Information and Cyber Security Policy for Government Organizations

SRI LANKA
CERT | CC

Sri Lanka Computer Emergency Readiness Team
(Sri Lanka CERT)
Ministry of Technology

Information and Cyber Security Policy for Government Agency - English Version
First Edition
Date of issue: <>
The Cabinet of Ministers has granted the approval for the implementation and enforcement of this policy effective from <> .

Document Classification: Public

Published by

Research, Policy and Projects Division
Sri Lanka CERT
Room 4-112, BMICH, Bauddhaloka Mawatha,
Colombo 7
Sri Lanka

Telephone: +94 11 269 1692, Fax: +94 11 269 1064
Email: cert@cert.gov.lk
Websites: www.cert.gov.lk, www.onlinesafety.lk

Table of Contents

Table of Contents 3

Acronyms 5

1. Introduction 6

2. Information and Cyber Security Policy Framework 7

3. Information and Cyber Security Policy 9

3.1. Objectives 9

3.2. Scope of the Policy 10

4. Policy Statements 13

4.1. Information and Cyber Security Governance 13
4.1.1. Leadership 13
4.1.2. Security Organization Structure 13
(a) Role of Information Security Officer (ISO) 14
(b) Role of Chief Innovation Officer (CIO) 14
(c) Role of (Chief) Internal Auditor (IA) 14
4.1.3. Information Security Committee (ISC) 14
4.1.4. Risk Management Committee (RMC) 14
4.1.5. Responsibilities of End Users 15
4.1.6. Capacity Building 15
4.1.7. Security Clearance of Staff 15
4.1.8. Strategic Alignment 15
4.1.9. Action Plans and Resource 15
4.1.10. Compliance 16

4.2. Identify Assets, Owners, Users and Risks 16
4.2.1. Identification of Information and Information Technology Assets 16
4.2.2. Identification of Critical National Information Infrastructure (CNII) 17
4.2.3. Responsibilities of Asset Owners, Custodians and Users 17
4.2.4. Maintaining Information and IT Assets 17
4.2.5. Assessments Risk 17
4.2.6. Classification of Assets 18

4.3. Protect Assets 18
4.3.1. Protection of Data-at-Rest 18
4.3.2 Protection of Data-in-Transit 19
4.3.3. Physical Protection 19
4.3.4. Identity Management and Access Control 19
4.3.5. Strong Authentication 20
4.3.6. Data Sovereignty and Cloud Computing 21
4.3.7. Licensed Software and Patch Updates 21
4.3.8. Antimalware 21
4.3.9. Official Emails 22
4.3.10. Security of Emails 22
4.3.11. Digital Signatures 22
4.3.12. Perimeter Security Controls 22
4.3.13. Secure Remote Access 23
4.3.14. Backup Strategy 23

4.3.15. Security of Assets Supplied by Government Organizations ... 23
4.3.16. Security-by-Design ... 24
4.3.17. Secure Disposal of Assets ... 24
4.3.18. Internal Information and Cyber Security Audit Process ... 25
4.3.19. Audits Prior to Deployment ... 25
4.3.20. Systems Hardening ... 25
4.3.21. Work from Home ... 25
4.3.22. Using Personal Devices for Official Work ... 26
4.3.23. Using Non-Secure Networks ... 26
4.3.24. Management of Suppliers ... 26
4.3.25. Change Management ... 27

4.4. Detect Incidents ... 27
4.4.1. Reporting Incidents ... 27
4.4.2. Reviewing Logs ... 28
4.4.3. Continuous Monitoring of Incidents ... 28
4.4.4. Reporting Incidents to Sri Lanka CERT ... 28

4.5. Respond to Incidents ... 28
4.5.1. Incident Response Plan ... 28
4.5.2. Activating Incident Response Plan ... 29
4.5.3. Forensic Investigations ... 29

4.6. Recover Normal Operations ... 30
4.6.1. Disaster Recovery Plan ... 30
4.6.2. Activating Disaster Recovery Plan ... 30
4.6.3. Crisis Communication ... 30

5. Policies to be Implemented on a Priority Basis ... 31

6. Methodology for Monitoring and Evaluating the Information and Cyber Security Policy ... 36

Glossary ... 41

References ... 44

Acronyms

AMC	Audit and Management Committee
CCTV	Closed-circuit Television
CD	Compact Disk
CERT	Computer Emergency Readiness Team
CII	Critical Information Infrastructure
CIO	Chief Innovation Officer
DVD	Digital Video Disc
HOO	Head of Organization
HTTPs	Hypertext Transfer Protocol Secure
ICTA	Information and Communication Technology Agency
IA	Internal Auditor
IPS/IDS	Intrusion Prevention System/Intrusion Detection System
ISC	Information Security Committee
ISO	Information Security Officer
ISO 27002	International Organization for Standardization for Information Technology – Security Techniques - Information Security Management Systems
IT	Information Technology
LGC	Lanka Government Cloud
LGN	Lanka Government Network
MFA	Multifactor Authentication
MISS	Minimum Information Security Standards
NDA	Non-Disclosure Agreement
NIST	National Institutes of Standards and Technology
PIN	Personal Identification Number
RMC	Risk Management Committee
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SFTP	Secure File Transfer Protocol
SIEM	Information and Event Management
SSD	Solid-state Drive
SLA	Service Level Agreement
SSL	Secure Socket Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VPN	Virtual Private Network

1. Introduction

1.1. Many government organizations in Sri Lanka now depend on the reliable functioning of digital systems and infrastructure. Malicious actors, however, can exploit these digital systems to cause harms such as theft of sensitive information, disruption of day to day operations, damage to the reputation of organizations which in turn can lead to the loss of public trust and confidence in government systems, and place nation's security, economy, safety and wellbeing at a risk.

1.2. To effectively address these information and cyber security risks and to protect the information, digital systems and infrastructure (hereinafter, information and information technology assets) of government organizations from various threats, Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), the organization which has the mandate to protect the cyberspace of Sri Lanka, has developed an Information and Cyber Security Policy for the use of government organizations. The Policy provides a risk-based approach for implementing an information and cyber security program at the organizational level. It also provides a set of actions that organizations should implement to identify and protect assets, detect information security incidents in a timely manner, respond to incidents and recover from cyberattacks in an efficient and effective manner.

1.3. The Information and Cyber Security Policy for Government Organizations is developed in line with the implementation of the Information and Cyber Security Strategy of Sri Lanka (2019: 2023). It is developed based on the international standards and best practices such as International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) of the United States of America, and has been extensively reviewed by information security experts and senior officers of the government.

1.4. All government organizations that are defined as 'Public Authorities' in the Right to Information Act No 12 of 2016, are required to comply with this Policy. The heads of government organizations shall be responsible and accountable for the implementation of the Policy to ensure safe and efficient service delivery within their organizations. Sri Lanka CERT shall facilitate and provide recommendations to all government organizations in implementing the Policy, and shall assess the performance of organizations in implementing the Policy on an annual basis.

2. Information and Cyber Security Policy Framework

2.1. The Information and Cyber Security Policy Framework introduces the guidance material required by government organizations to implement information and cyber security programs in an efficient and effective manner. It includes (a) the Information and Cyber Security Policy, (b) the Minimum Information Security Standards, (c) the Information and Cyber Security Implementation Guide, and (d) a methodology to monitor and evaluate the implementation of the Information and Cyber Security policy at government organizations. Figure 1 presents an overview of the Information and Cyber Security Policy Framework.

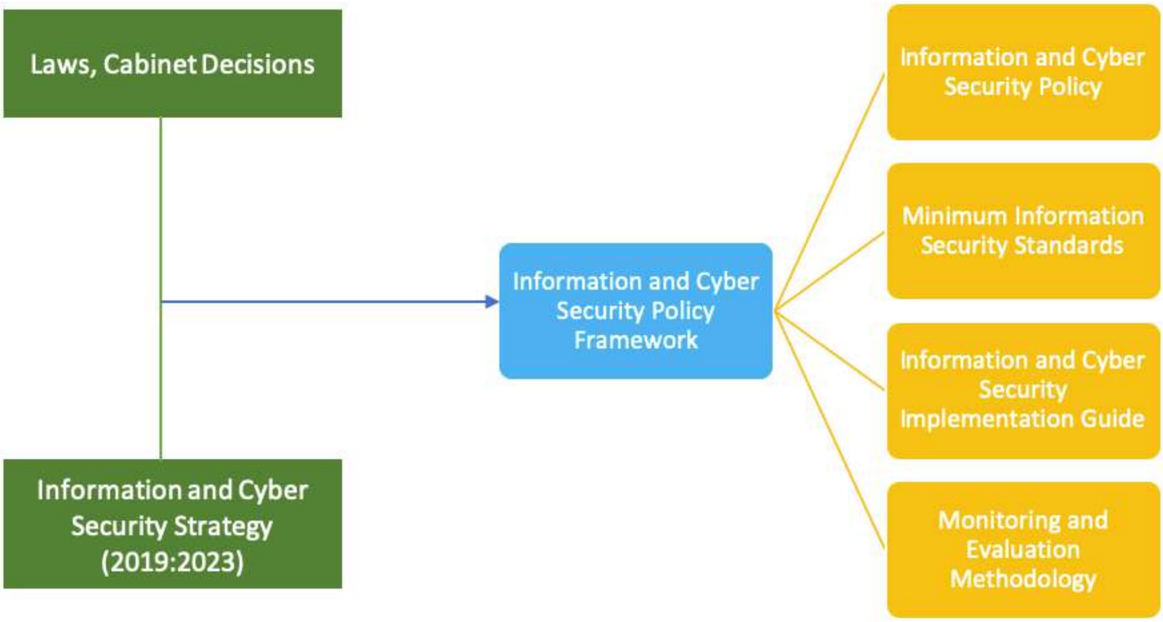
Laws, Cabinet Decisions
Information and Cyber Security Strategy (2019:2023)
Information and Cyber Security Policy Framework
Information and Cyber Security Policy
Minimum Information Security Standards
Information and Cyber Security Implementation Guide
Monitoring and Evaluation Methodology

Figure 1: Information and Cyber Security Policy Framework

2.2. The Information and Cyber Security Policy framework includes the following:

a. The Information and Cyber Security Policy: The main component of the Policy Framework is the Information and Cyber Security Policy. It provides a set of policies that the government organizations shall comply with, outlines the essential controls, and provides direction to government organizations in protecting information and information technology assets from information security events.

b. Minimum Information Security Standards: This document outlines the minimum acceptable standards of information security controls that shall be adhered to by the government organizations. Minimum Information Security Standards are available for the reference on www.onlinesafety.lk website of Sri Lanka CERT.

c. Information and Cyber Security Implementation Guide: This provides a comprehensive set of instructions to staff and stakeholders who require specific details on the implementation of the Policy. This guide includes instructions on the establishment of an information security governance structure, classification of assets, management of risks, protection of assets, methods of disaster recovery and backups, management of incidents, management of identity and access control and so forth. This document is available for reference on www.onlinesafety.lk website of Sri Lanka CERT.

d. Monitoring and Evaluation Methodology: This provides assessment criteria for evaluating the readiness of government organizations in adopting the Policy and for evaluating the progress of its implementation. Sri Lanka CERT uses the methodology mentioned in Section 6 of this document to evaluate the maturity of the information and cyber security activities of government organizations within a predefined time frame.

2.3. The Information and Cyber Security Policy Framework is governed by the relevant laws and regulations, Information and Cyber Security Strategy of Sri Lanka, policies on e-government and cabinet directives.

3. Information and Cyber Security Policy

3.1. Objectives

3.1.1. Information and cyber security refers to the protection of information assets from unauthorized access, use, modification, and destruction to ensure the confidentiality, integrity and availability of information. It includes the protection of IT assets that contain information assets from malicious actions of individuals with the use of cyber technology or other means, and protection of assets from other natural disasters such as floods and fires.

3.1.2. In this context, the main objective of the Information and Cyber Security Policy is to introduce a set of rules and guidelines to be followed by the government organizations to protect information and IT assets from damage caused by malicious activities of individuals and natural disasters.

3.1.3. The other objectives of the Policy are to,

a. establish a common information and cyber security standard across the public sector,

b. strengthen government organizations' resilience to information and cyber security events by mandating security standards, rules and processes related to the design, implementation, use and operations of information systems and digital infrastructure,

c. establish a mechanism to detect information and cyber security incidents in a timely manner, to minimize the impact of such incidents to organizations, and to efficiently restore any capabilities or services that were impaired due to such incidents, and

d. educate staff on the rules, best practices, standards and processes of information and cyber security, and build the confidence of staff in the security status of the organization.

3.1.4. This Policy is written in simple language. All staff and relevant third-party service providers, regardless of their knowledge of the subject, will be able to understand their responsibilities and accountabilities in relation to the implementation of the Policy.

3.1.5. This document will be updated periodically to provide technical and security guidance for government organizations to support good information security practices.

3.2. Scope of the Policy

3.2.1 This Policy is applicable to any government organization including Ministries, Departments, Public Corporations, Local Government Institutions, and any organization defined as ‘Public Authorities’ in the Right to Information Act No 12 of 2016. The Policy shall also be applicable to the relevant third-party service providers who manage IT services on behalf of government organizations.

3.2.2 Policies presented here are developed based on two levels. They are, (a) the policies applicable to all government organizations, and (b) the policies applicable to the Critical National Information Infrastructure providers (CNII). CNII providers are required to comply with all the policies specified in this Policy. Other organizations are required to comply with the policies applicable to all government organizations. It is, however, recommended for other organizations to comply with the policies which are applicable to CNII for better security.

3.2.3 CNII providers are defined as the organizations that maintain information and IT assets whose incapacity or destruction would have a debilitating impact on national security, governance, economy, health and social well-being of a nation. A list of CNII providers will be published by the Sri Lanka CERT.

3.2.4 This Policy is developed based on the information and cyber security governance principles, and several concurrent and continuous information security functions proposed by the NIST of the United States of America. These functions include (a) identifying information and IT assets of the organization (e.g. data, information, computers and other digital infrastructure), (b) taking necessary actions to protect assets, (c) detecting information and cyber security incidents, (d) responding to incidents, and (e) recovering any service that was disrupted due to an incident. The Policy also includes the information and cyber security governance mechanism for directing and controlling activities related to information and cyber security within the government organization. Figure 2 presents activities that government organizations should follow to protect information and IT assets.

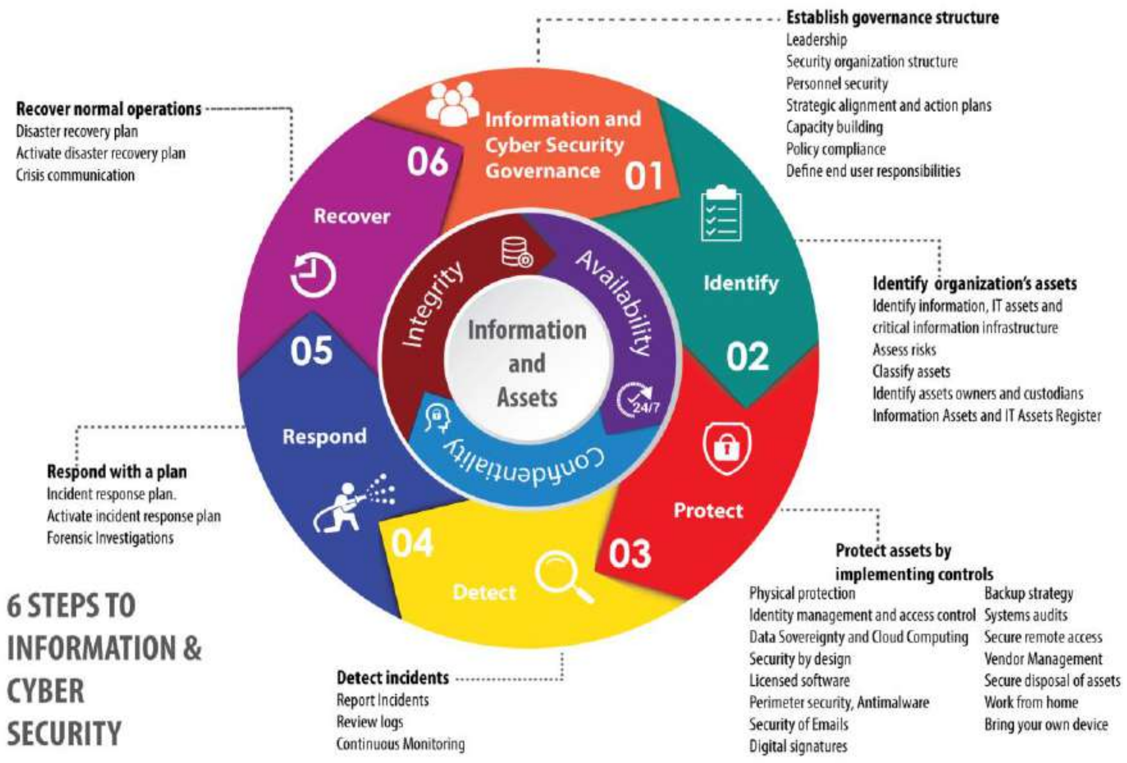
Establish governance structure
Leadership
Security organization structure
Personnel security
Strategic alignment and action plans
Capacity building
Policy compliance
Define end user responsibilities
Recover normal operations
Disaster recovery plan
Activate disaster recovery plan
Crisis communication
Information and Cyber Security Governance
01
06
Recover
Identify
Integrity
Availability
Information and Assets
Confidentiality
24/7
05
02
Identify organization's assets
Identify information, IT assets and critical information infrastructure
Assess risks
Classify assets
Identify assets owners and custodians
Information Assets and IT Assets Register
Respond
Protect
Respond with a plan
Incident response plan.
Activate incident response plan
Forensic Investigations
04
03
Detect
Protect assets by implementing controls
Physical protection
Identity management and access control
Data Sovereignty and Cloud Computing
Security by design
Licensed software
Perimeter security, Antimalware
Security of Emails
Digital signatures
Backup strategy
Systems audits
Secure remote access
Vendor Management
Secure disposal of assets
Work from home
Bring your own device
6 STEPS TO INFORMATION & CYBER SECURITY
Detect incidents
Report Incidents
Review logs
Continuous Monitoring

Figure 2: Steps to information and cyber security

3.2.5 The steps to be taken by an organization to protect assets by implementing this Policy, which is developed based on the information security functions mentioned in 3.2.4, are described below.

a. Information and Cyber Security Governance: Information and Cyber Security Governance generally refers to the governance mechanism that directs and controls the information and cyber security of an organization. In order to implement the information and cyber security governance, organizations are required to establish a security organizational structure and appoint officers responsible and accountable for information security, undertake capacity building of such officers, define the organizations' information and cyber security objectives, develop action plans, and allocate resources for related activities (Refer Section 4.1).

b. Identify Function: It facilitates government organizations to identify assets such as data, information, computers, systems, and digital infrastructure and, to identify and effectively manage the risks associated with those assets (Refer Section 4.2).

c. Protect Function: The Protect Function outlines appropriate controls required to ensure the protection of information and information technology assets in order to provide uninterrupted services. To comply with the Protect function, organizations shall implement appropriate controls such as managing user access to assets, installing firewalls and antimalware software, conducting systems audits, establishing a backup strategy, and shall implement policies mentioned in Section 4.3.

d. Detect Function: The Detect Function defines the activities required to identify the occurrence of information and cyber security incidents in a timely manner. Organizations shall deploy appropriate tools to analyze logs generated through computers and related devices to detect incidents in an efficient manner (Refer section 4.4).

e. Respond Function: The Respond Function defines the actions that should be taken in response to a detected incident. To respond to an incident in an efficient and effective manner, organizations shall develop and implement an Incident Response Plan as defined in Section 4.5.

f. Recover Function: The Recover Function identifies appropriate activities to restore any capabilities or services that were impaired due to an information and cyber security incident. To comply with the Recovery Function, the organization shall develop a Disaster Recovery Plan and activate the Plan to recover normal operations in an event of incident (Refer Section 4.6).

4. Policy Statements

Information and Cyber Security Policy for Government Organizations consists of six main policy domains namely, (a) establishment of an information and cyber security governance structure within the organization, (b) identification of assets, asset owners, custodians, and risks, (c) protection of asset, (d) identification of information and cyber security incidents (e) responding to security incidents, and (g) recovery of operations that were disrupted due to an incident. The policies to be complied with by government organizations in relation to the above six domains are presented below.

4.1. Information and Cyber Security Governance

This Section proposes a mechanism to direct and control information security in the organization. It specifies the leadership and accountability framework which is necessary to ensure that information security activities are properly managed within the organization. It also highlights the need of aligning information and cyber security activities to the vision and mission of the organization, the need for capacity building of responsible and accountable officials, effective information and cyber security planning, and the importance of government organizations adopting this Policy.

4.1.1. Policy on Leadership

The Head of the Organization (HOO) shall provide leadership to information security activities of the organization, and shall bear the ultimate responsibility and accountability for protecting information and assets of the organization.

HOO shall lead the implementation of the Information and Cyber Security Policy, set up information security goals and priorities that support the vision and mission of the organization, and ensure the availability of resources to implement the information security activities.

The HOO shall also provide leadership to create an information security culture within the organization, where users comply with information security policies and guidelines, and work proactively towards protection of information and systems they use.

Compliance: Applicable to all government organizations

4.1.2. Policy on Security Organization Structure

The organization shall establish an information security organizational structure. An effective information security organizational structure shall include key roles such as (a) Information Security Officer, (b) Chief Innovation Officer, and (c) (Chief) Internal Auditor.

The said structure is essential to execute, direct and manage information security activities of the organization, and to protect the organization against information and cyber security breaches, intrusions and interruptions.

Compliance: Applicable to all government organizations

(a) Policy on the Role of Information Security Officer (ISO)

The organization shall appoint an ISO. The ISO shall be a senior-level executive responsible for establishing the organization's information security objectives in consultation with HOO, managing information security risks, and implementing the Information and Cyber Security Policy to ensure that the organization's information and assets are adequately protected.

The role of the ISO shall be separated from the IT function, and the ISO shall directly report to the HOO with regards to the activities in relation to information security.

Compliance: Applicable to all CNII providers

(b) Policy on the Role of Chief Innovation Officer (CIO)

CIO or the officer in charge of the subject of IT shall be trained and assigned responsibilities to take appropriate steps to protect information and other IT assets, and to ensure the continuity of the business operations of the organization.

Note: In the case of the organization not having a suitable officer to be appointed as the ISO, the CIO or the officer in charge of the subject of information technology shall be empowered to play the role of the ISO.

Compliance: Applicable to all government organizations

(c) Policy on the Role of (Chief) Internal Auditor (IA)

(Chief) Internal Auditor shall be assigned the responsibilities of initiating and overseeing information security audits of the organization, assessing the progress of adopting the Information and Cyber Security Policy, and reporting information security related findings to the Audit and Management Committee (AMC) for further actions.

Compliance: Applicable to all CNII providers

4.1.3. Policy on Information Security Committee (ISC)

The organization shall establish an Information Security Committee to provide strategic directions to activities related to the implementation of the Information and Cyber Security Policy. This Committee shall be responsible for reviewing and approving all information security controls, action plans, assets classification schemes, incident response plans and disaster recovery plans and other activities carried out by the ISO in implementing the Policy. The HOO shall chair the Committee, and the Committee shall consist of the ISO, CIO, (Chief) IA, and Asset Owners. The policy on Asset Owners is presented in Section 4.2.3.

Compliance: Applicable to all government organizations

4.1.4. Policy on Risk Management Committee (RMC)

The organization shall establish a Risk Management Committee. This Committee shall be an independent committee directly reporting to the HOO, and holds the responsibility of overseeing the risk management of the organization with respect to information and IT assets.

The RMC shall identify and evaluate risks in relation to assets, and shall propose appropriate controls to ISC to take necessary actions to mitigate the risks. The Committee shall include Sectional Heads, Asset Owners, and the ISO. The Deputy Head of the organization shall be the chairperson of the Committee.

Compliance: Applicable to all CNII providers

4.1.5. Policy on Responsibilities of End Users

Information security is everyone's responsibility. All end users are required to behave responsibly and comply with an organizational policy regarding the protection of information and IT assets which they have access to.

End user responsibilities shall include but not be limited to appropriate use of information, computing devices, emails, internet, social media, telephones, and faxes. All users shall understand and adhere to end user responsibilities outlined in the Information and Cyber Security Implementation Guide, and applicable information security practices required by this Policy.

Misappropriate use of such resources would lead to disciplinary actions as stipulated in the Establishment Code and the legal actions under the Computer Crimes Act or any other applicable Acts of Law.

Compliance: Applicable to all government organizations

4.1.6. Policy on Capacity Building

The organization shall build the capacity of the accountable individuals such as ISO, CIO, (Chief) IA, Assets Owners, end users through information and cyber security awareness raising, education and trainings.

Such capacity building activities of the relevant officials should be carried out in a proper manner, and such activities should be included in the Annual Training Plan of the organization.

Compliance: Applicable to all government organizations

4.1.7. Policy on Security Clearance of Staff

Anyone who has been assigned or transferred to a position that deals with information classified as "Secret" or "Confidential", or has access to CNII must undergo a security clearance check prior to appointment or transfer to that position.

Background checks and periodic security clearance checks shall be carried out during their service.

Compliance: Applicable to all CNII providers

4.1.8. Policy on Strategic Alignment

The organization must align its information and cyber security activities with its corporate vision, mission and objectives. All information and cyber security strategies, programs, projects and activities implemented within the organization should be designed in a way that is in line with the vision, mission and objectives of the organization.

Compliance: Applicable to all government organizations

4.1.9. Policy on Action Plans and Resource

The organization shall develop and implement information security action plans (long, medium, and short term plans) which define the way in which security is to be guaranteed in realizing the vision, mission, and objectives of the organization. Those plans should be based on information security priorities determined by a risk assessment, and budgets should be allocated to implement plans.

Compliance: Applicable to all government organizations

4.1.10. Policy on Compliance

The organization shall comply with the Information and Cyber Security Policy. As noted in Sections 4.1.1 and 4.1.2 (a), the HOO and ISO shall hold the ultimate responsibility of ensuring that the organization complies with this Policy.

Sri Lanka CERT shall conduct annual information and cyber security readiness assessments to determine the level of compliance, and the organization shall facilitate Sri Lanka CERT to conduct such assessments.

Compliance: Applicable to all government organizations

4.2. Identify Assets, Owners, Users and Risks

The organization shall develop an understanding of their operating environment to manage the information security risks to organizational assets. The organization shall identify information, systems, and IT devices (assets) that are of value to the organization, owners and the users of the assets, their roles and responsibilities in protecting those assets, and current risks associated with assets. The following are the policies that the organization should adopt in this regard.

4.2.1. Policy on Identification of Information and Information Technology Assets

The organization shall identify all of its important information assets. An information asset is any information that is of value to the organization in performing its organizational functions. Examples of information assets include trade secrets, tender documents, budget sheets, employees' personal records, data gathered by application software related to services offered by the organization, etc. Information assets may come in many different forms such as paper documents, digital documents, databases, passwords or encryption keys or any other digital files.

The organization shall also identify IT assets. An IT asset is a software (e.g. operating systems, payroll systems, other software), hardware (e.g. computers, hard disks, servers, routers, firewalls), networks or other digital infrastructure facilities within an information technology environment.

The identification of assets (information and IT assets) shall be performed with the intention of protecting assets from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure integrity, confidentiality, and availability of assets.

Compliance: Applicable to all government organizations

4.2.2. Policy on Identification of Critical National Information Infrastructure (CNII)

Critical National Information infrastructures are the systems or facilities, the failure or destruction of which would have a devastating impact on national security, governance, economy, health and social well-being of a nation.

Organizations which maintain CNII shall take appropriate measures to protect such infrastructure as specified in this Policy. Identification of CNII shall be carried out by Sri Lanka CERT.

Compliance: Applicable to all CNII providers

4.2.3. Policy on Responsibilities of Asset Owners, Custodians and Users

The organization shall identify Asset Owners and Custodians. The Asset Owner is a senior executive level officer or an entity who has the approved management responsibility of controlling the lifecycle of an asset. Asset Owner shall understand the risks to assets and shall propose appropriate controls to protect such assets. It is necessary to formally assign ownership of the asset when it is created, or when assets are transferred to the organization or are acquired by the organization.

The Custodian is an officer or an entity who is responsible for the protection of the asset and for implementing the controls (as identified and approved by the owner of the information asset) related to the protection of the asset.

The Asset Owner and Custodian are also responsible for developing a Register of assets, classifying assets and protecting assets, defining and reviewing access restrictions to assets, ensuring appropriate handling when an asset is deleted or destroyed (adopted from ISO 27002).

The organization should also identify the users who use its assets. Users are the staff who use the assets for official purposes. Asset Owners must accurately identify the users who are required to use the assets for official purposes, and control access to those assets as specified in Section 4.3.4 and 4.3.5.

Compliance: Applicable to all government organizations

4.2.4. Policy on Maintaining Information and IT Assets

The organization shall record information assets in the Information Assets Register. An Information Assets Register is a formal inventory of the information assets that an organization holds and possesses. At a minimum, an organization shall record, the name of information asset, owner and custodian of the asset, level of classification, reason for the classification, date of classification, the computer system which processes assets, the storage location of asset, disposal method, impact of loss (compromise or disclose) and date to review the classification of asset.

The organization shall also record details of IT assets in the IT Assets Register. The IT Asset Register shall contain at a minimum, the type of the assets (e.g. hardware, software, server), location of the asset, operating system, license details, users, risk, classification level, estimated value and so forth. Assets Registries shall be accurate, up to date, and consistent with other inventories.

Compliance: Applicable to all government organizations

4.2.5. Policy on Assessments Risk

The organization shall conduct a formal risk assessment to determine the risks to the assets and their impact to the organization.

The purpose of a risk assessment is to identify the risks to the assets and determine what security measures should be taken to minimize those risks. Risk ratings should be developed based on the impact, and risks should be recorded in the Risk Register.

The organization shall take appropriate safety precautions for the risks recorded in the Risk Register by taking into account the policy considerations specified in Section 4.3.

The risk assessment shall be carried out by the RMC of the organization. In the event, where the organization does not possess appropriate skills for carrying out a risk assessment, a qualified and experienced firm shall be hired for this purpose. Sri Lanka CERT shall assist CNIIs to conduct Risk assessments.

Compliance: Applicable to CNII providers

4.2.6. Policy on Classification of Assets

The organization shall classify assets and determine the sensitivity of assets. The objective of the classification is to ensure that an asset receives an appropriate level of protection in accordance with its value to the organization and its sensitivity.

Classification of information assets shall be performed based on accepted guidelines. The classification levels for information assets shall be “Secret”, “Confidential”, “Limited Sharing”, “Public” and “Unclassified”.

IT assets shall be classified into four levels namely, “Very Critical IT assets”, “Critical IT assets”, “Non-Critical IT assets”, and “Unclassified IT assets”.

A description of the process of assets classification is available in the Information and Cyber Security Implementation Guide (Refer Section 2.2. c).

Compliance: Applicable to all government organizations

4.3. Protect Assets

Upon identification of the assets, the organization shall implement appropriate controls to prevent, limit or contain the impact of a potential information security incident. Controls applied shall be based on the classification of each asset. To comply with the Policy, the organization shall control access to assets, enforce processes in place to secure data, define security controls for data- in- transit and data-at-rest, use licensed software, and deploy protective technology to ensure cyber resilience. The policies which the organization shall comply with are presented below.

4.3.1. Policy on Protection of Data-at-Rest

The organization shall protect data-at-rest. Data at rest is the data that is not actively moving from device to device or network to network (e.g. data stored on a server, cloud, hard drive, laptop, flash drive, or data archived or stored).

It is essential to encrypt any data (information assets) which are classified as

"Secret" or "Confidential" prior to storing. Other means of protecting data at rest include, controlling user access through Identity Management and Access Control mechanism, and providing physical protection to assets.

Compliance: Applicable to all government organizations

4.3.2 Policy on Protection of Data-in-Transit

The organization shall protect data-in-transit. Data in transit is the data that is actively moving from one location to another such as across the Internet or through a private network (e.g. data being transferred from site A to B through an organization owned private network, including Wi-Fi).

In order to protect data in transit, the organization shall encrypt sensitive information (information classified as "Secret" or "Confidential") prior to moving and, use secure connections (HTTPS, TLS, SFTP, etc.) for data transfer.
Further, the organization shall ensure that security parameters on Wi-Fi settings have been enabled.

Compliance: Applicable to all government organizations

4.3.3. Policy on Physical Protection

The organization shall provide physical protection to assets to prevent physical intrusion and unauthorized access.

Based on the protection requirements of assets, each organization shall define secure areas to store or process assets which are important to the organization. Information assets classified as "Secret" and "Confidential" are to be stored and processed in the stated secure areas. Further, IT assets which are classified as "(very) Critical" shall be stored and operated in secure areas.

Secure areas shall be protected by physical walls and lockable doors, and multi-factor entry systems, and shall be monitored through CCTV continuously to prevent physical intrusions and unauthorized access.

Secure areas shall be protected to prevent threats from fire, flood, humidity, electromagnetic fields and temperature.
Furthermore, the organization shall use various technologies to control user access to information and IT assets. Such technologies include but are not limited to user identity and passwords, access cards, PINs and biometrics.

Moreover, access to the computers, systems or any devices shall be controlled through implementing an Identity Management and Access Control process (Refer Section 4.3.4).

Compliance: Applicable for all government organizations

4.3.4. Policy on Identity Management and Access Control

The organization shall control user access to both Information and IT assets. Identity management and access control is an approach to managing access to information and IT assets to keep them secure.

Identity management and access control is focused on verifying a user's identity and their level of access before granting them access to systems and information. Users shall only be granted access to the assets which they need to perform their tasks (need-to-know), and assets they need to use to perform tasks (need-to-use). The users shall always be given minimum access to systems and information necessary for their role only.

Based on the given principles, the organization shall develop an Identity Management and Access Control Process for its usage. Sri Lanka CERT has drafted an Identity Management and Access Control Process for government organizations which can be customized and adopted by the organization.

The organization shall ensure that the Identity Management and Access Control Process implemented by the organization is adequate and up-to-date. Further, all employees and all third-party service providers should adhere to the Identity Management and Access control process implemented by the government organization.

Any violations of the Identity Management and Access Control Process shall be reported to the ISC for necessary action. In a situation where an ISC is not established, such violations should be reported to HOO through ISO.

Compliance: Applicable to all government organizations

4.3.5. Policy on Strong Authentication

Authentication is the process of identifying a user. The authentication process provides access to the organization's assets through user identification (identification) and user verification (verification of identity) by evidence.

In accordance with the Organization's Identity Management and Access Control Process as presented in Policy 4.3.4, the organization must use strong authentication to verify a user's identity.

A combination of username and password, and the use of multifactor authentication (MFA) are recommended to authenticate user identity.

To ensure a strong authentication process, the organization shall address the following factors (but not limited to) in developing the organization's Identity Management and Access Control Process.

(a) Strong Password:

- Passwords must be at least 8 characters long and must consist of both upper and lower case characters (e.g. a-Z), digits (0,9), and special characters (!@$+/).
- All passwords must be changed after predetermined intervals which is 90 days for regular access. Privilege access should only be granted on a need basis.

(b) MFA:

- The organization shall implement MFA access for securing user accounts which have access to "Secret" and "Confidential" information.
- In designing MFA, organization shall take into account at least combination of user's knowledge (*what you know*, e.g. password), possession (*what you have*, e.g. token, access card), or inherence (*what you are*, e.g. biometric-finger print).

Passwords and any other authentication credentials provided to an employee who is leaving the organization shall be withdrawn and removed from all assets to prevent further access by the employee.

Compliance: Applicable to all government organizations

4.3.6. Policy on Data Sovereignty and Cloud Computing

Data sovereignty refers to the data subject to the laws and governance structures within the country where such data is collected, processed and stored. In this context, the government organization shall pay a high level of attention to data sovereignty particularly when cloud services are obtained from other countries to store and process the collected data.

Cloud computing generally refers to the ICT resources (e.g. such as storage, processing, application development platforms) available for users on-demand without direct management by the user. Many organizations nowadays are moving to cloud services due to cost savings, scalability and increased performance.

The organization, however, must be cautious about the risk of using cloud services, particularly, when using public clouds (public cloud is a cloud service available to anyone who wants to purchase them). Limited control over the cloud as they are operated in different jurisdictions, limited visibility of architectures and limited transparency of operations, possible significant mismatches in service-level agreements (SLAs) are common cloud risks. In fulfilling their cloud service needs, organizations shall give priority to obtaining services through the Lanka Government Cloud (LGC).

LGC is a government-owned private cloud service operated by the Information and Communication Technology Agency (ICTA), which was designed to fulfill the cloud service requirements of the government. It is, however, strictly recommended to the organizations to perform a proper risk assessment prior to obtaining services from any cloud service provider.

Furthermore, all activities of the organization in relation to collecting, storing and processing data or hosting software applications in other jurisdictions shall be performed in accordance with the relevant laws and regulations in Sri Lanka in relation to data protection.

Compliance: Applicable to all government organizations

4.3.7. Policy on Licensed Software and Patch Updates

The organization shall use licensed software with valid updates. This includes but is not limited to system software, utility programs, and application software (e.g. word processing packages, databases, browsers, antimalware, etc.).

Organization shall update operating systems and other relevant software with vendor supplied latest patches and fixes. Furthermore, organizations should enable automatic updates.

Further, prior to the installation of critical patches provided by the supplier, a proper assessment of the potential impact of their installation should be made (especially for IT assets classified as very critical and critical).

Compliance: Applicable to all government organizations

4.3.8. Policy on Antimalware

The organization shall install Antimalware software with a valid license. Antimalware tools shall remain active at any potential entry point, and malware signatures shall be up-to-date and automatic updates shall be enabled.

Malware detection must be configured for on-access scanning, including downloading or opening of files, folders on removable or remote storage, and web page scanning.

Users must be prohibited from changing the configuration of, uninstalling, deactivating or otherwise tampering with antimalware.

When a government organization communicates information to another organization or to the public, through electronic format sender shall ensure that the information is free of malware.

Compliance: Applicable to all government organizations

4.3.9. Policy on using Official Emails

The organization shall use official emails for official communications. Employees must not use official emails for personal communications.

Official emails are the email provided by the government with the domain name of “gov.lk”. Official email accounts are official assets and the organization has the right to access the account, read emails or delete the account.

All email attachments, regardless of the source or content, must be scanned for viruses and other destructive programs before being opened or stored on any government organization’s computer system.

Organizations are also required to comply with the regulations and guidelines issued by the government from time to time regarding official emails.

Compliance: Applicable to all government organizations

4.3.10. Policy on Security of Emails

The organization shall configure their email accounts with all applicable security features. To ensure the security of information, the email server shall be hosted in line with the relevant laws in relation to data protection.

The organization shall set up email filters to remove emails known to have malware attached and prevent the inbox from being cluttered by unsolicited and undesired (i.e. “spam”) email. Moreover, when sending sensitive information via emails, it must be encrypted.

In the case of email accounts provided by the Lanka Government Network (LGN), ICTA is required to ensure that the email service is securely configured, and security audit reports shall be obtained from Sri Lanka CERT on a periodic basis for supervisory or regulatory requirements.

Compliance: Applicable to all government organizations

4.3.11. Policy on Digital Signatures

Where appropriate, the organization shall implement digital signatures. Digital signatures should be used for emails to ensure authenticity, integrity and nonrepudiation.

Compliance: Applicable to all government organizations

4.3.12. Policy on Perimeter Security Controls

The organization shall install perimeter security controls such as Firewalls, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS), etc., to provide protection to assets (information, computers, networks and systems assets) against cyberattacks and prevent malicious software from accessing assets via the Internet.

The organization shall regularly update perimeter security threat databases, install antimalware with automatic updates enabled, update default settings with appropriate configurations, and disable default vendor supplied user accounts for such devices and systems.

An overview of the appropriate security configurations for perimeter security controlling devices is provided in the Information and Cyber Security Implementation Guide.

Compliance: Applicable to all government organizations

4.3.13. Policy on Secure Remote Access

The organization shall secure remote access to internal networks to prevent unauthorized access to assets through geographically distant locations.

Remote access brings many information security threats to the organization. Risk of eavesdropping as information travels over the public internet, unauthorized access to systems or data, monitoring and manipulation of data and malware infections are common security risks associated with remote access.

To mitigate the risk of remote access, the organization shall use secure Virtual Private Networks (VPNs), allow only authorized users to access systems based on the identity management and access control policy of the organization, implement multi-factor authentication, secure remote access from client devices, and use trusted networks.

Compliance: Applicable to all government organizations

4.3.14. Policy on Backup Strategy

The organization shall have a strategy to backup data, logs, systems, software, configuration details and any other information that are necessary to restore to normal operations in an event of a disaster. This strategy shall be aligned with the organization's Disaster Recovery Plan (Refer Section 4.6.1).

The organization must ensure that the backups can be used to fully restore or recover any disrupted services.
Data written onto backup media shall be preserved as per the regulatory requirements of the government.

The organization shall also define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to determine the frequency of backups.
It is recommended to have an air gap between the live data and backup data for protecting live data from any malicious attacks including ransomware.

It is further recommended that backups be stored at a secure location which is physically distant from the data processing site. There should also be a mechanism implemented to detect any changes made to the backups.

Backups containing information assets labeled as "Secret" and "Confidential" shall be stored as per the security requirements specified in the Assets Register.

Compliance: Applicable to all government organizations

4.3.15. Policy on the Security of Assets Supplied by Government Organizations

Today many government and non-government organizations operate on the information and IT assets provided by the government. In this context, ICTA or other government organizations must ensure the security, reliability, integrity, and accuracy of the information and IT assets developed by them. For example, the security of Lanka Government Network, Lanka Government Cloud, Email Service, Lanka Government Payment System, SMS Service, Document Management System or other services should be guaranteed by the relevant organization that developed such infrastructure. The required security certificates for these infrastructures should be obtained by the relevant organizations from Sri Lanka CERT or from any other qualified institution.

Compliance: Applicable to ICTA and all government organizations

4.3.16. Policy on Security-by-Design

The organization shall follow a security-by-design approach in software acquisitions and in-house software development. The security-by-design approach extends the traditional software development approach by adding security considerations to each stage of the software development lifecycle.

In developing software (or acquiring software), the organization must consider security planning and conducting risk assessments at the project planning stage, defining security requirements in bidding documents, reviewing the security architecture in the design stage, reviewing code at the development stage for identifying security-related weaknesses (flaws), and performing vulnerability assessments in the implementation stage to identify security weaknesses in the systems. Finally, at the system decommissioning stage, the systems shall be securely disposed to ensure that its data and other information assets cannot be accessed and recovered by unauthorized individuals.

Further, in developing websites and web applications, government organization shall adhere to the "Website Security Guidelines", "Web Application Security Guidelines" and "Technical Guidelines for Web Application and Website Security" issued by Sri Lanka CERT. These guidelines can be downloaded from https://www.onlinesafety.lk website.

Compliance: Applicable to all government organizations

4.3.17. Policy on Secure Disposal of Assets

Assets shall be disposed securely using a formal procedure when no longer required. It is required that the organization’s storage media, which includes but is not limited to optical media (CDs or DVDs), magnetic media (tapes or diskettes), disk drives (external, portable, or removed from information systems), flash memory storage devices (SSDs or USB flash drives) and documents (paper documents, paper output, or photographic media) are disposed securely.

If the media contains information that is no longer required, the information shall be deleted in an unrecoverable manner to prevent the retrieval of the original information. Low level sector-based formatting is a possible method of removing information assets contained in media. Shredding or punching are possible ways of permanently destroying media that contain information assets.

If the assets in the storage media are classified as “Secret” or “Confidential” the safest method of disposal is physical destruction of the media, after obtaining proper approval for the disposal action from ISC.

Compliance: Applicable to all government organizations

4.3.18. Policy on Internal Information and Cyber Security Audit Process

The organization shall have a formal internal information security audit program in place to conduct routine audits that includes but is not limited to IT security control audits, application security control reviews, network architecture reviews, IT process audits, security compliance reviews, internal and external vulnerability assessments, penetration testing, and web application penetration testing.

Assessments shall be performed periodically (at least annually), after an incident has occurred, after a change is introduced (to application or hosting environment), after changes to standard/guidelines, after spread of virus or malware, or as determined by the ISC.
The (Chief) IA of the organization shall coordinate the audit, and the Chief IA of each Ministry shall coordinate information security audits of the organizations under its purview.

A formal process to oversee the implementation of recommendations made in audit reports is to be established by the organization. The (Chief) IA of the organization shall take the leadership and bear the responsibility for this process.
Audits shall be performed by a party qualified to carry out such audits or the organization shall obtain the services of Sri Lanka CERT.

If the audits are to be carried out by a third party, it is essential that a Non-Disclosure Agreement (NDA) is to be signed to ensure the confidentiality of the organization's assets.

Compliance: Applicable to all government organizations

4.3.19. Policy on Audits Prior to Deployment

On par with the internal information security audit program, the organization shall perform vulnerability assessments and penetration tests prior to the deployment of any website, web application or system on the live environment.

The organization needs to obtain the service~~s~~ of Sri Lanka CERT to conduct these assessments or shall obtain the services of a qualified third-party organization in consultation with Sri Lanka CERT.

Compliance: Applicable to all government organizations

4.3.20. Policy on Systems Hardening

The organization shall harden IT assets (operating systems, servers, networks and network devices, databases, and virtual private networks) to reduce their surface of vulnerability by eliminating potential attack vectors and condensing the system's attack surface. Guidelines on systems hardening are presented in the Information and Cyber Security Implementation Guide.

Hardening systems shall only be carried out with the support of experienced and skilled personnel.

Compliance: Applicable to all government organizations

4.3.21. Policy on Work from Home

With the transition to working from home (or work from distant locations), there is an increase in information security threats. Therefore, employees shall adhere to "Information Security Guidelines for Working from Home" issued by Sri Lanka CERT which outline a set of security best practices when working remotely.

Further, officers responsible for IT activities shall adhere to the "Guidelines to Improve Cyber Security to Enable Work from Home: Minimal Guidelines for IT Administrators" issued by Sri Lanka CERT to ensure secure access to organization's IT assets when working remotely is permitted. These guidelines are issued in compliance with the work-from-home guidelines issued by the government. The guidelines are available for reference on www.onlinesafety.lk website of Sri Lanka CERT.

Compliance: Applicable to all government organizations

4.3.22. Policy on Using Personal Devices for Official Work

The organization shall not allow employees to use their personal laptops, smartphones and tabs to carry out official duties. However, under specific circumstances determined by the ISC, the organization may allow selected employees to use their personal devices to perform official duties, under the supervision of the ISO. In such circumstances, it is imperative to appropriately register such devices with the organization and ensure that those devices comply with this Policy. However, Employees' personal devices shall not be used to process or store information classified as "Secret" and "Confidential" under any circumstance.

When employees' personal devices are used to perform official duties, the organization shall ensure that user accounts are set up to have limited privileges, accounts are protected with strong passwords and multifactor authentication, antimalware software is installed and automatic updates are enabled, operating systems, utility software and other application software that is used have valid licenses with necessary patch updates.

Further, the organization reserves the right to review or retain personal and organizational information on such devices, or to release the information to government agencies or third parties during an investigation or legal requirement. Security of the personal device shall be the responsibility of the owner of the device. The organization shall not be liable for any loss or damage to the device including loss of personal data due to the use of the device.

Compliance: Applicable to all government organizations

4.3.23. Policy on Using Non-Secure Networks

The staff of the organization shall avoid the use of non-secure networks, such as untrusted Wi-Fi networks (e.g. available in hotels, restaurants, bus stops), and the use of publicly shared personal computers, kiosks and other related devices to access official email and other official software solutions.

Compliance: Applicable to all government organizations

4.3.24. Policy on Management of Suppliers

The organization shall ensure appropriate measures are taken when external parties (providers of hardware, software, networks, hosting, and managed services etc.) are involved in developing and managing the information and IT assets.

In carrying out vendor management, the organization has to take into consideration the following as a minimum: (a) identifying the responsibilities and obligations of the contracted party including but not limited to backup, storage, recovery and contingency arrangements, security configurations, access to Information and IT

Assets, etc., (b) adherence to established information security practices of the organization as defined by the government, (c) right to audit the contracted party processes and controls related to the agreement, and (d) monitoring and reporting on non-adherence to contractual terms and conditions. The responsibility for managing relationships with contracted parties shall be assigned to Asset Owners, designated officers or entities, as decided by the HOO.

Compliance: Applicable to all government organizations

4.3.25. Policy on Change Management

The organization shall control all changes. Unmanaged changes pose risks to information and IT assets and have the potential to cause operational disruptions. For example, uncontrolled installations (or uninstallations), insertions, deletions, and modifications to systems may impact confidentiality, integrity and availability attributes of data or even result in vulnerabilities to systems that may lead to compromise of the system.

Further, personnel involved in changes may also pose threats to the confidentiality of operational information. ISC, therefore, shall implement a formal change management process to mitigate the overall security risk for the system.

Compliance: Applicable to all government organizations

4.4. Detect Incidents

The organization shall implement appropriate measures to identify information and cyber security incidents in a timely manner. The organization shall instruct staff to report any cyber security incidents, vulnerabilities or policy violations to relevant officials. Further, the organization shall deploy mechanisms for analyzing logs to identify incidents and adopt continuous monitoring solutions that detect anomalous activities and other threats to operational continuity.

Policies which the organization shall comply with regards to detecting information and cyber security incidents are presented below.

4.4.1. Policy on Reporting Incidents

Staff shall be clearly advised to immediately report any suspicious activity or any security violation to the ISO. Security violations shall include but are not limited to unauthorized access to a network, telecommunication or computer system, the apparent presence of a virus on computers, the apparent presence of any asset prohibited by organizations, apparent tampering with any file by unauthorized user, and violations of these guidelines or security policy by another user or contractor.

Users shall also be instructed to report any vulnerabilities existing on IT assets.

The organization shall provide adequate awareness and trainings to staff on detection of incidents, reporting information security events detected, and preserving evidence.

Compliance: Applicable to all government organizations

4.4.2. Policy on Reviewing Logs

The organization shall maintain and review Logs (access logs, error logs, server logs, audit logs, firewall logs and antimalware logs) generated by systems and associated components to detect incidents.

The organization shall regularly review logs to detect malicious attacks on systems, and to determine the causes of errors or security breaches.

Logs shall be protected against tampering and unauthorized access. In the case of logs containing sensitive and personally identifiable information, appropriate privacy protection measures shall be taken prior to storing and analysis. Logs shall be retained for a period of 12 months or as determined by ISC.

Compliance: Applicable to all government organizations

4.4.3. Policy on Continuous Monitoring of Incidents

The organization shall monitor networks or systems for detecting malicious activities, and counter such activities through implementing Intrusion Detection Systems and Intrusion Prevention System (IPS/IDS). The organization can also use Security Information and Event Management (SIEM) systems for security monitoring, and advanced threat and incident detections.

Compliance: Applicable to all CNII providers

4.4.4. Policy on Reporting Incidents to Sri Lanka CERT

As determined by the ISC, the organization is advised to report critical information security incidents to Sri Lanka CERT immediately for technical advice and handling.

Compliance: Applicable to all government organizations

4.5. Respond to Incidents

In order to effectively respond to information and cyber security incidents, the organization shall develop an incident response plan, and activate the plan in the event of an incident. Policies that the organization shall comply in responding to information and cyber security incidents are presented below.

4.5.1. Policy on Incident Response Plan

The organization shall develop an Incident Response Plan which consists of a set of predetermined instructions and procedures to detect, respond, and limit the negative consequences of an information and cyber security incident against an organization’s assets. This shall also include a clear set of instructions and procedures to effectively recover from the incident.

The Incident Response Plan shall contain, at a minimum, incident reporting procedures, strategies for detection, analysis and, containment of incidents (eradication or recovery), allocation of information security responsibilities to designated staff, and procedures related to post-incidents reviews.

The Incident Response Plan shall be tested time to time and communicated to all staff members of the organization.
Guidelines to develop an Incident Response Plan are presented in the Information and Cyber Security Implementation Guide.

Compliance: Applicable to all government organizations

4.5.2. Policy on Activating Incident Response Plan

In the event of an information security incident, the designated authorized person shall activate the incident response plan to minimize the impact on the organizational operations, and to resume normal operations after the incident.

The organization shall maintain an Incident Register to record information related to the incidents. Incident Register shall contain the following information at a minimum: date and time of the incident, name and designation of the employee who reported the incident, description of the incident, nature of the impact, classification of the incident, action taken in response to the incident, officer in charge of handling the incident, current status of the incident and so forth.

Guidelines for responding to incidents are presented in the Information and Cyber Security Implementation Guide.

In the event of an information and cyber security incident, the organization has to initiate procedures to identify, collect and preserve information, which can serve as evidence that can be used in forensics investigations. The policies related to forensic investigation is presented in Section 4.5.3.

Compliance: Applicable to all government organizations

4.5.3. Policy on Forensic Investigations

In the event where forensic investigation is required, the organization shall follow a formal investigation process. The evidence related to forensic investigation can be captured through a wide range of electronic means such as physical documents, data on the hard disks, device logs, CCTV footage, email records, voice records and other electronic records, etc.

Since electronic evidence is different from traditional evidence as to its nature of intangibility, volatility and replicability, expert knowledge is essential to deal with such evidence. The organization shall obtain the technical assistance from Sri Lanka CERT or a relevant organization which has such technical capabilities.

In a forensic investigation, the chain of custody shall be maintained by the organization which requires the following information at a minimum: details of the incident and collected evidence, date and time of the evidence collected, the name and the designation from whom the evidence was obtained and the history of transferring the evidence. ISO shall maintain the chain of custody that shall be presented in an investigation.

It is required that the ISO of the organization has the responsibility of retaining and preserving all evidence that concerns ongoing, pending or foreseeable claims. This includes the responsibility of not to lose, destroy, or intentionally alter documents, electronic records, or similar instruments that can be used as evidence.

In a forensic investigation, legal frameworks related to personal data protection, computer crimes, payment device frauds, electronic transactions and any other relevant laws shall be applied.

Compliance: Applicable to all government organizations

4.6. Recover Normal Operations

The organization shall develop and implement a plan of effective activities to restore any capabilities or services that were impaired due to a disaster.

Policies that the organization shall comply in recovering from disasters or information and cyber security incidents are presented below.

4.6.1. Policy on Disaster Recovery Plan

The organization shall have a Disaster Recovery Plan that will be activated in an event of a disaster (or incident) to facilitate recovery from such disaster (or incident).

The Disaster Recovery Plan shall contain activities to be performed to recover from a disaster, and roles and responsibilities of each team member in the plan.

Disaster Recovery Plan shall be designed by conducting a risk assessment and a business impact analysis of the information and IT assets, and the recovery activities shall be designed by considering the earliest point in time at which it is acceptable to recover the data (recovery time objective), and the earliest point in time at which the organization’s operations and systems must be resumed after a disaster (recovery point objective).

The Disaster Recovery Plan shall be tested and updated on a periodic basis.

Compliance: Applicable to all government organizations

4.6.2. Policy on Activating Disaster Recovery Plan

In an event of a disaster, the designated authorized person shall activate the disaster recovery plan to minimize the impact on the organization’s operations, and to resume normal operations after the event.

Compliance: Applicable to all government organizations

4.6.3. Policy on Crisis Communication

In the event of a major crisis (e.g. critical disaster, cyber security incident), as decided by the HOO, the organization shall communicate with internal and external parties such as the ministry in charge of the organization, Sri Lanka CERT, victims, media, clients, and law enforcement authorities according to a plan. The organization shall appoint a senior responsible officer to communicate the crisis to the relevant stakeholders.

Compliance: Applicable to all government organizations

5. Policies to be Implemented on a Priority Basis

In order to implement the Information and Cyber Security Policy within the organization, the following policies need to be implemented at the priority basis.

Policy Area	Policy No.	Policies to be Implemented on a Priority Basis	All Organizations	CNII Providers
Information and Cyber Security Governance	4.1.1	Providing leadership to implement the Information and Cyber Security Policy by the HOO.	✓	✓
	4.1.2	Establishment of an Information and Cyber Security Organizational Structure.	✓	✓
	4.1.2 (a)	Appoint an ISO and delegate information and cyber security responsibilities.		✓
	4.1.2 (b)	In the absence of an ISO, assign responsibilities to the CIO to protect information and IT assets.	✓	
	4.1.2 (C)	Assign responsibilities to (Chief) IA to coordinate information and cybersecurity audits.	✓	✓
	4.1.3	Appoint an ISC.	✓	✓
	4.1.4	Appoint RMC.		✓
	4.1.5	Identify user responsibilities and communicate to users.	✓	✓

	4.1.6	Capacity building of officials responsible for information and cyber security.	✓	✓
	4.1.7	Perform security clearance and background checks on staff handling information assets classified as secret and confidential or staff using CNII.		✓
	4.1.8	Align information and cybersecurity activities with the vision, mission and objectives of the organization.	✓	✓
	4.1.9	Develop and implement information and cyber security action plans.	✓	✓
Identify Assets, Asset Owners and Risks	4.2.1	Identify information, IT assets and CNII.	✓	✓
	4.2.3	Identify Asset Owners, Custodians and assign responsibilities to protect assets.	✓	✓
	4.2.4	Maintain information and IT assets registers.	✓	✓
	4.2.5	Perform risk assessments for information and IT assets.		✓
	4.2.6	Classify information and IT assets based on their value and sensitivity.	✓	✓
Protect Assets	4.3.1	Protect data at rest.	✓	✓
	4.3.2	Protect data at transit.	✓	✓
	4.3.3	Ensure physical security of information and IT assets.	✓	✓
	4.3.4	Control user access to information and IT assets.	✓	✓

	4.3.5	Ensure strong authentication.	✓	✓
	4.3.6	Ensure data Sovereignty in an appropriate manner.	✓	✓
	4.3.7	Use valid licensed software and update the latest patches.	✓	✓
	4.3.8	Install antimalware software.	✓	✓
	4.3.9	Use official email for official communications.	✓	✓
	4.3.10	Ensure security of emails.	✓	✓
	4.3.11	Use digital signatures as appropriate.	✓	✓
	4.3.12	Implement perimeter security controls.	✓	✓
	4.3.13	Use secure remote access methods.	✓	✓
	4.3.14	Use a backup strategy.	✓	✓
	4.3.16	Ensure security by design principles in software development and acquisition.	✓	✓
	4.3.17	Ensure secure disposal of Assets.	✓	✓
	4.3.18	Implement an internal information security audit process.	✓	✓

	4.3.19	Perform risk assessments and penetration tests prior to the official launch of website, web application or any other system.	✓	✓
	4.3.20	Strengthen the security resilience of IT assets.	✓	✓
	4.3.21	Follow work from home guidelines in remote working.	✓	✓
	4.3.23	Prevent using untrusted networks.	✓	✓
	4.3.24	Manage suppliers.	✓	✓
	4.3.25	Manage changes.	✓	✓
Detect Incidents	4.4.1	Instruct staff to report incidents.	✓	✓
	4.4.2	Review logs to identify incidents.	✓	✓
	4.4.3	Identify incidents by continuously monitoring the events.		✓
	4.4.4	Report incidents to Sri Lanka CERT.	✓	✓
Respond to Incidents	4.5.1	Develop Incident Response Plan.	✓	✓
	4.5.2	Activate Incident Response Plan in an event of incident.	✓	✓
	4.5.3	Perform forensic investigations on incidents.	✓	✓

Recover Normal Operations	4.6.1	Develop Disaster Recovery Plan.	✓	✓
	4.6.2	Activate Disaster Recovery Plan in an event of disaster.	✓	✓
	4.6.3	Develop Crisis Communication Plan.	✓	✓

6. Methodology for Monitoring and Evaluating the Information and Cyber Security Policy

6.1 Prior to the implementation of the Policy, it is essential to understand the overall information and cyber security readiness of the government organization. This assessment tool is therefore designed to assess the overall information and cyber security readiness, and the progress of the adoption of the Policy by government organizations.

6.2 Accordingly, the Sri Lanka CERT shall perform a preliminary assessment of the readiness of government organizations in implementing the Policy based on the questions presented in Section 6.6. Based on the findings, recommendations will be made to government organizations in implementing the Policy.

6.3 Sri Lanka CERT shall evaluate the level of policy compliance by each government organization on an annual basis, and shall present the level of compliance on an Information Security Index. Based on the revaluation results, Sri Lanka CERT shall make recommendations to improve the overall information and cyber security readiness of the organization.

6.4 To evaluate the performance (or readiness) of implementing the Policy within the organization, the questionnaire presented in Section 6.6 which contains approximately 50 questions, will be used. ISO, CIO or Officer in charge of the subject of IT shall complete and submit the questionnaire to Sri Lanka CERT on or before October 30th of each year, with the signature of the HOO.

6.5 Should the respondent wish to provide a detailed response to each question, the respondent can provide details in the remarks section at the end of the survey questionnaire. Respondents can refer to the Glossary of this document for detailed explanation of relevant terms.

6.6 Assessment Questionnaire

All government organizations are required to respond to every question up to the best of their knowledge.

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Information and Cyber Security Governance					
Security Organization Structure	1. Has the organization appointed an ISO?	4.1.2 (a)			
	2. Has the organization assigned information and cyber security responsibilities to ISO?	4.1.2 (a)			
	3. In an absence of ISO, has the CIO or the officer in charge of the subject of IT been assigned information and cyber security responsibilities?	4.1.2 (b)			
	4. Has the organization assigned information security audit responsibilities to (Chief) IA?	4.1.2 (c)			
	5. Does the organization have a Committee to make decisions on information and cyber security?	4.1.3			
	6. Does the organization have a committee to make decisions on information and cyber security risks?	4.1.4			
End User Responsibilities	7. Has organization explained the end user responsibilities to users?	4.1.5			
Capacity Building	8. Has the organization taken any steps to develop the information security capacity of accountable individuals?	4.1.6			
Background Checks	9. Does your organization perform background checks and security clearance on officials dealing with “Secret” or “Confidential”, information assets or having access to CNII ?	4.1.7			
Strategic Alignment	10. In designing and implementing the organization’s functions, policies, strategies or projects, has your organization taken information security into account?	4.1.8			
Action Plan	11. Does your organization have financial provisions for information security activities?	4.1.9			
	12. Has your organization developed action plans to achieve its information security objectives?	4.1.10			

Identify Assets, Owners, Users, and Risks					
Identification of Assets	13. Has your organization identified information assets that have a value to the organization?	4.2.1			
	14. Has your organization assessed risk associated with information assets?	4.2.5			
	15. Has your organization classified information assets based on their sensitivity or other means?	4.2.6			
	16. Has your organization recorded information assets in an Information Assets Register?	4.2.4			
	17. Has your organization identified IT assets?	4.2.1			
	18. Has your organization recorded IT assets in an IT Assets Register?	4.2.4			
	19. Has your organization classified IT assets based on their criticality?	4.2.6			
	20. Has your organization identified the Owners of the assets?	4.2.3			
Protect Assets					
Encryption	21. Does your organization encrypt sensitive information prior to storage?	4.3.1			
	22. Does your organization encrypt sensitive information prior to moving through electronic channels?	4.3.2			
Physical Protection	23. Does your organization process or store sensitive information in secure areas?	4.3.3			
	24. Has your organization taken appropriate measures to protect secure areas from fire, flood, humidity and temperature?	4.3.3			
	25. Does your organization prevent unauthorized entry to secure areas?	4.3.3			
Identity Management and Access Control	26. Does your organization have an Identity Management and Access Control Policy?	4.3.4			
	27. Does your organization use strong authentication?	4.3.5			
Data Sovereignty	28. Does your organization ensure Data Sovereignty?	4.3.6			
	29. Does your organization assess risk prior to obtaining cloud service?	4.3.6			
Licensed Software and Patch Updates	30. Does the organization use operating systems (OSs) with valid License(s)?	4.3.7			
	31. Have the OSs (s) of the organization been updated with vendor supplied latest patches and fixes?	4.3.7			

	32. Does your organization have a procedure in place to ensure vendor supplied critical patches are installed on time?	4.3.7			
Antimalware	**33.** Has the organization installed Antimalware software with a valid license in all machines?	4.3.8			
Email	**34.** Does your organization restrict users from using personal emails for official communications?	4.3.9			
	35. Does your organization set up email filters to remove emails known to have malware attached?	4.3.10			
	36. Does your organization use encryption when sending sensitive information via email?	4.3.10			
Perimeter Security Devices	**37.** Does your organization have a Firewall in your computer network?	4.3.12			
Secure Remote Access	**38.** Does your organization use secure Virtual Private Networks (VPNs) for remote access?	4.3.13			
	39. Do all the users connecting remotely use VPN?	4.3.13			
Backup Strategy	**40.** Does your organization backup data?	4.3.14			
	41. Are the backups stored at a fire proof, secure location which is physically distant from the data processing site?	4.3.14			
Secure Disposal of Assets	**42.** Does your organization follow any of the following to dispose electronic media that contain sensitive information? - Shredding, punching, physically damaging, degaussing.	4.3.17			
Internal Information Security Audit Program	**43.** Does your organization have internal information security audit program?	4.3.18			
	44. Does your organization perform VAPTs through Sri Lanka CERT prior to any deployment of software applications?	4.3.19			
	45. Have you performed VAPT for your computer network?	4.3.19			
Work from Home	**46.** Does your organization adhere to the work from home guidelines issued by Sri Lanka CERT?	4.3.21			
	47. Does your organization have a formal procedure to register personal devices?	4.3.22			

Using Personal Devices for Official Work	**48.** Does your organization allow personal devices to process or store critical data?	4.3.22			
Detect Information Security Incidents					
Report Incidents	**49.** Has the organization instructed staff to report any suspicious activity, contact, theft, virus, vulnerability, unauthorized access, tampering with files, or violation of security policy to the person in charge of Information security?	4.4.1			
	50. Have you ever reported cyber security incidents to Sri Lanka CERT or any other party?	4.4.4			
Respond to Incidents					
Incident Response Plan and Activate the Plan	**51.** Has your organization developed an Incident Response Plan?	4.5.1			
	52. In the event of an information and cyber security event, does the organization activate an Incident Response Plan to minimize the impact on its operations and restore that operation?	4.5.2			
Recover from Incidents					
Disaster Recovery Plan and Activate the Plan	**53.** Does your organization have a Disaster Recovery Plan developed to facilitate the recovery in an event of a disaster?	4.6.1			
	54. In the event of a disaster (or event), does the organization activate its Disaster Recovery Plan to restore disrupted services?	4.6.2			

Glossary

Antimalware	Anti-malware is a software designed to identify malware in devices or prevent malware from infecting computer systems or electronic devices. Malware is any software intentionally designed to cause damage to a computer, server, or computer network (e.g. viruses, worms, ransomware).
Assets Classification	Classification is the process of categorizing information assets based on the level of sensitivity and criticality of that information. The primary objective of asset classification is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
Assets Custodian	Person in the organization who has the responsibility to protect an information asset throughout the lifecycle as it is stored, transported, or processed in line with the requirements defined by the information asset owner.
Assets Owner	An asset owner is a senior executive grade official responsible for the day-to-day management of assets. The asset owner controls the entire life cycle of the asset and must identify the risks to the assets and suggest appropriate security measures to protect them.
Availability of Information	Availability ensures timely and reliable access to and use of information.
Confidentiality of Information	Confidentiality refers to the assurance that information is not disclosed to unauthorized people and organizations.
Sensitive Information Assets	Any information the loss, alteration, misuse, disclosure or failure of which could adversely affect the interests of the organization or relevant individuals or entities. These information assets can be classified as “secret” and “confidential” by the government organization.
Critical IT Assets	Critical IT assets are systems, the unauthorized access, misuse, or failure of which can adversely affect data, organization, or individuals. These IT assets can be classified as “very critical” and “critical” by the organization. Further, these IT assets require a high level of security and may also exist in the form of CNII as defined below.
Critical National Information Infrastructure (CNII)	Critical information infrastructure are the systems or facilities, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy, health and social well-being of a nation.
Digital Signature	Digital Signature is a mathematical scheme for verifying the authenticity of digital messages or documents. It provides sender authenticity (identity of the users), message integrity (guarding against improper modification or destruction), and nonrepudiation (the claimed sender cannot later deny generating the document).
Encryption	Encryption is the process of converting a plaintext message into a secure-coded form of text, which cannot be understood without converting it back via decryption.
Government Organizations	The government organizations are the public authorities defined in the Right to Information Act No. 12 of 2016.

Information Security Controls	Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to information and IT assets. Controls could be technologies, policies, procedures, or processors put in place to protect information assets.
Information Security Officer (ISO)	An Information Security Officer is a senior-level executive responsible for establishing and maintaining the organization's objectives, strategy, and action plans to ensure information assets are adequately protected.
Information Security Committee (ISC)	In implementing the policy, this committee is responsible for reviewing and approving all information security controls, action plans, asset classification schemes, incidents response plans and disaster recovery plans and other activities carried out by the ISO.
Information and Event Management systems (SIEM)	SIEM is a solution that combines the collection data from log files for analysis and reports on security threats and events, and conduct real-time system monitoring, notifies network admins about important issues and establishes correlations between security events to provide real-time analysis of security alerts generated by applications and network hardware.
Information and Cyber Security	Information and cyber security is the protection of information assets from unauthorized access, use, modification, or destruction to ensure confidentiality, integrity and availability of the information. This includes protection of IT assets that contain or use informational assets from malicious actions of individuals with the use of cyber technology or other means, and from other natural disasters such as floods and fires.
Information Assets	Information asset is information or data that is of value to the organization. This includes the documents available in an electronic format, database records as well as the documents available in paper format. Examples for information assets: word file, images, employees personal record in a database.
IT Assets	IT asset is any IT equipment, information system, software, storage media that is of value to the organization. Examples for IT assets are computers, servers, routers, disks, networks, software, information systems and its components.
Intrusion Detection and Prevention Systems (IPS/IDS)	Intrusion Detection Systems are devices that analyze network traffic to identify known cyberattacks. Intrusion Prevention Systems devices analyzes network traffic to identify known cyberattacks, however, it can stop attacks by preventing packet from being delivered based on type of attacks it detects
Integrity of Information	Integrity refers to guarding information against improper modification. It ensures that information remains in its original form.
Official Email	Official emails are the email accounts supplied by the government with the domain name of “gov.lk
Private Cloud	Services offered over the Internet or over a private internal network to only select users. E.g. Lanka Government Cloud
Public Cloud	Cloud service available to anyone who wants to purchase them
Recovery Point Objective (RPO)	RPO is a measure of how often the organization should take backups, and it gives an indication of how up to date the recovered data will be. It indicates the earliest possible time in which it is acceptable to recover the data. For example, if a disaster occurs between backups, can the

	organization afford to lose 2 minutes' worth of data, or 2 hours or full day.
Recovery Time Objective (RTO)	RTO indicates the amount of downtime a business can tolerate. It is the earliest point in time at which the organization's operations and systems must be resumed after a disaster.
Systems Hardening	System hardening is the process of securing a system through changing the default configuration and settings to reduce IT vulnerability and the possibility of being compromised. This can be done by reducing the attack surface and attack vectors which attackers continuously try to exploit for the purpose of malicious activity.
Virtual Private Network (VPN)	Virtual Private Network, establishes a secure connection by utilizing an encrypted tunnel for data communication over the internet.

References

1. Information Security Implementation Guide. Published in 2022, by Research, Policy and Project Division of Sri Lanka CERT. Document can be accessed through www.onlinesafety.lk.

2. Minimum Information Security Guidelines. Published by Research, Policy and Project Division of Sri Lanka CERT. Document can be accessed through www.onlinesafety.lk.

3. Information and Cyber Security Strategy of Sri Lanka (2019:2023), Published in November 2019 by Research and Policy Unit, Sri Lanka CERT. Document can be accessed through https://cert.gov.lk/documents/NCSStrategy.pdf.

4. NIST Cybersecurity Framework. Published by National Institute of Standards and Technology, U.S Department of Commerce. Resource can be accessed through https://www.nist.gov/cyberframework/online-learning/five-functions.

5. Information Security Guidelines for Working from Home. Published by Sri Lanka CERT. Document can be access through https://www.onlinesafety.lk.

6. Website Security Guidelines for Government Organizations. Published by Research, Policy and Projects Division of Sri Lanka CERT, in 2022. Document can be accessed through https://www.onlinesafety.lk.

7. Web Application Security Guidelines for Government Organizations. Published by Research, Policy and Projects Division of Sri Lanka CERT, in 2022. Document can be accessed through https://www.onlinesafety.lk.

8. Technical Guidelines for Web Application and Website Security. Published by Research, Policy and Projects Division of Sri Lanka CERT in 2022. Document can be accessed through https://www.onlinesafety.lk.

9. ISO 27002 (2013): Information Technology – Security Techniques - Information Security Management Systems – Requirements, International Standards Organization, Published by International Standard Organization. Document can be accessed through https://www.iso.org.