guidelines*" of the Procurement Division of the Department of Public Finance, Ministry of Finance and Planning or any successor thereto, and in accordance with other related regulations. Guidance from ICTA is to be obtained in relation to the operational aspects of procurement.

020102 Refer decision of Cabinet of Ministers where all government agencies are required to consult ICTA before embarking on any major ICT Project (over Rs 2 Million), in order to (a) ensure that they are in conformity with general standards applicable to all government agencies, and (b) to ensure that such projects can be fully integrated to the government wide ICT system (section 010406 and 010407 above)

0202: ICT Technical Evaluation Committees

020201: Composition of Technical Evaluation Committees (TEC): In major ICT projects, the Composition could include one person nominated by ICTA. The relevant government organization should request a nomination from ICTA, in this regard.

0203: Budget and Procurement Plan

020301: Budget:

02030101: Plan: The annual procurement plan should be drafted aligned to section 010106

02030102: Funds: Every government organization should allocate adequate funds in its annual budget for ICT procurements and sufficient funds for the maintenance of existing equipment, systems and networks. The assistance for cost estimating and recommendation for such estimates can be obtained from ICTA.

02030103: Template: The template for the budget to be used by government organizations should be in accordance with the budget template of the Ministry of Finance and Planning.

020302: Specifications:

02030201 Specifications should address scalability. Flexible and extensible systems architecture is recommended. The terms used in the specifications should be technology neutral.

0204: Contractual Issues in procurement

020401 Hardware:

02040101: Government organizations when procuring hardware should ensure that appropriate warranties are obtained and also ensure that warranty terms are adequate to take care of defects. Maintenance terms for the hardware after the warranty period should also be negotiated in advance, and should include escalation costs and availability of spares for the life period of the equipment.

020402: Software:

02040201: Licensing: Government organizations should use only licensed software; such licenses can be for either proprietary software, or for open source software. Use of software without a valid license or making modifications and carrying out customisations 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)

02040202: Warranties: When securing proprietary or commercial open source software, government organizations should ensure that the warranty terms would include a statement stating that the software would conform to the stated specifications and that the software would adhere to the required quality assurance standards. The warranty period should be negotiated in advance.

02040203: Maintenance: Support and maintenance of software which was under warranty beyond the warranty period as well as the level of service should be agreed upon in advance with the solutions provider. Procedures and terms for support and maintenance of software, and future modifications should be planned and documented in advance.

0205: Intellectual Property Rights

Adherence to Intellectual property (IP) laws to protect owners, inventors, and creators of intellectual property from unauthorized use.

020501: In the deployment of software solutions in Government there is likely to be several options available. Some of the options available would include:

(a) Procurement of retail or "common off- the-shelf" software
(b) Customisation or modification to existing licensed software
(c) Provision of "green field" or "built from scratch" software

020502 In the case of option (a) above it is essential to ensure that appropriate licenses fees are paid for, if required. If payments are required and a large number of users are involved, "bulk" or "volume" licenses could be negotiated with the Software provider. This would entail costs which should be planned and budgeted by the entity concerned. (See Section 02040201 to avoid maintenance problems.)

020503 In the case of option (b) above, Government entities could hire software engineers or Service Providers to modify or customise the licensed software. It is important to require the Service Provider to adhere to license conditions imposed by the creators or owners of such Software (See section 02040201). Note: There would be service or customisation cost involved in modification or carrying out customisations to this category of software, which should be budgeted by the Government entity. Some of the license categories under this option could provide access to the Source Code, enabling the Government entity to maintain the software using its own resources or a Service Provider or Software Engineers. Replication or re-deployment under this category could take place without incurring license fees, although costs may have to be incurred in respect of services.

020504 In relation to option (c) above, the ownership of Intellectual Property rights would depend on the Agreement between the parties. Such an agreement may include two options:

(i) Total ownership of Intellectual Property Rights
(ii) Joint ownership of Intellectual Property Rights

If the option (ii) is exercised, the Government entity could have access and ownership to the source code upon completion of the software warranty period, provided that the source code is managed through a "source code management repository" arrangement to be agreed by the two parties. Software developed in this manner would enable both the Government entity and the Service Provider to revise, further develop, replicate or deploy without any restriction after the warranty period.

If the Government entity is providing significant input to the design of the software it could exercise the right to have total ownership.

020505: If business methods or work routines (confidential or otherwise) belonging to the government organization are to be included in the Software Development activity, then, appropriate non-disclosure terms should accompany the Software Development Agreement (clearly identifying such components). Non-disclosure agreements should be signed with individual software developers, in addition to being signed with the solutions provider.

Section 3: Communication Interface

0301: Government Web Portal and Web Sites:

Government web sites to be developed to ensure interoperability and to maximize access and participation of users. All government websites should conform to the web standards publish by ICTA

030101: The URL www.gov.lk will be given to the government Web Portal.

030102: The government Web Portal will be an integrated Internet based system to make available the latest and a wide range of citizen services and government information, from a single point. All government organizations should ensure that their available web services can be accessed through the links on the government Portal.

030103: Every government organization should make available information related to the government organization and all possible services using ICT, especially through the web.

030104: All government websites shall be compliant to the “web standards and guidelines” published by Re-engineering Government Programme of ICTA.

030105: Government organizations should ensure that the content on their website is available in Sinhala, Tamil and English. The web pages in local languages should be Unicode compliant.

030106: Content on the web sites of government organizations should be relevant to the mandate of the government organization.

030107: Content must be provided adequately and organized systematically. An open standards-based content management solution should be provided to facilitate the content publishing work flow. It should support all popular web browsers and platforms.

030108: Each government organization should appoint a ‘Content Management Team’ (CMT) to approve the content on its website. It should be headed by a Content Manager who could be either the CIO or another staff officer appointed by the government organization. Content Manager is responsible for keeping the contents regularly updated. An appropriate content management and publishing process should be adopted.

030109: Content on government web sites should be organized so that easy navigation for citizens is facilitated.

030110: Content that is obscene, misleading or offensive to any ethnic group, gender, accepted religion, culture or to any tradition of Sri Lanka should not be included in government web sites.

030111: All important government policies, Acts, Regulations, Notifications, Circulars and forms should be made available through the relevant government web site and other appropriate electronic means.

030112: The language used in government websites must be simple, clear, unambiguous and easy to understand.

030113: There should be no linking to political sites from government sites.

030114: Whenever a website of a Government institution facilitates commercial advertisements, they should not be contrary in Government policies. Competition should not be restricted. The content of these advertisements should not be prejudicial to the dignity and the good name of the Government and the institution. All commercial advertisements should be personally approved by the Head of the institution.

030115: Government organizations should use their web sites as a means of promoting transparency by publishing information on the web.

030116: Government organization's web sites should be interactive as far as possible, and requests for information made through web sites should be responded to as soon as possible after the receipt of the request.

030117: Government organizations should ensure sufficient security for their web sites to ensure the integrity of the information made available and to prevent unauthorized modifications, amendments, deletions, and other malicious attacks.

030118: Government organizations should post documents; i.e. circulars, publications, white papers etc, on their web sites in standard portable document format for web (e.g. PDF files) with appropriate security settings to prevent unauthorized modifications.

030119: Government organizations should make their web sites accessible to the disabled, and adhere to the guidelines given in the latest version of the World Wide Web Consortium's Web Content Accessibility Guidelines.

030120: The web browser should be adopted by government organizations as the key interface for access of government information systems; other interfaces to be used if necessary in addition to browser-based ones

030121: Contact information: All government websites should publish all possible contact information of the organization comprising email address, phone and fax numbers and office address and contact person / designation.

030122: Copyright and Disclaimer notice: A notice on copyright and a disclaimer stating that all materials provided on government sites are provided "as is", without warranty of any kind, either express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose and non-infringement, to be posted on web sites of all government agencies.

030123: Government organizations should migrate towards overall consistency in design of their web sites.

0302: Government Domain Names

030201 All central government ministries, departments, provincial level organizations and diplomatic missions abroad will be registered under the gov.lk domain.

030202: Central government agencies (Ministries, Dept, Commissions, etc) should be registered as Third Level Domains under gov.lk domain.

030203: Provincial Councils (PCs): PCs are registered in the third level and agencies under PCs (Ministries, Departments, etc) are registered under the fourth domain level.

03020301: District Secretariats: Each District Secretariat is registered as fourth level domain under dist.gov.lk domain

03020302: Divisional Secretariats: Each Divisional Secretariat is registered as fourth level domain under div.gov.lk domain.

03020303: Local Government (LG) agencies: Each local government agency is registered as fourth level domain under respective third level domains reserved for different types of LG bodies, which are as follows: mc.gov.lk for Municipal Councils, uc.gov.lk for Urban Councils and ps.gov.lk for Pradeshiya Sabhas.

030204: Diplomatic missions: Diplomatic missions of Sri Lanka abroad (Embassies and High Commissions) are registered as fourth level domains to represent the country under embassy.gov.lk domain.

030205: All government organization should follow the Domain Nomenclature Guidelines for domain embassy.gov.lk as described below.

03020501: Single short name (word) should be used when it makes sense to establish the identity of the agency (eg. immigration, customs, statistics, tourism, etc.) provided such name is not a common/generic name which is shared by more than one agency. Such a short name is less likely to be impacted by change of Government machinery (e.g. Ministries). However if the short name is common for more than one agency (e.g. health, education, labour, etc.) the agency type (Min, Dept, etc) should be suffixed/prefixed with the domain name. e.g. labourdept.gov.lk, labourmin.gov.lk .

03020502: Abbreviations could be used when they are easy to remember (moe, mof, mod, mia etc). This is more appropriate for agencies with permanent existence (e.g. departments)

03020503: Prefix or suffix D or M could be used to denote Department or Ministry and letter “O” could be inserted to denote “Of” within an abbreviation to make it more memorisable. e.g. moe.gov.lk for Ministry of Education.

03020504: Use shorten forms if it makes sense (met for meteorology, exams for examinations)

03020505: When unrelated/multiple subjects have been assigned to one ministry, choose most important or well known subject (which is less likely to change) for the domain name. Eg.pubad.gov.lk

03020506: In case of Districts, Divisions and Local Government agencies where the area name is long it can be shortened in a meaningful and memorisable manner.

03020507: Dash is not normally recommended and characters like $, @, %, and underscore are not allowed

Section 4: Networking and Connectivity

Government email shall be used productively and the rules and regulations that apply to other forms of communication shall apply to email.

0401: **Email:**

040101: It is recommended that emails on the organization's domain are used only for organizational purposes.

040102: All official electronic communications should be carried out using the official email address.

040103: Content that is obscene, misleading or offensive to any ethnic group, gender, accepted religion, culture or to any tradition of Sri Lanka should not be sent out, and any form of harassment should not be carried out using emails on the organization's domain.

040104: Emails on the organization's domain should not be used for sending out unsolicited email messages unrelated to the organization's mandate.

040105: Retention and deletion periods for emails should meet organizational requirements, legal requirements and the requirements of any relevant circulars.

040106: Organizational filing procedures used for paper documents should be used for email communications – the procedures, if decided on, could be electronic procedures.

040107: There should be a common email address for each organization in the format info@organization.gov.lk to be used for public communication purposes. Government organizations should ensure that this account is checked frequently and mail directed to the relevant officers with minimum delay.

040108: Government organizations should designate a person to be responsible for checking and relaying to the appropriate officers, and for responding if necessary, email sent to info@organization.gov.lk.

040109: Each government organization should adopt the following nomenclature in providing email addresses to employees; i.e. the user name should be standardized and the domain should be organization.gov.lk; the nomenclature recommended is as follows:

For staff officers who are transferable: designation@organization.gov.lk
For the officers who are permanent to the organization:
lastname.initials@organization.gov.lk
For non-staff officers: lastname.initials@organization.gov.lk

040110: Designation based emails must be accessible by the relevant person's designated assistant in order to enable prompt response in the absence of the officer to whom the mail is directed.

040111: An email address should be provided for employees as decided by each government organization. Organizational emails should include a standard official signature: name, designation, organizational name and contact information and the organization's URL.

040112: Emails should contain a standard disclaimer.

040113: The writing style used in business emails should be consistent with other forms of the organization's written communications.

040114: Emails should be responded to, as far as possible, in the language (Sinhala, Tamil or English) in which they are received.

040115: Attachments: When sending attachments the precautions specified in the government Information Security Policy (refer Annex 1) should be followed.

040116: Each government organization has the right to assign, monitor, and delete any email account or content within purview of the organization.

0402: Desktop Systems and Mobile Computer Devices/Systems:

040201: Installation of software on desktops should not violate intellectual property rights. Only the systems administrator or an authorized person should have the authority to install software applications.

040202: Each government organization should standardize on a single user-platform (operating system) within the organization.

040203: It is recommended that PCs, laptops and handheld devices assigned to employees should only be used for relevant official work.

040204: Government organizations should ensure that all computers and mobile devices are regularly updated with the required security patches.

Section 5: Web Presence

0501: Internet / Intranet:

050101: Each government organization may, further to the Lanka Government Network (LGN) policies, have its own policies in assigning, controlling and monitoring Internet access, and should follow the guidelines specified in the government Information Security Policy.

050102: Organizations should implement Internet/Intranet usage policies to guide users on Internet/Intranet usage. Internet usage should comply with the policies and codes of conduct of the organization.

050103: Information access restrictions applicable to physical files should be applicable with better audit trails and security to information available in Intranet.

Section 6: Government Network

0601: Government Network Connectivity:

060101 All government organizations should connect to the common government Wide Area Network infrastructure i.e. Lanka Government Network (LGN)

0602: LAN Account Management:

060201: LAN accounts should be created only after clearance by the organization's management and disabled on the same day of employee's departure from the organization.

060202: Government organizations should define a standard format for the LAN accounts and for the names of the PCs and servers in the network.

0603: Backup Measures:

060301: The government organization should identify and document its critical organizational processes relating to its core business, and the critical assets and resources involved in the organizational processes.

060302: A plan should be developed and implemented to ensure the safety of personnel and organizational property including information and information processing facilities.

060303: Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or a media failure.
(Also refer section 10.5 of ISO/IEC 17799)

Section 7: Human Resource Development

Government organizations shall strive towards computer literacy for all State sector employees.

0701: Needs Assessment:

070101: Government organizations should carry out an assessment of the training and skills needed for all levels of staff to address organizational ICT requirements on an annual basis. The organization's ICT planning should include a component for ICT related training of employees.

0702: Staff:

070201: All staff including senior management and middle management staff in Government organizations must be competent in the use of ICT in their daily work, and necessary awareness and training should be provided to achieve this competency.

070202 Senior management should implement suitable incentive schemes for staff who are proficient in ICT and / or obtain relevant qualifications in ICT.

0703: Certification:

070301 All staff in government organizations should be encouraged to obtain government approved computer qualifications.

0704: CIO Training:

070401: All government Chief Innovation Officers (CIOs) should undergo adequate training to enable them to perform their duties in ICT related projects.

Annex 1: Documents referred to in the Policy

Government Information Security Policy

This model policy is aligned to the information security standard ISO /IEC 17799. Government organizations may modify and customize this policy to suit their respective organizations' needs, and thus create organizational information security policies. The policy is available in the Re-engineering government section in www.icta.lk.

ISO 8601

The International Standard for the representation of dates and times. The standard describes a large number of date/time formats. The document can be purchased from the Sri Lanka Standards Institution, Elvitigala Mawatha, Colombo 08.

ISO 10646

ISO/IEC 10646 was published in 1993. Its name is “Universal Multiple-Octet Coded Character Set”. It is a standardized coded character set with the purpose to eventually include ***all*** characters used in all the written languages in the world (and, in addition, all mathematical and other symbols). The current edition covers at least all major languages.

ISO / IEC 17799

The international Information Security standard, ISO/IEC 17799, Second Edition, 2005, is comprehensive in its coverage of security issues, and establishes guidelines and general principles for initiating, implementing, maintaining and improving security management in an organization. The standard was originally prepared by the British Standards Institution (as BS 7799 Part 1) and was later adopted by ISO (the International Organization for Standardization and IEC (the International Electro-technical Commission).The document can be purchased from the Sri Lanka Standards Institution, Elvitigala Mawatha, Colombo 08.

Section 15:

obligations, and of any security requirements. Especially, relevant is section 15.1.3 Protection of organizational records, wherein the following controls are given;

Important records should be protected from loss, destruction, and falsification in accordance with statutory, regulatory, contractual, and business requirements.

Consideration should be given to deterioration of media used for the storage of records. Storage and handling procedures should be implemented in accordance to the manufacturer's recommendations. With electronic storage media, procedures to ensure the ability to access (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change.

Section 7:

Section 7 of the standard addresses the following; the necessity for an inventory of assets to be drawn up and maintained, acceptable use of assets, ownership of organizational assets, and information classification.

Lanka Interoperability Framework (LIFe):

This is an initiative undertaken by Ministry of Public Administration and Home Affairs in collaboration with Information and Communication Technology Agency (ICTA) to establish recommendations for common data architecture and standards for data exchange for the Government of Sri Lanka. The Lanka Interoperability Framework is formulated to provide guidelines for different government information systems to standardize data architecture and data exchange. The scope of the first version of Lanka Interoperability Framework (LIFe) is limited to "Personal Data".

National Archives Act no 48 of 1973

A law to provide for the establishment of a Department of National Archives; to provide for the transfer of public records to the National Archives, to make better provision for the custody and preservation of public archives and public records.

NEA - Guidelines on Standards

Nationwide Enterprise Architecture (NEA) addresses the underlying technologies that are required in the implementation of ICT systems in an organization (e.g. Single Agency, Cross-agencies or Nationwide). It covers the Data Architecture, Application Architecture and Technology Architecture which all technology components such as network infrastructure, computing platforms, operating systems, database management systems, middleware, security components and management tools that make up an ICT system. The Addendum dated September 2007, supersedes the previous version.

Procurement Guidelines

Guidelines were originally prepared by the National Procurement Agency (NPA) and now being improved by the Department of Public Finance, to be used in the procurement and disposal of public assets, available at the government Publications Bureau.

SLS 1134 : 2004

Sri Lanka standard Sinhala character code for information interchange. This standard provides specifications for code sequences and keyboard sequences. It also provides a revised keyboard, based on the layout in the original version of this standard, which in turn is based on the Wijesekara typewriter keyboard. This standard is compliant with the Unicode standard and with ISO/IEC 10646-1. Parts 1 and 2 of the standard provide for the Sinhala collation sequence and “Requirements and methods of Test” respectively. [Available at the Sri Lanka Standards Institution, (SLSI) Elvitigala Mawatha, Colombo 08.]

SLS 1326: 2008

Sri Lanka Standard Tamil character code for information interchange. This standard is compliant with the Unicode standard version 5.1 and with ISO/IEC 10646. It is available at the Sri Lanka Standards Institution.

Unicode

“UNIversal CODE” “The Unicode Standard is the universal character encoding standard used for representation of text for computer processing. Versions of the Unicode Standard are fully compatible and synchronized with the corresponding versions of International Standard ISO/IEC 10646. Unicode provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language”. From www.unicode.org

Annex 2: Benefits of Implementing e-Government Services

The government organizations should accept the following factors, which are intrinsic to eGovernment, as key principles on which ICT solutions will be implemented. These issues are addressed in the body of the Policy and some issues are addressed in the government Information Security Policy, but are emphasized below.

- Accessibility: Providing information and citizen services over the web and ICT channels will make them available to a larger section of general public. Therefore all possible measures should be taken to make the services accessible to the public without discriminating on ethnicity, language, religion, gender, for differently-abled persons, or based on geographical locations, time, or on economic levels. It is essential that all citizens including differently-abled persons should be taken into account while devising e-government solutions.

- Transparency: ICT based solutions should improve the transparency by allowing the pubic to monitor the mandate of the organization, functionality, decision making processes, the progress of a process at different stages and clearly informing them of the type and the quality of the services they obtain. The e-government models should always encourage transparency within government.

- Efficacy: It is important that the services provided by Government organizations using ICTs, meet and exceed the expectation of the citizens. The efficacy at which the services offered should be a key factor that determines the quality of the services provided through using ICTs.

- Efficiency: Services should be available to the public within the minimum possible time. A concept popular in e-government solutions is “same day service”; where a service requested by a citizen in the morning should be made available to him/her before the end of the same day. Although it is difficult to expect this level of delivery from every service from the inception, all government organizations are expected to provide citizen services efficiently so that the public is not made to wait for the services requested.

- Citizen centric: In providing information and services, government organizations should establish a citizen centric approach instead of a traditional organization centric approach. In order to do so, government organizations should reengineer their processes to convert the government organizations to “one stop shops” thus making their services citizen-friendly. Citizens should be able to then obtain services through submitting minimum necessary supporting documents and visiting a minimum number of organizations.

- Interoperability: Government organizations should ensure when implementing ICT programmes that these are interoperable - enabling electronic data sharing and data exchange between different systems - throughout all government organizations, and also with the industry and other key sectors.

- Confidentiality, integrity and availability: All government organizations should preserve the confidentiality, integrity and availability of the information within their purview.

This entails that citizens should have the assurance that government information is shared only among authorized persons or organizations, that the information is authentic and complete and can be relied on for the purpose for which it is needed, and also that it is accessible when needed by those who need it. This area is further addressed in the government Information Security Policy.

- Accountability: Government organizations should be accountable towards the citizens and for the services provided, so as to foster confidence in citizens in the use of such services, and in interacting with government organizations.

Annex 3: Definitions

The definitions manual is given to explain the context in which the terms are used.

Confidential

Information maintained by government organizations that is exempt from being disclosed and disseminated.

Desktop system

A computer with a chassis containing a system board which holds a CPU, and has slots for expansion cards, buses, storage controllers, display, removable media writer, networking, input, and other peripherals.

External audit

An audit carried out by an independent/outside party, usually the Auditor General’s Department.

Government Information infrastructure

This refers to LGN a shared government wide network expected to serve different users with varying performance and bandwidth requirements.

Government organizations

Ministries, government Departments, Provincial Councils, District Secretariats, and Divisional Secretariats Local Government Authorities, government owned companies and statutory boards.

Hub

Organizations where the central databases are located to which data is sent from one or more directions /organizations.

ICT literacy

The ability to use word processing software, spreadsheets, email, browse the Internet and search, and the ability to organize and manage files and folders.

ICT Services

Activities such as hardware support, Consulting, Software support and implementation services, and web designing etc.

Internal auditors

An internal audit, which is usually carried out by people in the Audit Units of the relevant Ministry, and carried out for reasons of good management.

Lanka Government Network (LGN)

Lanka Government Network (LGN) is the highly available and reliable underlying network infrastructure that connects all the government agencies and departments of GoSL in a cost-effective and secure manner.

- Provide inter-connectivity to all Government of Sri Lanka (GoSL) organizations.
- Provide centrally managed Internet access to all GoSL organizations.
- Provide centrally managed email access (with web based email access) to all GoSL organizations.
- Provide centrally managed IP telephony facility to GoSL organizations.
- Provide centrally managed trusted secure connection to authorized agencies that are outside of the purview of GoSL

Metadata

Data which describes data. Common data vocabulary and definitions are critical for e-government solutions that include cross-organizational functions and system boundaries. This includes operational data, analytic data and web content.

Multilingual Data

Multilingual data is data which need to be stored in multiple languages when an application needs to support multilingualism. This should include Reference Data, most of Master Data, and sometimes Transactional Data.

National level ICT Projects

large-scale projects involving generally several government and other organizations of which the impact is experienced beyond a single or limited number of organizations, and the implantation of which impact the operations of these organizations.

Open standard

The following are defined as a set of requirements should be followed by a provider of specifications to qualify as an Open Standard; transparency (due process is public and all technical discussions, etc are archived and referencable), relevance, openness (anybody can participate), impartiality and consensus, availability, maintenance (source W3C). At present, ISO/IEC 26300:2006 is an adopted open standard that meets the common definitions of an open standard.

Shared IPR

Intellectual property rights developed by a government agency and a technology provider working in partnership, and where both parties share interests in the property rights.

Source Code Management Repository

Source Code Management Repository is electronic repository (server location) used for management of multiple revisions of the same unit of information. It is most commonly used in engineering and software development to manage ongoing development of digital documents like application source code

Annex 4: Document Change Record

Version	Effective date	Summary of changes
0.20	2005:02:01	Section on Data Protection (0104) added.
0.30	2005-02-10	030102: Deleted "organized by function" from policy element. - The government Web Portal will be an integrated Internet based system to make available the latest and a wide range of citizen services and government information ,*organized by function*, from a single point.
0.30	2005-02-10	030201: Include "All possible services" - Every government organization should provide *all possible services* through ICT, especially through the web.
0.30	2005-02-10	030203: Deleted "commercial advertising on government web sit4es will be made only with the approval of the relevant authorities in each government agency."
0.30	2005-02-10	030204: Deleted "team" - Links to sites of government agencies will be approved by a forum (*team)* in each government agency, designated to do so.
0.30	2005-02-10	030222: Added policy element - government organizations should designate a person to be responsible for checking and relaying to the appropriate officers, and for responding if necessary, email sent to info@organization.gov.lk
0.30	2005-02-10	040102: added - format for emails.
0.30	2005-02-10	040104: added, new policy element - Designation based emails must be accessible by the relevant person's designated assistant in order to enable prompt response in the absence of the officer to whom the mail is directed.
0.30	2005-02-10	040109: Added "content" - Each government organization has the right to assign, monitor, and delete any email account / *content*
0.30	2005-02-10	040105: "….Organizational emails should include *identification:* name, designation, organizational name and contact information and the organization's URL" replaced with "….. Organizational emails should *include a standard official signature:* name, designation, organizational name and contact information and the organization's URL.
0.30	2005-02-10	0402: "Desktop systems" replaced with "Desktop systems and mobile computer devices / systems".
0.30	2005-02-10	040202: Added "platform" - Each government organization should standardize on a *platform* (Operating system) within the agency.
0.30	2005-02-10	050101: Added "further to the LGN policies" - Each government agency may, *further to the LakGovNet policies*, have its own policies in assigning, controlling and monitoring Internet access, and should follow the guidelines specified in the Information Security Policy.
0.30	2005-02-10	050103: Replaced "Access restrictions which are applied to source systems on an organization should also apply to the organization's Intranet" with "Information access restrictions applicable to physical files should be applicable with better audit trails and security to Intranet information."
0.30	2005-02-10	050104: Added new policy element: "Organizations should implement Internet/Intranet usage policies to guide users on Internet/Intranet usage."
0.30	2005-02-10	060101: Deleted "pure" from "All *pure* government organizations"

Version	Effective date	Summary of changes
0.30	2005-02-10	060101: Added “WAN” in All Government organizations should connect to the common government *WAN* infrastructure; LakGovNet (LGN).
0.30	2005-02-10	060101: Deleted “Any existing LANs in government organizations should migrate towards connecting to the LGN.”
0.30	2005-02-10	060202: “deleted (logical deletion)” replaced with “disabled” - LAN accounts should be created only after clearance by the organization’s management and *disabled* on the same day of employee’s departure from the organization.
0.30	2005-02-10	060203: Added new policy element - government organizations should define a standard format for the LAN accounts and for the names of the PCs and servers in the network.
0.30	2005-02-10	0701 “Gap Analysis” replaced with “Needs Assessment”.
0.30	2005-02-10	0702: “For Senior Management” replaced with “For all staff”.
0.30	2005-02-10	070201: Policy element re-worded to read as - All staff including senior management and middle management staff in government organizations must be competent in the use of ICT in their daily work, and necessary awareness and training should be provided to achieve this competency.
0.30	2005-02-10	0703: “Administrative staff” replaced with “Certification”
0.30	2005-02-10	070301: “Agencies involved in administrative duties must undergo a basic ICT training in order to be ready to operated the government services. The course should include training in such areas as computer skills, wp, spreadsheet, Internet and email” replaced with “All staff in government organizations should be encouraged to obtain government approved computer qualifications”
0.30	2005-02-10	0704: Added “CIO training”
0.30	2005-02-10	070401: Added new policy element – “All government Chief Innovation Officers (CIOs) should undergo adequate training to enable them to perform their duties in ICT related projects.”
0.31	2005-02-17	Added section “Salient Points” as recommended at the meeting with ICTA Focus Groups / Working Groups, held on 3rd February 2005.
0.32	2005-02-21	Added “Contractual issues”
1.1	2005-09-01	Added “The Computer Crimes Act, which provides for the identification of computer crimes and to provide the procedure for the investigation and enforcement of such crimes, was passed in August 2005” Changed timeframe to September “The implementation time frame is to be 3 years, commencing September 2005.”
3.3	2005-10-13	Added “The Computer Crimes Legislation, which provides for the identification of computer crimes and to provide the procedure for the investigation and enforcement of such crimes, was debated in Parliament on 23rd August 2005 and there was overall consensus that it should be adopted”
3.4	2006-03-03	Amendments made to sections; 010302, 010303, 0110, 030218, 050101, and 060101.
3.42	2006-08-14	Page 05: inserted “Electronic Transactions Act no. 19 of 2006

Version	Effective date	Summary of changes
3.45	2007-03-08	Added SLS 1134 to the following section: Government organizations should be in conformity with SLS 1134 and with Unicode / ISO 10646 for all ICT use with respect to local languages, such as for local language documents and web sites and in the electronic transmission of information. – added SLS 1134
3.45	2007-03-08	Added the following under emails: "The nomenclature used for domains under .gov.lk should be in conformity to the *"Policy on Domains under gov.lk"*
3.50	2007-03-09	Section 030203: Added detailed section on structure for domain names under go dot lk
3.60	2007-03-14	Updated "Enabling Legal Environment" Added section under "Preservation and Management of Government Records" to include reference to the "e-Transactions Act". Under "Procurement and Contractual Issues" the section "IPR" was amended.
3.61	2007-04-23	Recommendations of the Reengineering Government Focus Group taken into account: Document restructured; "*Salient points*" brought down to the end of the document, and renamed "*Benefits* ….." "Documents referred to in the Policy" etc defined as Annexes. Added the following under ICT Governance: "Government may set up a central ICT Support Unit, comprising persons who are proficient in ICT, to provide technical advice and support to government organizations, as required." Small amendments under background, Timeframe, Scope. Added "Senior management should implement suitable incentive schemes for staff who are proficient in ICT and / or obtain relevant qualifications in ICT" under "Training".
3.72	2008-02-12	Moved content to ODF format and made necessary formatting changes.
3.77	2008-07-21	Modified content under the Background. Modified content under the IPR section.
4	2008-10-15 2009-03-10	050104 was merged with 050102, section 3 revised creating separate sub section for domain names Re-formatting of the document and some grammatical editing.
5	2009-0702	0102: Information Life Cycle Management was changed by including 010201 to 010203 address language issues in databases