Information and Cyber Security Policy for Government Organizations

Sri Lanka Computer Emergency Readiness Team

Ministry of Technology

Version 1

Document Classification: Public

Versions

Version	Prepared by	Reviewed by	Authorized by	Issue Date	Description
1	Research, Policy and Projects Team of Sri Lanka CERT Date: 25th August 2021	Policy Review Committee, Senior Management of Sri Lanka CERT Date: 08th October 2021	Board of Directors of Sri Lanka CERT Date:		Version 1

Attribution

This publication shall be attributed as follows
Democratic Socialist Republic of Sri Lanka, Sri Lanka CERT|CC, Information and Cyber Security Policy for Government Organizations – Version 1, October 2021

Published by

Research, Policy and Projects Division
Sri Lanka CERT|CC
Room 4-112, BMICH, 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

Note

This publication will remain as a “Draft Version” until being approved by the relevant Authority to adopt as a Policy.

Table of Contents

Acronyms

AMC	Audit and Management Committee
CCTV	Closed-circuit Television
CD	Compact Disk
CERT	Computer Emergency Readiness Team
CIA	Chief Internal Auditor
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
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

Executive Summary

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.

To effectively address these cyber security risks, the Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), the organization which has the mandate for protecting the cyber space in Sri Lanka, has developed an Information and Cyber Security Policy for use by government organizations in order to protect their digital systems and resources from various cyber security threats. The policy provides a risk based approach for implementing an information security program at organizational level, and guides organizations in identifying digital assets that should be protected, developing appropriate measures to protect assets, detecting information security incidents and in responding to and recovering from cyber security attacks in an efficient and effective manner.

The policy is developed based on the international best practices and standards such as International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST), and has been extensively reviewed by the information security experts and senior government officers.

Approval from the Cabinet of Ministers will be obtained for the Policy for mandatory use by all the government organizations, with the instructions that all the heads of organizations are accountable for the implementation of the policy. Sri Lanka CERT shall facilitate and provide recommendations to all government organizations in implementing the policy, and shall evaluate the performance of organizations in implementing the on an annual basis.

1. Introduction

1.1. Government organizations in Sri Lanka have progressed rapidly over the past decade in developing digital systems to carry out their daily administrative work and to provide services to the general public, other government organizations as well as to the private sector. As organizations become increasingly dependent on digital systems, protecting information and digital infrastructure from unauthorized access, disclosure and destruction, and from natural disasters such as floods and fire have also become a high priority. Information and cyber security policies therefore, should be implemented in organizations to protect digital systems and reduce the risk of operational disruptions in order to provide services in a secure and efficient manner.

1.2. This document presents the information and cyber security policy for government organizations. It provides a set of policy statements that specifies the direction upon which controls, standards and guidelines should be implemented by government organizations in handling information security threats, protecting hardware, software and data, mitigating vulnerabilities, and establishing an information and cyber security governance structure. It further provides guidelines to employees on their responsibilities in relation to information and cyber security.

1.3. All the government organizations that are defined as public authorities in the Right to Information Act No 12 of 2016[1], are required to comply with the policy statements outlined in this document. Heads of organizations are required to understand the content of the policy, provide leadership to the implementation of the policy, and assume ultimate accountability and responsibility for the organization's information security activities and staff.

1.4. The policy statements shall be used to benchmark each organization’s status in adopting information and cyber security measures on an annual basis. This will enable organizations to identify the areas which need attention and where improvements need to be carried out to secure the organization against various cyber security threats.

2. Information Security Policy Framework

2.1. In line with the implementation of the Information and Cyber Security Strategy (2019:2023)[2], the Information Security Policy Framework is developed to assist government organizations to implement Information and Cyber Security Policy. The Policy Framework facilitates government organizations by providing other necessary resources such as the Minimum Information Security Standards (MISS)[3], the Information Security Implementation Guide[4], and the Technical Guides that are necessary for organizations to protect information, systems and digital assets from various information security events. Figure-1 presents an overview of the Information Security Policy Framework.

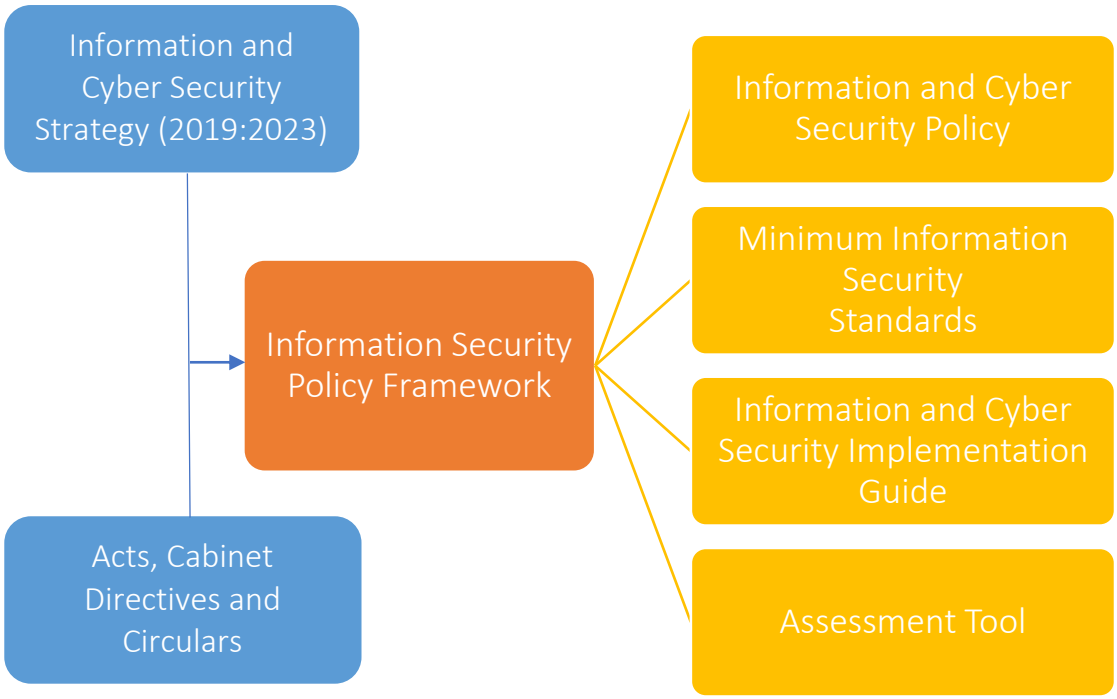

Figure-1. Information Security Policy Framework

2.2. The information security policy framework includes the following:

2.2.1. Information Security Policy which is the main focus of this document, provides a set of policy statements which organizations shall comply with. These policy statements outline the essential controls and provides direction to government organizations in protecting information, systems and infrastructure from information security events.

2.2.2. Minimum Information Security Standards[3] outline the minimum acceptable level of information security controls that shall be adhered to by the respective organizations. Two sets of minimum security standards are developed; one for organizations maintaining critical national information infrastructure (CNII), and the other for organizations which fall into the category of non CNIIs. Organizations maintaining CNII are required to adhere to a higher level of standards as disruption to such services would have a significant impact on the country's economy, national security and public health.

2.2.3. Information and Cyber Security Implementation Guide[4] provides a comprehensive set of instructions to staff and stakeholders who require more specific details on implementing the Policy. These technical guides include the Web Application Security[5], Identity Management and Access Control Policy[6], and Work from Home Guidelines (for general users[7] and IT administrators[8]).

2.2.4. Readiness Assessment Tool provides an assessment criterion to assess performance and the readiness in respect to adoption of Information and Cyber Security Policy at government organizations. Through this tool organization's overall information security maturity will be measured by the Sri Lanka CERT over a predefined time frame. A sample assessment instrument developed for this purpose is presented in Section 5 of this document.

2.3. The Information Security Policy Framework is governed by Acts of Parliament (forthcoming Cyber Security Act and Data Protection Act), Cabinet directives, and Circulars issued on this subject, and it is consistent with recognized international information security standards such as the International Organization for Standards (ISO) 27002: 2013[9] and National Institute of Standards and Technology (NIST) of United States[10],[11], and national policies such as e-Government Policy of Sri Lanka[12], and National Data Sharing Policy of Sri Lanka[13]. Further, the development of the Policy Framework has taken into consideration the experience of the Sri Lanka CERT, opinions of the information security professionals in the industry, and expert advice of the public sector senior executives.

3. Information and Cyber Security Policy

3.1. Introduction

3.1.1. The Information and Cyber Security Policy sets forth rules, guidelines and processes for government organizations, creating a standard for the acceptable use of organization's information technology, including information, systems and digital infrastructure to preserve confidentiality, integrity and availability of information and systems used by organizations.

3.1.2. The specific objectives of the policy are,

- To establish a common information and cyber security standard across different administration layers of the public sector.
- To establish a governance framework at organizational level to direct and control the activities in relation to information and cyber security.
- To 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.
- To 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.
- To educate staff on the best practices and national standards on information and cyber security, and build staff confidence over the organization's security status.

3.1.3. This Policy is written in simple language, and it is expected that all staff and relevant third party service providers, regardless of their knowledge of the subject, will be able to read the policy and understand the responsibilities of the organizations, and the expected outcome of the policy implementation in relation to protection of government information, critical information infrastructure and IT assets.

3.1.4. This Policy is applicable to any type of government organization that are defined as public authorities in the Right to Information Act No 12 of 2016[1]. The Policy shall also be applicable to the relevant third party service providers who manage IT services on behalf of the government organizations.

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. The Information and cyber security policy is developed based on information security governance principles, and several concurrent and continuous information security functions (identify, protect, detect, respond and recover) proposed by the NIST[10]. Figure 2 presents an overview of the information and cyber security policy, and Table 1 summarizes the scope of the policy statements.

Figure-2. Overview of the Policy

3.2.1.1. **Information security governance principle:** Information security governance principle generally refers to the principle that directs and controls the IT security of an organization[14,15].

An acceptable governance principle would require the organizations to establish a security organizational structure and appoint officers responsible for information security, undertake capacity building of such officers, define

organizations' information security objectives, develop action plans, and secure funding for information security activities.

3.2.1.2. Identify function: The identify function facilitates organizations to develop an adequate understanding of how to effectively manage information and cyber security risk to systems, assets, data, and functionalities (adopted from NIST[10]).

To comply with the identify function, organizations shall identify assets which are in the forms of information, critical information infrastructure and IT devices, and assess the risks associated with those assets to establish a formal asset management system.

3.2.1.3. Protect function: The protect function outlines appropriate safeguards required to ensure uninterrupted delivery of critical infrastructure services (adopted from NIST[10]).

To comply with the 'protect' function, organizations shall implement appropriate controls and safeguards to prevent, limit or contain the impact of a potential information security event or incident. This includes but is not limited to controlling user access to assets, installing firewalls, antimalware software, conducting systems audits, data encryption, and establishing backup strategy.

3.2.1.4. Detect function: The detect function defines the appropriate mechanisms required to identify the occurrence of a cybersecurity event (adopted from NIST[10]).

To comply with policy statements covered by the 'detect' function, the organizations shall put in place mechanisms to detect information and cyber security activities and events in a timely manner. Organizations shall analyze logs and deploy automated tools to detect incidents in an efficient manner.

3.2.1.5. Respond function: The respond function defines the actions that should be taken in response to a detected information and cybersecurity incident or an event (adopted from NIST[10]).

To comply with this function, organizations shall develop and implement incident response plan for responding to an information and cyber security event in efficient and effective manner.

3.2.1.6. Recover function: The recover function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an information and cyber security incident (adopted from NIST[10]).

To comply with 'recover' function, the organization shall develop disaster recovery plan and activate disaster recovery plan to timely recover normal operations to reduce the impact from an information and cyber security incident.

Table 1. Scope of Policy Coverage

Policy Aspect	Description
Governance – *establish governance structure*	○ Information security leadership ○ Security organization structure ○ Personnel security ○ Strategic alignment, action plans ○ Capacity building ○ Policy compliance ○ End user responsibilities
Identify – *identify organization's assets*	○ Identify information, IT assets and critical information infrastructure ○ Risk assessment ○ Classify assets ○ Identify assets owners
Protect – *protect assets by implementing controls*	○ Protect assets based on the risk associated with each asset ○ Implement appropriate controls/measures such as: - Physical protection - Restrict user access - Security by design - Licensed software - Perimeter security, Antimalware - Backup strategy - Systems audits - Secure remote access - Secure disposal of assets - Security best practices for work from home, Bring your owned devices
Detect – *detect incidents*	○ Detect the occurrence of security events in timely manner - Identify incidents by staff - Review logs generated by systems ○ Implement systems to monitor cybersecurity event ○ Report incidents to Sri Lanka CERT
Respond – *respond to incidents*	○ Develop incident response plan ○ Activate incident response
Recover - *recover from incidents*	○ Develop disaster recovery plan ○ Activate disaster recovery plan ○ Crisis communication

4. Policy Statements

4.1. Information Security Governance

Information security governance 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 further specifies the importance of strategic alignment, capacity building of accountable individuals, development of action plans, and policy compliance.

4.1.1. 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 establish the organization's information and cyber security program, set up information security goals and priorities that support the vision and mission of the organization, and ensure resources are available to support the information security activities and make it successful.

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 organizations

4.1.2. Security Organization Structure

The organization shall establish an information security organizational structure. 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. An effective information security organizational structure includes key roles such as (1) Information Security Officer, (2) Chief Innovation Officer, and (3) Chief Internal Auditor.

A. Information Security Officer (ISO)

As per the instructions given in the Circular MDIT/Dev/07/15 (23-05-2019), 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 information security

strategies, policies and action plans to ensure that the organization's information and assets are adequately protected.

The ISO shall be the "point of contact" for the subject of information security, and will be responsible for coordinating security policy compliance efforts with Sri Lanka CERT and other stakeholders.

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 CNII operators

B. 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 IT shall be empowered to play the role of the ISO.

Compliance: Applicable to all organizations

C. Chief Internal Auditor (CIA)

CIA shall be assigned the responsibilities of initiating and overseeing information security audits of the organization, assessing the progress of adopting information security and standards, and reporting information security related findings to the Audit and Management Committee (AMC) for further actions.

Compliance: Applicable to CNII operators

4.1.3. Information Security Committee (ISC)

The organization shall establish an Information Security Committee to provide strategic directions to activities related to information security. This committee shall be responsible for reviewing and approving all information security controls, action plans, assets classification schemes, security policies, incident response plans and disaster recovery plans developed by the ISO, and shall monitor the implementation of such plans. The HOO shall chair the Committee, and the Committee shall consist of the ISO, CIO, CIA, and asset owners.

Compliance: Applicable to CNII operators

4.1.4. 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 process owners (sectional heads), asset owners, and the ISO. The deputy Head of the organization shall be the chairperson of the Committee.

Compliance: Applicable to CNII operators

4.1.5. End User Responsibilities

Information security is everyone's responsibility. All end users are required to behave responsibly and comply with the 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[4], and applicable information security practices required by this Policy.

Misappropriation 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 organizations

4.1.6. Capacity Building

The organization shall build the information security capacity of the accountable individuals (ISO, CIO, CIA, Assets Owners, etc.) and the end users through conducting information security awareness and training.

Information security awareness activities shall be carried out to promote security, and to inform the staff of security measures. Training activities are essentials to build relevant and needed security knowledge and skills among the government staff.

Information security capacity building shall be an ongoing activity of the organization and it shall be included in the annual training plan.

Compliance: Applicable to all organizations

4.1.7. Personnel Security

Any one appointed or transferred to a role or position that involves dealing with information classified as "Secret" or "Confidential", or accessing CNII must go through a security clearance before they are appointed for or transferred to such position, and

periodic security clearance checks during their tenure.

Wherever necessary the organization shall review the background of designated officials before they are appointed to positions related to information security.

Compliance: Applicable to CNII operators

4.1.8. Action Plans

The organization shall develop and implement information security action plans (long term, medium and short term plans) which defines the way in which security is to be guaranteed in realizing the objectives of the organization.

Based on the information security priorities determined by a risk assessment, the organization shall also allocate a budget for information security activities in the action plans.

Compliance: Applicable to all organizations

4.1.9. Strategic Alignment

The organization's information security action plans which include projects and activities shall be designed in such a way that those initiatives are linked with the organization's objectives.

Each organization shall analyze the organizational objectives to identify dependencies on information security, and then link information security objectives to overall organizational activities.

Compliance: Applicable to all organizations

4.1.10. Policy Compliance

The organization shall comply with the Information and Cyber Security Policy. Sri Lanka CERT shall conduct annual information 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 organizations

4.2. Identify Assets, Owners, Users and Risks

The organization shall develop the 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 of the assets their roles and responsibilities, and current risks associated with assets.

4.2.1. Information Assets and IT Assets

The organization shall identify it's all 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, and 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 a paper document, a digital document, a database, a password or encryption key or any other digital file.

The organization shall also identify IT assets. An IT asset is a software (e.g. operating system, payroll system, CNII) or hardware (e.g. computers, hard disks, servers, routers, networks, firewalls) 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 organizations

4.2.2. Critical National Information Infrastructure (CNII)

Critical National Information Infrastructure 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. Organizations declared as CNIIs will be subject to a set of instructions which will be supported by the forthcoming Cyber Security Act for enforcement of instructions.

Compliance: Applicable to CNII operators

4.2.3. Asset Owners and Custodians

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. It is necessary to formally assign ownership of the asset when it is created, or when assets are transferred to the organization or acquired by the organization.

The custodian of the information asset will be 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 an inventory for assets, classifying assets and protecting assets, defining and reviewing access restrictions to assets, ensuring appropriate handling when asset is deleted or destroyed (adopted from ISO 27002[9]).

Compliance: Applicable to all organizations

4.2.4. Information Assets and IT Assets Register

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 process.

At a minimum, an organization shall record, the name of information asset, the location of information asset, owner and custodian of the information asset, date of classification, the computer system which processes assets, reason for the classification, disposal requirements, date to review classification, impact of loss/compromise or disclose. The information assets register shall be accurate, up to date, consistent and aligned with other inventories.

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. The IT asset register shall be accurate, up to date, consistent and aligned with other inventories.

Compliance: Applicable to all organizations

4.2.5. Risk Assessments

The organization shall conduct a risk assessment to determine the threats to and vulnerabilities of the organization's assets, and their impact on assets. The objective of a risk assessment is to identify vulnerabilities and threats to assets (data, computer systems or other digital infrastructure) and decide on which security measures shall be taken in order to reduce risk to an acceptable level.

Based on the risk assessment, organization shall prioritize risks and record risks in a risk register.

Risk assessment shall be carried out by the RMC of the organization. In the event, where the organization does not possess the appropriate skills, a qualified and experienced firm shall be hired for this purpose.

Sri Lanka CERT shall assist CNIIs to conduct Risk and Vulnerability assessments.

Compliance: Applicable to CNII operators

4.2.6. Classify Assets

The organization shall classify assets and determine the sensitivity and criticality of assets. The objective of the classification is to ensure that an asset receives an appropriate level of protection in accordance with its importance to the organization and its sensitivity. Asset classifications shall be performed based on guidelines given in the "National Data Sharing Policy"[13]. Classification levels provided in the Data Sharing Policy are, "Secret", "Confidential", "Limited Sharing" and "Public".

IT assets shall be classified into three levels namely, "Critical Systems", "Sensitive Systems", and "Non-Sensitive Systems", or components of such systems. A description of the IT assets classification scheme is available in the "Information and Cyber Security Implementation Guide[4]".

Compliance: Applicable to all 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 event or incident. Controls applied shall be based on the classification of each asset.

To comply, 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, authorized software, and deploy protective technology to ensure cyber resilience.

To protect assets, the organization is required to define and implement policies such as Identity Management and Access Control Policy[5], Password Policy, etc. (Refer policy statement 4.3.4).

In such instances, the organization shall ensure that all employees including third party contractors adhere to the policies. Periodic revisions shall also be made to these policies to ensure that the policies are adequate and up-to-date. Any violations of these policies shall be reported to the ISC for necessary action.

4.3.1. Protect 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 archived/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 Policy and providing physical protection to assets.

Compliance: Applicable to all organizations

4.3.2. Protect 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 as prescribed in the latest version of "Information and Cyber Security Implementation Guide"[4]. Further, the organization shall ensure that security parameters on Wi-Fi settings have been enabled.

Compliance: Applicable to all organizations

4.3.3. 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.

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. Access to the computers, systems or any devices shall be controlled through implementing an Identity Management and Access Control Policy (refer policy statement 4.3.4).

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.

Compliance: Applicable for all organizations

4.3.4. 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 the 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.

Note: Sri Lanka CERT has drafted an "Identity Management and Access Control Policy"[6] for government organizations which can be customized and adopted by the organization.

Compliance: Applicable to all organizations

4.3.5. Strong Authentication

In accordance with the Identity Management and Access Control Policy, the organization shall use strong authentication for verifying the identity of a user. Username and password combination, and use of multifactor authentication (MFA) are recommended to authenticate user identity. To ensure a strong authentication process, the organization shall implement a policy for passwords and MFA.

A password policy shall be formulated and implemented by the organization, taking the following measures:

- Passwords must be at least 8 characters long and must consist of both upper and lower case characters (e.g. a-Y), digits (1,9), 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.

Note: Guidelines for developing a password policy are also presented in the Identity Management and Access Control Policy[6].

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 organizations

4.3.6. Cloud Computing and Data Sovereignty

Cloud computing generally refers to the availability of ICT resources such as storage, processing, application development platforms etc., 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 extremely 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.

The organization shall ensure data sovereignty. Data sovereignty refers to that the data subject to the laws and governance structures within the country where it is collected.

All activities of the organization in relation to storing and processing data or hosting software applications in other jurisdictions shall be performed in accordance with the forthcoming "Data Protection Act" of Sri Lanka.

Further, it is strictly recommended to the organizations to perform a proper risk assessment prior to obtaining any cloud service.

Organizations are encouraged to obtain the services of Lanka Government Cloud (LGC) for cloud service requirements. LGC is a government owned private cloud service operated by the Information and Communication Technology Agency (ICTA), which was designed to fulfil the cloud service requirements of the government.

Compliance: Applicable to all organizations

4.3.7. 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. Organizations should enable automatic updates.

Compliance: Applicable to all organizations

4.3.8. 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.

Compliance: Applicable to all organizations

4.3.9. Official Emails

The organization shall use official emails for official 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.

The organization shall use emails with "gov.lk" domain for official communications, and each employee shall use official email for official communication only. Employees must not use official emails for personal communication.

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.

All employees must adhere to guidelines given in the "Safe and Appropriate Use of E-mail" section of the "Information Security and Cyber Implementation Guide"[4].

Compliance: Applicable to all organizations

4.3.10. 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 regulatory framework of the forthcoming Data Protection Act.

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 confidential 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 on a periodic basis for supervisory or regulatory requirements.

Compliance: Applicable to all organizations

4.3.11. Digital Signatures

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

Compliance: Applicable to CNII operators

4.3.12. Perimeter Security Controls

The organization shall install perimeter security controls such as Firewalls, Intrusion Detection Systems, 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 database, install antimalware with automatic updates enabled, update default settings with appropriate configurations, and disable default vendor supplied user accounts for such devices and systems. Information and Cyber Security Implementation Guide presents an overview of configuration details.

Compliance: Applicable to all organizations

4.3.13. 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, and monitoring and manipulation of data 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 multifactor authentication, secure remote access from client devices, and use trusted networks.

Compliance: Applicable to all organizations

4.3.14. 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).

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 that there shall be an air gap[16] between the live data and backup data for protecting live data from any malicious attacks including ransomware.

It is further recommended that backups shall be stored at a fire proof, 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 organizations

4.3.15. Security-by-Design

The organization shall follow 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 and development stage, reviewing code at the coding 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.

“Information and Cyber Security Implementation Guide”[3] provides details on the secure application development lifecycle.

In developing web applications, the organization shall adhere to the “Technical Guidelines for Web Application Security”[5] provided by Sri Lanka CERT.

Compliance: Applicable to all organizations

4.3.16. 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 organizations

4.3.17. Internal Information Security Audit Program

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.

A formal process to oversee the implementation of recommendations raised in previous audit reports is to be established.

The CIA of the organization shall coordinate the audit, and the CIA of each Ministry shall coordinate information security audits of the organizations under its purview.

Audits shall be performed by a party qualified to carry out such audits. 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 CNII operators

4.3.18. 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 services of Sri Lanka CERT to conduct these assessments or a qualified third party nominated by Sri Lanka CERT.

Compliance: Applicable to all organizations

4.3.19. 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.

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

Compliance: Applicable to all organizations

4.3.20. Work from Home

With the transition to working from home, there is an increase in information security threats. Therefore, employees shall adhere to "Information Security Guidelines for Working from Home"[7] issued by Sri Lanka CERT which outline a set of security best practices when working remotely. IT Administrators shall adhere to the "Minimum Guidelines for IT Administrators"[8] issued by Sri Lanka CERT to ensure secure access to organization's IT assets when working remotely is permitted.

Compliance: Applicable to all organizations

4.3.21. Bring Your Own Device (BYOD)

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.

The organization's security policies are applied to BYOD.

Employees' personal devices shall not be used to process or store information classified as "Secret" and "Confidential" under any circumstances.

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.

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 organizations

4.4. Detect Information Security Incidents

The organization shall implement appropriate measures to identify cybersecurity incidents in a timely manner. The organization shall instruct staff to report any cyber security incidents or policy violations, analyze logs to identify

incidents, and adopt continuous monitoring solutions that detect anomalous activity and other threats to operational continuity.

4.4.1. Report 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 systems, the apparent presence of a virus on computers, the apparent presence of any information resource prohibited by guidelines, 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 organizations

4.4.2. Review 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 CNII operators

4.4.3. Continuous Monitoring of Events

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 CNII operators

4.4.4. Report 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 organizations

4.5. Respond to Incidents

To comply with the 'respond' function, the organization shall develop an incident response plan, and activate the plan in an event of an incident.

4.5.1. Incident Response Plan

The organization shall develop an incident response plan which consists of a set of instructions to detect, respond, and recover from information security incidents.

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 and communicated to all staff members of the organization.

Compliance: Applicable to CNII operators

4.5.2. Activate Incident Response Plan

In an 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 an event.

In case of an information security incident, the organization has to initiate procedures to identify, collect and preserve information, which can serve as evidence for performing forensics investigations. The general rule is that a person or organization has a duty to retain and preserve all evidence or electronic records/documents concerning pending or foreseeable claims. This includes the responsibility of not to lose, destroy, or meaningfully alter documents or similar instruments.

An Incident Register shall be maintained at each organization listing information related to cybersecurity incidents.

Compliance: Applicable to all 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.

4.6.1. Disaster Recovery Plan

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

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 organizations

4.6.2. Activate 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 organizations

4.6.3. Crisis Communication

In the event of a major crisis (critical disaster, cyber security incident), the organization shall communicate with internal and external parties such as line ministries, victims, media, clients, and law enforcement authorities according to a plan. The organization shall appoint a senior responsible officer as the Media Spokesman to communicate the crisis to the relevant stakeholders.

Compliance: Applicable to all organizations

5. Assessment Framework

5.1. Prior to the implementation of the Information and Cyber Security Policy, it is essential to identify the present status of government organizations in adopting information security to protect government resources, and this assessment is therefore, designed to capture the present status of the government organization in implementing information security.

5.2. Findings of the assessment will be used by Sri Lanka CERT to establish a baseline for the organizations in adopting information security, and provide recommendations to government organizations in implementing the Information and Cyber Security Policy at their organizations.

5.3. This assessment will be repeated annually, and each year Sri Lanka CERT shall assess the level of adoption of the Information and Cyber Security Policy at the relevant organization, and recommendations will be made to improve the overall information and cyber security readiness of the organization.

5.4. Any organization desiring to assess their level of Information and Cyber Security Policy adoption could use this assessment framework to evaluate their progress at any given time.

5.5. Information Security Officer, Chief Innovation Officer, or the officer in charge of the subject of IT, is required to fill this assessment, and forward to Sri Lanka CERT with the signature of the Head of Organization on or before 30th October of each year.

5.6. This assessment questionnaire consists of 50 questions. All government organizations are required to indicate their response (Yes/No) to each question to the best of their knowledge.

5.7. 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 Information and Cyber Security Policy for detailed explanation of relevant terms.

5.8. Assessment

Policy Reference	Assessment Criteria	Organization's Response Yes	Organization's Response No	Remarks Section
Information Security Governance				
Security Organization Structure	1. Has the organization appointed an ISO?			
	2. Has the organization assigned information security responsibilities to ISO?			
	3. If no ISO has been appointed, has the CIO or the officer in charge of the subject of IT been assigned information security responsibilities?			
	4. Does the organization have a committee to make decisions on Information Security or IT?			
	5. Does the HOO proactively lead information security initiatives?			
	6. Has the organization assigned information security audit responsibilities to CIA?			
Capacity Building	7. Has the organization taken any steps to develop the information security capacity of accountable individuals?			
Strategic Alignment	8. In designing and implementing the organization's functions, policies, strategies or projects, has your organization taken information security into account?			
Information Security Action Plan	9. Does your organization has financial provisions for information security activities?			
	10. Has your organization developed action plans to achieve its information security objectives?			
Identify Assets, Owners, Users and Risks				
Assets	11. Has your organization identified information assets that have a value to the organization?			
	12. Has your organization assessed the risk associated with information assets?			
	13. Has your organization classified information assets based on their sensitivity, criticality, impact of sharing or other means?			
	14. Has your organization recorded information assets in an information assets register?			
	15. Has your organization identified IT assets?			
	16. Has your organization recorded IT assets in an IT assets register?			
	17. Has your organization classified IT assets based on their criticality?			
	18. Has your organization identified the owners of the assets?			
Protect Assets				

Encryption	19. Does your organization encrypt sensitive information prior to storage?			
	20. Does your organization encrypt sensitive information prior to moving through electronic channels?			
Physical Protection	21. Does your organization process or store sensitive information in secure areas?			
	22. Has your organization taken appropriate measures to protect secure areas from fire, flood, humidity and temperature?			
	23. Does your organization prevent unauthorized entry to secure areas?			
Identity Management and Access Control	24. Does your organization have an Identity Management and Access Control Policy?			
	25. Does your organization use strong authentication?			
Data Sovereignty	26. Does your organization obtain the service of clouds or other digital infrastructure which operate from other jurisdictions? 27. Does your organization assess risk prior to obtaining cloud service?			
Licensed Software and Patch Updates	28. Does the organization use operating systems (OSs) with valid License(s)?			
	29. Have the OSs (s) of the organization been updated with vendor supplied latest patches and fixes? 30. Does your organization have a procedure in place to ensure vendor supplied critical patches are installed on time?			
Antimalware	31. Has the organization installed Antimalware software with a valid license in all machines?			
Email	32. Do the employees of your organization use personal emails for official communication even if they have been given official emails by the organization? 33. Does your organization restrict users using personal emails for official communications?			
Perimeter Security Devices	34. Does your organization have a Firewall in your computer network?			
Secure Remote Access	35. Does your organization use secure Virtual Private Networks (VPNs) for remote access?			
	36. Do all the users connecting remotely use VPN?			
Backup Strategy	37. Does your organization backup data?			
	38. Are the backups stored at a fire proof, secure location which is physically distant from the data processing site?			

Secure Disposal of Assets	39. Does your organization follow any of the following to dispose electronic media that contain sensitive information? - Shredding, punching, physically damaging, degaussing.			
Internal Information Security Audit Program	40. Does your organization have internal information security audit program? 41. Does your organization perform VAPTs through Sri Lanka CERT prior to any deployment of software applications? 42. Have you performed VAPT for your computer network?			
	43. Does your organization perform VAPTs for software applications on a periodic basis?			
Work from Home	44. Does your organization adhere to the work from home guidelines issued by Sri Lanka CERT?			
Bring your Own Device (BYOD)	45. Does your organization have a formal procedure to register BYOD?			
	46. Does your organization allow BYOD to process or store critical data?			
Detect Information Security Incidents				
Report incidents	47. 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? 48. Have you ever reported cyber security incidents to Sri Lanka CERT or any other party?			
Respond to Incidents				
Incident Response Plan	49. Has your organization developed an Incident Response Plan?			
Recovery from Incidents				
Disaster Recovery Plan	50. Does your organization have a Disaster Recovery Plan developed to facilitate the recovery in an event of a disaster?			

Glossary

Air Gap	"An air gap is a technical configuration of the backup environment where backup data is stored offline and completely separate from the production environment. Because the data is stored in this way, it's much harder for malicious parties to access the data remotely and sabotage or delete it"[16]
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 its level of sensitivity, criticality and the impact of the sharing of that information. The primary objective 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 the person responsible for the day-to-day management of assets
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.
Criticality of Information	A measure of the degree to which an organization depends on the information or IT assets for the success of a mission or of an organization function. Criticality is comprised of two components, Integrity and Availability. Integrity Criticality is the degree to which the value of the information is determined by its reliability. Availability Criticality is the degree to which the value of the information is determined by its accessibility when needed.
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.
Cyber Security	It is a subsect of information security, which refers to the protection of information and IT assets from being compromised or attacked through cyber means (with the use of Internet Technologies).
Digital Signature	Digital Signatures are 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)	Information Security Officer is a senior-level executive responsible for establishing and maintaining the organizations objectives, strategy, and action plans to ensure information assets are adequately protected.
Information Security Committee (ISC)	Information Security Committee is responsible in leading and managing all Information Security related activities within the organization, including information security planning, funding, implementation and monitoring the implementation of information security measures.
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 Security	Information security means protecting assets from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure integrity, confidentiality, and availability.
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.
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 or destruction. 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	Service available to anyone who wants to purchase them

Sensitivity of Information	The degree to which the value of the information is determined by its secrecy.
Recovery Point Objective (RPO)	RPO indicates the earliest point in time in which it is acceptable to recover the data. For example, if a process can afford to lose data up to hours before disaster, then the latest backup available shall be up to 4 hours before disaster. The transactions which occurred after RPO period shall be entered after recovery.
Recovery Time Objective (RTO)	RTO indicates the earliest point in time at which the organizations 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 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. Right to Information Act No 12 of 2016. Document can be accessed through https://www.rti.gov.lk/.
2. Information and Cyber Security Strategy of Sri Lanka (2019:2023), Published by Research and Policy Unit, Sri Lanka CERT, November 2019. Document can be accessed through https://cert.gov.lk/documents/NCSStrategy.pdf
3. Minimum Information Security Guidelines. Published by Research, Policy and Project Division of Sri Lanka CERT. Document can be accessed through https://www.onlinesafety.lk/wp-content/uploads/2021/07/Minimum Information_Security_Standards_Version1_14-07-2021.pdf
4. Information Security Implementation Guide. Published by Research, Policy and Projects Division of Sri Lanka CERT, (forthcoming).
5. Technical Guidelines for Web Application Security. Published by Research, Policy and Projects Division of Sri Lanka CERT. Document can be accessed through https://www.onlinesafety.lk/wp-content/uploads/2021/04/Technical-Guidelines-for-Web-Application-Security.vf1-1.pdf
6. Identity Management and Access Control Policy for Government. Published by Research, Policy and Projects Division of Sri Lanka CERT. Document can be accessed through https://www.onlinesafety.lk/wp-content/uploads/2021/04/Attachment-03_Logical-Access-Control-Policy.pdf
7. Information Security Guidelines for Working from Home. Published by Sri Lanka CERT. Document can be access through https://www.onlinesafety.lk/wp-content/uploads/2021/01/IS-Guidelines-for-Working-from-Home.pdf
8. Minimal Guidelines for IT Administrators: Guidelines to Improve Cyber Security to Enable Work from Home. Published by Sri Lanka CERT. Document can be accessed through https://www.onlinesafety.lk/wp-content/uploads/2021/01/IS-Guidelines-for-Working-from-Home.pdf
9. ISO 27002 (2013): Information Technology – Security Techniques - Information Security Management Systems – Requirements, International Standards Organization, Published by International Standard Organization.
10. NIST Cybersecurity Framework. Published by National Institute of Standards and Technology, U.S Department of Commerce. Resources can be accessed through https://www.nist.gov/cyberframework/online-learning/five-functions
11. NIST (2006): Information Security Handbook: A Guide for Managers, Published by National Institute of Standards and Technology, U.S Department of Commerce. Resources can be accessed through https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

12. e-Government Policy of Sri Lanka (2009). Published by Information and Communication Technology Agency of Sri Lanka (ICTA).

13. National Data Sharing Policy of Government, Published by Information and Communication Technology Agency of Sri Lanka (ICTA). Document can be accessed through http://www.data.gov.lk/download/file/fid/362

14. Educause, Information Security Governance Information Security Governance. Document can be accessed through https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/information-security-governance

15. ISO/IEC 38500:2015 Information technology — Governance of IT for the organization.

16. Carbonite (2021), Can Air-Gapped Backup Provide an Extra Measure of Security? Document can be accessed through https://www.carbonite.com/.