Minimum Information Security Standards

Version 1

Sri Lanka Computer Emergency Readiness Team

An Agency under the Ministry of Technology

Table of Contents

Document Control

Owner	Sri Lanka Computer Emergency Readiness Team
Version	Version 1
Issue date	July 2021
Document ID	Minimum Information Security Standards
Classification	Public: Approved for public release

Version History

Version	Prepared by	Reviewed by	Authorized by	Issue Date	Description
1	Information Security Research, Policy and Project Team of Sri Lanka CERT Date: 10th May 2021	Senior Management of Sri Lanka CERT Date: 18th May 2021	Board of Directors of Sri Lanka CERT Date: 09th July 2021	12th July 2021	Version 1.0 Initial release

Acronyms

CCTV	Closed-circuit Television
CERT	Computer Emergency Readiness Team
CIO	Chief Innovation Officer
FTPS	File Transfer Protocol Secure
HOO	Head of Organization
HTTPs	Hypertext Transfer Protocol Secure
ICTA	Information and Communication Technology Agency
ISO	Information Security Officer
ISO 27002	Information Technology – Security Techniques - Information Security Management Systems
ISC	Information Security Committee
IT	Information Technology
MISS	Minimum Information Security Standards
NIST	National Institutes of Standards and Technology
SSL	Secure Socket Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
VAPT	Vulnerability Assessments and Penetration Tests

An Overview of the Minimum Information Security Standards

1. Introduction

1.1. Sri Lanka Computer Emergency Response Team (Sri Lanka CERT) has prepared the following guidelines to ensure the safety and security of information and IT Systems (Hardware and Software) used by the government organizations. These "Minimum Information Security Standards (MISS)" have been developed using Global Standards such as National Institute of Science and Technology USA, and International Standards Organizations (27002), and follows the global best practices in developing information security standards (e.g. UK Government's Minimum Cyber Security Standard, Information Security Policy Manual of New Zealand). These guidelines provide a set of measures including advice, guidance and security controls that needs to be adopted to ensure cyber resilience of the organization's Information and IT Systems. These guidelines will be incorporated into Information Security Policy Framework for Government Organizations, which will be published later this year.

1.2. Although developed for government organizations, these guidelines can also be used by any other organization to protect IT Systems and valuable information.

1.3. Minimum Information Security Standards are developed based on following six (06) Information Security Principles.

(a). Information Security Governance: This specifies the strategic alignment and accountability framework that provides insight to ensure that information security activities are properly managed within the organization.

(b). Identify: This identifies organization's assets (information and IT assets), and the risks associated with those assets.

(c). Protect: This outlines the controls that shall be implemented to prevent, limit or contain the impact of a potential information security event or incident.

(d). Detect: This outlines the activities that shall be carried out to discover information security events in a timely manner.

(e). Respond: Provides guidance on activities related to planning and testing responses to cyber security incidents, and to initiate these in case of a cyber-attack.

(f). Recovery: Provide guidance on activities that shall be carried out to resume normal operations after a cybersecurity incident or disaster. Figure 1 shows the scope of the Minimum Information Security Standards.

Figure 1. Scope of the Minimum Information Security Standards

1.4. If any organization or individual require clarifications on the content of this document, please contact Sri Lanka CERT using the contact information available in www.cert.gov.lk.

1.5. Guidelines provided in this document are to be treated as the minimum requirements for cyber resilience. Organizations with Critical National Information Infrastructure will be provided with additional measures by Sri Lanka CERT.

1.6. A self-assessment questionnaire to test the cyber readiness of the organizations is available at the end of this document. Same form is available at www.cert.gov.lk and organizations are invited to fill this form to obtain recommendations from Sri Lanka CERT to improve the security of your digital infrastructure.

2. Information Security Governance

2.1. Information Security Governance specifies the framework that is required to implement the Cybersecurity related activities. It also defines the roles and responsibilities assigned to staff members who have been nominated to handle these issues.

2.2. Chief Innovation Officer (CIO) is a role introduced by the Information and Communication Technology Agency (ICTA) to support Government Organizations in modernizing the internal systems, especially converting manual systems to digital systems.

2.3. Considering the fact that all public sector IT projects are led by the CIO, information security responsibilities including implementing controls to protect IT systems shall be assigned to CIOs.

2.4. The circular previously published by the Ministry of Digital Infrastructure and Information Technology, MDIIT/SEC/2019/CS001 (date: 2019-05-23) has instructed all Government Organizations to nominate an Information Security Officer (ISO) to handle issues related to information security. This circular is now being updated and will be re-published by the Ministry of Technology.

2.5. The Minimum Information Security Standards provide a risk based approach to protecting information and IT assets. That is, a comprehensive risk assessment shall be performed on each asset to determine the level of sensitivity and criticality, and to develop appropriate controls to protect such asset. Minimum Information Security Standards introduced in this document refer to "Classification of Assets" as a mandatory step in assessing the risk associated with information and IT Assets. This classification has to be in line with the "National Data Sharing Policy" of the Government. The complete document is available at "Open Data Portal" (http://www.data.gov.lk/).

2.6. In securing the organization's digital infrastructure, it is essential for both the CIO and ISO to coordinate their work closely in introducing IT based systems and appropriate security measures.

2.7. Information Security Organizational Structure

2.7.1. Head of the Organization (HOO) shall provide leadership to all information security activities within the organization, and shall be the ultimate responsible and accountable party for protecting information and IT assets of the organization.

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

2.7.3. The Organization shall nominate an ISO and assign information security responsibilities and the corresponding accountability. ISO shall report directly to the HOO on the matters related to information security.

2.7.4. In a case of there is no suitable officer to appoint as the ISO, the CIO (or the officer responsible for the subject of IT) shall be assigned with information security responsibilities and corresponding accountability.

2.7.5. An Information Security Committee (ISC) shall be appointed with clearly defined information security responsibilities and corresponding accountability. The ISC is responsible in leading and managing all information security related activities within the organization, including information security planning, funding, implementation and monitoring of information security activities.

2.8. Personnel Security

2.8.1. Government officers appointed or transferred to a role or position that involves dealing with information classified as Secret or Confidential shall go through a security clearance before they are appointed for or transferred to such position, and periodic security clearance checks are required to be conducted during their tenure.

2.9. Capacity Building of Accountable Individuals

2.9.1. The organization shall ensure that the individuals assigned with the responsibilities for information security activities shall receive appropriate awareness, education and training on cyber security. This shall be an ongoing activity for the organization and it shall be included in the annual Training Plan of the organization.

2.10. Strategic Alignment

2.10.1. The organization shall identify information security objectives, which need be aligned with organizational objectives. All strategies, programs, projects, and activities shall be designed in a way that those initiatives are linked with information security.

2.11. Information Security Action Plan and Budget

2.11.1. For information security activities, an information Security Action Plan shall be developed.

2.11.2. The organization shall allocate a budget for information security activities specified in the action plans.

2.12. Compliance

2.12.1. The organization shall comply with the Minimum Information Security Standards and shall participate for the Annual Information Security Readiness Assessments conducted by Sri Lanka CERT.

3. Identify Assets, Owners, Users and Risk

3.1. Identify Information Assets

3.1.1. The organization shall identify critical information that they hold (Information Assets). Identification of such information shall be carried out with the intention of protecting the information assets from unauthorized access, disclosure, disruption, modification, or destruction.

3.2. Risk Assessment and Assets Classification

3.2.1. Through a risk assessment, the organization shall classify information assets based on their importance to the organization and sensitivity. Objective of the classification is to ensure that an asset receives an appropriate level of protection. Asset classification shall be carried out based on guidelines given in the National Data Sharing Policy of the Government. The classification levels provided in the Data Sharing Policy are, Secret, Confidential, Limited sharing and Public.

3.3. Information Assets Inventory

3.3.1. The organization shall record such Information in an Information Assets Inventory. At a minimum, organization shall record: name of information asset, location of information asset, owner and custodian of information assets, classification date, computer system process assets, reason for the classification, disposal requirements, date to review classification, impact of loss/compromise or disclose.

3.4. Identify IT Assets

3.4.1. The organization shall identify IT assets such as systems, computers, software, databases or other digital infrastructure. Identification of such IT Assets shall be performed with the intention of protecting them from unauthorized access, use, disruption, or destruction.

3.5. IT Assets Inventory

3.5.1. The organization shall record all IT Assets in the IT Assets Inventory. The IT Assets Registry shall contain at a minimum, the type of the assets (e.g. system, hardware, software,

and server), location of the asset, operating system, license details, users, risk, classification level, estimated value.

3.6. Assets Owners and Custodians

3.6.1. The organization shall identify assets owners and custodians, and assign responsibilities to protect assets.

4. Protect Assets

4.1. Security of Assets

4.1.1. The organizations should ensure the security of Assets. Based on the Classification of each Asset, the organization should take appropriate measures to protect the assets. Measures to protect assets are summarized in Items 4.1 to 4.14.

4.1.2. The organization should protect data-at-rest (e.g data stored on a server, cloud, hard drive, laptop, flash drive, or archived/stored). Encrypting sensitive data is essential prior to storage.

4.1.3. The Organization should protect data-in-transit. Data in transit is the data that is actively moving from one location to another across the Internet or through a private network. For protecting data in transit, the organization should encrypt sensitive data prior to moving and use secure connections (HTTPS, and latest versions of SSL, TLS, FTPS, etc.).

4.2. Physical Protection of Assets

4.2.1. The Organization shall provide physical protection to its Assets. Assets classified as "secret" shall be stored in Secure Locations which are protected through multifactor authentication entry systems, 24 x 7 CCTV operations.

4.2.2. Secure Locations shall be protected to prevent threats from fire, flood, electricity and temperature fluctuations.

4.3. Identity Management and Access Control.

4.3.1. The organization shall identify the users who shall have access to both information and IT Assets.

4.3.2. Users shall only be granted access to the information which they need to perform their tasks (need-to-know), and users shall only be granted access to IT Assets that those users need to perform tasks (need-to-use).

4.3.3. Users shall be given minimum access to sensitive information necessary for their role. Access shall be removed immediately when individuals leave their role or the organization.

4.4. Strong Authentication

4.4.1. The organization shall use strong authentication for verifying the identity of a user. Passwords and Multifactor Authentications are recommended to develop a strong authentication.

4.4.2. Password must be strong, and at least 8 characters long and it must be consisted of both upper and lower chase characters (e.g. a-Y), and digits (1-9), and special characters (e.g. !,@,$,#, %). All passwords must be changed at predetermined intervals.

4.4.3. Access to the information classified as Secret and Confidential shall be restricted through a multifactor authentication system. Multifactor authentication shall be designed by taking into account the following: Something only the user knows (e.g password), something only the user has (access card), and something only the user is (e.g. finger print).

4.5. Security of Emails

4.5.1. The organization shall use emails with "gov.lk" domain for official communication, and each employee shall use Official emails for official communication. Employees must not use official emails for personnel communication.

4.5.2. 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.

4.5.3. In the case where government organization maintains its own Mail Server, hosting of email server shall be located within the Jurisdiction of Sri Lanka, set up email filters to remove emails known to have malware attached and prevent inbox from being cluttered by unsolicited and undesired (i.e. "spam") email.

4.5.4. The organization shall also configure emails for security as per the email security guidelines specified in the Information Security Implementation Guide, which will be published in due course.

4.6. Data Sovereignty

4.6.1. Data sovereignty is the concept that data is subject to the laws and governance structures within the country in which it is collected. All the 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 and any other related law/regulation introduced by the Government of Sri Lanka.

4.7. Cloud Risk

4.7.1. The organization shall assess cloud risk prior to use cloud services. Prior to obtaining cloud services, the risks for any Cloud Service adopted are to be identified, understood and formally accepted by the HOO.

4.8. Vulnerability Assessment and Penetration Tests

4.8.1. Prior to the deployment of any website or system on the live environment, the organization must obtain the service of Sri Lanka CERT to do a Vulnerability Assessment and Penetration test (VAPT). Government organizations must fix the security issues identified through the VAPT immediately, and get the system certified by a follow up VAPT.

4.8.2. Government organizations shall perform VAPTs, at least annually. The other circumstance in which that organization shall perform VAPTs include, after an incident has occurred or after a change is made to the application, or after changes have been made to the platform or hosting environment, or after changes to standards, policies and guidelines, after the spread of virus/malware, or as determined by the ISC.

4.9. Licensed Software and Update Patches

4.9.1. The organization shall use operating systems (OS) and other relevant software with valid License(s).

4.9.2. The organization shall update the OS and other relevant software with vendor supplied latest patches and fixes. The Organization shall enable automatic updates.

4.10. Anti-malware

4.10.1. The Organization shall install Licensed Antimalware Software on all existing devices and components connected to the organization's network.

4.10.2. Organizations shall make sure that antimalware tools remain active at any potential entry point. The signatures of the antimalware software shall be up-to-date and automatic update shall be enabled. Users must be prohibited from changing the configuration of, uninstalling, deactivating or tampering with any Anti Malware software that has been installed on systems used by them.

4.10.3. Malware detection shall be configured for on-demand scanning, scanning when downloading or opening of files, scanning on removable or remote storage, and web page scanning.

4.11. Firewalls

4.11.1. Organizations shall install Firewalls, and shall regularly update the firewall threat database.

4.11.2. Default Firewall settings shall be updated with appropriate configurations, and default vendor supplied user accounts shall also be disabled.

4.12. Secure Remote Access

4.12.1. Staff shall adhere to the latest version of the Work from Home Guidelines issued by Sri Lanka CERT.

4.12.2. The organization shall use secure Virtual Private Networks (VPNs), implement multifactor authentication systems, use secure remote accessible devices, and use trusted networks to ensure the security of remote access. As per the Access Control Policy, the organization shall allow only the authorized persons to use remote access.

4.13. Backup Strategy

4.13.1. The organization shall backup data, audit logs, systems, software, and configuration data or any other information that are necessary to restore normal operations in an event of a disaster. Data written onto backup media shall be preserved as per the regulatory requirements of the government.

4.13.2. Backups shall be stored offsite and the off-site storage copies of the backups will be stored in a safe location, physically distant from the data processing center.

4.14. Secure Disposal of Assets

4.14.1. If media is no longer required, the content of the media shall be removed in an unrecoverable manner. Any sensitive information assets shall be deleted unrecoverable manner to prevent original information retrievable (Sector base formatting, shredding or punching).

5. Detect Incidents

5.1. Reporting Incidents

5.1.1. The organization shall instruct staff to report any suspicious activity, contact, theft, virus, vulnerability, unauthorized access, tampering file, or violation of security policy to the ISC.

5.2. Reporting Incidents to Sri Lanka CERT

5.2.1. The organization is advised to report critical information security incidents to Sri Lanka CERT for technical advice, as determined by the Information Security Committee of the organization.

6. Response to an Incident

6.1. Incident Response Plan

6.1.1. The organization shall develop and test the Incident Response Plan. The purpose of an incident response plan is to protect sensitive data during a security breach.

6.1.2. Incident Response Plan will clearly define the measures that need to be adopted, the responsibilities of each person involved in carrying out the Incident Response Plan and any other specific activity related to protecting organization's Information and IT Assets, during a security incident to mitigate the impact.

6.2. Activate Incident Response Plan

6.2.1. A designated authorized person must activate the Incident Response Plan upon immediate detection of a cybersecurity incident and notify the relevant authorities of the action taken.

6.2.2. Isolate the compromised asset or system to ensure that the security breach is contained.

6.2.3. All efforts shall be taken to preserve evidence related to the incident to enable a post incident investigation.

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

7. Recovery from an Incident

7.1. Disaster Recovery Plan

7.1.1. The organization shall develop a Disaster Recovery Plan to ensure continuity of business processes after a service disruption. The disaster recovery plan shall contain the activities to be performed to recover from a disaster, and roles and responsibilities of staff activating the plan.

7.1.2. The disaster recovery plan shall be tested and updated on periodic basis.

7.2. Activate Disaster Recovery Plan

7.2.1. In an event of a disaster, the designated authorized person must activate the Disaster Recovery Plan to recover from the disaster.

Glossary

Information Security	Information security means protecting assets from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure integrity, confidentiality, and availability.
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).
Information Assets	Information asset is any information or data that has a value to the organization. This includes the documents available in electronic format, database records or the documents available in paper format. Examples for information assets include word file, images, employees personal record in a database.
IT Assets	IT asset is any IT equipment, information system, software, storage media that has a value to the organization. Examples for IT assets are computers, servers, routers, disks, networks, software, information systems and its components.
Assets Owner	An asset owner is the person responsible for the day-to-day management of assets
Assets Custodian	Person in the organization who has the responsibility to protect an information asset as it is stored, transported, or processed in line with the requirements defined by the information asset owner
Official Email	Official emails are the email supplied by the government with the domain name of “gov.lk”
Confidentiality of Information	Confidentiality refers to the assurance that information is not disclosed to unauthorized people and organizations.
Integrity of Information	Integrity refers to guarding information against improper modification or destruction. It ensures that information remains in its original form.
Availability of Information	Availability ensures timely and reliable access to and use of information.
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.
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.
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.
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. Encryption however, cannot prevent the loss of data.

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, ransom ware).
VPN	Virtual Private Network establishes a secure connection to another network over the Internet. It creates an encrypted tunnel for data communication over the internet.
Assets Classification	Classification is the process of categorizing information assets based on its level of sensitivity and the impact to the organization. Primary objective is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
VAPT	Vulnerability Assessment and Penetration Testing (VAPT) are security services that focus on identifying vulnerabilities in the network, server and system infrastructure.

Self-Assessment on Information Security Readiness

Ser. No.	Information Security Activity	Yes	No
Information Security Governance			
1.	Is there a CIO or ISO in your organization?		
2.	Has the organization assigned information security responsibilities to CIO or ISO?		
3.	Do you have a clearly defined information security objectives?		
4.	Do you train your staff on Information Security?		
Identify Assets, Owners, Users and Risk			
5.	Has your organization identified information assets that have a value to the organization?		
6.	Has your organization classified information assets based on their sensitivity, criticality, impact of sharing or other means?		
7.	Has your organization recorded information assets in an information assets inventory?		
8.	Has your organization recorded IT assets in an IT assets inventory?		
9.	Has your organization classified IT assets based on their criticality?		
10.	Has your organization assessed the risk associated with information assets and IT assets?		
Protect Assets			
11.	Do you use encryption in any of your information related operations?		
12.	Does your organization process or store sensitive information in a secure manner?		
13.	Does your organization backup data?		
14.	Does your organization have an Identity Management and Access Control Policy?		
15.	Do you have a password policy?		
16.	Do you use multi factor authentication in allowing access to your network?		
17.	Does the organization use operating systems with valid License(s)?		
18.	Do you update your operating systems with vendor supplied latest patches and fixes?		
19.	Has the organization installed Antimalware software with a valid license in all machines?		

20.	Do the employees of your organization use public emails such as Gmail, Yahoo etc, for official work?		
21.	Does your organization have a Firewall in your computer network?		
22.	Does your organization use secure Virtual Private Networks (VPNs) for remote access?		
23.	Do all the users connecting remotely use VPN?		
24.	Does your organization adhere to the work from home guidelines issued by Sri Lanka CERT?		
Detect Information Security Incidents			
25.	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?		
26.	Have you ever reported cyber security incidents to Sri Lanka CERT or any other party?		
Respond to Incidents			
27.	Do you have a plan or a procedure for responding to cyber incidents?		
Recovery from Incidents			
28.	Is there a Disaster Recovery Plan developed to facilitate the recovery in an event of a cyber incident/attack?		

Acknowledgement

Sri Lanka CERT hereby acknowledge the consulting of following publications in preparing the information presented in this document.

1. Information and Cyber Security Strategy of Sri Lanka (2019:2023), Research and Policy Unit, Sri Lanka CERT, November 2019.

2. Information Security Implementation Guide (2021), Research and Policy Unit, Sri Lanka CERT, (forthcoming)

3. ISO 27002 (2013): Information Technology – Security Techniques - Information Security Management Systems – Requirements, International Standards Organization.

5. NIST (2006): Information Security Handbook: A Guide for Managers, National Institute of Standards and Technology, US.

6. National Data Sharing Policy of Government, Information and Communication Technology Agency of Sri Lanka.

7. New Zealand Information Security Policy Manual, Government of Communication and Security Bureau

Please contact Sri Lanka CERT (www.cert.gov.lk) if you require any clarification on Minimum Information Security Standards.