Sri Lanka

High Level Information Security Policy

April 2005

INTRODUCTION

BACKGROUND

The Government of Sri Lanka is planning out a common technology infrastructure to enable efficient sharing of information and resources between Government agencies, in order to electronically deploy citizen services in the most efficient manner. This would be carried out by re-engineering and technologically empowering Government business processes, and improving the way Government works. Under this program we intend to interconnect Government agencies to achieve a higher level of productivity through improved interaction, and create a "single window" for citizens to access e-services provided by the Government.

The implementation of the Re-engineering Government program would result in Government agencies being able to work together more easily, electronically, information being reusable from one agency to another, and reducing the effort required by citizens to deal with the Government agencies.

With the networking of Government agencies and the establishment of databases with personal records pertaining to citizens, Government agencies will need to balance between giving employees real-time access to applications and information, and addressing the corresponding concern for the security of information and the information systems. Balancing these needs necessitates secure information systems.

Specifically, Government agencies should be able to ensure the following:

- confidentiality (protecting against unauthorized disclosure and ensuring the authenticity of the data's source)
- integrity (preventing unauthorized modification)
- availability (preventing against data delays and denials (removals) and ensuring accessibility to those authorized to do so)

Ensuring the security of information and information systems is not just a technical issue, but also involves risk assessment and management, organizational structures, physical security, operational procedure and responsibilities, reporting mechanisms, and accountability. Thus a strong framework, recommendations, and tools are needed for Government agencies seeking to improve their organizational security. Adoption of a Government Information Security Policy represents the essential first step in the process of securing information and information systems, complying with Government regulations and relevant legislation, and increasing efficiency. It is intended to build confidence in citizens in using e-services; if not citizens would tend to be wary of using the e-services provided, under the Re-engineering Government program.

An Information Security policy will serve as a basis for the implementation of more detailed policies, action plans and procedures and be the base for rules and guidelines for all stakeholders. It should be accepted and followed throughout Government agencies comprising the proposed network. A high level Information Security Policy would thus help Government agencies which can adopt it as a model in drafting its own organizational security policies.

POLICY STRUCTURE

This High Level Information Security Policy document contains separate sections (domains) which address specific areas on information systems security. Each domain in the policy document contains the following elements:

Domain: This section identifies the name of the policy or the specific area relating to information systems security.

Identifier: This is the identification number for a particular domain. This is reflected as "HPOL#" in the document.

Version: This number within the domain is to track changes made to the particular domain, and affords a means of document control. This is reflected as "Ver" in the header section of the document.

Table of Contents: The areas of coverage of the domain.

Document History Log: A log to record the summary of changes made to a domain, together with the corresponding version number.

Scope and Objectives: This section clearly states the purpose of the policy with regard to information systems security related needs.

Policy Statement: This section describes the high level information security policies of the government organization for a given domain.

ENQUIRIES

Protecting information is a top priority for the government organizations and requires the cooperation of all stakeholders. Any enquiries relating to the High Level Information Security Policy document or the application of this policy should be referred to the Chief Innovation Officers (CIOs).

ICT IN THE GOVERNMENT DEPARTMENTS

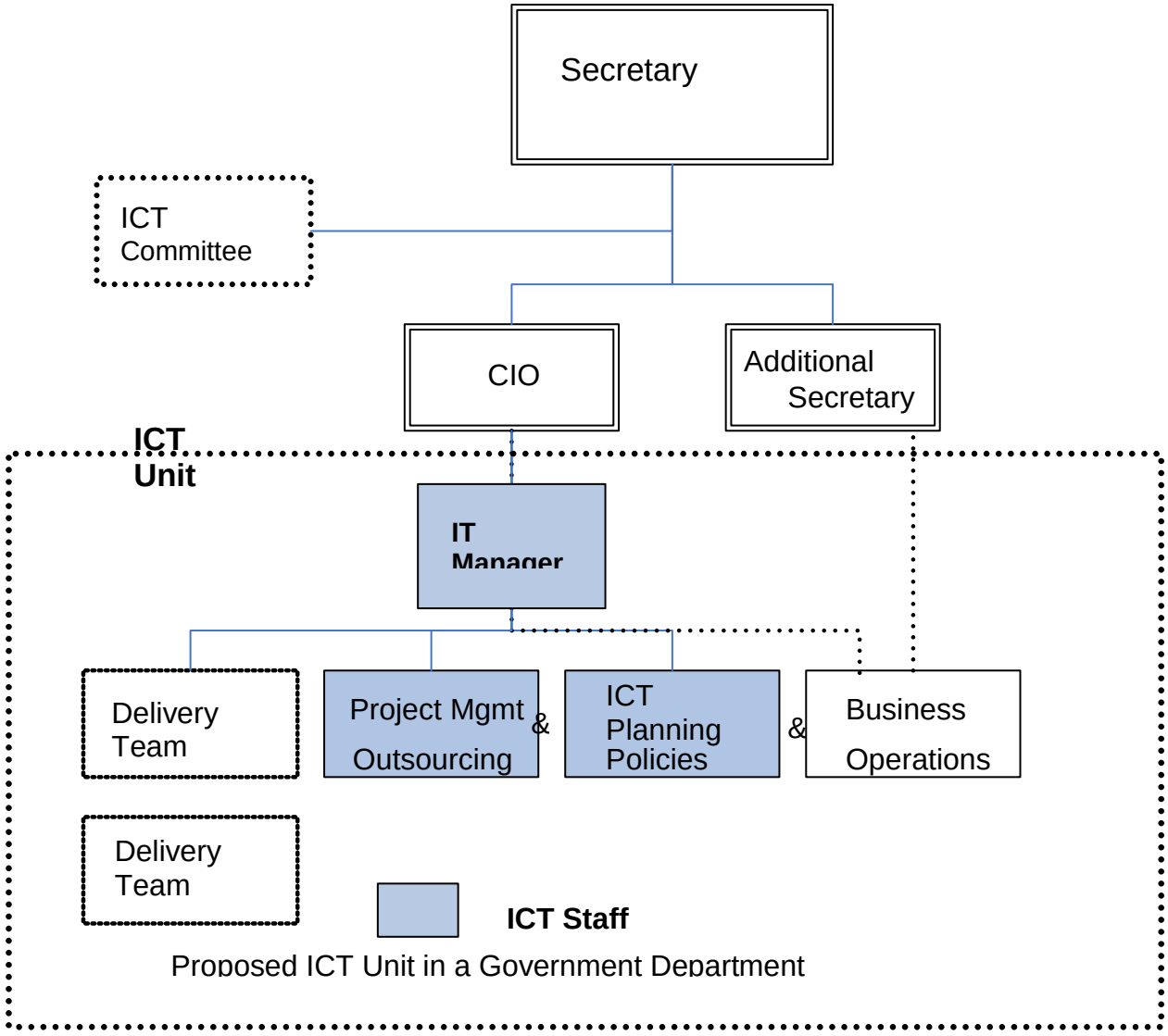
Each Government department shall appoint a Chief Innovation Officer, CIO (or equivalent). The CIO reports directly to the head of the department (e.g., Secretary).

Each Government department shall have a unit that manages all ICT functions within the department, including planning, funding, implementation and monitoring of ICT projects.

The ICT Unit (ICTU) will be run by an ICT Manager. In terms of line function, he/she shall report to the Chief Innovation Officer or equivalent.

The ICTU shall conform to all ICT Authority defined standards and policies for managing projects.

The organization of the ICT Unit is as shown below:



Proposed ICT Unit in a Government Department

DOMAIN COVERAGE

The High Level Information Security Policy addresses the following:

- Organizational Security
- Asset Classification and Control
- Personnel Security Infrastructure
- Privacy Related Issues for Outside Entities
- Physical and Environmental Security
- Acquisition and Maintenance of Hardware
- Acquisition, Development, and Maintenance of Software
- Communications and Operations Management
- Logical Access Control
- Business Continuity Management
- Compliance Measurement
- Information Systems Acceptable Use
- Internet and Electronic Mail Security
- Virus and Malicious Software Protection
- Privacy and Citizen Information Protection
- Fraud Management

DEFINITIONS

The definitions given below explain the context in which the terms are used.

Accountability: The guarantee that an action can be linked to an identified subject and that this subject is made accountable for all selected actions.

Availability: Ensuring that authorized users have access to information and associated assets when required.

Critical: Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

Fraud: Fraud includes, but is not limited to the following activities:

- Forgery or alteration of documentation relating to information assets.
- Any misappropriation of information assets including intangible assets.
- Seeking or accepting anything of material value from vendors, consultants or contractors doing business with the government organization in violation of the government organization's policies in this regard.
- Unauthorized use or misuse of the government organization's ICT infrastructure including related equipment, materials or records.
- Any computer related activity involving the alteration, destruction, forgery or manipulation of data for fraudulent purposes whether or not for personal benefit.
- Misappropriation of the government organization's software or information assets or divulging government organization information or information assets (specifically classified information or information assets in accordance with the government organization's Asset Classification and Control Policy) to unauthorized parties whether or not for personal benefit.
- Any similar or related irregularity.

Government organizations: Ministries, Government Departments, Provincial Councils, District Secretariats, Divisional Secretariats, and Local Authorities.

Section: A sub-unit of a government organization.