



INFORMATION AND CYBER SECURITY POLICY FOR GOVERNMENT ORGANIZATIONS

රාජ්‍ය ආයතන සඳහා තොරතුරු සහ
සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය

அரசாங்க நிறுவனங்களுக்கான
தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கை



Funded by the
European Union

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

© Sri Lanka CERT 2022. All rights reserved.

Information and Cyber Security Policy for Government Organizations - English
Version

First Print : January 2023

The Cabinet of Ministers has granted the approval for the implementation
and enforcement of this Policy effective from 22 August 2022

Document Classification: Public

Published by

Research, Policy and Projects Division

Sri Lanka CERT

Room 4-112, BMICH, Bauddhaloka Mawatha, Colombo 7

Sri Lanka

Telephone : +94 11 269 1692, Fax: +94 11 269 1064

Email : cert@cert.gov.lk

Websites : www.cert.gov.lk | www.onlinesafety.lk

ISBN 978-624-6352-00-4



Contents

1.	Introduction	7
2.	Information and Cyber Security Policy Framework	9
3.	Information and Cyber Security Policy	12
3.1.	Objectives	12
3.2.	Scope of the Policy	13
4.	Policy Statements	18
4.1.	Information and Cyber Security Governance	18
4.1.1.	Leadership	19
4.1.2.	Security Organization Structure	19
(a)	Role of Information Security Officer (ISO)	20
(b)	Role of Chief Innovation Officer (CIO)	20
(c)	Role of (Chief) Internal Auditor (IA)	20
4.1.3.	Information Security Committee (ISC)	21
4.1.4.	Risk Management Committee (RMC)	21
4.1.5.	Responsibilities of End Users	21
4.1.6.	Capacity Building	22
4.1.7.	Security Clearance of Staff	22

	4.1.8.	Strategic Alignment	23
	4.1.9.	Action Plans and Resource	23
	4.1.10.	Compliance	23
4.2.		Identify Assets, Owners, Users and Risks	24
	4.2.1.	Identification of Information and Information Technology Assets	24
	4.2.2.	Identification of Critical National Information Infrastructure (CNII)	25
	4.2.3.	Responsibilities of Asset Owners, Custodians and Users	25
	4.2.4.	Maintaining Information and IT Assets	26
	4.2.5.	Assessments Risk	27
	4.2.6.	Classification of Assets	27
4.3.		Protect Assets	28
	4.3.1.	Protection of Data-at-Rest	28
	4.3.2	Protection of Data-in-Transit	29
	4.3.3.	Physical Protection	29
	4.3.4.	Identity Management and Access Control	30
	4.3.5.	Strong Authentication	31
	4.3.6.	Data Sovereignty and Cloud Computing	32
	4.3.7.	Licensed Software and Patch Updates	34
	4.3.8.	Antimalware	34
	4.3.9.	Official Emails	35
	4.3.10.	Security of Emails	35
	4.3.11.	Digital Signatures	36
	4.3.12.	Perimeter Security Controls	36
	4.3.13.	Secure Remote Access	36
	4.3.14.	Backup Strategy	37
	4.3.15.	Security of Assets Supplied by Government Organizations	38
	4.3.16.	Security-by-Design	39
	4.3.17.	Secure Disposal of Assets	39

4.3.18.	Internal Information and Cyber Security Audit Process	40
4.3.19.	Audits Prior to Deployment	41
4.3.20.	Systems Hardening	41
4.3.21.	Work from Home	42
4.3.22.	Using Personal Devices for Official Work	43
4.3.23.	Using Non-Secure Networks	44
4.3.24.	Management of Suppliers	44
4.3.25.	Change Management	44
4.4.	Detect Incidents	45
4.4.1.	Reporting Incidents	45
4.4.2.	Reviewing Logs	46
4.4.3.	Continuous Monitoring of Incidents	47
4.4.4.	Reporting Incidents to Sri Lanka CERT	47
4.5.	Respond to Incidents	47
4.5.1.	Incident Response Plan	48
4.5.2.	Activating Incident Response Plan	48
4.5.3.	Forensic Investigations	49
4.6.	Recover Normal Operations	50
4.6.1.	Disaster Recovery Plan	51
4.6.2.	Activating Disaster Recovery Plan	51
4.6.3.	Crisis Communication	51
5.	Policies to be Implemented on a Priority Basis	52
6.	Methodology for Monitoring and Evaluating the Information and Cyber Security Policy	56
	Glossary	67
	References	71



Acronyms

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



1. Introduction

- 1.1 Many government organizations in Sri Lanka now depend on the reliable functioning of digital systems and infrastructure. Malicious actors, however, can exploit these digital systems to cause harms such as theft of sensitive information, disruption of day to day operations, damage to the reputation of organizations which in turn can lead to the loss of public trust and confidence in government systems, and place nation's security, economy, safety and wellbeing at a risk.
- 1.2 To effectively address these information and cyber security risks and to protect the information, digital systems and infrastructure (hereinafter, information and information technology assets) of government organizations from various threats, Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), the organization which has the mandate to protect the cyberspace of Sri Lanka, has developed an Information and Cyber Security Policy for the use of government organizations. The Policy provides a risk-based

approach for implementing an information and cyber security program at the organizational level. It also provides a set of actions that organizations should implement to identify and protect assets, detect information security incidents in a timely manner, respond to incidents and recover from cyberattacks in an efficient and effective manner.

- 1.3 The Information and Cyber Security Policy for Government Organizations is developed in line with the implementation of the Information and Cyber Security Strategy of Sri Lanka (2019: 2023). It is developed based on the international standards and best practices such as International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) of the United States of America, and has been extensively reviewed by information security experts and senior officers of the government.
- 1.4 All government organizations that are defined as 'Public Authorities' in the Right to Information Act No 12 of 2016, are required to comply with this Policy. The heads of government organizations shall be responsible and accountable for the implementation of the Policy to ensure safe and efficient service delivery within their organizations. Sri Lanka CERT shall facilitate and provide recommendations to all government organizations in implementing the Policy, and shall assess the performance of organizations in implementing the Policy on an annual basis.





2. Information and Cyber Security Policy Framework

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

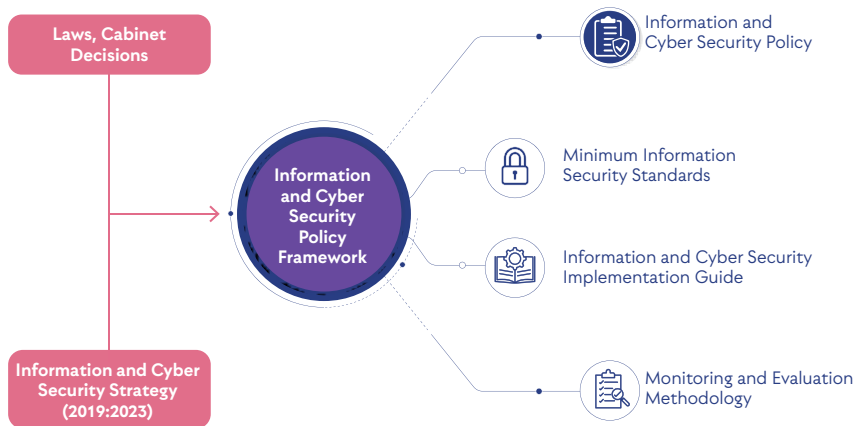


Figure 1: Information and Cyber Security Policy Framework

- 2.2 The Information and Cyber Security Policy framework includes the following:
- a. The Information and Cyber Security Policy: The main component of the Policy Framework is the Information and Cyber Security Policy. It provides a set of policies that the government organizations shall comply with, outlines the essential controls, and provides direction to government organizations in protecting information and information technology assets from information security events.
 - b. Minimum Information Security Standards: This document outlines the minimum acceptable standards of information security controls that shall be adhered to by the government organizations. Minimum Information Security Standards are available for the reference on www.onlinesafety.lk website of Sri Lanka CERT.
 - c. Information and Cyber Security Implementation Guide: This provides a comprehensive set of instructions to staff and stakeholders who require specific details on the implementation of the Policy. This guide includes instructions on the establishment of an information security governance structure, classification of assets, management of risks, protection of assets, methods of disaster recovery and backups,

management of incidents, management of identity and access control and so forth. This document is available for reference on www.onlinesafety.lk website of Sri Lanka CERT.

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

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





3. Information and Cyber Security Policy

3.1 Objectives

- 3.1.1 Information and cyber security refers to the protection of information assets from unauthorized access, use, modification, and destruction to ensure the confidentiality, integrity and availability of information. It includes the protection of IT assets that contain information assets from malicious actions of individuals with the use of cyber technology or other means, and protection of assets from other natural disasters such as floods and fires.
- 3.1.2 In this context, the main objective of the Information and Cyber Security Policy is to introduce a set of rules and guidelines to be followed by the government organizations to protect information and IT assets from damage caused by malicious activities of individuals and natural disasters.

3.1.3 The other objectives of the Policy are to,

- a. establish a common information and cyber security standard across the public sector,
- b. strengthen government organizations' resilience to information and cyber security events by mandating security standards, rules and processes related to the design, implementation, use and operations of information systems and digital infrastructure,
- c. establish a mechanism to detect information and cyber security incidents in a timely manner, to minimize the impact of such incidents to organizations, and to efficiently restore any capabilities or services that were impaired due to such incidents, and
- d. educate staff on the rules, best practices, standards and processes of information and cyber security, and build the confidence of staff in the security status of the organization.

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

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

3.2 Scope of the Policy

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

3.2.2 Policies presented here are developed based on two levels. They are, (a) the policies applicable to all government organizations, and (b) the policies applicable to the Critical National Information

Infrastructure providers (CNII). CNII providers are required to comply with all the policies specified in this Policy. Other organizations are required to comply with the policies applicable to all government organizations. It is, however, recommended for other organizations to comply with the policies which are applicable to CNII for better security.

- 3.2.3 CNII providers are defined as the organizations that maintain information and IT assets whose incapacity or destruction would have a debilitating impact on national security, governance, economy, health and social well-being of a nation. A list of CNII providers will be published by the Sri Lanka CERT.
- 3.2.4 This Policy is developed based on the information and cyber security governance principles, and several concurrent and continuous information security functions proposed by the NIST of the United States of America. These functions include (a) identifying information and IT assets of the organization (e.g. data, information, computers and other digital infrastructure), (b) taking necessary actions to protect assets, (c) detecting information and cyber security incidents, (d) responding to incidents, and (e) recovering any service that was disrupted due to an incident. The Policy also includes the information and cyber security governance mechanism for directing and controlling activities related to information and cyber security within the government organization. Figure 2 presents activities that government organizations should follow to protect information and IT assets.





Figure 2: Steps to Information and Cyber Security.

- 3.2.5 The steps to be taken by an organization to protect assets by implementing this Policy, which is developed based on the information security functions mentioned in 3.2.4, are described below.
- a. Information and Cyber Security Governance: Information and Cyber Security Governance generally refers to the governance mechanism that directs and controls the information and cyber security of an organization. In order to implement the information and cyber security governance, organizations are required to establish a security organizational structure and appoint officers responsible and accountable for information security, undertake capacity building of such officers, define the organizations' information and cyber security objectives, develop action plans, and allocate resources for related activities (Refer Section 4.1).
 - b. Identify Function: It facilitates government organizations to identify assets such as data, information, computers, systems, and digital infrastructure and, to identify and effectively manage the risks associated with those assets (Refer Section 4.2).
 - c. Protect Function: The Protect Function outlines appropriate controls required to ensure the protection of information and information technology assets in order to provide uninterrupted services. To comply with the Protect function, organizations shall implement appropriate controls such as managing user access to assets, installing firewalls and antimalware software, conducting systems audits, establishing a backup strategy, and shall implement policies mentioned in Section 4.3.
 - d. Detect Function: The Detect Function defines the activities required to identify the occurrence of information and cyber security incidents in a timely manner. Organizations shall deploy appropriate tools to analyze logs generated through computers and related devices to detect incidents in an efficient manner (Refer section 4.4).
 - e. Respond Function: The Respond Function defines the actions that should be taken in response to a detected incident. To respond to an incident in an efficient and effective manner, organizations shall develop and implement an Incident Response Plan as defined in Section 4.5.

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





4. Policy Statements

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

4.1 Information and Cyber Security Governance

This Section proposes a mechanism to direct and control information security in the organization. It specifies the leadership and accountability framework which is necessary to ensure that information security activities are properly managed within the organization. It also

highlights the need of aligning information and cyber security activities to the vision and mission of the organization, the need for capacity building of responsible and accountable officials, effective information and cyber security planning, and the importance of government organizations adopting this Policy.

4.1.1 Policy on Leadership

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



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

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

Compliance: *Applicable to all government organizations*

4.1.2 Policy on Security Organization Structure

The organization shall establish an information security organizational structure. An effective information security organizational structure

shall include key roles such as (a) Information Security Officer, (b) Chief Innovation Officer, and (c) (Chief) Internal Auditor.

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

Compliance: Applicable to all government organizations

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

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

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

Compliance: Applicable to all CNII providers

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

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

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

Compliance: Applicable to all government organizations

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

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

Compliance: Applicable to all CNII providers

4.1.3 Policy on Information Security Committee (ISC)

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

Compliance: Applicable to all government organizations

4.1.4 Policy on Risk Management Committee (RMC)

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

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

Compliance: Applicable to all CNII providers

4.1.5 Policy on Responsibilities of End Users

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

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

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

Compliance: Applicable to all government organizations



4.1.6 Policy on Capacity Building

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

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

Compliance: Applicable to all government organizations

4.1.7 Policy on Security Clearance of Staff

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

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

Compliance: Applicable to all CNII providers

4.1.8 Policy on Strategic Alignment

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

Compliance: *Applicable to all government organizations*

4.1.9 Policy on Action Plans and Resource

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

Compliance: *Applicable to all government organizations*

4.1.10 Policy on Compliance

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



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

Compliance: Applicable to all government organizations

4.2 Identify Assets, Owners, Users and Risks

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



4.2.1 Policy on Identification of Information and Information Technology Assets

The organization shall identify all of its important information assets. An information asset is any information that is of value to the organization in performing its organizational functions. Examples of information assets include trade secrets, tender documents, budget sheets, employees' personal records, data gathered by application software related to services offered by the organization, etc. Information assets may come

in many different forms such as paper documents, digital documents, databases, passwords or encryption keys or any other digital files.

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

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

Compliance: Applicable to all government organizations

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

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

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

Compliance: Applicable to all CNII providers



4.2.3 Policy on Responsibilities of Asset Owners, Custodians and Users

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

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

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

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

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

Compliance: Applicable to all government organizations

4.2.4 Policy on Maintaining Information and IT Assets

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



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

Compliance: Applicable to all government organizations

4.2.5 Policy on Assessments Risk

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

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

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

Compliance: Applicable to CNII providers

4.2.6 Policy on Classification of Assets

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

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

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

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

Compliance: Applicable to all government organizations

4.3 Protect Assets



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

4.3.1 Policy on Protection of Data-at-Rest

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

It is essential to encrypt any data (information assets) which are classified as "Secret" or "Confidential" prior to storing. Other means of protecting data at rest include, controlling user access through Identity Management and Access Control mechanism, and providing physical protection to assets.

Compliance: Applicable to all government organizations

4.3.2 Policy on Protection of Data-in-Transit

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

In order to protect data in transit, the organization shall encrypt sensitive information (information classified as "Secret" or "Confidential") prior to moving and, use secure connections (HTTPS, TLS, SFTP, etc.) for data transfer.

Further, the organization shall ensure that security parameters on Wi-Fi settings have been enabled.

Compliance: Applicable to all government organizations

4.3.3 Policy on Physical Protection

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

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

Further, IT assets which are classified as "(very) Critical" shall be stored and operated in secure areas.

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

Secure areas shall be protected to prevent threats from fire, flood, humidity, electromagnetic fields and temperature.

Furthermore, the organization shall use various technologies to control user access to information and IT assets. Such technologies include but are not limited to user identity and passwords, access cards, PINs and biometrics.



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

Compliance: Applicable for all government organizations

4.3.4 Policy on Identity Management and Access Control

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

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

Based on the given principles, the organization shall develop an Identity Management and Access Control Process for its usage. Sri Lanka CERT

has drafted an Identity Management and Access Control Process for government organizations which can be customized and adopted by the organization.



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

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

Compliance: Applicable to all government organizations

4.3.5 Policy on Strong Authentication

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



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

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

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

a) Strong Password:

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

b) MFA:

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

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

Compliance: Applicable to all government organizations

4.3.6 Policy on Data Sovereignty and Cloud Computing

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



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

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

In fulfilling their cloud service needs, organizations shall give priority to obtaining services through the Lanka Government Cloud (LGC).

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

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

Compliance: Applicable to all government organizations

4.3.7 Policy on Licensed Software and Patch Updates

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



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

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

Compliance: Applicable to all government organizations

4.3.8 Policy on Antimalware

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

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

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

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

Compliance: Applicable to all government organizations

4.3.9 Policy on using Official Emails

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

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

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

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

Compliance: Applicable to all government organizations

4.3.10 Policy on Security of Emails

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

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

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

Compliance: Applicable to all government organizations

4.3.11 Policy on Digital Signatures

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

Compliance: Applicable to all government organizations

4.3.12 Policy on Perimeter Security Controls

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

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

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

Compliance: Applicable to all government organizations

4.3.13 Policy on Secure Remote Access

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

Remote access brings many information security threats to the organization. Risk of eavesdropping as information travels over the public internet, unauthorized access to systems or data, monitoring and

manipulation of data and malware infections are common security risks associated with remote access.



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

Compliance: Applicable to all government organizations

4.3.14 Policy on Backup Strategy

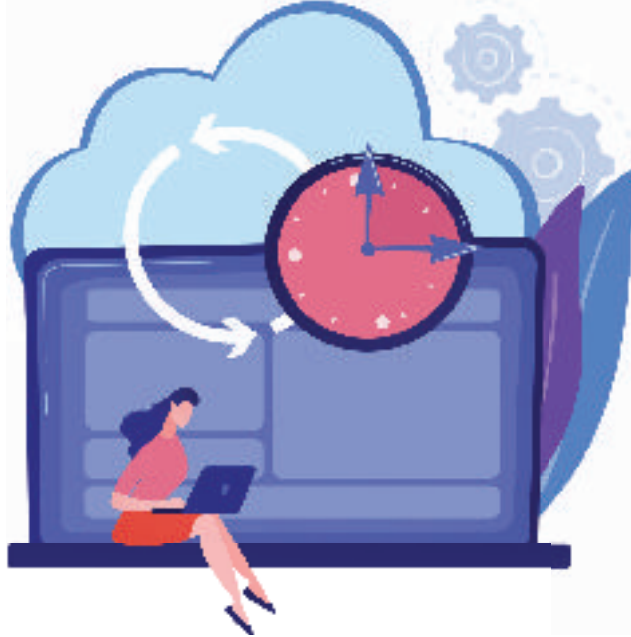
The organization shall have a strategy to backup data, logs, systems, software, configuration details and any other information that are necessary to restore to normal operations in an event of a disaster. This strategy shall be aligned with the organization's Disaster Recovery Plan (Refer Section 4.6.1).

The organization must ensure that the backups can be used to fully restore or recover any disrupted services.

Data written onto backup media shall be preserved as per the regulatory requirements of the government.

The organization shall also define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to determine the frequency of backups.

It is recommended to have an air gap between the live data and backup data for protecting live data from any malicious attacks including ransomware.



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

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

Compliance: Applicable to all government organizations

4.3.15 Policy on the Security of Assets Supplied by Government Organizations

Today many government and non-government organizations operate on the information and IT assets provided by the government. In this context, ICTA or other government organizations must ensure the security, reliability, integrity, and accuracy of the information and IT assets developed by them. For example, the security of Lanka Government

manipulation of data and malware infections are common security risks associated with remote access.



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

Compliance: Applicable to all government organizations

4.3.14 Policy on Backup Strategy

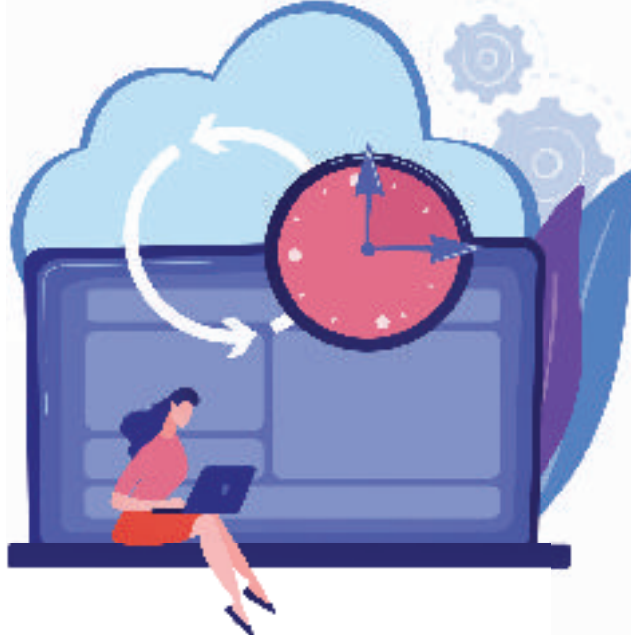
The organization shall have a strategy to backup data, logs, systems, software, configuration details and any other information that are necessary to restore to normal operations in an event of a disaster. This strategy shall be aligned with the organization's Disaster Recovery Plan (Refer Section 4.6.1).

The organization must ensure that the backups can be used to fully restore or recover any disrupted services.

Data written onto backup media shall be preserved as per the regulatory requirements of the government.

The organization shall also define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to determine the frequency of backups.

It is recommended to have an air gap between the live data and backup data for protecting live data from any malicious attacks including ransomware.



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

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

Compliance: Applicable to all government organizations

4.3.15 Policy on the Security of Assets Supplied by Government Organizations

Today many government and non-government organizations operate on the information and IT assets provided by the government. In this context, ICTA or other government organizations must ensure the security, reliability, integrity, and accuracy of the information and IT assets developed by them. For example, the security of Lanka Government

Network, Lanka Government Cloud, Email Service, Lanka Government Payment System, SMS Service, Document Management System or other services should be guaranteed by the relevant organization that developed such infrastructure. The required security certificates for these infrastructures should be obtained by the relevant organizations from Sri Lanka CERT or from any other qualified institution.

Compliance: Applicable to ICTA and all government organizations

4.3.16 Policy on Security-by-Design

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

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

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

Compliance: Applicable to all government organizations

4.3.17 Policy on Secure Disposal of Assets

Assets shall be disposed securely using a formal procedure when no longer required.

It is required that the organization's storage media, which includes but is not limited to optical media (CDs or DVDs), magnetic media (tapes or diskettes), disk drives (external, portable, or removed from information

systems), flash memory storage devices (SSDs or USB flash drives) and documents (paper documents, paper output, or photographic media) are disposed securely.



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

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

Compliance: Applicable to all government organizations

4.3.18 Policy on Internal Information and Cyber Security Audit Process

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

Assessments shall be performed periodically (at least annually), after an incident has occurred, after a change is introduced (to application or hosting environment), after changes to standard/guidelines, after spread of virus or malware, or as determined by the ISC.

The (Chief) IA of the organization shall coordinate the audit, and the Chief IA of each Ministry shall coordinate information security audits of the organizations under its purview.

A formal process to oversee the implementation of recommendations made in audit reports is to be established by the organization. The (Chief) IA of the organization shall take the leadership and bear the responsibility for this process.

Audits shall be performed by a party qualified to carry out such audits or the organization shall obtain the services of Sri Lanka CERT.

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

Compliance: Applicable to all government organizations

4.3.19 Policy on Audits Prior to Deployment

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

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

Compliance: Applicable to all government organizations

4.3.20 Policy on Systems Hardening

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



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

Compliance: Applicable to all government organizations

4.3.21 Policy on Work from Home

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

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

Compliance: Applicable to all government organizations

4.3.22 Policy on Using Personal Devices for Official Work

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



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

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

Compliance: Applicable to all government organizations

4.3.23 Policy on Using Non-Secure Networks

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

Compliance: Applicable to all government organizations

4.3.24 Policy on Management of Suppliers

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

In carrying out vendor management, the organization has to take into consideration the following as a minimum: (a) identifying the responsibilities and obligations of the contracted party including but not limited to backup, storage, recovery and contingency arrangements, security configurations, access to Information and IT Assets, etc., (b) adherence to established information security practices of the organization as defined by the government, (c) right to audit the contracted party processes and controls related to the agreement, and (d) monitoring and reporting on non-adherence to contractual terms and conditions. The responsibility for managing relationships with contracted parties shall be assigned to Asset Owners, designated officers or entities, as decided by the HOO.

Compliance: Applicable to all government organizations

4.3.25 Policy on Change Management

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

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

Compliance: Applicable to all government organizations

4.4 Detect Incidents



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

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

4.4.1 Policy on Reporting Incidents

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

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



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

Compliance: Applicable to all government organizations

4.4.2 Policy on Reviewing Logs

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

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

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

Compliance: Applicable to all government organizations

4.4.3 Policy on Continuous Monitoring of Incidents

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

Compliance: Applicable to all CNII providers

4.4.4 Policy on Reporting Incidents to Sri Lanka CERT

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

Compliance: Applicable to all government organizations

4.5 Respond to Incidents



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

4.5.1 Policy on Incident Response Plan

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

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

The Incident Response Plan shall be tested time to time and communicated to all staff members of the organization.

Guidelines to develop an Incident Response Plan are presented in the Information and Cyber Security Implementation Guide.

Compliance: Applicable to all government organizations

4.5.2 Policy on Activating Incident Response Plan

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

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

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

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

Compliance: Applicable to all government organizations

4.5.3 Policy on Forensic Investigations



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

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

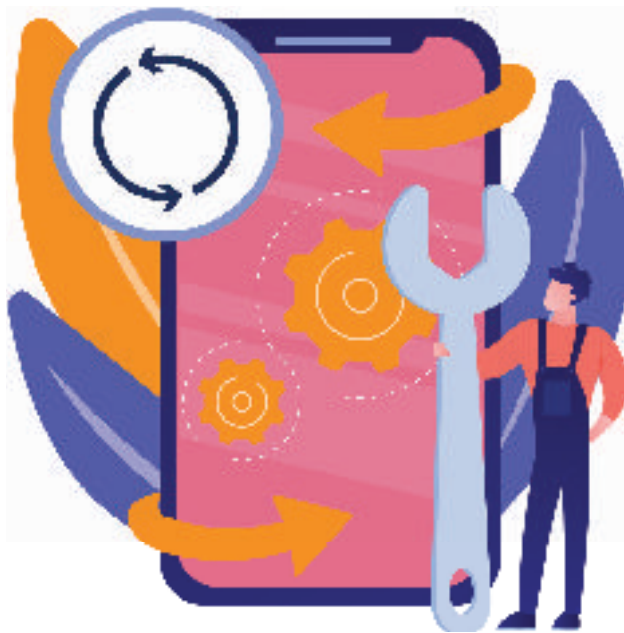
In a forensic investigation, the chain of custody shall be maintained by the organization which requires the following information at a minimum: details of the incident and collected evidence, date and time of the evidence collected, the name and the designation from whom the evidence was obtained and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

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

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

Compliance: Applicable to all government organizations

4.6 Recover Normal Operations



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

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

4.6.1 Policy on Disaster Recovery Plan

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

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

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

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

Compliance: Applicable to all government organizations

4.6.2 Policy on Activating Disaster Recovery Plan

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

Compliance: Applicable to all government organizations

4.6.3 Policy on Crisis Communication

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

Compliance: Applicable to all government organizations

5. Policies to be Implemented on a Priority Basis

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

Policy Area	Policy No.	Policies to be Implemented on a Priority Basis	All Organizations	CNII Providers
Information and Cyber Security Governance	4.1.1	Providing leadership to implement the Information and Cyber Security Policy by the HOO.	✓	✓
	4.1.2	Establishment of an Information and Cyber Security Organizational Structure.	✓	✓
	4.1.2 (a)	Appoint an ISO and delegate information and cyber security responsibilities.		✓
	4.1.2 (b)	In the absence of an ISO, assign responsibilities to the CIO to protect information and IT assets.	✓	
	4.1.2 (C)	Assign responsibilities to (Chief) IA to coordinate information and cybersecurity audits.	✓	✓
	4.1.3	Appoint an ISC.	✓	✓
	4.1.4	Appoint RMC.		✓
	4.1.5	Identify user responsibilities and communicate to users.	✓	✓
	4.1.6	Capacity building of officials responsible for information and cyber security.	✓	✓
	4.1.7	Perform security clearance and background checks on staff handling information assets classified as secret and confidential or staff using CNII.		✓

Policy Area	Policy No.	Policies to be Implemented on a Priority Basis	All Organizations	CNII Providers
	4.1.8	Align information and cybersecurity activities with the vision, mission and objectives of the organization.	✓	✓
	4.1.9	Develop and implement information and cyber security action plans.	✓	✓
<i>Identify Assets, Asset Owners and Risks</i>	4.2.1	Identify information, IT assets and CNII.	✓	✓
	4.2.3	Identify Asset Owners, Custodians and assign responsibilities to protect assets.	✓	✓
	4.2.4	Maintain information and IT assets registers.	✓	✓
	4.2.5	Perform risk assessments for information and IT assets.		✓
	4.2.6	Classify information and IT assets based on their value and sensitivity.	✓	✓
<i>Protect Assets</i>	4.3.1	Protect data at rest.	✓	✓
	4.3.2	Protect data at transit.	✓	✓
	4.3.3	Ensure physical security of information and IT assets.	✓	✓
	4.3.4	Control user access to information and IT assets.	✓	✓
	4.3.5	Ensure strong authentication.	✓	✓
	4.3.6	Ensure data Sovereignty in an appropriate manner.	✓	✓
	4.3.7	Use valid licensed software and update the latest patches.	✓	✓
	4.3.8	Install antimalware software.	✓	✓

Policy Area	Policy No.	Policies to be Implemented on a Priority Basis	All Organizations	CNII Providers
	4.3.9	Use official email for official communications.	✓	✓
	4.3.10	Ensure security of emails.	✓	✓
	4.3.11	Use digital signatures as appropriate.	✓	✓
	4.3.12	Implement perimeter security controls.	✓	✓
	4.3.13	Use secure remote access methods.	✓	✓
	4.3.14	Use a backup strategy.	✓	✓
	4.3.16	Ensure security by design principles in software development and acquisition.	✓	✓
	4.3.17	Ensure secure disposal of Assets.	✓	✓
	4.3.18	Implement an internal information security audit process.	✓	✓
	4.3.19	Perform risk assessments and penetration tests prior to the official launch of website, web application or any other system.	✓	✓
	4.3.20	Strengthen the security resilience of IT assets.	✓	✓
	4.3.21	Follow work from home guidelines in remote working.	✓	✓
	4.3.23	Prevent using untrusted networks.	✓	✓
	4.3.24	Manage suppliers.	✓	✓
	4.3.25	Manage changes.	✓	✓

Policy Area	Policy No.	Policies to be Implemented on a Priority Basis	All Organizations	CNII Providers
Detect Incidents	4.4.1	Instruct staff to report incidents.	✓	✓
	4.4.2	Review logs to identify incidents.	✓	✓
	4.4.3	Identify incidents by continuously monitoring the events.		✓
	4.4.4	Report incidents to Sri Lanka CERT.	✓	✓
Respond to Incidents	4.5.1	Develop Incident Response Plan.	✓	✓
	4.5.2	Activate Incident Response Plan in an event of incident.	✓	✓
	4.5.3	Perform forensic investigations on incidents.	✓	✓
Recover Normal Operations	4.6.1	Develop Disaster Recovery Plan.	✓	✓
	4.6.2	Activate Disaster Recovery Plan in an event of disaster.	✓	✓
	4.6.3	Develop Crisis Communication Plan.	✓	✓

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

- 6.1 Prior to the implementation of the Policy, it is essential to understand the overall information and cyber security readiness of the government organization. This assessment tool is therefore designed to assess the overall information and cyber security readiness, and the progress of the adoption of the Policy by government organizations.
- 6.2 Accordingly, the Sri Lanka CERT shall perform a preliminary assessment of the readiness of government organizations in implementing the Policy based on the questions presented in Section 6.6. Based on the findings, recommendations will be made to government organizations in implementing the Policy.
- 6.3 Sri Lanka CERT shall evaluate the level of policy compliance by each government organization on an annual basis, and shall present the level of compliance on an Information Security Index. Based on the reevaluation results, Sri Lanka CERT shall make recommendations to improve the overall information and cyber security readiness of the organization.
- 6.4 To evaluate the performance (or readiness) of implementing the Policy within the organization, the questionnaire presented in Section 6.6 which contains approximately 50 questions, will be used. ISO, CIO or Officer in charge of the subject of IT shall complete and submit the questionnaire to Sri Lanka CERT on or before October 30th of each year, with the signature of the HOO.
- 6.5 Should the respondent wish to provide a detailed response to each question, the respondent can provide details in the remarks section at the end of the survey questionnaire. Respondents can refer to the Glossary of this document for detailed explanation of relevant terms.
- 6.6 **Assessment Questionnaire**
All government organizations are required to respond to every question up to the best of their knowledge.

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Information and Cyber Security Governance					
Security Organization Structure	1. Has the organization appointed an ISO?	4.1.2 (a)			
	2. Has the organization assigned information and cyber security responsibilities to ISO?	4.1.2 (a)			
	3. In an absence of ISO, has the CIO or the officer in charge of the subject of IT been assigned information and cyber security responsibilities?	4.1.2 (b)			
	4. Has the organization assigned information security audit responsibilities to (Chief) IA?	4.1.2 (c)			
	5. Does the organization have a Committee to make decisions on information and cyber security?	4.1.3			
	6. Does the organization have a committee to make decisions on information and cyber security risks?	4.1.4			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
End User Responsibilities	7. Has organization explained the end user responsibilities to users?	4.1.5			
Capacity Building	8. Has the organization taken any steps to develop the information security capacity of accountable individuals?	4.1.6			
Background Checks	9. Does your organization perform background checks and security clearance on officials dealing with "Secret" or "Confidential", information assets or having access to CNII ?	4.1.7			
Strategic Alignment	10. In designing and implementing the organization's functions, policies, strategies or projects, has your organization taken information security into account?	4.1.8			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Action Plan	11. Does your organization have financial provisions for information security activities?	4.1.9			
	12. Has your organization developed action plans to achieve its information security objectives?	4.1.10			
Identify Assets, Owners, Users, and Risks					
Identification of Assets	13. Has your organization identified information assets that have a value to the organization?	4.2.1			
	14. Has your organization assessed risk associated with information assets?	4.2.5			
	15. Has your organization identified information assets that have a value to the organization?	4.2.1			
	16. Has your organization assessed risk associated with information assets?	4.2.5			
	17. Has your organization classified information assets based on their sensitivity or other means?	4.2.6			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
	18. Has your organization recorded IT assets in an IT Assets Register?	4.2.4			
	19. Has your organization classified IT assets based on their criticality?	4.2.6			
	20. Has your organization identified the Owners of the assets?	4.2.3			
Protect Assets					
Encryption	21. Does your organization encrypt sensitive information prior to storage?	4.3.1			
	22. Does your organization encrypt sensitive information prior to moving through electronic channels?	4.3.2			
Physical Protection	23. Does your organization process or store sensitive information in secure areas?	4.3.3			
	24. Has your organization taken appropriate measures to protect secure areas from fire, flood, humidity and temperature?	4.3.3			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Protect Assets					
	25. Does your organization prevent unauthorized entry to secure areas?	4.3.3			
Physical Protection	23. Does your organization process or store sensitive information in secure areas?	4.3.3			
	24. Has your organization taken appropriate measures to protect secure areas from fire, flood, humidity and temperature?	4.3.3			
	25. Does your organization prevent unauthorized entry to secure areas?	4.3.3			
Identity Management and Access Control	26. Does your organization have an Identity Management and Access Control Policy?	4.3.4			
	27. Does your organization use strong authentication?	4.3.5			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Data Sovereignty	28. Does your organization ensure Data Sovereignty?	4.3.6			
	29. Does your organization assess risk prior to obtaining cloud service?	4.3.6			
Licensed Software and Patch Updates	30. Does the organization use operating systems (OSs) with valid License(s)?	4.3.7			
	31. Have the OSs (s) of the organization been updated with vendor supplied latest patches and fixes?	4.3.7			
	32. Does your organization have a procedure in place to ensure vendor supplied critical patches are installed on time?	4.3.7			
Antimalware	33. Has the organization installed Antimalware software with a valid license in all machines?	4.3.8			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Email	34. Does your organization restrict users from using personal emails for official communications?	4.3.9			
	35. Does your organization set up email filters to remove emails known to have malware attached?	4.3.10			
	36. Does your organization use encryption when sending sensitive information via email?	4.3.10			
Perimeter Security Devices	37. Does your organization have a Firewall in your computer network?	4.3.12			
Secure Remote Access	38. Does your organization use secure Virtual Private Networks (VPNs) for remote access?	4.3.13			
	39. Do all the users connecting remotely use VPN?	4.3.13			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Backup Strategy	40. Does your organization backup data?	4.3.14			
	41. Are the backups stored at a fire proof, secure location which is physically distant from the data processing site?	4.3.14			
Secure Disposal of Assets	42. Does your organization follow any of the following to dispose electronic media that contain sensitive information? - Shredding, punching, physically damaging, degaussing.	4.3.17			
Internal Information Security Audit Program	43. Does your organization have internal information security audit program?	4.3.18			
	44. Does your organization perform VAPTs through Sri Lanka CERT prior to any deployment of software applications?	4.3.19			
	45. Have you performed VAPT for your computer network?	4.3.19			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Work from Home	46. Does your organization adhere to the work from home guidelines issued by Sri Lanka CERT?	4.3.21			
Using Personal Devices for Official Work	47. Does your organization have a formal procedure to register personal devices?	4.3.22			
	48. Does your organization allow personal devices to process or store critical data?	4.3.22			
Detect Information Security Incidents					
Report Incidents	49. Has the organization instructed staff to report any suspicious activity, contact, theft, virus, vulnerability, unauthorized access, tampering with files, or violation of security policy to the person in charge of Information security?	4.4.1			
	50. Have you ever reported cyber security incidents to Sri Lanka CERT or any other party?	4.4.4			

Policy Domains	Assessment Criteria	Policy	Compliance		Remarks
			Yes	No	
Respond to Incidents					
Incident Response Plan and Activate the Plan	51. Has your organization developed an Incident Response Plan?	4.5.1			
	52. In the event of an information and cyber security event, does the organization activate an Incident Response Plan to minimize the impact on its operations and restore that operation?	4.5.2			
Recover from Incidents					
Disaster Recovery Plan and Activate the Plan	53. Does your organization have a Disaster Recovery Plan developed to facilitate the recovery in an event of a disaster?	4.6.1			
	54. In the event of a disaster (or event), does the organization activate its Disaster Recovery Plan to restore disrupted services?	4.6.2			

Glossary

Antimalware

Anti-malware is a software designed to identify malware in devices or prevent malware from infecting computer systems or electronic devices. Malware is any software intentionally designed to cause damage to a computer, server, or computer network (e.g. viruses, worms, ransomware).

Assets Classification

Classification is the process of categorizing information assets based on the level of sensitivity and criticality of that information. The primary objective of asset classification is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

Assets Custodian

Person in the organization who has the responsibility to protect an information asset throughout the lifecycle as it is stored, transported, or processed in line with the requirements defined by the information asset owner.

Assets Owner

An asset owner is a senior executive grade official responsible for the day-to-day management of assets. The asset owner controls the entire life cycle of the asset and must identify the risks to the assets and suggest appropriate security measures to protect them.

Availability of Information

Availability ensures timely and reliable access to and use of information.

Confidentiality of Information

Confidentiality refers to the assurance that information is not disclosed to unauthorized people and organizations.

Sensitive Information Assets

Any information the loss, alteration, misuse, disclosure or failure of which could adversely affect the interests of the organization or relevant individuals or entities. These information assets can be classified as "secret" and "confidential" by the government organization.

Critical IT Assets

Critical IT assets are systems, the unauthorized access, misuse, or failure of which can adversely affect data, organization, or individuals. These IT assets can be classified as “very critical” and “critical” by the organization. Further, these IT assets require a high level of security and may also exist in the form of CNII as defined below.

Critical National Information Infrastructure (CNII)

Critical information infrastructure are the systems or facilities, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy, health and social well-being of a nation.

Digital Signature

Digital Signature is a mathematical scheme for verifying the authenticity of digital messages or documents. It provides sender authenticity (identity of the users), message integrity (guarding against improper modification or destruction), and nonrepudiation (the claimed sender cannot later deny generating the document).

Encryption

Encryption is the process of converting a plaintext message into a secure-coded form of text, which cannot be understood without converting it back via decryption.

Government Organizations

The government organizations are the public authorities defined in the Right to Information Act No. 12 of 2016.

Information Security Controls

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to information and IT assets. Controls could be technologies, policies, procedures, or processors put in place to protect information assets.

Information Security Officer (ISO)

An Information Security Officer is a senior-level executive responsible for establishing and maintaining the organization’s objectives, strategy, and action plans to ensure information assets are adequately protected.

Information Security Committee (ISC)

In implementing the policy, this committee is responsible for reviewing and approving all information security controls, action plans, asset classification schemes, incidents response plans and disaster recovery plans and other activities carried out by the ISO.

Information and Event Management systems (SIEM)

SIEM is a solution that combines the collection data from log files for analysis and reports on security threats and events, and conduct real-time system monitoring, notifies network admins about important issues and establishes correlations between security events to provide real-time analysis of security alerts generated by applications and network hardware.

Information and Cyber Security

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

Information Assets

Information asset is information or data that is of value to the organization. This includes the documents available in an electronic format, database records as well as the documents available in paper format. Examples for information assets: word file, images, employees personal record in a database.

IT Assets

IT asset is any IT equipment, information system, software, storage media that is of value to the organization. Examples for IT assets are computers, servers, routers, disks, networks, software, information systems and its components.

Intrusion Detection and Prevention Systems (IPS/IDS)

Intrusion Detection Systems are devices that analyze network traffic to identify known cyberattacks. Intrusion Prevention Systems devices analyzes network traffic to identify known cyberattacks, however, it can stop attacks by preventing packet from being delivered based on type of attacks it detects

Integrity of Information

Integrity refers to guarding information against improper modification. It ensures that information remains in its original form.

Official Email

Official emails are the email accounts supplied by the government with the domain name of "gov.lk"

Private Cloud

Services offered over the Internet or over a private internal network to only select users. E.g. Lanka Government Cloud

Public Cloud

Cloud service available to anyone who wants to purchase them

Recovery Point Objective (RPO)

RPO is a measure of how often the organization should take backups, and it gives an indication of how up to date the recovered data will be. It indicates the earliest possible time in which it is acceptable to recover the data. For example, if a disaster occurs between backups, can the organization afford to lose 2 minutes' worth of data, or 2 hours or full day.

Recovery Time Objective (RTO)

RTO indicates the amount of downtime a business can tolerate. It is the earliest point in time at which the organization's operations and systems must be resumed after a disaster.

Systems Hardening

System hardening is the process of securing a system through changing the default configuration and settings to reduce IT vulnerability and the possibility of being compromised. This can be done by reducing the attack surface and attack vectors which attackers continuously try to exploit for the purpose of malicious activity.

Virtual Private Network (VPN)

Virtual Private Network, establishes a secure connection by utilizing an encrypted tunnel for data communication over the internet.

References

1. Information Security Implementation Guide. Published in 2022, by Research, Policy and Project Division of Sri Lanka CERT. Document can be accessed through www.onlinesafety.lk.
2. Minimum Information Security Guidelines. Published by Research, Policy and Project Division of Sri Lanka CERT. Document can be accessed through www.onlinesafety.lk.
3. Information and Cyber Security Strategy of Sri Lanka (2019:2023), Published in November 2019 by Research and Policy Unit, Sri Lanka CERT. Document can be accessed through <https://cert.gov.lk/documents/NCSStrategy.pdf>.
4. NIST Cybersecurity Framework. Published by National Institute of Standards and Technology, U.S Department of Commerce. Resource can be accessed through <https://www.nist.gov/cyberframework/online-learning/five-functions>.
5. Information Security Guidelines for Working from Home. Published by Sri Lanka CERT. Document can be access through <https://www.onlinesafety.lk>.
6. Website Security Guidelines for Government Organizations. Published by Research, Policy and Projects Division of Sri Lanka CERT, in 2022. Document can be accessed through <https://www.onlinesafety.lk>.
7. Web Application Security Guidelines for Government Organizations. Published by Research, Policy and Projects Division of Sri Lanka CERT, in 2022. Document can be accessed through <https://www.onlinesafety.lk>.
8. Technical Guidelines for Web Application and Website Security. Published by Research, Policy and Projects Division of Sri Lanka CERT in 2022. Document can be accessed through <https://www.onlinesafety.lk>.
9. ISO 27002 (2013): Information Technology – Security Techniques - Information Security Management Systems – Requirements, International Standards Organization, Published by International Standard Organization. Document can be accessed through <https://www.iso.org>.



රාජ්‍ය ආයතන සඳහා
තොරතුරු හා
සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය

© ශ්‍රී ලංකා සර්ටි 2022, සියලු කතු හිමිකම් ඇවිරිණි.

රාජ්‍ය ආයතන සඳහා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය - සිංහල අනුවාදය
පලමු මුද්‍රණය : 2023 ජනවාරි

මෙම ප්‍රතිපත්තිය 2022 අගෝස්තු 22 දින සිට ක්‍රියාත්මක කිරීමට අමාත්‍ය මණ්ඩල
අනුමැතිය ලබා දී ඇත.

ලේඛන වර්ගීකරණය : පොදු

ප්‍රකාශනය

පර්යේෂණ, ප්‍රතිපත්ති සහ ව්‍යාපෘති අංශය,

ශ්‍රී ලංකා සර්ටි ආයතනය,

කාමර අංක 4-112, බණ්ඩාරනායක ජාත්‍යන්තර සම්මන්ත්‍රණ ශාලාව,

බොද්දාලෝක මාවත, කොළඹ 7.

ශ්‍රී ලංකාව.

දුරකථන : + 94 11 269 1692 ෆැක්ස් + 94 11 269 1604

විද්‍යුත් තැපෑල : cert@cert.gov.lk

වෙබ් : www.cert.gov.lk | www.onlinesafety.lk



පටුන

1.	හැඳින්වීම	77
2.	තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව	79
3.	තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය	82
3.1.	අරමුණු	82
3.2.	ප්‍රතිපත්තියේ විෂය පථය	82
4.	ප්‍රතිපත්ති සංග්‍රහය	88
4.1.	තොරතුරු සහ සයිබර් ආරක්ෂණ පාලනය	88
4.1.1	නායකත්වය	89
4.1.2	ආරක්ෂණ ආයතනික ව්‍යුහය	90
(අ)	තොරතුරු ආරක්ෂණ නිලධාරීගේ කාර්යභාරය	90
(ආ)	ප්‍රධාන නව්‍යකරණ නිලධාරීගේ කාර්යභාරය	90
(ඇ)	(ප්‍රධාන) අභ්‍යන්තර විගණකගේ කාර්යභාරය	90
4.1.3	තොරතුරු ආරක්ෂණ කමිටුව	91
4.1.4	අවදානම් කළමනාකරණ කමිටුව	91
4.1.5	පරිශීලකයන්ගේ වගකීම්	91
4.1.6	ධාරිතා සංවර්ධනය	92
4.1.7	කාර්ය මණ්ඩලය සඳහා ආරක්ෂක නිෂ්කාශන පරීක්ෂාව	92

4.1.8	උපායමාර්ගික පෙළගැස්වීම	93
4.1.9	ක්‍රියාකාරී සැලසුම් සහ ප්‍රතිපාදන	93
4.1.10	ප්‍රතිපත්ති අනුකූලතාවය	93
4.2	වත්කම්, හිමිකරුවන්, පරිශීලකයන් සහ අවදානම් හඳුනා ගැනීම	94
4.2.1	තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් හඳුනා ගැනීම	94
4.2.2	තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් හඳුනා ගැනීම.	95
4.2.3	වත්කම් හිමිකරුවන්, භාරකරුවන් සහ පරිශීලකයන්ගේ වගකීම්	95
4.2.4	තොරතුරු වත්කම් සහ තොරතුරු තාක්ෂණ වත්කම් පවත්වා ගැනීම	96
4.2.5	අවදානම තක්සේරු කිරීම	97
4.2.6	වත්කම් වර්ගීකරණය කිරීම	97
4.3	වත්කම් ආරක්ෂා කිරීම	98
4.3.1.	නිශ්චලව පවතින දත්ත ආරක්ෂා කිරීම	98
4.3.2	සංවරණය වෙමින් පවතින දත්ත ආරක්ෂා කිරීම	99
4.3.3	භෞතික ආරක්ෂාව	99
4.3.4	අන්‍යන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය	100
4.3.5	ශක්තිමත් සත්‍යාපනය	101
4.3.6	දත්ත ස්වෛරීභාවය සහ මේසගත පරිගණක භාවිතය	102
4.3.7	වලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතය සහ සරිමා යාවත්කාලීන කිරීම්	104
4.3.8	ප්‍රති - අනිෂ්ට මෘදුකාංග භාවිතය	104
4.3.9	නිල විද්‍යුත් තැපැල්	105
4.3.10	විද්‍යුත් තැපැලෙහි ආරක්ෂාව	105
4.3.11	බිෂ්ටල් අත්සන් භාවිතය	106
4.3.12	පරිමිති ආරක්ෂණ පාලනයන්	106
4.3.13	ආරක්ෂිත දුරස්ථ ප්‍රවේශ භාවිතය	107
4.3.14	උපස්ථ උපාය මාර්ග	107
4.3.15	තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වල ආරක්ෂාව	108
4.3.16	ආරක්ෂාව තහවුරු කරගත් මෘදුකාංග සංවර්ධනය සහ භාවිතය	108
4.3.17	වත්කම් සුරක්ෂිතව බැහැර කිරීම	109

4.3.18	අභ්‍යන්තර තොරතුරු හා සයිබර් ආරක්‍ෂණ විගණන ක්‍රියාවලිය	110
4.3.19	භාවිතය ආරම්භ කිරීමට පෙර සිදු කරන විගණන	111
4.3.20	තොරතුරු තාක්ෂණ වත්කම්වල ආරක්‍ෂණ ප්‍රතිරෝධය ශක්තිමත් කිරීම	111
4.3.21	නිවසේ සිට රාජකාරි කටයුතුවල නිරතවීම්	112
4.3.22	රාජකාරි කටයුතු සඳහා තම පෞද්ගලික මෙවලම් භාවිතය	112
4.3.23	අන්තර්ජාල ජාල භාවිතය	113
4.3.24	වත්කම් සැපයුම්කරුවන් කළමනාකරණය	114
4.3.25	වෙනස්වීම් කළමනාකරණය	114
4.4	ආරක්‍ෂණයට බලපාන සිදුවීම් හඳුනා ගැනීම	115
4.4.1	ආරක්‍ෂණ සිදුවීම් වාර්තා කිරීම	115
4.4.2	ලොග් සටහන් සමාලෝචනය	116
4.4.3	ආරක්‍ෂණයට බලපාන සිදුවීම් අධීක්ෂණය අධීක්ෂණය කිරීම	117
4.4.4	ආරක්‍ෂණයට බලපාන සිදුවීම් ශ්‍රී ලංකා සර්ව ආයතනය වෙත වාර්තාකිරීම	117
4.5	ආරක්‍ෂණයට බලපාන සිදුවීම්වලට ප්‍රතිචාර දැක්වීම	117
4.5.1	ආරක්‍ෂණයට බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම	118
4.5.2	ආරක්‍ෂණයට බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සක්‍රිය කිරීම	118
4.5.3	වෝහාරික පරීක්ෂණ	119
4.6	මෙහෙයුම් ප්‍රතිසාධනය කිරීම	121
4.6.1	ආපදා ප්‍රතිසාධන සැලැස්ම	121
4.6.2	ආපදා ප්‍රතිසාධන සැලැස්ම සක්‍රිය කිරීම	122
4.6.3	තීරණාත්මක ආපදා හෝ සිදුවීම් සන්නිවේදනය	122
5.	ප්‍රමුඛතා පදනමින් ක්‍රියාත්මක කළ යුතු ප්‍රතිපත්තිය කරුණු	123
6.	තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය අධීක්‍ෂණය කිරීමේ සහ ඇගයීමේ ක්‍රමවේදය	127
	අර්ථ දැක්වීම්	138
	භාවිත ලේඛන	142





1. හැඳින්වීම

- 1.1 ශ්‍රී ලංකාවේ බොහෝ රාජ්‍ය ආයතන වර්තමානයේ රඳා පවතින්නේ ඩිජිටල් පද්ධති සහ යටිතල පහසුකම්වල විශ්වාසනීය ක්‍රියාකාරීත්වය මත ය. කෙසේ වෙතත්, ඇතැම් පුද්ගලයන් විසින් ද්වේෂ සහගත අරමුණින් සයිබර් තාක්ෂණය අවහාවිතා කරමින් ඩිජිටල් පද්ධතිවලට අනවසරයෙන් ඇතුළු වී සංවේදී තොරතුරු සොරකම් කිරීම, ආයතනයේ මෙහෙයුම් කටයුතුවලට බාධා පැමිණවීම, වෙබ් අඩවිවල අන්තර්ගතය විකෘති කරමින් ආයතනවල කීර්ති නාමයට හානි කිරීම වැනි අනර්ථ ක්‍රියා සිදුකරනු දැකිය හැකිය. එහි ප්‍රතිඵලයක් ලෙස රජයේ ආයතනවල ඇති ඩිජිටල් පද්ධති සහ යටිතල පහසුකම් කෙරෙහි ජනතාව තුළ පවතින විශ්වාසය පළමුව පමණක් නොව ජාතික ආරක්ෂාවට ද, රටෙහි ආර්ථික කටයුතුවලට සහ යහපැවැත්මට ද බලපෑම් ඇති විය හැකිය.
- 1.2 මෙම තොරතුරු හා සයිබර් ආරක්ෂණ අවදානම් ඵලදායී ලෙස කළමනාකරණය කර ගැනීම සඳහා රාජ්‍ය ආයතන අනුගත විය යුතු තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තියක්, ශ්‍රී ලංකාවේ සයිබර් අවකාශය ආරක්ෂා කිරීමේ අරමුණින් පිහිටුවා ඇති ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය (Sri Lanka Computer Emergency Readiness Team) හෙවත් ශ්‍රී ලංකා සර්ට් ආයතනය (Sri Lanka CERT) විසින් සකස් කර ඇත. මෙම ප්‍රතිපත්තිය මගින් ආයතනික මට්ටමින් තොරතුරු සහ සයිබර් ආරක්ෂණ වැඩපිළිවෙලක් ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය වන තොරතුරු හා සයිබර් ආරක්ෂණ අවදානම මූලික කර ගත් ආරක්ෂණ කළමනාකරණ ක්‍රමවේදයක් හඳුන්වා දී ඇත. තවද, ආයතනය විසින් ආරක්ෂා කළ යුතු වටිනා තොරතුරු සහ තොරතුරු තාක්ෂණ මෙවලම් (තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්) හඳුනා ගැනීම,

ඒවායේ ආරක්ෂණයට බලපාන අවදානම් සහ සිදුවීම් හඳුනා ගැනීම, වත්කම් ආරක්ෂා කිරීම සඳහා සුදුසු ක්‍රියාමාර්ග ගැනීම සහ සයිබර් ප්‍රහාරයන්ට කාර්යක්ෂමව සහ ඵලදායීව ප්‍රතිචාර දක්වමින් බිඳ වැටුණු හෝ අඩපණ වූ වත්කම් යථා තත්ත්වයට පත් කිරීමට ආයතනය ගත යුතු ක්‍රියාමාර්ග මෙම ප්‍රතිපත්තියේ දැක්වේ.

- 1.3 රාජ්‍ය ආයතන සඳහා වන තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ශ්‍රී ලංකාවේ තොරතුරු සහ සයිබර් ආරක්ෂණ උපායමාර්ගය (2019 :2023) ක්‍රියාත්මක කිරීමට අනුකූලව සකස් කර ඇති අතර එය ජාත්‍යන්තර ප්‍රමිති සංවිධානය (International Organization for Standardization) සහ එක්සත් ජනපදයේ ජාතික ප්‍රමිති සහ තාක්ෂණ ආයතනය (National Institute of Standards and Technology) වැනි පිළිගත් අන්තර්ජාතික තොරතුරු ආරක්ෂණ ප්‍රමිතීන්ට අනුකූල වන පරිදි කෙටුම්පත් කර ඇති අතර තොරතුරු ආරක්ෂණ විශේෂඥයින් සහ රජයේ ජ්‍යෙෂ්ඨ නිලධාරීන් විසින් පුළුල් ලෙස සමාලෝචනය කර ඇත.

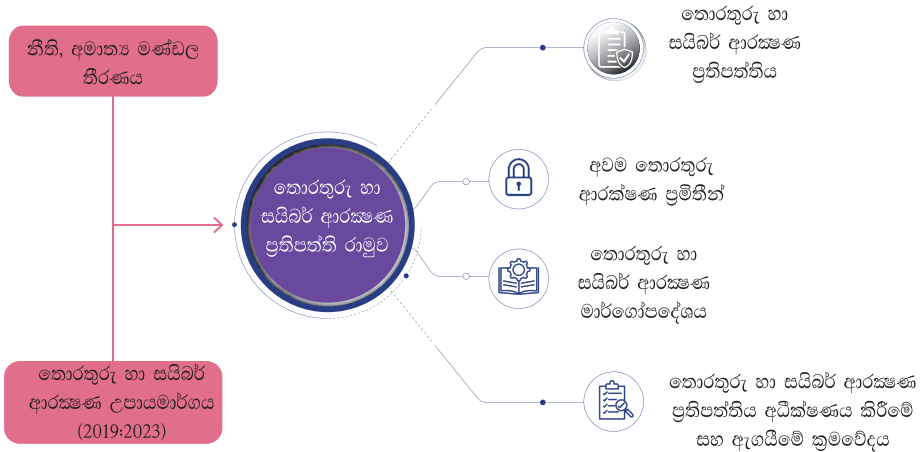
- 1.4 2016 අංක 12 දරණ තොරතුරු දැනගැනීමේ අයිතිවාසිකම් පිළිබඳ පනතේ 'පොදු අධිකාරිය' ලෙස අර්ථ දක්වා ඇති සියලුම රාජ්‍ය ආයතන මෙම ප්‍රතිපත්තියට අනුකූල විය යුතු අතර ආයතන ප්‍රධානීන් මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කර ආරක්ෂිත හා කාර්යක්ෂම සේවා සම්පාදනයක් ස්වකීය ආයතන තුළ සහතික කිරීමට වගකීමෙන් බැඳී සිටියි. මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේදී ශ්‍රී ලංකා සර්ව ආයතනය රාජ්‍ය ආයතන වලට අවශ්‍ය තාක්ෂණික උපදෙස් හා මගපෙන්වීම් ලබා දෙනු ලබන අතර ප්‍රතිපත්තිය ආයතන තුළ ක්‍රියාත්මක කිරීමේ ප්‍රගතිය පිළිබඳව වාර්ෂික ඇගයීමක් ද සිදු කරනු ඇත.





2. තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්ති රාමුව

2.1 රාජ්‍ය ආයතන තුළ තොරතුරු සහ සයිබර් ආරක්‍ෂණ වැඩසටහන් වඩාත් කාර්ය-ක්‍ෂමව සහ ඵලදායී ලෙස ක්‍රියාවට නැංවීම සඳහා අවශ්‍ය මෙවලම් තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්ති රාමුව මගින් හඳුන්වා දී ඇත. එමගින් (අ) තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය (Information and Cyber Security Policy), (ආ) රාජ්‍ය ආයතන අනුගමනය කළ යුතු අවම තොරතුරු ආරක්‍ෂණ ප්‍රමිතීන් (Minimum Information Security Standards), (ඇ) තොරතුරු හා සයිබර් ආරක්‍ෂණය ක්‍රියාත්මක කිරීමේ මාර්ගෝපදේශය (Information and Cyber Security Implementation Guide), සහ (ඈ) රාජ්‍ය ආයතනවල තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේ අධීක්‍ෂණය කිරීමේ සහ ඇගයීමේ ක්‍රමවේදයක් ද (Monitoring and Evaluation Methodology) ඇතුළත් වේ. තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්ති රාමුව පිළිබඳ දළ විශ්ලේෂණයක් රූප සටහන අංක 1 මගින් ඉදිරිපත් කර ඇත.



රූප සටහන අංක 1 තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව.

2.2 තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුවට පහත සඳහන් ප්‍රධාන සංරචක ඇතුළත් වේ.

- අ. තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය (Information and Cyber Security Policy) :
 තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්ති රාමුව තුළ ප්‍රමුඛතම අවධානය යොමු කෙරෙනුයේ රාජ්‍ය ආයතන සඳහා වන තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට ය. එම ප්‍රතිපත්තිය තුළ රජයේ ආයතන විසින් තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීම සඳහා අනුගමනය කළ යුතු ආරක්ෂණ ක්‍රමවේදයන් ඇතුළත් ප්‍රතිපත්ති මාලාවක් ඉදිරිපත් කරයි.
- ආ. අවම තොරතුරු ආරක්ෂණ ප්‍රමිතීන් (Minimum Information Security Standards) :
 රජයේ ආයතන විසින් පිළිපැදිය යුතු අවම තොරතුරු ආරක්ෂණ ප්‍රමිතීන් මේ යටතේ දැක්වේ. මෙම ලේඛනය ශ්‍රී ලංකා සර්ව ආයතනයේ www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැකිය.
- ඇ. තොරතුරු හා සයිබර් ආරක්ෂණ මාර්ගෝපදේශය (Information and Cyber Security Implementation Guide) : මෙමගින් නිලධාරීන්ට සහ පාර්ශ්වකරුවන්ට තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියේ අඩංගු එක් එක් ප්‍රතිපත්තිය කාරුණි ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය වන උපදෙස් මාලාවක් සපයයි. තොරතුරු ආරක්ෂණ පාලන ව්‍යුහයක් ස්ථාපිත කිරීම, වත්කම් වර්ගීකරණය, අවදානම් කළමනාකරණය, වත්කම් ආරක්ෂා කිරීම, උපස්ථ ක්‍රම සහ ආපදා ප්‍රතිසාධන ක්‍රම, සිදුවීම් කළමනාකරණය, අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය සහ ආරක්ෂාව තහවුරු කරගත් මෘදුකාංග සංවර්ධනය යනාදී ක්‍රියා සඳහා අවශ්‍ය වන තාක්ෂණික උපදෙස් මෙම මාර්ගෝපදේශයෙහි ඇතුළත් වේ. මෙම මාර්ගෝපදේශය www.onlinesafety.lk යන ශ්‍රී ලංකා සර්ව ආයතනයේ වෙබ් අඩවියෙන් බාගත කළ හැකිය.

ඇ. තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම අධීක්‍ෂණය කිරීමේ සහ ඇගයීමේ ක්‍රමවේදය. (Monitoring and Evaluation Methodology) : රාජ්‍ය ආයතනවල තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය අනුගමනය කිරීමට ඇති සුදානම සහ එය ක්‍රියාත්මක කිරීමේ කාර්යසාධනය සහ අධීක්‍ෂණය සහ ඇගයීම සඳහා තක්සේරුකරණ නිර්ණායක අඩංගු ක්‍රමවේදයක් මෙමගින් සැපයේ. ශ්‍රී ලංකා සර්වි ආයතනය මෙම ලේඛනයේ අංක 6 පරිච්ඡේදයේ විස්තර කර ඇති එම ක්‍රමවේදය භාවිතා කරමින් රාජ්‍ය ආයතනයේ තොරතුරු හා සයිබර් ආරක්‍ෂණ ක්‍රියාකාරකම්වල පරිණතභාවය නිශ්චිත කාල රාමුවක් තුළ ඇගයීමකට ලක් කෙරේ.

2.3 තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්ති රාමුව, ශ්‍රී ලංකාවේ තොරතුරු සහ සයිබර් ආරක්‍ෂණ උපාය මාර්ග, ඉ- රාජ්‍ය පිළිබඳ ප්‍රතිපත්තීන් සහ කලින් කලට පනවනු ලබන නීති, රෙගුලාසි සහ අමාත්‍ය මණ්ඩල තීරණවලට අනුකූලව ක්‍රියාත්මක කෙරෙනු ඇත.





3. තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය

3.1. අරමුණු

3.1.1 තොරතුරු හා සයිබර් ආරක්ෂණය යනු තොරතුරු වත්කම්වල රහස්‍යභාවය (confidentiality), උපයෝජ්‍යතාවය (confidentiality), සහ විශ්වසනීයභාවය (integrity) සහතික කිරීම සඳහා ඒවා වෙත අනවසරයෙන් වන ප්‍රවේශ වීම්, හාවික කිරීම්, වෙනස් කිරීම් හෝ විනාශ කිරීම් වලින් තොරතුරු වත්කම් ආරක්ෂා කිරීමයි. මේ යටතේ තොරතුරු වත්කම් අඩංගු හෝ භාවිතා වන තොරතුරු තාක්ෂණ මෙවලම් පුද්ගලයන් විසින් ද්වේශසහගතව සයිබර් තාක්ෂණය හෝ වෙනත් ක්‍රමවේදයන් භාවිතා කොට සිදු කරන හානිදායී ක්‍රියාවලින් ආරක්ෂා කර ගැනීම හෝ ජල ගැලීම්, ගිනි ගැනීම් වැනි වෙනත් ස්වභාවික විපත් මගින් සිදුවන හානිවලින් ආරක්ෂා කර ගැනීම ද ඇතුළත් වේ.

3.1.2 මෙම සන්දර්භය තුළ තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය මගින් රාජ්‍ය ආයතනයන්හි භාවිතා වන තොරතුරු වත්කම් සහ ඒවා පරිහරණය කරන තොරතුරු තාක්ෂණ වත්කම්, ස්වභාවික ආපදා සහ පුද්ගල ක්‍රියාකාරකම් මගින් වන හානිවලින් ආරක්ෂා කර ගැනීම සඳහා අනුගමනය කළ යුතු නීති රීති සහ මාර්ගෝපදේශ මාලාවක් හඳුන්වා දීම මෙම ප්‍රතිපත්තියේ මූලික අරමුණ වේ.

3.1.3 ප්‍රතිපත්තියේ අනෙකුත් අරමුණු වනුයේ,

- අ. රාජ්‍ය අංශයේ සියලුම ආයතන සඳහා පොදු තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රමිතියක් ස්ථාපිත කිරීම.
- ආ. තොරතුරු, පද්ධති සහ ඩිජිටල් යටිතල පහසුකම් සැලසුම් කිරීම, ක්‍රියාත්මක කිරීම සහ භාවිතය සම්බන්ධයෙන් වන ආරක්‍ෂණ ප්‍රමිතීන්, නීති රීති සහ ක්‍රියාවලීන් රාජ්‍ය ආයතන සඳහා අනිවාර්ය කිරීම තුළින් තොරතුරු සහ සයිබර් ආරක්‍ෂණ සිදුවීම්වලට සාර්ථකව මුහුණ දීම සඳහා රාජ්‍ය ආයතනවල ප්‍රත්‍යවර්ථතාවය වැඩිදියුණු කිරීම.
- ඇ. තොරතුරු සහ සයිබර් ආරක්‍ෂණ සිද්ධීන් ක්‍ෂණිකව හඳුනාගැනීමට, එවැනි සිදුවීම්වලින් ආයතනවලට වන බලපෑම අවම කිරීමට සහ එවැනි සිදුවීම් හේතුවෙන් දුර්වල වූ හෝ බිඳ වැටුණු ඕනෑම ආයතනික සේවාවක් කාර්යක්‍ෂමව යථා තත්වයට පත් කිරීමට සුදුසු යාන්ත්‍රණයක් ස්ථාපනය කිරීම.
- ඈ. තොරතුරු සහ සයිබර් ආරක්‍ෂාව පිළිබඳ සුදුසුම භාවිතයන්, ආරක්‍ෂණ ප්‍රමිතීන්, නීති රීති සහ ක්‍රියාවලීන් පිළිබඳව කාර්ය මණ්ඩලය දැනුවත් කිරීම සහ ආයතනයේ සුරක්‍ෂිතභාවය පිළිබඳව කාර්ය මණ්ඩලයේ විශ්වාසය ගොඩනැගීම.

3.1.4 සියලුම රාජ්‍ය ආයතන වල කාර්ය මණ්ඩලයන්ට සහ අදාළ තෙවන පාර්ශවීය සේවා සපයන්නන්ට මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම සම්බන්ධයෙන් ඔවුන් වෙත පැවරී ඇති වගකීම් සහ ඔවුන්ගේ වගවීම් පිළිබඳව පහසුවෙන් කියවා තේරුම් ගත හැකි ආකාරයට මෙම ප්‍රතිපත්තිය නිර්මාණය කර ඇත.

3.1.5 මෙම ප්‍රතිපත්තියේ අඩංගු තොරතුරු ආරක්‍ෂණ ප්‍රමිතීන්, සුදුසුම භාවිතයන් සහ තාක්‍ෂණික මාර්ගෝපදේශයන් රාජ්‍ය ආයතනයේ තොරතුරු, පද්ධති සහ ඩිජිටල් යටිතල පහසුකම් ආරක්‍ෂා කිරීම පිණිස කාලානුරූපීව යාවත්කාලීන කරනු ඇත.

3.2. ප්‍රතිපත්තියේ විෂය පරාසය

3.2.1 මෙම ප්‍රතිපත්තිය ඕනෑම අමාත්‍යාංශයක්, දෙපාර්තමේන්තුවක්, රාජ්‍ය සංස්ථාවක්, පළාත් පාලන ආයතනයක්, රාජ්‍ය ආයතන වෙනුවෙන් තොරතුරු තාක්‍ෂණ සේවා කළමනාකරණය කරන අදාළ තෙවන පාර්ශව සේවා සපයන්නන් ද ඇතුළුව 2016 අංක 12 දරණ තොරතුරු දැනගැනීමේ අයිතිවාසිකම් පිළිබඳ පනතේ පොදු අධිකාරීන් ලෙස අර්ථ දක්වා ඇති ඕනෑම ආකාරයක ආයතනයකට මෙම ප්‍රතිපත්තිය අදාළ වේ.

3.2.2 මෙම ප්‍රතිපත්තියේ අඩංගු ප්‍රතිපත්ති ප්‍රකාශන කොටස් දෙකකින් සමන්විත වේ. ඒවානම්, සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වන ප්‍රතිපත්ති ප්‍රකාශන සහ තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වන ප්‍රතිපත්ති ප්‍රකාශන වේ. තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන මෙම ප්‍රතිපත්තියේ අඩංගු, ඔවුන් සඳහා විශේෂ වූ ප්‍රතිපත්ති ප්‍රකාශන ඇතුළුව අනෙකුත් සියලුම ප්‍රතිපත්තිවලට ද අනුගත විය යුතුය. අනෙකුත් ආයතන සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වන ප්‍රතිපත්ති ප්‍රකාශනවලට අනුගත විය යුතු අතර තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වන ප්‍රතිපත්ති ප්‍රකාශන වලටද සුදුසු පරිදි අනුගත වන්නේ නම් මැනවි.

3.2.3 මෙහි තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන ලෙස හඳුන්වන්නේ බිඳ වැටීමකදී හෝ අඩපණ වීමකදී ජාතික ආරක්‍ෂාව, රාජ්‍ය පාලනය, ආර්ථිකය, සෞඛ්‍ය සහ සමාජ යහපැවැත්ම කෙරෙහි සාමාන්‍යමය බලපෑමක් ඇති කරන තොරතුරු හා තොරතුරු තාක්‍ෂණ වත්කම් පවත්වාගෙන යන ආයතන වේ. එම ආයතන ශ්‍රී ලංකා සර්ව ආයතනය විසින් හඳුනාගෙන ප්‍රකාශයට පත්කරනු ඇත.

3.2.4 තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය, එක්සත් ජනපදයේ ජාතික ප්‍රමිති සහ තාක්‍ෂණ ආයතනය විසින් හඳුන්වා දෙනු ලැබූ සුවිශේෂී තොරතුරු ආරක්‍ෂණ කාර්යයන් කිහිපයක් මත පදනම්ව සකස් කොට ඇත. ඒවා නම් (අ) ආයතනයේ තොරතුරු හා තොරතුරු තාක්‍ෂණ වත්කම් හඳුනා ගැනීම (හඳුනා ගැනීමේ කාර්යය) (ආ) එම වත්කම් ආරක්‍ෂා කිරීමට අවශ්‍ය ක්‍රියා මාර්ග ගැනීම (ආරක්‍ෂා කිරීමේ කාර්යය), (ඇ) එම වත්කම් සඳහා වන තොරතුරු හා සයිබර් ආරක්‍ෂණ සිදුවීම් අනාවරණය කර ගැනීම (අනාවරණය කරගැනීමේ කාර්යය), (ඈ) එම සිදුවීම්වලට සාර්ථකව ප්‍රතිචාර දැක්වීම (ප්‍රතිචාර දැක්වීමේ කාර්යය) සහ (ඉ) යම් සිදුවීමක් හේතුවෙන් දුර්වලවූ හෝ බිඳ වැටුණු ඕනෑම සේවාවක් කාර්යක්‍ෂමව යථා තත්ත්වයට පත් කිරීම වේ (ප්‍රතිසාධන කාර්යය). තවද තොරතුරු සහ සයිබර් ආරක්‍ෂාව සම්බන්ධ ක්‍රියාකාරකම් මෙහෙයවීම සහ පාලනය කිරීම සඳහා ආයතනික මට්ටමින් පාලන ව්‍යුහයක් ස්ථාපිත කිරීම ද මෙයට ඇතුළත් ය. රූප සටහන් අංක 2 මගින් තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කරමින් ආයතනයේ තොරතුරු හා තොරතුරු තාක්‍ෂණ වත්කම් ආරක්‍ෂා කිරීමට ආයතනය ගත යුතු ක්‍රියාමාර්ග දැක්වේ.





රූප සටහන අංක 2 : තොරතුරු සහ සයිබර් ආරක්ෂණ පියවර.

3.2.5 ඉහත අංක 3.2.4 හි සඳහන් වූ සුවිශේෂී තොරතුරු ආරක්ෂණ කාර්යයන් පදනම්ව නිර්මාණය කරන ලද මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කරමින් තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීමට ආයතනය ගත යුතු ක්‍රියාමාර්ග පහතින් විස්තර කෙරේ.

- අ. තොරතුරු හා සයිබර් ආරක්ෂණ පාලනය (Information and Cyber Security Governance): මෙමගින් හඳුන්වනුයේ ආයතනයක තොරතුරු සහ සයිබර් ආරක්ෂාව මෙහෙයවන සහ පාලනය කරන ක්‍රමවේදය වේ. මේ යටතේ ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ කටයුතු ක්‍රියාත්මක කිරීම සඳහා ආයතනික ව්‍යුහයක් ස්ථාපනය කිරීම, තොරතුරු සහ සයිබර් ආරක්ෂාව සඳහා වගකිව යුතු සහ වගවිය යුතු නිලධාරීන් පත් කිරීම සහ එවැනි නිලධාරීන්ගේ ධාරිතාවන් සංවර්ධනය කිරීම, ආයතනික තොරතුරු සහ සයිබර් ආරක්ෂක අරමුණු ස්ථාපනය කිරීම, ක්‍රියාකාරී සැලසුම් සකස් කිරීම සහ තොරතුරු ආරක්ෂක කටයුතු සඳහා සම්පත් සැපයීම කළ යුතුය. (පරිච්ඡේද අංක 4.1)

- ආ. හඳුනා ගැනීමේ කාර්යය (Identify Function) : ආයතනය සතු දත්ත, තොරතුරු, පරිගණක පද්ධති සහ තීරණාත්මක ඩිජිටල් යටිතල පහසුකම් වැනි තොරතුරු, තාක්ෂණ වත්කම් හඳුනාගැනීමත්, ඒවා සඳහා වන තොරතුරු සහ සයිබර් ආරක්ෂණ අවදානම් හඳුනාගෙන එම අවදානම් ඵලදායී ලෙස කළමනාකරණය කරන්නේ කෙසේද යන්න පිළිබඳ උපදෙස් මේ යටතේ පෙළගස්වා ඇත. (පරිච්ඡේද අංක 4.2) මේ අනුව, රාජ්‍ය ආයතන තමන් සතු තොරතුරු තාක්ෂණ වත්කම් හොඳින් හඳුනාගෙන, ඒවාට ඇති අවදානම තක්සේරුකරමින් එම වත්කම් මනාලෙස කළමනාකරණය කළ යුතුය.

- ඇ. ආරක්ෂා කිරීමේ කාර්යය (Protect Function): ආරක්ෂා කිරීමේ කාර්යය මගින්, රාජ්‍ය ආයතන සිය තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කරගනිමින් සිය සේවාවන් අඛණ්ඩව පවත්වාගෙන යාම සහතික කිරීම සඳහා ගතයුතු තොරතුරු සහ සයිබර් ආරක්ෂණ ක්‍රමවේදයන් විස්තර කෙරේ. ආයතනය සතු තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීම සඳහා ඒවා වෙත වන ප්‍රවේශය පාලනය කිරීම, ගිනිපවුරු (firewalls) සහ ප්‍රති-අනිෂ්ට මෘදුකාංග (anti-malware) ස්ථාපනය කිරීම, තොරතුරු ආරක්ෂණ විගණන පැවැත්වීම සහ උපස්ථ පිටපත් (backups) තබා ගැනීම ඇතුළුව පරිච්ඡේද අංක 4.3 හි සඳහන් ප්‍රතිපත්තීන් ක්‍රියාවට නැංවිය යුතුය.

- ඈ. අනාවරණ කරගැනීමේ කාර්යය (Detect Function): මෙම කාර්යය මගින් තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීමක් අනාවරණය කර ගැනීමට අවශ්‍ය ක්‍රියාමාර්ග විස්තර කෙරේ. ආයතන විසින් සිදුවීම් ක්ෂණිකව හඳුනා ගැනීමට සුදුසු යාන්ත්‍රණයන් ක්‍රියාත්මක කළ යුතු අතර පරිගණක සහ අදාල මෙවලම් මගින් උත්පාදනය කරන ලොග් සටහන් විශ්ලේෂණය කරමින් සහ සිදුවීම් හඳුනා ගැනීමේ මෙවලම් භාවිතයෙන් එම සිදුවීම් කාර්යක්ෂම ලෙස හඳුනා ගැනීමට කටයුතු කළ යුතු වේ. (පරිච්ඡේද අංක 4.4).

- ඉ. ප්‍රතිචාර දැක්වීමේ කාර්යය (Respond Function): මෙම කාර්යය මගින් හඳුනාගත් තොරතුරු සහ සයිබර් ආරක්ෂණ සිද්ධීන්ට ප්‍රතිචාර දැක්විය යුතු ආකාරය විස්තර කෙරේ. ඒ සඳහා, පරිච්ඡේද අංක 4.5 හි සඳහන් කර ඇති පරිදි, රාජ්‍ය ආයතන, තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීම්වලට කාර්යක්ෂම සහ ඵලදායී ලෙස ප්‍රතිචාර දැක්වීම සඳහා ආරක්ෂණ සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් පිළියෙලකොට ක්‍රියාවෙහි නැංවිය යුතුය.



4. ප්‍රතිපත්ති සංග්‍රහය

රාජ්‍ය ආයතන සඳහා වන තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ප්‍රධාන ප්‍රතිපත්ති අංශ හයකින් සමන්විත වේ. ඒවානම්, (අ) තොරතුරු හා සයිබර් ආරක්ෂණ පාලනයක් ආයතනය තුළ ස්ථාපනය කිරීම, (ආ) වත්කම්, ඒවායේ හිමිකරුවන් සහ භාරකරුවන්, සහ වත්කම් සඳහා වන අවදානම් හඳුනා ගැනීම, (ඇ) වත්කම් ආරක්ෂා කරගැනීම (ඈ) වත්කම් සම්බන්ධ තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම, (ඉ) ආරක්ෂණයට බලපාන සිදුවීම්වලට ප්‍රතිචාර දැක්වීම සහ (උ) ආපදාවකදී බිඳ වැටුණ හෝ අඩපන වූ මෙහෙයුම් ප්‍රතිසාධනය වේ. ඉහත දැක්වූ අංශ හයට අදාළව රාජ්‍ය ආයතන අනුකූල විය යුතු ප්‍රතිපත්තීන් එක් එක් අංශය යටතේ පෙළගස්වා ඇත.

4.1 තොරතුරු සහ සයිබර් ආරක්ෂණ පාලනය

මෙම පරිච්ඡේදය මගින් ආයතනයේ තොරතුරු සුරක්ෂිතතාව මෙහෙයවීම සහ පාලනය කිරීම සඳහා යාන්ත්‍රණයක් යෝජනා කරන අතර ආයතනය තුළ තොරතුරු ආරක්ෂණ ක්‍රියාකාරකම්වල නිසි කළමනාකරණයක් සහතික කිරීම සඳහා අවශ්‍ය නායකත්වය සහ වගවීම සම්බන්ධයෙන් මෙහි සඳහන් වේ. තවද ආයතනයේ මෙහෙවර හා දැක්ම සාක්‍ෂාත් කර ගැනීම සඳහා තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරකම් සක්‍රීය ලෙස දායක කර ගැනීමේ අවශ්‍යතාවය, වගවියයුතු නිලධාරීන්ගේ ධාරිතා සංවර්ධනයේ අවශ්‍යතාවය, ක්‍රමවත් තොරතුරු හා සයිබර් ආරක්ෂණ සැලසුම් සැකසීමේ සහ මෙම ප්‍රතිපත්තිය සඳහා රාජ්‍ය ආයතන අනුගත වීමේ වැදගත්කම මෙහි තවදුරටත් සඳහන් වේ.

මේ අනුව පහත දක්වා ඇති ප්‍රතිපත්තිමය කාරණා සඳහා රාජ්‍ය ආයතන අනුකූල වීම අපේක්ෂා කෙරේ.

4.1.1 නායකත්වය පිළිබඳ ප්‍රතිපත්තිය

ආයතන ප්‍රධානියා විසින් ආයතනයේ තොරතුරු ආරක්‍ෂණ ක්‍රියාකාරකම් සඳහා නායකත්වය සැපයිය යුතු අතර, ආයතනයේ තොරතුරු සහ තොරතුරු තාක්‍ෂණ වත්කම් ආරක්‍ෂා කිරීමේ පරම වගකීම සහ වගවීම ද දැරිය යුතු වේ.



ආයතන ප්‍රධානියා විසින් ආයතනයේ මෙම තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම සඳහා මූලිකත්වය ගෙන කටයුතු කළ යුතු අතර, ආයතනයේ දැක්ම සහ මෙහෙවර සාක්‍ෂාත් කර ගැනීම සඳහා අවශ්‍ය වන තොරතුරු ආරක්‍ෂණ ඉලක්ක සැකසීමත්, තොරතුරු ආරක්‍ෂක ක්‍රියාකාරකම් සඳහා අවශ්‍ය සම්පත් සැපයීමත් සිදු කළ යුතුය.

තවද ආයතනයේ පරිගණක පරිශීලකයන්, මෙම ප්‍රතිපත්තියට අනුගත වෙමින් ඔවුන් භාවිතා කරන තොරතුරු සහ තොරතුරු තාක්‍ෂණ වත්කම් ආරක්‍ෂා කිරීම සඳහා සක්‍රීයව දායකත්වය සපයන තොරතුරු ආරක්‍ෂණ සංස්කෘතියක් ආයතනය තුළ නිර්මාණය කිරීම සඳහා ද ආයතන ප්‍රධානියා විසින් අවශ්‍ය නායකත්වය සැපයිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.2 ආරක්ෂණ ආයතනික ව්‍යුහය පිළිබඳ ප්‍රතිපත්තිය

රාජ්‍ය ආයතනය තුළ තොරතුරු හා සයිබර් ආරක්ෂණ ආයතනික ව්‍යුහයක් ස්ථාපිත කළ යුතුය. ඵලදායී ආයතනික තොරතුරු ආරක්ෂණ ව්‍යුහයක් තුළ (අ) තොරතුරු ආරක්ෂණ නිලධාරී, (ආ) ප්‍රධාන නව්‍යකරණ නිලධාරී සහ (ඇ) (ප්‍රධාන) අභ්‍යන්තර විගණක වැනි තනතුරු ඇතුළත් විය යුතුය. ආයතනයේ තොරතුරු, ආරක්ෂණ ක්‍රියාකාරකම් තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුව ක්‍රියාත්මක කිරීම, මෙහෙයවීම සහ කළමනාකරණය කිරීම සඳහාත්, ආයතනයේ තොරතුරු සහ තොරතුරු ආරක්ෂණ වත්කම් සයිබර් ප්‍රහාරයන්ගෙන් ආරක්ෂා කර ගැනීම සඳහාත් මෙම ව්‍යුහාත්මක වගකීම් දරන නිලධාරීන් අවශ්‍ය වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

(අ) තොරතුරු ආරක්ෂණ නිලධාරීන්ගේ කාර්යභාරය පිළිබඳ ප්‍රතිපත්තිය.

ආයතන ප්‍රධානියා විසින් රාජ්‍ය ආයතනය සඳහා තොරතුරු ආරක්ෂණ නිලධාරියෙකු පත් කළ යුතුය. ඵම නිලධාරියා, ආයතන ප්‍රධානියාගේ අනුදැනුම සහ මගපෙන්වීම යටතේ, ආයතනයේ තොරතුරු ආරක්ෂණ අරමුණු ස්ථාපිත කිරීම, තොරතුරු ආරක්ෂණ අවදානම් කළමනාකරණය කිරීම සහ ආයතනයේ තොරතුරු තාක්ෂණ වත්කම් ප්‍රමාණවත් ලෙස ආරක්ෂා කර ඇති බව සහතික කිරීම සඳහා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම යන වගකීම් දරන ජ්‍යෙෂ්ඨ මට්ටමේ විධායක නිලධාරියකු විය යුතුය.

රාජ්‍ය ආයතනය තුළ තොරතුරු ආරක්ෂණ නිලධාරීන්ගේ කාර්යභාරය තොරතුරු තාක්ෂණ විෂය පථයෙන් ස්වයංක්‍රීය විය යුතු අතර, තොරතුරු ආරක්ෂණයට අදාළ ක්‍රියාකාරකම් සම්බන්ධයෙන් ආයතන ප්‍රධානියා වෙත සෘජුවම වාර්තා කළ යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

(ආ) ප්‍රධාන නව්‍යකරණ නිලධාරීන්ගේ කාර්යභාරය පිළිබඳ ප්‍රතිපත්තිය.

ප්‍රධාන නව්‍යකරණ නිලධාරී හෝ තොරතුරු තාක්ෂණ විෂය භාර නිලධාරියා ආයතනයේ තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීමට අවශ්‍ය ක්‍රියාමාර්ග ගැනීමට සහ ආයතනයේ පරිපාලන කටයුතු අඛණ්ඩව පවත්වාගෙන යාම සහතික කිරීමට අවශ්‍ය තොරතුරු ආරක්ෂණ පුහුණුව ලබාදී නිසි වගකීම් පැවරිය යුතුය.

සටහන: තොරතුරු ආරක්ෂණ නිලධාරියකු ආයතනය තුළ පත්කර නොමැති අවස්ථාවකදී, තොරතුරු තාක්ෂණ විෂය භාර නිලධාරියා ආයතනයේ තොරතුරු ආරක්ෂණ නිලධාරියා ලෙස කටයුතු කිරීමට බල ගැන්විය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

(ඇ) (ප්‍රධාන) අභ්‍යන්තර විගණකගේ කාර්යභාරය පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ තොරතුරු ආරක්ෂණ විගණන ආරම්භ කිරීම සහ අධීක්ෂණය කිරීම, තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය ආයතනය තුළ ක්‍රියාත්මක කිරීමේ ප්‍රගතිය තක්සේරු කිරීම සහ තොරතුරු ආරක්ෂාව හා සම්බන්ධ කටයුතු වලදී විගණන හා කළමනාකරණ කමිටුවට (Audit and Management Committee) වාර්තා කිරීම යන වගකීම් ආයතනයේ අභ්‍යන්තර විගණක නිලධාරියා (හෝ ප්‍රධාන අභ්‍යන්තර විගණක නිලධාරියා) වෙත පැවරේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.3 තොරතුරු ආරක්‍ෂණ කමිටුව පිළිබඳ ප්‍රතිපත්තිය

තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමට අදාළ ක්‍රියාකාරකම් සඳහා උපාය මාර්ගික උපදෙස් සැපයීම සඳහා ආයතනය තොරතුරු ආරක්‍ෂණ කමිටුවක් පිහිටුවිය යුතුය. ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේදී තොරතුරු ආරක්‍ෂණ නිලධාරියා විසින් සිදු කරනු ලබන සියලුම තොරතුරු ආරක්‍ෂණ පාලනයන්, ක්‍රියාකාරී සැලසුම්, තොරතුරු තාක්‍ෂණ වත්කම් වර්ගීකරණයට අදාළ ක්‍රමවේද, සිද්ධීන්ට ප්‍රතිචාර දැක්වීමේ සැලසුම් සහ ආපදා ප්‍රතිසාධන සැලසුම් ඇතුළු අනෙකුත් ක්‍රියාකාරකම් සමාලෝචනය කිරීම සහ අනුමත කිරීම සඳහා මෙම කමිටුව වගකිව යුතුය. ආයතන ප්‍රධානියා කමිටුවේ මූලසුන දැරිය යුතු අතර එම කමිටුව තොරතුරු ආරක්‍ෂණ නිලධාරී, ප්‍රධාන නව්‍යකරණ නිලධාරී, (ප්‍රධාන) අභ්‍යන්තර විගණක නිලධාරී සහ වත්කම් හිමියන්ගෙන් සමන්විත විය යුතුය. වත්කම් හිමිකරුවන් පිළිබඳ ප්‍රතිපත්තිය අංක 4.2.3 යටතේ දක්වා ඇත.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.4 අවදානම් කළමනාකරණ කමිටුව පිළිබඳ ප්‍රතිපත්තිය

ආයතනය තුළ අවදානම් කළමනාකරණ කමිටුවක් පිහිටුවිය යුතුය. මෙම කමිටුව ආයතන ප්‍රධානී වෙත සෘජුවම වාර්තා කරන ස්වාධීන කමිටුවක් විය යුතු අතර, තොරතුරු සහ තොරතුරු තාක්‍ෂණ වත්කම් සම්බන්ධයෙන් ආයතනයේ අවදානම් කළමනාකරණය අධීක්‍ෂණය කිරීමේ වගකීම දැරිය යුතු වේ.

මෙම කමිටුව ආයතනයේ තොරතුරු තාක්‍ෂණ වත්කම් සම්බන්ධයෙන් වන අවදානම් හඳුනාගෙන ඒවා නිසි ඇගයීමට ලක් කළ යුතු අතර, එම හඳුනාගත් අවදානම් අවම කිරීම සඳහා අවශ්‍ය ක්‍රියාමාර්ග ගැනීමට තොරතුරු ආරක්‍ෂණ කමිටුව වෙත සුදුසු ක්‍රමවේද යෝජනා කළ යුතුය. මෙම කමිටුවට ආයතනයේ අංශ ප්‍රධානීන්, තොරතුරු තාක්‍ෂණ වත්කම් හිමිකරුවන් සහ තොරතුරු ආරක්‍ෂණ නිලධාරී ඇතුළත් විය යුතුය. ආයතනයේ නියෝජ්‍ය ප්‍රධානියා මෙම කමිටුවේ සභාපතිවරයා විය යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

4.1.5 පරිශීලකයන්ගේ වගකීම් පිළිබඳ ප්‍රතිපත්තිය

තොරතුරු ආරක්‍ෂණය ආයතනයේ සෑම කෙනෙකුගේම පොදු වගකීමකි. සියලුම තොරතුරු තාක්‍ෂණ පරිශීලකයින් ඔවුන්ට ප්‍රවේශයට අවසර ඇති තොරතුරු සහ තොරතුරු තාක්‍ෂණ වත්කම් ආරක්‍ෂා කිරීම සම්බන්ධයෙන් වන ආයතනික ප්‍රතිපත්තියකට අනුගතව වගකීමෙන් ක්‍රියාකළ යුතු වේ.

පරිශීලක වගකීම්වලට තොරතුරු, පරිගණක මෙවලම්, ඊමේල්, අන්තර්ජාලය, සමාජ මාධ්‍ය, දුරකථන සහ ෆැක්ස් නිසි ලෙස භාවිත කිරීම ඇතුළත් වන අතර, තොරතුරු හා සයිබර් ආරක්‍ෂණ මාර්ගෝපදේශයේ දක්වා ඇති පරිශීලක වගකීම්, සහ මෙම ප්‍රතිපත්තියේ දක්වා ඇති තොරතුරු සහ සයිබර් ආරක්‍ෂණ භාවිතයන් මනාව තේරුම් ගෙන පිළිපැදිය යුතුය.

එවැනි වත්කම් අවභාවිතයන් සඳහා ආයතන සංග්‍රහයේ දක්වා ඇති විනය ක්‍රියාමාර්ගවලට සහ පරිගණක අපරාධ පනතේ හෝ වෙනත් අදාළ පනත්වල ඇති නීතිමය ප්‍රතිපාදන යටතේ කටයුතු කරනු ලැබිය හැකිය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.



4.1.6 ධාරිතා සංවර්ධනය පිළිබඳ ප්‍රතිපත්තිය

තොරතුරු ආරක්‍ෂණය සම්බන්ධයෙන් වගකිව යුතු සහ වගවිය යුතු නිලධාරීන්ගේ (උදා: තොරතුරු ආරක්‍ෂණ නිලධාරී, ප්‍රධාන නව්‍යකරණ නිලධාරී, අභ්‍යන්තර විගණක නිලධාරී, වත්කම් හිමිකරුවන්, පරිශීලකයන්) තොරතුරු ආරක්‍ෂණය පිළිබඳ ධාරිතා සංවර්ධනය කිරීම සඳහා ආයතනය විසින් නිසි පියවර ගත යුතුය. ඒ අනුව අදාළ නිලධාරීන්ට අවශ්‍ය තොරතුරු ආරක්‍ෂණ දැනුම හා කුසලතා ගොඩනැගීම සඳහා අවශ්‍ය පුහුණුවීම්, අධ්‍යාපනය සහ දැනුවත් කිරීම් නිසි ක්‍රමවේදයකට අනුව සිදු කළ යුතු අතර එවැනි වැඩසටහන් ආයතනයේ වාර්ෂික පුහුණු සැලැස්මට ඇතුළත් කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.7 කාර්ය මණ්ඩලය සඳහා ආරක්‍ෂක නිෂ්කාශන පරීක්ෂාව පිළිබඳ ප්‍රතිපත්තිය

ඉතා රහසිගත හෝ රහසිගත ලෙස වර්ගීකරණය කර ඇති තොරතුරු සමග කටයුතු කරන හෝ තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම්වලට ප්‍රවේශ වන යම් තනතුරකට පත් කරන ලද හෝ ස්ථාන මාරුවක් ලද ඕනෑම අයෙකු එම තනතුර සඳහා පත් කිරීමට හෝ ස්ථාන මාරු කිරීමට පෙර ආරක්‍ෂක නිෂ්කාශන පරීක්ෂාවකට සහ පසුබිම් පරීක්ෂාවකට ලක් කළ යුතු අතර ඔවුන්ගේ සේවා කාලය තුළ ද වරින් වර ආරක්‍ෂක නිශ්කාශන පරීක්ෂණවලට ලක් කළ යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

4.1.8 උපායමාර්ගික පෙළගැස්වීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය, සිය තොරතුරු ආරක්ෂක ක්‍රියාකාරකම්, එහි ආයතනික දැක්ම, මෙහෙවර සහ අරමුණු සමඟ පෙළ ගැස්විය යුතුය. ආයතනය තුළ ක්‍රියාත්මක කරන සියලුම තොරතුරු ආරක්ෂක උපාය මාර්ග, ව්‍යාපෘති සහ ක්‍රියාකාරකම් සැලසුම් කළ යුත්තේ ඒවා ආයතනයේ දැක්ම, මෙහෙවර සහ අරමුණුවලට අනුකූල වන ආකාරයට ය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.9 ක්‍රියාකාරී සැලසුම් සහ ප්‍රතිපාදන පිළිබඳ ප්‍රතිපත්තිය

ආයතනික දැක්ම, මෙහෙවර සහ අරමුණු සාක්ෂාත් කර ගැනීමේදී ආයතනයේ තොරතුරු තාක්ෂණ ආරක්ෂාව සහතික කළ යුතු ආකාරය විදහා දැක්වෙන තොරතුරු ආරක්ෂක ක්‍රියාකාරී සැලසුම් (දිගු කාලීන, මධ්‍ය කාලීන හා කෙටි කාලීන සැලසුම්) ආයතනය විසින් සකස් කර ක්‍රියාත්මක කළ යුතුය. එම සැලසුම් අවදානම් තක්සේරුවකින් තීරණය කරනු ලබන තොරතුරු ආරක්ෂණ ප්‍රමුඛතා මත පදනම්ව සකස් කළ යුතු අතර ඒවා ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය ප්‍රතිපාදන ද වෙන් කරගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.1.10 ප්‍රතිපත්ති අනුකූලතාවය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය මෙම ලේඛනයේ විස්තර කර ඇති තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුකූල විය යුතුය. මෙහි අංක 4.1.1 සහ 4.1.2 (අ) හි සඳහන් කර ඇති පරිදි, මෙම ප්‍රතිපත්තියට අනුකූලව ආයතනය කටයුතු කිරීමේ පූර්ණ වගකීම ආයතන ප්‍රධානී සහ තොරතුරු ආරක්ෂණ නිලධාරී විසින් දැරිය යුතුය.



ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුකූල වීමේ කාර්ය සාධන මට්ටම තක්සේරු කිරීම සඳහා වාර්ෂිකව තොරතුරු ආරක්ෂණ සූදානම තක්සේරු කිරීමේ පරීක්ෂණයක් ශ්‍රී ලංකා සර්ව ආයතනය විසින් සිදු කළ යුතු අතර, එම තක්සේරු පරීක්ෂණය සිදුකිරීම සඳහා පහසුකම් ආයතනය විසින් සැලසිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.2 වත්කම්, හිමිකරුවන්, පරිශීලකයන් සහ අවදානම් හඳුනා ගැනීම

ආයතනික වත්කම් සඳහා වන තොරතුරු ආරක්ෂණ අවදානම් ඵලදායී ලෙස කළමනාකරණය කිරීම සඳහා ආයතන ඔවුන් ක්‍රියාත්මක වන ව්‍යවස්ථාපිත පිළිබඳව මනා අවබෝධයක් ඇති කර ගත යුතු වේ. ඒ අනුව ආයතනයට වටිනාකමක් ඇති වත්කම් (තොරතුරු, පද්ධති ඇතුළු තොරතුරු තාක්ෂණ උපාංග), ඒවායේ හිමිකරුවන්, භාරකරුවන් සහ පරිශීලකයන්, එම වත්කම් ආරක්ෂා කිරීම සඳහා ඔවුන්ගේ වගකීම්, සහ එම වත්කම් සඳහා වන තොරතුරු සහ සයිබර් ආරක්ෂණ අවදානම් ආයතනය විසින් නිවැරදිව හඳුනා ගත යුතුය. මේ පිළිබඳව ආයතනය අනුගත විය යුතු ප්‍රතිපත්තින් පහත දැක්වේ.



4.2.1 තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් හඳුනාගැනීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය එහි සියළුම වැදගත් තොරතුරු වත්කම් (information assets) නිවැරදිව හඳුනා ගත යුතුය. තොරතුරු වත්කමක් යනු එහි ආයතනික කාර්යයන් ඉටු කිරීමේදී ආයතනයට වැදගත් සහ වටිනා ඕනෑම තොරතුරකි. තොරතුරු වත්කම් සඳහා උදාහරණ ලෙස වෙළඳ රහස්, ටෙන්ඩර් ලියකියවිලි, විදේශ ගමන් බලපත්‍රයක අඩංගු තොරතුරු, අයවැය පත්‍රිකා සහ සේවකයන්ගේ පෞද්ගලික වාර්තා ඇතුළත් වේ. තොරතුරු වත්කම්, කඩදාසි ලේඛනයක්, ඉලෙක්ට්‍රොනික මාධ්‍යයෙන් ඇති ලේඛනයක්, ඩිජිටල් දත්ත ගබඩාවක්, මුරපදයක් හෝ සංකේතාංක යතුරක් (encryption key) හෝ වෙනත් ඕනෑම ඩිජිටල් ලිපිගොනුවක් වැනි විවිධ ස්වරූපවලින් පැවතිය හැකිය.

තවද ආයතනය එහි සියළුම වැදගත් තොරතුරු තාක්ෂණ වත්කම් ද (IT assets) නිවැරදිව හඳුනා ගත යුතුය. තොරතුරු තාක්ෂණ වත්කම් යනු තොරතුරු තාක්ෂණ පරිසරයක් තුළ ඇති මෘදුකාංග (උදා: මෙහෙයුම් පද්ධති, වැටුප් ගෙවීමේ පද්ධති, වෙනත් මෘදුකාංග) දෘඩාංග (උදා: පරිගණක, දෘඩ තැටි, සර්වර් පරිගණක රවුටර, ගිනිපවුරු) ජාල සහ වෙනත් ඩිජිටල් යටිතල පහසුකම් යනාදිය වේ. වත්කම් (තොරතුරු හා තොරතුරු තාක්ෂණ) හඳුනා ගැනීම සිදු කළ යුත්තේ, එම වත්කම් අනවසර ප්‍රවේශයන්, හාවිතයන්, හෙළිදරව් කිරීම්, බාධා කිරීම්, වෙනස් කිරීම් හෝ විනාශ කිරීම් වැනි ක්‍රියාකාරකම්වලින් ආරක්ෂා කර ඒවායේ රහස්‍යභාවය, විශ්වාසනීයභාවය සහ උපයෝජ්‍යතාවය සුරැකීමේ අරමුණෙනි.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.2.2 තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් හඳුනා ගැනීම පිළිබඳ ප්‍රතිපත්තිය

තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් යනු බිඳ වැටීමකදී හෝ අසාද්‍රව්‍ය විමකදී ජාතික ආරක්ෂාව, පාලනය, ආර්ථිකය, සෞඛ්‍ය සහ සමාජ යහපැවැත්ම කෙරෙහි සෘණාත්මක බලපෑමක් ඇති කරන තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් වේ. තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් පවත්වාගෙන යන ආයතන මෙම ප්‍රතිපත්තියේ නිශ්චිතව දක්වා ඇති ආකාරයෙන් එවන් වත්කම් ආරක්ෂා කිරීමට සුදුසු පියවර ගත යුතුය. තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් හඳුනා ගැනීම ශ්‍රී ලංකා සර්ව ආයතනය විසින් සිදු කළ යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.



4.2.3 වත්කම් හිමිකරුවන්, භාරකරුවන් සහ පරිශීලකයන්ගේ වගකීම් පිළිබඳ ප්‍රතිපත්තිය

ආයතනය වත්කම් හිමිකරුවන්, පරිශීලකයන් සහ භාරකරුවන් හඳුනා ගත යුතුය. වත්කම් හිමිකරු යනු, වත්කමක මුළු ජීවන චක්‍රයම පාලනය කිරීමේ වගකීම දරන සහ වත්කමක ආරක්ෂාව පිළිබඳව වගකියන ඉහළ මට්ටමේ විධායක ශ්‍රේණියේ නිලධාරියෙකු හෝ ආයතනයක් වේ. වත්කම් හිමිකරු වත්කම් වලට ඇති අවදානම හඳුනා ගත යුතු අතර වත්කම් ආරක්ෂා කිරීම සඳහා සුදුසු ක්‍රමවේද යෝජනා කළ යුතුය. වත්කමක් ආයතනය තුළ නිල වශයෙන් නිර්මාණය කිරීමේදී, අත්පත් කර ගැනීමේදී හෝ වෙනත් ආයතනයකට මාරු කිරීමේදී වත්කම් හිමිකරු වෙත නිල වශයෙන් අයිතිය පැවරීම අත්‍යවශ්‍ය වේ.

වත්කම් භාරකරු යනු වත්කම් ආරක්ෂා කිරීම සම්බන්ධයෙන් වත්කම් හිමිකරු විසින් අනුමත කරන ලද සුදුසු ආරක්ෂණ ක්‍රමවේද ක්‍රියාත්මක කිරීම සඳහා වගකියනු ලබන නිලධාරියෙකු හෝ ආයතනයක් වේ.

වත්කම් සඳහා වත්කම් ලේඛනයක් සෑදීම, වත්කම් වර්ගීකරණය සහ ආරක්ෂණය, වත්කම් සඳහා ප්‍රවේශ සීමා හඳුන්වා දීම, හෝ වත්කමක් නිල වශයෙන් ඉවත් කිරීමේදී හෝ විනාශ කිරීමකදී එය නිසි පරිදි සිදු වන්නේදැයි සහතික කිරීම වත්කම හිමිකරුගේ සහ භාරකරුගේ වගකීම වේ.

ආයතනය සිය වත්කම් භාවිතා කරන පරිශීලකයන් ද හඳුනා ගත යුතු වේ. පරිශීලකයන් යනු රාජකාරීමය කටයුතු සඳහා වත්කම් භාවිතා කරන කාර්ය මණ්ඩලය වේ. වත්කම් හිමිකරුවන් විසින්, තමන් භාරයේ පවතින වත්කම් රාජකාරීමය අවශ්‍යතා සඳහා භාවිතා කළ යුතු පරිශීලකයන් නිවැරදිව හඳුනා ගත යුතු අතර එම වත්කම් සඳහා වන ප්‍රවේශයන් මෙහි අංක 4.3.4 සහ 4.3.5 හි දක්වා ඇති ආකාරයට පාලනය කළ යුතු වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.2.4 තොරතුරු වත්කම් සහ තොරතුරු තාක්ෂණ වත්කම් පවත්වා ගැනීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය විසින් තොරතුරු වත්කම් හඳුනාගෙන තොරතුරු වත්කම් ලේඛනයක (Information Assets Register) සටහන් කළ යුතුය. තොරතුරු වත්කම් ලේඛනය යනු ආයතනයක් සතු තොරතුරු වත්කම් පිළිබඳ විධිමත් ඉන්වෙන්ට්‍රියකි. ආයතනයක් අවම වශයෙන් තොරතුරු වත්කම් ලේඛනයේ, වත්කමේ නම, වත්කමේ හිමිකරු සහ භාරකරු, වර්ගීකරණයේ මට්ටම, වර්ගීකරණයට හේතුව, වර්ගීකරණ දිනය, වත්කම් සකසන පරිගණක පද්ධතිය, වත්කම් ගබඩා කරන ස්ථානය, විනාශ කිරීමේ ක්‍රමය, වත්කම නැති වීමකදී විනාශ වීමකදී හෝ හෙළිදරව් වීමකදී ඇතිවන බලපෑම සහ වත්කමේ වර්ගීකරණය සමාලෝචනය කිරීමේ දිනය සටහන් කළ යුතුය.



ආයතනය සිය තොරතුරු තාක්ෂණ වත්කම් පිළිබඳ විස්තර ද තොරතුරු තාක්ෂණ ලේඛනයක (IT Assets Register) සටහන් කළ යුතුය. අවම වශයෙන් තොරතුරු තාක්ෂණ වත්කම් ලේඛනයේ වත්කම් වර්ගය (උදා: දෘඩාංග, මෘදුකාංග, සර්වර් පරිගණක), වත්කම පිහිටා ඇති ස්ථානය, එහි මෙහෙයුම් පද්ධතිය, බලපත්‍ර විස්තර, පරිශීලකයන්, අවදානම් වර්ගීකරණ මට්ටම, ඇස්තමේන්තුගත වටිනාකම යනාදී තොරතුරු සඳහන් කළ යුතුය. තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් ලේඛනය නිවැරදි සහ යාවත්කාලීන විය යුතු අතර ඒවා ආයතනයේ අනෙකුත් භාණ්ඩ හා තොග සමග ගැලපිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.2.5 අවදානම තක්සේරු කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ වත්කම්වලට ඇති අවදානම් සහ එමගින් වන බලපෑම තීරණය කිරීම සඳහා විධිමත් තක්සේරුවක් සිදු කළ යුතුය. අවදානම් තක්සේරුවක පරමාර්ථය වනුයේ වත්කම් සඳහා ඇති අවදානම් හඳුනා ගැනීමත් එම අවදානම් අවම කිරීම සඳහා ගත යුතු ආරක්‍ෂක පියවරයන් මොනවාද යන්න තීරණය කිරීමත් ය. අවදානම් තක්සේරුව මත පදනම්ව ආයතනය තුළ අවදානම් ශ්‍රේණි ගත කළ යුතු අතර එම අවදානම් ලේඛනයක (Risk Register) විධිමත්ව සටහන් කළ යුතුය.

ආයතනය විසින් අංක 4.3 හි සඳහන් ප්‍රතිපත්තිමය කරුණු සැලකිල්ලට ගනිමින් අවදානම් ලේඛනයේ සටහන් කර ඇති අවදානම් සඳහා සුදුසු ආරක්‍ෂක පියවර ගත යුතුය. අවදානම් තක්සේරුව ආයතනයේ අවදානම් කළමනාකරණ කමිටුව විසින් සිදු කළ යුතුය. එවන් අවදානම් තක්සේරුවක් සිදුකිරීම සඳහා ආයතනය තුළ සුදුසු හැකියාවක් නොමැති අවස්ථාවක, සුදුසුකම් ලත් පළපුරුදු සමාගමක සේවය ලබාගත හැකිය. මේ සඳහා ශ්‍රී ලංකා සර්ව ආයතනය අදාළ ආයතනයට අවශ්‍ය සහයෝගය ලබාදිය යුතුය.

අනුකූලතාව: සියලුම තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

4.2.6 වත්කම් වර්ගීකරණය කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය වත්කම් වර්ගීකරණය කළ යුතුය. වත්කම් වර්ගීකරණයේ පරමාර්ථය වනුයේ ආයතනයට එම වත්කමේ ඇති වටිනාකමට සහ එහි සංවේදීතාවයට අනුව සුදුසු මට්ටමේ ආරක්‍ෂාවක් ලැබෙන බව සහතික කිරීමයි.

තොරතුරු වත්කම් සහ තොරතුරු තාක්ෂණ වත්කම් වර්ගීකරණය පිළිගත් මාර්ගෝපදේශවලට අනුව සිදු කළ යුතු අතර තොරතුරු වත්කම් වර්ගීකරණය “ඉතා රහසිගත” (Secret), “රහසිගත” (Confidential), “සීමිත හුවමාරුව, (Limited Sharing), “පොදු” (Public) සහ “වර්ගීකරණය නොකළ” (Unclassified) ලෙස වර්ග කළ යුතුය.

තොරතුරු තාක්ෂණ වත්කම් “ඉතා තීරණාත්මක තොරතුරු තාක්ෂණ වත්කම්” (Very Critical), “තීරණාත්මක තොරතුරු තාක්ෂණ වත්කම්” (Critical), “තීරණාත්මක නොවන තොරතුරු තාක්ෂණ වත්කම්” (Non-Critical) සහ “වර්ගීකරණය නොකළ තොරතුරු තාක්ෂණ වත්කම්” (Unclassified) ලෙස මට්ටම් හතරකට වර්ග කළ යුතුය.

වත්කම් වර්ගීකරණය පිළිබඳ ක්‍රමවේදයක් තොරතුරු සහ සයිබර් ආරක්‍ෂණ මාර්ගෝපදේශයෙහි දක්වා ඇත. (මෙහි අංක 2.2 (ඇ) හි දක්වා ඇති යොමුව හා බැඳේ).

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3 වත්කම් ආරක්‍ෂා කිරීම



හඳුනාගත් වත්කම් සඳහා ඇති විය හැකි තොරතුරු ආරක්‍ෂණ සිදුවීමක බලපෑම වැළැක්වීම හෝ සීමා කිරීම සඳහා සුදුසු ආරක්‍ෂණ ක්‍රමවේද ආයතනය විසින් ක්‍රියාත්මක කළ යුතුය. එසේ යොදනු ලබන ක්‍රමවේදයන්, එක් එක් වත්කමට අදාළ වර්ගීකරණය මත පදනම් විය යුතුය. මෙම ප්‍රතිපත්තියට අනුකූලව කටයුතු කිරීම සඳහා ආයතනය විසින් වත්කම් වෙත සිදුවන ප්‍රවේශයන් පාලනය කිරීම, දත්ත සුරක්‍ෂිත කිරීම සඳහා සුදුසු ක්‍රමවේද භාවිතා කිරීම, සංවරණය වන හා නිශ්චල දත්තවල ආරක්‍ෂණය සඳහා වන ප්‍රමිතීන්ට අනුගත වීම, වලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතා කිරීම, සයිබර් ආරක්‍ෂණ සිදුවීම්වලට ඔරොත්තුදීමේ හැකියාව සහතික කිරීම සඳහා අවශ්‍ය වෙනත් තාක්‍ෂණික ක්‍රමවේද භාවිතා කිරීම ඇතුළත් ක්‍රියාකාරකම් සිදුකළ යුතුය. වත්කම් ආරක්‍ෂා කරගැනීම සම්බන්ධයෙන් ආයතනය අනුගත විය යුතු ප්‍රතිපත්ති පහත දැක්වේ.

4.3.1 නිශ්චලව පවතින දත්ත ආරක්‍ෂා කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය ඔවුන් සතුව ඇති නිශ්චලව පවතින දත්ත (තොරතුරු වත්කම්) ආරක්‍ෂා කිරීමට කටයුතු කළ යුතුය. නිශ්චලව පවතින දත්ත යනු උපාංගයෙන් උපාංගයට හෝ ජාලයකින් ජාලයකට ක්‍රියාකාරීව සංවරණය නොවන නිශ්චලව පවතින දත්ත වේ. උදාහරණ ලෙස පරිගණකයක, මේසයක, දෘඩ තැටියක ගබඩා කර ඇති දත්ත නිශ්චල දත්ත ලෙස දැක්විය හැකිය.

ආයතනයක් තුළ ඇති “ඉතා රහසිගත” හෝ “රහසිගත” ලෙස වර්ගීකරණය කර ඇති ඕනෑම තොරතුරු වත්කමක් ගබඩා කිරීමට පෙර කේතනය (encrypt) කිරීම අත්‍යවශ්‍ය වේ. තවද නිශ්චලව පවතින දත්ත ආරක්‍ෂා කිරීමේ වෙනත් ක්‍රම අතරට අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලන ක්‍රමවේද හරහා පරිශීලක ප්‍රවේශය පාලනය කිරීම සහ වත්කම් සඳහා භෞතික ආරක්‍ෂාව සැපයීම ඇතුළු මෙම ප්‍රතිපත්තියේ දක්වා ඇති අනෙකුත් අදාළ ක්‍රමවේද ද ඇතුළත් වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.2 සංවරණය වෙමින් පවතින දත්ත ආරක්‍ෂා කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය විසින් ඔවුන් සතු සංවරණය වන දත්ත ආරක්‍ෂා කිරීමට කටයුතු කළ යුතුය. සංවරණය වන දත්ත යනු අන්තර්ජාලය හරහා හෝ වෙනත් ජාලයක් හරහා එක් ස්ථානයක සිට තවත් ස්ථානයකට සක්‍රීයව ගමන් කරන දත්ත වේ. උදාහරණ ලෙස එක් ස්ථානයක සිට තවත් ආයතනයක් තුළ ඇති “ඉතා රහසිගත” හෝ “රහසිගත” ලෙස වර්ගීකරණය කර ඇති ඕනෑම තොරතුරු වත්කමක් ගබඩා කිරීමට පෙර කේතනය (encrypt) කිරීම අත්‍යවශ්‍ය වේ. තවද නිශ්චලව පවතින දත්ත ආරක්‍ෂා කිරීමේ වෙනත් ක්‍රම අතරට අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලන ක්‍රමවේද හරහා පරිශීලක ප්‍රවේශය පාලනය කිරීම සහ වත්කම් සඳහා භෞතික ආරක්‍ෂාව සැපයීම ඇතුළු මෙම ප්‍රතිපත්තියේ දක්වා ඇති අනෙකුත් අදාළ ක්‍රමවේද ද ඇතුළත් වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.3 භෞතික ආරක්‍ෂාව පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සතු වත්කම්වලට සිදුවන අනවසර ප්‍රවේශයන්, සොරා ගැනීම් හෝ වෙනත් අනවසර අත්පත් කර ගැනීම් වැළැක්වීම සඳහා ආයතනය විසින් එම වත්කම් සඳහා අවශ්‍ය භෞතික ආරක්‍ෂාව සැපයිය යුතුය.

තොරතුරු වත්කම්වල ආරක්‍ෂණ අවශ්‍යතා මත පදනම්ව, වත්කම් ගබඩා කිරීම හෝ ඒවා සැකසීම (store or process) සඳහා ආරක්‍ෂිත ස්ථාන හඳුන්වා දිය යුතුය. “ඉතා රහසිගත” සහ “රහසිගත” ලෙස වර්ගීකරණය කර ඇති තොරතුරු වත්කම් ආරක්‍ෂිත ස්ථානවල ගබඩා කිරීම හෝ සැකසීම අනිවාර්ය වේ.

තවද (ඉතා) තීරණාත්මක ලෙස වර්ගීකරණය කරන ලද තොරතුරු තාක්‍ෂණ වත්කම් ආරක්‍ෂිත ස්ථානවල ගබඩා කර ක්‍රියාත්මක කළ යුතුය.

භෞතික වශයෙන් වන ආක්‍රමණයන් සහ අනවසර ප්‍රවේශයන් වැළැක්වීම සඳහා ආයතනයේ ආරක්‍ෂිත ස්ථානයන් බිත්ති වැනි භෞතික ආවරණයන් (පවුරු), අගුලු දැමිය හැකි දොරවල් සහ ආරක්‍ෂිත උපක්‍රම කිහිපයකින් සමන්විත බහු-සාධක ප්‍රවේශ පද්ධති (multi-factor entry systems) මගින් ආරක්‍ෂා කළ යුතු අතර, අඛණ්ඩව ආරක්‍ෂිත කැමරා මගින් ද නිරීක්‍ෂණය කළ යුතුය.

ආයතනයේ ආරක්ෂිත ස්ථානයන්ට ගිනිගැනීම්, ජලගැලීම්, ආර්ථිකවය, විද්‍යුත් චුම්භක ක්ෂේත්‍ර සහ උෂ්ණත්ව වෙනස්වීම් වලින් වන හානි වැළැක්වීම සඳහා අවශ්‍ය ක්‍රියාමාර්ග ගත යුතුය. තවද, තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් වෙත වන පරිශීලක ප්‍රවේශයන් පාලනය කිරීම සඳහා මුරපද, ප්‍රවේශ කාඩ්පත්, රහස් අංක සහ ජෛවමිතික ක්‍රමවේද වැනි තාක්ෂණයන් ආයතනය විසින් භාවිතා කළ යුතුය.



ආයතනයේ තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් වෙත අනවසර ප්‍රවේශයන් ක්‍රමවත්ව පාලනය කිරීම සඳහා අනන්‍යතා කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයක් ක්‍රියාත්මක කිරීම ද අත්‍යවශ්‍ය වේ. (ප්‍රතිපත්ති අංක 4.3.4 හි සඳහන් පරිදි.)

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.4 අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය, සිය තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට ඇති පරිශීලක ප්‍රවේශ පාලනය කළ යුතු වේ.

අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලනය යනු ආයතනයේ තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සුරක්ෂිතව තබා ගැනීමට එම වත්කම් භාවිතා කරන්නන්ගේ අනන්‍යතාවය තහවුරු කර ඒවා ඔවුන්ට භාවිතා කිරීමට ඇති අවශ්‍යතාවය මත ප්‍රවේශ වීමේ අවසරය ලබාදීමේ ක්‍රියාවලියකි.

පරිශීලකයින්ට ඔවුන්ට නියමිත කාර්යයන් ඉටු කිරීමට දැනගත යුතු තොරතුරු සහ භාවිතා කළ යුතු වත්කම් සඳහා පමණක් අවශ්‍ය ප්‍රවේශ අවසරය ලබා දිය යුතුය. මෙම කරුණු පදනම් කරගනිමින්, ආයතනය විසින් සිය භාවිතය පිණිස අනන්‍යතා කළමනාකරණ ක්‍රමවේදයක් නිර්මාණය කර ගත යුතු වේ. ශ්‍රී ලංකා සර්ව ආයතනය විසින් රාජ්‍ය ආයතන සඳහා අනන්‍යතා කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයක් සකස් කර ඇති අතර එය ආයතනයේ අවශ්‍යතාවය පරිදි ගලපා භාවිතයට ගත හැකිය.

ආයතනය විසින් ක්‍රියාත්මක කරන අන්‍යෝන්‍ය කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයෙහි ප්‍රමාණවත් බවත්, යාවත්කාලීන බවත් ආයතනය සහතික කළ යුතු අතර එවැනි ක්‍රමවේදයක් ආයතනය තුළ ක්‍රියාත්මක වන අවස්ථාවන්හිදී සියලුම ආයතන සේවකයින්ට අමතරව තෙවන පාර්ශවීය සේවා සැපයුම්කරුවන් ද එම අන්‍යෝන්‍ය කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයට අනුගතව කටයුතු කරන බවට ආයතනය සහතික විය යුතුය.

අන්‍යෝන්‍ය කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදය උල්ලංඝනය කිරීමකදී අවශ්‍ය පියවර ගැනීම සඳහා තොරතුරු ආරක්‍ෂණ කමිටුව වෙත වාර්තා කළ යුතු අතර ආයතනය තුළ තොරතුරු ආරක්‍ෂණ කමිටුවක් පිහිටුවා නොමැති අවස්ථාවකදී එම සිදුවීම ආයතනයේ තොරතුරු ආරක්‍ෂණ නිලධාරියා මගින් ආයතන ප්‍රධානී වෙත වාර්තා කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.



4.3.5 ශක්තිමත් සත්‍යාපනය පිළිබඳ ප්‍රතිපත්තිය

සත්‍යාපනය යනු පරිශීලකයෙකුගේ අන්‍යෝන්‍යතාවය හඳුනා ගැනීමේ ක්‍රියාවලියයි. සත්‍යාපන ක්‍රියාවලියේදී පරිශීලකයා හඳුනාගැනීම (අන්‍යෝන්‍යතාවය හඳුනා ගැනීම) සහ සාක්‍ෂි මගින් පරිශීලකයා තහවුරු කරගැනීම (අන්‍යෝන්‍යතාවය සත්‍යාපනය කිරීම) තුළින් ආයතනයේ තොරතුරු සහ තොරතුරු තාක්‍ෂණ වත්කම් වෙත ප්‍රවේශය සපයනු ලැබේ.

ප්‍රතිපත්ති අංක 4.3.4 හි සඳහන් ආයතනික අන්‍යෝන්‍ය කළමනාකරණය සහ ප්‍රවේශ පාලන ක්‍රමවේදයට අනුකූලව, පරිශීලකයෙකුගේ අන්‍යෝන්‍යතාවය තහවුරු කිරීම සඳහා ආයතනය ශක්තිමත් සත්‍යාපනයක් භාවිතා කළ යුතුය.



පරිශීලක නාමය සහ මුරපද සංයෝජනය සහ බහු සාධක සත්‍යාපනය (multi-factor authentication) භාවිතා කිරීම වැනි ශක්තිමත් ක්‍රමවේද පරිශීලක අන්‍යෝන්‍යතාවය සත්‍යාපනය කිරීම සඳහා නිර්දේශ කෙරේ.

ශක්තිමත් සත්‍යාපන ක්‍රියාවලියක් සහතික කිරීම සඳහා ආයතනය, සිය අන්‍යෝන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලන ක්‍රමවේදය සැකසීමේදී ශක්තිමත් මුරපද භාවිතය සහ බහු සාධක සත්‍යාපනය පිළිබඳ පහත සඳහන් කරුණු ද ආවරණය කළ යුතුය.

(අ) ශක්තිමත් මුරපද:

- මුරපද අවම වශයෙන් අක්ෂර 8 කින් සමන්විත විය යුතු අතර එය ඉංග්‍රීසි හෝ චීනයේ කැපිටල් සහ සිම්පල් අකුරු (උදා: a - Z) ඉලක්කම් (0-9) සහ විශේෂ අක්ෂරවලින් (! @ \$+/) සමන්විත විය යුතුය.
- සාමාන්‍ය පරිශීලකයන්ගේ සියලුම මුරපද දින 90 කට වරක් වෙනස්කළ යුතුය. වරප්‍රසාද සහිත පරිශීලකයන් සඳහා (privileged users) ප්‍රවේශ ලබා දිය යුත්තේ අවශ්‍යතා පදනම මත පමණි.

(ආ) බහු සාධක සත්‍යාපනය:

- “ඉතා රහසිගත” සහ “රහසිගත” තොරතුරු වෙත ප්‍රවේශය ඇති පරිශීලක ගිණුම් සුරැකි කිරීම සඳහා ආයතනය බහු සාධක සත්‍යාපන ප්‍රවේශය ක්‍රියාත්මක කළ යුතුය.
- බහු සාධක සත්‍යාපන ක්‍රමයක් සැලසුම් කිරීමේදී, ආයතනය අවම වශයෙන් පරිශීලකයා දන්නා යම් කරුණක් (උදා: පරිශීලක මුරපදය), පරිශීලකයා සන්නකයේ ඇති යමක් (උදා: ටෝකනය, ප්‍රවේශ කාඩ්පත) හෝ ජීවමිතික දත්තයක් (උදා: ඇඟිලි සලකුණ) යන සංයෝජන සැලකිල්ලට ගත යුතුය.

කුමන හේතුවක් මත හෝ ආයතනය හැර යන සේවකයෙකු, තවදුරටත් ආයතනික වත්කම් වෙත ප්‍රවේශ වීම වැළැක්වීම සඳහා එම සේවකයාට ලබා දී ඇති ගිණුම් සහ වෙනත් සත්‍යාපන දත්ත ආයතනය විසින් වහාම ඉවත් කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.6 දත්ත ස්වෛරීභාවය සහ මේසගත පරිගණක භාවිතය පිළිබඳ ප්‍රතිපත්තිය

දත්ත ස්වෛරීභාවය (data sovereignty) දත්ත (තොරතුරු වත්කම්) එක්රැස් කිරීම, සැකසීම සහ ගබඩා කිරීම සිදු කරනු ලබන රට තුළ පවතින නීති සහ පාලන ව්‍යුහයන්ට එම ක්‍රියාවන් නෛතිකව බැඳී පවතින බවයි. මෙම සන්දර්භය තුළ රාජ්‍ය ආයතනය, දත්ත එක්රැස් කිරීම, සැකසීම සහ ගබඩා කිරීම සඳහා වෙනත් රටවලින් මේසගත සේවා (cloud services) ලබා ගන්නා විට එම දත්තවල ස්වෛරීභාවය ගැන අනිශ්චිත සැලකිලිමත් විය යුතුය.

මේසගත පරිගණක භාවිතය යනු පරිශීලකයන්ගේ සෘජු කළමනාකරණයකින් තොරව ඉල්ලුම මත දත්ත ගබඩා කිරීම, සැකසීම, යෙදවුම් සංවර්ධන වේදිකා (development platforms) වැනි තොරතුරු සහ සන්නිවේදන තාක්ෂණ සම්පත් ලබා ගැනීමේ හැකියාවයි. වර්තමානයේ බොහෝ ආයතන පිරිවැය ඉතිරිකිරීම් සහ කාර්ය සාධනය වැඩිකිරීමේ අරමුණින් මේසගත සේවා ලබාගැනීමට යොමු වේ.

නමුත්, දත්ත ස්වෛරීභාවය තහවුරු කිරීම සඳහා මේසගත සේවා භාවිතා කිරීමේ අවදානම පිළිබඳව ආයතනය ප්‍රවේශම් විය යුතු අතර, විශේෂයෙන් පොදු මේසගත සේවා (public cloud services) භාවිතා කිරීමේ අවදානම පිළිබඳව වඩාත් සැලකිලිමත් විය යුතු වේ. පොදු මේසගත සේවා යනු, ඒවා මිලදී ගැනීමට කැමති ඕනෑම කෙනෙකුට ලබාගත හැකි සේවාවන් ය. මේසගත සේවා විවිධ රටවල නීතිවලට යටත්ව ක්‍රියාත්මක වන බැවින් ඒවා පාලනය කිරීමේ ඇති දුෂ්කරතා, එහි නිර්මාණාත්මක ව්‍යුහයේ ඇති සීමිත පාරදෘශ්‍යභාවය, මෙහෙයුම් ක්‍රියාවලිවල ඇති සීමිත විනිවිදභාවය සහ සේවා ගිවිසුම්වල ඇති සැලකිය යුතු නොගැලපීම් මේසගත සේවාවන් ලබාගැනීමේදී ඇති අවදානම් වේ.

මේසගත සේවා අවශ්‍යතා සඳහා ආයතන, ශ්‍රී ලංකා රාජ්‍ය මේසය (Lanka Government Cloud) මගින් සේවාවන් ලබා ගැනීමට ප්‍රමුඛතාවය ලබා දිය යුතුය. ශ්‍රී ලංකා රාජ්‍ය මේසය යනු රජයේ මේසගත සේවා අවශ්‍යතා සපුරාලීම සඳහා පිහිටුවන ලද, තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය යටතේ ක්‍රියාත්මක වන, රජය සතු රාජ්‍ය ආයතන සඳහා පමණක් සීමා වූ මේසගත සේවාවකි. කෙසේවෙතත්, ආයතනය විසින් ඕනෑම ආකාරයක මේසගත සේවාවක් ලබා ගැනීමට පෙර නිසි අවදානම් තක්සේරුවක් අනිවාර්යයෙන්ම සිදු කළ යුතු වේ.

තවද, ආයතනයේ දත්ත රැස් කිරීම, ගබඩා කිරීම සහ සැකසීම හෝ මෘදුකාංග සඳහා සන්කාරකත්වය ලබාගැනීම ආදී සියලුම ක්‍රියාකාරකම් ශ්‍රී ලංකාවේ දත්ත ආරක්ෂණයට අදාළව පවතින නීති සහ රෙගුලාසිවලට අනුකූලව සිදු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.



4.3.7 වලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතය සහ සර්මා යාවත්කාලීන කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය වලංගු බලපත්‍ර සහිත සහ නිසි පරිදි යාවත්කාලීන කරන ලද මෘදුකාංග භාවිතා කළ යුතුය. මෙයට පද්ධති මෘදුකාංග, උපයෝගීතා වැඩසටහන් සහ යෙදුම් මෘදුකාංග ආදිය ඇතුළත්ය. උදාහරණ ලෙස මෙහෙයුම් පද්ධති, වචන සැකසුම් පැකේජ, දත්ත ගබඩා, වෙබ් බ්‍රවුසර්, ප්‍රති-අනිෂ්ට මෘදුකාංග යනාදිය වලංගු බලපත්‍රයන් සහිතව භාවිතා කළ යුතු අතර ඒවායේ සර්මා (patch updates) යාවත්කාලීන කිරීම ද නිසි පරිදි සිදු කළයුතුය.

ආයතනය විසින් මෙහෙයුම් පද්ධති සහ අනෙකුත් අදාළ මෘදුකාංග සපයන්නන් විසින් සපයන ලද නවතම සර්මා මගින් යාවත්කාලීන කළ යුතුය. තවද, ආයතන සිය මෘදුකාංගයන්හි ස්වයංක්‍රීය යාවත්කාලීන කිරීම් සක්‍රීය කළ යුතුය.



තවද සැපයුම්කරු විසින් සපයන ලද තීරණාත්මක සර්මා ස්ථාපනය කිරීමට පෙර ඒවා ස්ථාපනය කිරීමෙන් ඇතිවිය හැකි බලපෑම පිළිබඳ නිසි ඇගයීමක් සිදු කළ යුතුය. (විශේෂයෙන්ම ඉතා තීරණාත්මක හෝ තීරණාත්මක ලෙස වර්ගීකරණය කර ඇති තොරතුරු තාක්ෂණ වත්කම් සඳහා).

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.8 ප්‍රති-අනිෂ්ට මෘදුකාංග භාවිතය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය වලංගු බලපත්‍රයක් සහිත ප්‍රති-අනිෂ්ට මෘදුකාංග ස්ථාපනය කළ යුතුය. ප්‍රති-අනිෂ්ට මෘදුකාංග ඕනෑම තොරතුරු තාක්ෂණ වත්කමකට ප්‍රවේශ වීමේ හැකියාවක් අති ස්ථානවල (උදා: පරිගණක හා ඒවා ආශ්‍රිත මෙවලම්, අන්තර්ජාලයට නිරාවරණය වන මුහුණත් සහිත තොරතුරු තාක්ෂණ මෙවලම් ආදිය) සක්‍රීයව පැවතිය යුතුය. තවද එම ප්‍රති-අනිෂ්ට මෘදුකාංග යාවත්කාලීන විය යුතු අතර ඒවා ස්වයංක්‍රීයව යාවත්කාලීන වන ලෙස වින්‍යාස ගත (configure) කළ යුතුය.

වෙබ් අඩවි වෙත පිවිසීමේදී, ඩිජිටල් ලිපිගොනු බාගත කිරීම හෝ විවෘත කිරීමේදී, ඉවත් කළ හැකි දත්ත ගබඩාකරන මෙවලම් (removable storage devices) භාවිතයේදී ඒවා ස්වයංක්‍රීයව පරිලෝකනය (scan) කර අනිෂ්ට මෘදුකාංග හඳුනාගැනීමට හැකි වන පරිදි ප්‍රති-අනිෂ්ට මෘදුකාංග වින්‍යාස ගත කළ යුතුය.

ප්‍රති-අනිෂ්ට මෘදුකාංගවල වින්‍යාසය වෙනස් කිරීම, අස්ථාපනය කිරීම, අක්‍රීය කිරීම හෝ වෙනත් ආකාරයකින් විකෘති කිරීම පරිශීලකයින්ට තහනම් කළ යුතුය.

රාජ්‍ය ආයතනයක් තවත් ආයතනයකට හෝ මහජනතාව වෙත ඉලෙක්ට්‍රොනික මාධ්‍යයෙන් තොරතුරු සන්නිවේදනයේදී ඒවා අනිෂ්ට මෘදුකාංගවලින් තොර බව සහතික කර ගැනීමෙන් අනතුරුව එම සන්නිවේදනයන් සිදු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.9 නිල විද්‍යුත් තැපැල් පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සිය නිල සන්නිවේදන කටයුතු සඳහා නිල විද්‍යුත් තැපැල් ලිපින පමණක් භාවිතා කළ යුතුය. සේවකයින් සිය පෞද්ගලික සන්නිවේදන කටයුතු සඳහා නිල ඊමේල් ලිපින භාවිතා නොකළ යුතුය.

නිල විද්‍යුත් තැපැල් යනු "gov.lk" වසම් නාමය යටතේ රජය විසින් සපයන ලද විද්‍යුත් තැපැල් ලිපින වේ. නිල විද්‍යුත් තැපැල් ගිණුම් ආයතනය සතු නිල වත්කමක් වන අතර ඕනෑම අවස්ථාවක එම ගිණුම්වලට ප්‍රවේශ වීමට විද්‍යුත් තැපැල් කියවීමට හෝ ගිණුම් ඉවත් කිරීමට ආයතනයට අයිතිය ඇත්තේය.

සියලුම විද්‍යුත් තැපැල් ඇමුණුම්, එහි මූලාශ්‍රය හෝ අන්තර්ගතය කුමක් වුවත්, ආයතනයේ පරිගණකයක හෝ පද්ධතියක විවෘත කිරීමට හෝ ගබඩා කිරීමට පෙර වෛරස සහ වෙනත් අනිෂ්ට මෘදුකාංග තිබේදැයි පරිලෝකනය කර බැලිය යුතුය. තවද ආයතන සිය නිල විද්‍යුත් තැපැල් සම්බන්ධයෙන් රජය විසින් කලින් කලට නිකුත් කරනු ලබන රෙගුලාසි සහ මාර්ගෝපදේශයන්ට අනුකූලව කටයුතු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.10 විද්‍යුත් තැපැලෙහි ආරක්‍ෂාව පිළිබඳ ප්‍රතිපත්තිය

ආයතනයක් ඔවුන්ගේ විද්‍යුත් තැපැල් ගිණුම්වලට අදාළ ආරක්‍ෂක විශේෂාංග ඇතුළත් කොට වින්‍යාස ගත කළ යුතුය. තොරතුරුවල ආරක්‍ෂාව සහතික කිරීම සඳහා, විද්‍යුත් තැපැල් සේවාදායක පරිගණකය (email server) දත්ත ආරක්‍ෂණය සම්බන්ධයෙන් වන නීතිමය විධිවිධානවලට අනුගතව ස්ථාපනය කළ යුතුය.

ආයතනය, විද්‍යුත් තැපැල් පෙරහන් (email filters) සක්‍රීය කිරීම මගින් අනිෂ්ට මෘදුකාංග ඇතුළුකොට ඇති විද්‍යුත් තැපැල් ඉවත්කිරීමද, අයාවිත විද්‍යුත් ලිපි (spam emails) ලැබීම අවම කිරීමට ද ක්‍රියාමාර්ග ගත යුතුය. තවද විද්‍යුත් තැපැල් හරහා සංවේදී තොරතුරු යැවීමේදී ඒවා අනිවාර්යයෙන්ම කේතනය කර යැවිය යුතුය.

ආයතනයේ විද්‍යුත් තැපැල් ගිණුම් ලංකා රාජ්‍ය ජාලය විසින් සපයනු ලබන අවස්ථාවන්හිදී, එම විද්‍යුත් තැපැල් සේවාව ආරක්‍ෂිතව වින්‍යාස කර ඇති බව ශ්‍රී ලංකා තොරතුරු තාක්‍ෂණ නියෝජිතායතනය සහතික විය යුතු අතර, අධීක්‍ෂණ හෝ නියාමන අවශ්‍යතා සඳහා වරින් වර ආරක්‍ෂක විගණන වාර්තා ශ්‍රී ලංකා සර්වි ආයතනයෙන් ලබා ගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.11 ඩිජිටල් අත්සන් භාවිතය පිළිබඳ ප්‍රතිපත්තිය

සුදුසු අවස්ථාවලදී, ආයතනය විසින් ඩිජිටල් අත්සන් ක්‍රියාත්මක කළ යුතුය. එමගින්, විද්‍යුත් තැපැල්වල නිරවද්‍යතාවය, තර්ථතාවය (authenticity), සහ යථා ලබන පුද්ගලයා විසින්ම අදාළ විද්‍යුත් තැපෑල යවන ලද බව තහවුරු කළ හැකි බව සහතික කළ හැකිය. (non-repudiation).

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.12 පරිමිති ආරක්‍ෂණ පාලනයන් පිළිබඳ ප්‍රතිපත්තිය

අනිෂ්ට මෘදුකාංග අන්තර්ජාලය හරහා ආයතනයේ තොරතුරු හා තොරතුරු තාක්‍ෂණ වත්කම්වලට ප්‍රවේශ වීම වැළැක්වීමට සහ අනෙකුත් සයිබර් ප්‍රහාරවලින් එම වත්කම්වලට ආරක්‍ෂාව සැපයීමට ආයතනය විසින් ගිනිපවුරු සහ ආක්‍රමණ හඳුනාගැනීමේ හා ආක්‍රමණ වැළැක්වීමේ පද්ධති (Intrusion Detection Systems/ Intrusion Prevention Systems) වැනි පරිමිති ආරක්‍ෂණ ක්‍රමවේද (perimeter security methods) ස්ථාපනය කළ යුතුය.

ආයතනය විසින් ස්ථාපනය කර ඇති පරිමිති ආරක්‍ෂණ උපාංගවල තර්ජන පිළිබඳ විස්තර ඇතුළත් වන දත්ත ගබඩා (threat databases) නීතිපතා යාවත්කාලීන කිරීම, ප්‍රති-අනිෂ්ට මෘදුකාංග ස්ථාපනය කර ඒවා ස්වයංක්‍රීයව යාවත්කාලීන වීමට සැකසීම, සුදුසු ආරක්‍ෂක වින්‍යාසයන් යොදාගනිමින් පෙරනිමි සැකසුම් (default settings) යාවත්කාලීන කිරීම, සහ සැපයුම්කරු විසින් නිර්මාණය කරන ලද පරිශීලක ගිණුම් (vendor supplied user accounts) අක්‍රිය කිරීම යනාදී කටයුතු සිදු කළ යුතුය. පරිමිති ආරක්‍ෂණ මෙවලම් සඳහා සුදුසු ආරක්‍ෂක වින්‍යාස පිළිබඳ විශ්ලේෂණයක් තොරතුරු සහ සයිබර් ආරක්‍ෂණ මාර්ගෝපදේශයේ දක්වා ඇත.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.



4.3.13 ආරක්ෂිත දුරස්ථ ප්‍රවේශ භාවිතය පිළිබඳ ප්‍රතිපත්තිය

වෙනත් ස්ථානවල සිට (භූගෝලීය වශයෙන් දුරස්ථ ස්ථාන) ආයතනයේ තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම්වලට වන අනවසර ප්‍රවේශයන් වැළැක්විය යුතුය. ඒ සඳහා දුරස්ථ ක්‍රම භරණා ආයතනයේ අභ්‍යන්තර ජාල වෙත සිදු කෙරෙන ප්‍රවේශ පාලනය කළ යුතුය. දුරස්ථ ප්‍රවේශ ක්‍රම භරණා ආයතනය වෙත බොහෝ තොරතුරු ආරක්ෂණ තර්ජන පැමිණේ. දුරස්ථ ප්‍රවේශය හා සම්බන්ධ ආරක්ෂක අවදානම් ලෙස අන්තර්ජාලය භරණා තොරතුරු සංවරණයේදී අනවසරයෙන් එම දත්ත නිරාවරණය කිරීම, දත්ත වෙත අනවසරයෙන් ප්‍රවේශ වීම, අනවසරයෙන් දත්ත වෙනස් කිරීම සහ වෙනත් අනිෂ්ට මෘදුකාංග ආයතනයේ පද්ධතියට ඇතුළු වී හානි සිදු කිරීම ආදිය දැක්විය හැකිය.

දුරස්ථ ප්‍රවේශයන් නිසා ආයතනයට ඇති වන අවදානම් අවම කිරීම සඳහා, ආයතනය විසින් ආරක්ෂිත තත්‍වයේ පෞද්ගලික ජාල (Virtual Private Networks) භාවිතා කිරීම, ආයතනයේ අනන්‍යතා කළමනාකරණය සහ ප්‍රවේශ පාලන ප්‍රතිපත්තිය මත පදනම්ව ආයතනික පද්ධති වෙත ප්‍රවේශ වීමට බලයලත් පරිශීලකයින්ට පමණක් ඉඩ සැලසීම, බහු සාධක සත්‍යාපනය ක්‍රියාත්මක කිරීම සහ විශ්වාසදායී ජාල පමණක් භාවිතා කිරීම ආදී ක්‍රියාමාර්ග ගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.14 උපස්ථ උපාය මාර්ග පිළිබඳ ප්‍රතිපත්තිය

ආපදා අවස්ථාවකදී බිඳ වැටුණු හෝ අඩපණ වූ ආයතනයේ එදිනෙදා ක්‍රියාකාරකම් ප්‍රතිස්ථාපනය කිරීම සඳහා අවශ්‍ය දත්ත, ලොග් සටහන්, පද්ධති, මෘදුකාංග, වින්‍යාස විස්තර (configuration details) සහ වෙනත් ඕනෑම තොරතුරක් උපස්ථ කිරීම (backup) සඳහා ආයතනය සතුව ක්‍රමවේදයක් තිබිය යුතුය. මෙම උපායමාර්ගය ආයතනයේ ආපදා ප්‍රතිසාදන සැලැස්මට (Disaster Recovery Plan) අනුකූල විය යුතුය. (ආක 4.6.1 හි සඳහන් පරිදි) ආයතනය විසින් තම උපස්ථ භාවිත කොට ආයතනයේ අඩපණ වූ හෝ බිඳ වැටුණු සේවා නිසි පරිදි ක්‍රියාත්මක කළ හැකි බව අනිවාර්යයෙන්ම තහවුරු කර ගත යුතුය.



උපස්ථ මාධ්‍යයන්හි ගබඩා කර ඇති දත්ත රජයේ නියාමන අවශ්‍යතාවය මත සංරක්ෂණය කළ යුතුය. උපස්ථ කළ යුතු කාල පරාසය තීරණය කිරීම සඳහා ආයතනය විසින් ප්‍රතිසාධන කාල අරමුණ සහ ප්‍රතිසාධන ලක්ෂ්‍ය අරමුණ (Recovery Time Objective and Recovery Point Objective) ද හඳුන්වා දිය යුතුය.

රැන්සම්වෙයා ඇතුළු ඕනෑම ද්වේශසහගත සයිබර් ප්‍රහාරයකින් සජීවී දත්ත ආරක්ෂා කිරීම සඳහා එම සජීවී දත්ත ඊට අදාළ උපස්ථ දත්ත වලින් සම්පූර්ණයෙන්ම වෙන් කොට තිබිය යුතුය.

තවද උපස්ථගත කරන ලද දත්ත හා තොරතුරු එහි දත්ත සැකසුම් ස්ථානයෙන් දුරස්ථ ආරක්ෂිත ස්ථානයක ගබඩා කළ යුතුය. උපස්ථකරණය සඳහා සිදු කරන ලද ඕනෑම වෙනස්කමක් හඳුනා ගැනීමට හැකි වන ක්‍රමවේදයක් ද තිබිය යුතුය.

“ඉතා රහසිගත” සහ “රහසිගත” ලෙස වර්ගීකරණය කර ඇති තොරතුරු වත්කම්වල උපස්ථ, වත්කම් ලේඛනයේ දක්වා ඇති ආරක්ෂක අවශ්‍යතාවයන්ට අනුගතව ගබඩා කළ යුතුය.

4.3.15 රාජ්‍ය ආයතන විසින් සපයන තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වල ආරක්ෂාව පිළිබඳ ප්‍රතිපත්තිය

වර්තමානයේ මහජනතාව සහ බොහෝ රාජ්‍ය සහ රාජ්‍ය නොවන ආයතන රජය විසින් සපයන තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් (ඩිජිටල් යටිතල පහසුකම්, ඉ-සේවා, යෙදවුම්) මත පදනම්ව කටයුතු කරනු දැකිය හැකිය. එවන් පසුබිමක් තුළ, ශ්‍රී ලංකා තොරතුරු සන්නිවේදන තාක්ෂණ නියෝජිතායතනය හෝ වෙනත් රාජ්‍ය ආයතන විසින් නිර්මාණය කරන ලද යෙදවුම් හෝ ඩිජිටල් යටිතල පහසුකම්වල ආරක්ෂාව, ඒවායේ විශ්වාසනීයභාවය, අඛණ්ඩතාවය සහ නිරවද්‍යතාවය සහතික කළ යුතු වේ. උදාහරණ ලෙස, ලංකා රාජ්‍ය ජාලය (Lanka Government Network), ලංකා රාජ්‍ය මේසය, විද්‍යුත් තැපැල් සේවා, ලංකා රාජ්‍ය ගෙවීම් පද්ධතිය (Lanka Government Payment System), කෙටි පණිවුඩ සේවාව, ලේඛන කළමනාකරණ පද්ධති හෝ වෙනත් සේවාවන්වල ආරක්ෂාව අදාළ ආයතනය විසින් සහතික කළ යුතුය. මේ සඳහා අවශ්‍ය ආරක්ෂණ සහතිකයන් අදාළ ආයතනය විසින් ශ්‍රී ලංකා සර්ටි ආයතනයෙන් හෝ වෙනත් සුදුසුකම් ඇති ආයතනයකින් ලබාගත යුතුය.

අනුකූලතාව: තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය සහ සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.16 ආරක්ෂාව තහවුරු කරගත් මෘදුකාංග සංවර්ධනය සහ භාවිතය පිළිබඳ ප්‍රතිපත්තිය

ආයතනයක්, අලුතින් මෘදුකාංග මිලදී ගැනීමේදී හෝ ආයතනය තුළම සිය මෘදුකාංග සංවර්ධනය කිරීමේදී ආරක්ෂාව අනුබද්ධ කරගත් මෘදුකාංග සංවර්ධන ක්‍රමවේදයක් අනුගමනය කළ යුතුය. මෙම ක්‍රමවේදය අනුගමනය කිරීමේදී සම්ප්‍රදායික මෘදුකාංග සංවර්ධන ක්‍රමවේදයට වඩා ඉදිරි පියවරක් ගනිමින් මෘදුකාංගයක සංවර්ධන ජීවන චක්‍රයේ සෑම අදියරකටම තොරතුරු හා සයිබර් ආරක්ෂක කරුණු එක් කිරීම සිදු කරනු ලබයි.

මෘදුකාංග සංවර්ධනය කිරීමේදී (හෝ මෘදුකාංග මිලදී ගැනීමේදී), ආයතනය විසින් ව්‍යාපෘතිය සැලසුම් කිරීමේ (planning) අදියරේ සිටම මෘදුකාංගයේ ආරක්‍ෂාව සැලසුම් කිරීමත්, අවදානම් තක්සේරු කිරීමත්, ලංසු ලේඛනවල ආරක්‍ෂක අවශ්‍යතා පිළිබඳව පැහැදිලිව සඳහන් කිරීමත් සිදු කළ යුතුය. නිර්මාණකරණ (designing) අදියරේදී සංවර්ධනය කළ යුතු මෘදුකාංගයේ යෝජිත ආරක්‍ෂක නිර්මාණාත්මක ව්‍යුහය සමාලෝචනය කිරීම ද, සංවර්ධනය කරන (development) අදියරේදී ආරක්‍ෂාව සම්බන්ධයෙන් වන දුර්වලතා (දෝෂ) හඳුනා ගැනීම සඳහා කේතය සමාලෝචනය කිරීමත් කළ යුතුය.

එකී මෘදුකාංගය ක්‍රියාත්මක කිරීමේ (implementation) අදියරේදී එහි වෙනත් ආරක්‍ෂක දුර්වලතා හඳුනා ගැනීම සඳහා ආරක්‍ෂණ විගණනයක් සිදු කිරීමත් කළ යුතුය. අවසාන වශයෙන්, පද්ධතිය ආයතනයෙන් ඉවත් කිරීමේ (decommissioning) අදියරේදී අනවසර පුද්ගලයින්ට එහි දත්ත සහ අනෙකුත් තොරතුරු වත්කම් වෙත ප්‍රවේශ වීමට හෝ නැවත එම දත්ත ප්‍රතිසාධනය කිරීමට නොහැකිවන සේ පද්ධති (හෝ මෘදුකාංග) ආරක්‍ෂිතව බැහැර කළ යුතුය.

තවද ආයතනය වෙබ් අඩවි සහ වෙබ් අඩවි යෙදවුම් සංවර්ධනය කිරීමේදී, ශ්‍රී ලංකා සර්ව ආයතනය විසින් රාජ්‍ය ආයතන වෙත නිකුත් කර ඇති “වෙබ් අඩවි ආරක්‍ෂණ මාර්ගෝපදේශය” “වෙබ් යෙදවුම් ආරක්‍ෂණ මාර්ගෝපදේශය” සහ තාක්‍ෂණික කරුණු අඩංගු “වෙබ් යෙදවුම් ආරක්‍ෂාව සඳහා වන තාක්‍ෂණික මාර්ගෝපදේශය” පිළිපැදිය යුතුය. මෙම මාර්ගෝපදේශයන් ශ්‍රී ලංකා සර්ව ආයතනයේ <https://www.onlinesafety.lk> වෙබ් අඩවියෙන් බාගත කළ හැකිය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.17 වත්කම් සුරක්ෂිතව බැහැර කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයක්, සිය වත්කමක් තවදුරටත් අවශ්‍ය නොවන විටකදී විධිමත් ක්‍රියාපටිපාටියක් අනුගමනය කරමින් එම වත්කම් ආරක්‍ෂිතව බැහැර කළ යුතුය. ආයතනය සිය දත්ත ගබඩා මාධ්‍යයන් වන ප්‍රකාශ මාධ්‍ය (ඩිස්ක්), චුම්බක මාධ්‍ය (ටේප් හෝ ඩිස්කට්), තැටි ධාවක, ෆ්ලෑෂ් ගබඩා උපාංග සහ ලේඛන (කඩදාසි ලේඛන හෝ ඡායාරූප මාධ්‍ය) යනාදිය ආරක්‍ෂිතව බැහැර කිරීමට කටයුතු කළ යුතුය.



අදාළ ගබඩා මාධ්‍යයේ තවදුරටත් අවශ්‍ය නොවන තොරතුරු තිබේ නම්, එම තොරතුරු ලබා ගැනීම හෝ ප්‍රතිස්ථාපනය වැලැක්වීම සඳහා, ඒවා නැවත ලබාගත නොහැකි ආකාරයෙන් ඉවත් කළ යුතුය. අවම වශයෙන් දත්ත ගබඩා මාධ්‍යයේ අංශ පදනම් කරගත් ආකෘතිකරණය කර (sector-based formatting) මාධ්‍යවල ඇති තොරතුරු විනාශ කළ යුතුය.

ගබඩා මාධ්‍යයේ ඇති වත්කම් “ඉතා රහසිගත” හෝ “රහසිගත” ලෙස වර්ගීකරණය කර ඇත්නම්, ඒ සඳහා තොරතුරු ආරක්‍ෂණ කමිටුව වෙතින් ලබාගත් නිර්දේශ මත බැහැර කිරීමේ ක්‍රියාවලිය ආරම්භ කළ යුතුය.

තවද, දත්ත ගබඩා මාධ්‍ය කොටස්වලට කපා දැමීමෙන් හෝ සිදුරු කිරීමෙන් තොරතුරු වත්කම් අඩංගු මාධ්‍ය ස්ථිරවම පාරිසරික ආරක්‍ෂණ නීති සහ රෙගුලාසිවලට යටත්ව භෞතික වශයෙන් විනාශ කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.18 අභ්‍යන්තර තොරතුරු හා සයිබර් ආරක්‍ෂණ විගණන ක්‍රියාවලිය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය විසින් තොරතුරු ආරක්‍ෂණ විගණන වැඩසටහන් ක්‍රියාත්මක කළ යුතු අතර එම විගණනයන් සඳහා, ආයතනය තුළ ස්ථාපනය කර ඇති විවිධ තොරතුරු ආරක්‍ෂණ ක්‍රමවේදවල ප්‍රමාණාත්මකභාවය, පරිගණක යෙදවුම්වල පවතින ආරක්‍ෂණ ක්‍රියාමාර්ගයන්, පරිගණක ජාලයන්හි නිර්මාණාත්මක ව්‍යුහයේ ඇති ආරක්‍ෂාව, ආයතනයේ තොරතුරු ආරක්‍ෂක අනුකූලතා, අභ්‍යන්තර සහ බාහිර තොරතුරු ආරක්‍ෂණ දුර්වලතා ආදිය පිළිබඳ වන ඇගයීම් (Vulnerability Assessments) සහ සමාලෝචනයන් ද සැබෑ සයිබර් ප්‍රහාර කෘතීමව ඇති කරමින් ආයතනයේ තොරතුරු ආරක්‍ෂණ සුදානම ඇගයීම සඳහා සිදු කරනු ලබන විනිවිදයාමේ පරීක්‍ෂණයන් (Penetration Tests) ද ඇතුළත් විය යුතුය.

තවද ආයතනයට අදාළ තොරතුරු ආරක්‍ෂණ සිදුවීමකින් පසු, තොරතුරු හෝ තොරතුරු තාක්‍ෂණ වත්කම්වලට සිදු කරනු ලැබූ යම් වෙනසකින් පසු, ආයතනය අනුගත විය යුතු සම්මත මාර්ගෝපදේශයන්ට සිදුවන වෙනස් වීමකින් පසු, වෛරස් හෝ අනිෂ්ට මෘදුකාංග පැතිරීමකින් පසු හෝ තොරතුරු ආරක්‍ෂණ කමිටුව විසින් නිර්දේශ කරනු ලබන අවස්ථාවකදී තොරතුරු ආරක්‍ෂණ විගණනයන් සිදු කළ යුතුය. ඉහත කරුණු වලින් ස්වායක්තව, ආයතනයේ තොරතුරු ආරක්‍ෂණ විගණනයන් අවම වශයෙන් වසරකට වරක් හෝ සිදු කිරීම අනිවාර්ය වේ.

ආයතනයේ (ප්‍රධාන) අභ්‍යන්තර විගණක විසින් ඉහත විගණනයන් සම්බන්ධීකරණය කළ යුතු අතර, එක් එක් අමාත්‍යාංශයේ ප්‍රධාන අභ්‍යන්තර විගණක එහි විෂය පථය යටතේ ඇති ආයතනවල තොරතුරු ආරක්‍ෂණ විගණනයන් සම්බන්ධීකරණය කළ යුතුය.

විගණන වාර්තා මගින් ඉදිරිපත් කරන ලද නිර්දේශ ක්‍රියාත්මක වීම අධීක්‍ෂණය කිරීම සඳහා ආයතනය විසින් විධිමත් ක්‍රියාවලියක් ස්ථාපිත කිරීම කළ යුතුය. ඒ සඳහා ආයතනයේ (ප්‍රධාන) විගණක නිලධාරී මූලිකත්වය සහ වගකීම ගෙන කටයුතු කළ යුතුය.

තොරතුරු ආරක්‍ෂණ විගණනයන් ඒ සඳහා සුදුසුකම් ලත් පාර්ශ්වයක් විසින් හෝ ශ්‍රී ලංකා සර්ටි ආයතනය විසින් සිදු කළ යුතුය. වෙනත් පාර්ශ්වයක් විසින් එම විගණනයන් සිදු කරන්නේ නම්, එහි රහස්‍යභාවය තහවුරු කිරීම සඳහා හෙළිදරව් නොකිරීමේ ගිවිසුමක් අදාළ පාර්ශ්වය සමඟ ඇති කර ගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.19 භාවිතය ආරම්භ කිරීමට පෙර සිදු කරන විගණන පිළිබඳ ප්‍රතිපත්තිය

අභ්‍යන්තර තොරතුරු ආරක්‍ෂණ විගණන වැඩසටහනට සමගාමීව, ආයතනය ඕනෑම වෙබ් අඩවියක්, වෙබ් යෙදුමක් හෝ පද්ධතියක් නිල වශයෙන් දියත් කිරීමට පෙර අවදානම් තක්සේරු කිරීම් සහ විනිවිද යාමේ පරීක්‍ෂණ (Vulnerability Assessments and Penetration Tests) සිදු කළ යුතුය.

එම තොරතුරු ආරක්‍ෂණ විගණනයන් සඳහා ශ්‍රී ලංකා සර්ටි ආයතනයෙහි සේවාව හෝ ශ්‍රී ලංකා සර්ටි ආයතනයේ අනුදැනුම මත තෝරාගනු ලැබූ සුදුසුකම් ලත් වෙනත් පාර්ශ්වයකගේ සහාය ලබා ගැනීම අවශ්‍ය වේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.20 තොරතුරු තාක්‍ෂණ වත්කම්වල ආරක්‍ෂණ ප්‍රතිරෝධය ශක්තිමත් කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සිය තොරතුරු තාක්‍ෂණ වත්කම්වල ආරක්‍ෂාව දැඩි කිරීමට ඒවා ශක්තිමත් කළ යුතුය. (hardening). මෙහෙයුම් පද්ධති, පරිගණක, පරිගණක ජාල සහ ජාල උපාංග, දත්ත ගබඩා සහ තත්‍යසම පෞද්ගලික ජාල යනාදී තොරතුරු තාක්‍ෂණ වත්කම්වල ආරක්‍ෂණ සැකසුම් සක්‍රීය කොට, ඒවායේ ඇති ආරක්‍ෂණ දුර්වලතා සඳහා විසඳුම් ලබා දී, ඇතිවිය හැකි ප්‍රහාර සඳහා වන ප්‍රවේශ මාර්ග අවහිර කොට එම වත්කම් සයිබර් ප්‍රහාරවලට දක්වන ප්‍රතිරෝධය වැඩි කිරීම සිදුකරනු ලබයි. තොරතුරු තාක්‍ෂණ වත්කම් ශක්තිමත් කිරීම සඳහා වන උපදෙස් තොරතුරු සහ සයිබර් ආරක්‍ෂණ මාර්ගෝපදේශයේ දක්වා ඇත.



මෙම තොරතුරු තාක්ෂණ වත්කම් ශක්තිමත් කිරීම සඳහා සුදුසුකම්ලත් පළපුරුදු තොරතුරු ආරක්ෂණ වෘත්තිකයන්ගේ සහාය ලබා ගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.21 නිවසේ සිට රාජකාරි කටයුතුවල නිරතවීම් පිළිබඳ ප්‍රතිපත්තිය

නිවසේ සිට (හෝ දුරස්ථව) තොරතුරු තාක්ෂණය භාවිතා කරමින් රාජකාරි ස්ථානවල තොරතුරු තාක්ෂණ වත්කම්වලට ප්‍රවේශ වීමේදී තොරතුරු ආරක්ෂණ තර්ජනවලට ලක්වීමේ සම්භාවිතාවක් පවතී. එබැවින්, කාර්යමණ්ඩල සේවකයින් දුරස්ථව රාජකාරි කටයුතුවල නියැලීමේදී, දැනටමත් රජය විසින් නිකුත් කර ඇති නිවසේ සිට වැඩකිරීමට සම්බන්ධ විධිවිධානවලට අනුකූලව ශ්‍රී ලංකා සර්ව ආයතනය විසින් නිකුත් කර ඇති “නිවසේ සිට වැඩ කිරීම සඳහා වන තොරතුරු ආරක්ෂණ මාර්ගෝපදේශ” පිළිපැදිය යුතුය.

තවද, තොරතුරු තාක්ෂණ විෂය සම්බන්ධයෙන් කටයුතු කිරීමට අවසරලත් කාර්යමණ්ඩලය ශ්‍රී ලංකා සර්ව ආයතනය විසින් නිකුත් කර ඇති “පද්ධති පරිපාලකයින් සඳහා නිවසේ සිට වැඩ කිරීමේ මාර්ගෝපදේශය” ට අනුව කටයුතු කළ යුතුය. මෙම මාර්ගෝපදේශයන් ශ්‍රී ලංකා සර්ව ආයතනයේ www.onlinesafety.lk වෙබ් අඩවියෙන් බාගත කළ හැකිය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.22 රාජකාරි කටයුතු සඳහා තම පෞද්ගලික මෙවලම් භාවිතය පිළිබඳ ප්‍රතිපත්තිය

ආයතනය සිය සේවකයින්ට නිල රාජකාරි ඉටු කිරීම සඳහා ඔවුන්ගේ පෞද්ගලික ජංගම පරිගණක, ස්මාර්ට් දුරකථන සහ ටැබ්ලට් පරිගණක යනාදී මෙවලම් භාවිතා කිරීමට අවසර ලබා නොදිය යුතුය. කෙසේ වෙතත්, ආයතනයේ තොරතුරු ආරක්ෂණ කමිටුව විසින් තීරණය කරනු ලබන විශේෂිත තත්වයන් යටතේ, තොරතුරු ආරක්ෂණ නිලධාරීගේ අධීක්ෂණය යටතේ නිල රාජකාරි ඉටු කිරීම සඳහා තෝරාගත් සේවකයින්ට ඔවුන්ගේ පුද්ගලික මෙවලම් භාවිතා කිරීමට අවසර දිය හැකිය. එවැනි අවස්ථාවන්හිදී එම මෙවලම් ආයතනය තුළ ක්‍රමවත්ව ලියාපදිංචි කර ඒවා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුගත වන ලෙස ක්‍රියාවේ යෙදවීම අත්‍යවශ්‍ය වේ. එනමුදු, කිසිදු තත්වයක් යටතේ “ඉතා රහසිගත” සහ “රහසිගත” ලෙස වර්ගීකරණය කර ඇති තොරතුරු සැකසීමට හෝ ගබඩා කිරීමට සේවකයින්ගේ පෞද්ගලික මෙවලම් භාවිතා කිරීමට අවසර නොදිය යුතුය.

නිල රාජකාරි ඉටු කිරීම සඳහා සේවකයින්ගේ පෞද්ගලික මෙවලම් භාවිතා කිරීමට අවසර දී ඇතිවිට, ඔවුන්ගේ පරිශීලක ගිණුම් සඳහා සීමිත වරප්‍රසාද ඇති බවටත්, ගිණුම් ශක්තිමත් මුරපද සහ බහු සාධක සත්‍යාපනයෙන් ආරක්ෂා කර ඇති බවටත්, ප්‍රති-අනිෂ්ට මෘදුකාංග ස්ථාපනය කර ඒවායේ ස්වයංක්‍රීය යාවත්කාලීන කිරීම් සක්‍රීය කර ඇති බවටත්, මෙහෙයුම් පද්ධති, උපයෝගිතා මෘදුකාංග සහ භාවිතා කරන අනෙකුත් යෙදුම් මෘදුකාංග වලටද බලපත් සහිත බවට සහ ඒවා යාවත්කාලීන කර ඇති බවටත් ආයතනය සහතික විය යුතුය.



වෝහාරික පරීක්ෂණයක් සිදු වන අවස්ථාවකදී, රාජකාරි කටයුතු සඳහා භාවිත වන පෞද්ගලික උපාංගවල ඇති පුද්ගලික සහ ආයතනික තොරතුරු විමර්ශනය කිරීමට හෝ පරීක්ෂණ කටයුතු සඳහා එම මෙවලම් රඳවා තබා ගැනීමට සහ තීනිමය අවශ්‍යතා මත රාජ්‍ය ආයතන හෝ පාර්ශවයන් වෙත නිකුත් කිරීමට ආයතනයට අයිතිය ඇත.

සිය පෞද්ගලික මෙවලම්වල ආරක්ෂාව මෙවලම් හිමිකරුගේ වගකීමක් විය යුතුය. උපාංගය භාවිතා කිරීම හේතුවෙන් පෞද්ගලික දත්ත නැතිවීම ඇතුළුව මෙවලම්වලට සිදුවන හානියක් හෝ අස්ථානගත වීමක් සඳහා ආයතනය වගකිව යුතු නොවේ.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.23 අන්‍යාරක්ෂිත ජාල භාවිතය පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ කාර්ය මණ්ඩලය සිය රාජකාරි විද්‍යුත් තැපැල් ගිණුම්වලට හෝ අනෙකුත් කාර්යාලීය තොරතුරු තාක්ෂණ මෘදුකාංග වෙත ප්‍රවේශ වීම සඳහා විශ්වාසදායී නොවන සහ අන්‍යාරක්ෂිත වයි-ෆයි ජාල (උදා: ආපනශාලා, හෝටල්, බස් නැවතුම් පොළවල ස්ථාන ගත කර ඇති) හෝ පොදුවේ පරිහරණය කරන පරිගණක, පොදු අන්තර්ජාල සේවා සපයන මධ්‍යස්ථාන සහ වෙනත් එවැනි මෙවලම් භාවිතයෙන් වැළකිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.24 වත්කම් සැපයුම්කරුවන් කළමනාකරණය පිළිබඳ ප්‍රතිපත්තිය

තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සංවර්ධනය කිරීම සහ කළමනාකරණය කිරීම සඳහා බාහිර පාර්ශ්වයන් (දෘඩාංග, මෘදුකාංග, ජාල, සත්කාරක සහ කළමනාකරණ සේවා ආදිය සපයන්නන්) සම්බන්ධ වන විට සුදුසු ආරක්ෂිත පියවර ආයතනය විසින් ගත යුතුය.

සැපයුම්කරුවන් කළමනාකරණය කිරීමේදී, ආයතනය අවම වශයෙන් පහත සඳහන් කරුණු සැලකිල්ලට ගත යුතුය. එනම් (අ) උපස්ථ, ගබඩා කිරීම, ප්‍රතිසාධනය සහ හදිසි විධිවිධාන, ආරක්ෂක විනයාස කිරීම්, තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට ප්‍රවේශවීම ඇතුළු කටයුතු සඳහා ගිවිසුම්ගත පාර්ශ්වයේ වගකීම් සහ බැඳීම් හඳුනා ගැනීම, (ආ) මෙම ප්‍රතිපත්තියේ අඩංගු කරුණු සහ රජය විසින් හඳුන්වා දී ඇති අනෙකුත් තොරතුරු ආරක්ෂණ ප්‍රමිතීන්ට අනුගතව කටයුතු කිරීම, (ඇ) ගිවිසුමට අදාළ පාර්ශ්වවල ක්‍රියාවලීන් සහ පාලනයන් විගණනය කිරීමට ආයතනයට ඇති අයිතිය සහ (ඈ) ගිවිසුම්ගත නියමයන් සහ කොන්දේසිවලට පාර්ශ්වකරුවන් අනුකූල නොවීම් අධීක්ෂණය සහ වාර්තා කිරීම් ආදිය වේ.

ගිවිසුම්ගත පාර්ශ්වයන් සමඟ ගනුදෙනු කළමනාකරණය කිරීමේ වගකීම ආයතන ප්‍රධානියා විසින් තීරණය කරන ලද පරිදි තොරතුරු තාක්ෂණ වත්කමෙහි හිමිකරුවන්ට, වෙනත් නම් කරන ලද නිලධාරියෙකුට හෝ ආයතනයකට පැවරිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.3.25 වෙනස්වීම් කළමනාකරණය පිළිබඳ ප්‍රතිපත්තිය

ආයතන සිය තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම්වලට අදාළ වන සියලු වෙනස්කම් කළමනාකරණය කළ යුතුය. නිසිලෙස කළමනාකරණය නොකරන ලද වෙනස්කම්, ආයතනයේ තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට අවදානම් ඇති කරන අතරම එහි මෙහෙයුම්වලට ද බාධා ඇති කළ හැකිය. උදාහරණ ලෙස, නිසි පාලනයකින් තොරවු ස්ථාපනයන් (හෝ අස්ථාපනය කිරීම්), ඇතුළත් කිරීම්, ඉවත් කිරීම් සහ පද්ධති වෙනස් කිරීම්, තොරතුරුවල රහස්‍යභාවය, නිරවද්‍යතාවය සහ උපයෝජ්‍යතාවය වැනි කරුණු කෙරෙහි සෘණාත්මක වශයෙන් බලපෑම් ඇති කළ හැකිය.

තවද, එවන් වෙනස්කම් තොරතුරු තාක්ෂණ වත්කම්වල ආරක්ෂක දුර්වලතාවයන් ඇති කළ හැකි අතරම, එම වත්කම් අනිසි පුද්ගලයන්ගේ ග්‍රහණයට හසුවීම ද සිදුවිය හැකිය. එබැවින්, තොරතුරු තාක්ෂණ වත්කම් සඳහා වන සමස්ත ආරක්ෂක අවදානම අවම කිරීම සඳහා තොරතුරු ආරක්ෂණ කමිටුව විසින් විධිමත් වෙනස්කම් කළමනාකරණ ක්‍රියාවලියක් ක්‍රියාත්මක කළයුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4' 4 ආරක්‍ෂණයට බලපාන සිදුවීම් හඳුනා ගැනීම.



ආයතනය විසින් තොරතුරු සහ සයිබර් ආරක්‍ෂණ සිදුවීම් ක්‍ෂණිකව හඳුනා ගැනීම සඳහා සුදුසු ක්‍රියාමාර්ග ගත යුතුය. මේ සඳහා කිසියම් තොරතුරු සහ සයිබර් ආරක්‍ෂණ සිදුවීමක්, තොරතුරු තාක්‍ෂණ වත්කම්වල හඳුනා ගන්නා ලද දුර්වලතා පිළිබඳ හෝ තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තීන්ට අදාළ කරුණු කඩ කිරීමක් පිළිබඳව තොරතුරු ආරක්‍ෂණය සම්බන්ධයෙන් කටයුතු කරන නිලධාරීන්ට වාර්තා කරන ලෙස ආයතනය විසින් කාර්ය මණ්ඩලයට උපදෙස් ලබා දිය යුතුය. තවද, ආයතනය, තොරතුරු සහ සයිබර් ආරක්‍ෂණ සිද්ධීන් හඳුනා ගැනීම සඳහා ලොග් සටහන් විශ්ලේෂණය කිරීම සහ වෙනත් තර්ජන හඳුනාගත හැකි අධිකාරී අධීක්‍ෂණ විසඳුම් පද්ධතීන් හඳුන්වාදිය යුතු වේ.

තොරතුරු සහ සයිබර් ආරක්‍ෂණ සිදුවීම් අනාවරණය කර ගැනීම සම්බන්ධයෙන් ආයතනය අනුගත විය යුතු ප්‍රතිපත්තීන් පහත දැක්වේ.

4.4.1 ආරක්‍ෂණ සිදුවීම් වාර්තා කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ තොරතුරු සහ සයිබර් ආරක්‍ෂණය සම්බන්ධයෙන් වන කිසියම් සැක කටයුතු ක්‍රියාකාරකමක් හෝ උල්ලංඝනය කිරීමේ සිදුවීමක් සිදු වූ වහාම එය තොරතුරු ආරක්‍ෂණ නිලධාරී වෙත වාර්තා කරන ලෙස කාර්ය මණ්ඩලයට පැහැදිලිව උපදෙස් දිය යුතුය. මෙබඳු ආරක්‍ෂණ කඩකිරීම්වලට උදාහරණ ලෙස, ආයතනයේ පරිගණක ජාලයට, සන්නිවේදන හෝ පරිගණක පද්ධතිවලට අනවසරයෙන් ප්‍රවේශ වීම, පරිගණක පද්ධතිය තුළ යම් වෛරසයක් හඳුනා ගැනීම, ආයතනය මගින් තහනම් කර ඇති කිසියම් අනවසර මෙවලමක් ආයතනය තුළ හඳුනා ගැනීම, අනවසර පරිශීලකයන් විසින් කිසියම් ලිපි ගොනුවක් විකෘති කිරීම සහ වෙනත් පරිශීලකයෙකු හෝ පාර්ශවකරුවකු විසින් මෙම මාර්ගෝපදේශ හෝ ආරක්‍ෂක ප්‍රතිපත්ති උල්ලංඝනය කිරීම ආදිය හැක්විය හැකිය.

තවද, තොරතුරු තාක්‍ෂණ වත්කම්වල පවතින යම් යම් දුර්වලතා වාර්තා කරන ලෙස ද පරිශීලකයන් දැනුවත් කළ යුතුය.



තොරතුරු ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම, අනාවරණය කරගත් තොරතුරු ආරක්ෂණ සිදුවීම් වාර්තා කිරීම සහ ඊට අදාළ සාක්ෂි සංරක්ෂණය කිරීම සම්බන්ධයෙන් කාර්ය මණ්ඩලය සඳහා ප්‍රමාණවත් දැනුවත් කිරීම් සහ පුහුණුවක් ආයතනය විසින් ලබා දිය යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.4.2 ලොග් සටහන් සමාලෝචනය පිළිබඳ ප්‍රතිපත්තිය.

ආයතනයේ සිදුවන ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම සඳහා එහි පරිගණක පද්ධති සහ ආශ්‍රිත වෙනත් මෙවලම් මගින් ජනනය කරන ලද ලොග් සටහන් (ප්‍රවේශ ලොග් සටහන්, දෝෂ ලොග් සටහන්, සේවාදායක පරිගණක ලොග් සටහන්, විගණන ලොග් සටහන්, ගිනිපවුරු ලොග් සටහන් සහ ප්‍රති-අනිෂ්ට මෘදුකාංග ලොග් සටහන් යනාදිය) ආයතනය විසින් මනාව නඩත්තු කරමින් ඒවා සමාලෝචනය කළ යුතුය.

ආයතනයේ පරිගණක පද්ධති වෙත එල්ලවන ද්වේශසහගත ප්‍රහාර හඳුනා ගැනීමට සහ පද්ධතියේ දෝෂ හෝ ආරක්ෂාව කඩවීම් සඳහා හේතු අනාවරණය කර ගැනීමට ද ආයතනය විසින් ලොග් සටහන් සමාලෝචනය කළ යුතුය.

ලොග් සටහන් විකෘති කිරීම් සහ ඒවා වෙත සිදු කරන අනවසර පිවිසුම්වලින් ආරක්ෂා කළ යුතුය. සංවේදී සහ පෞද්ගලිකව හඳුනාගත හැකි තොරතුරු අඩංගු ලොග් සටහන්, ගබඩා කිරීම සහ විශ්ලේෂණය කිරීමට පෙර ඒවායේ රහස්‍යභාවය ආරක්ෂා කිරීම සඳහා සුදුසු පියවර ගත යුතුය.

ලොග් සටහන්, මාස 12 ක් හෝ තොරතුරු තාක්ෂණ කමිටුව විසින් තීරණය කරනු ලබන කාල සීමාවක් සඳහා පවත්වාගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.4.3 ආරක්‍ෂණයට බලපාන සිදුවීම් අඛණ්ඩව අධීක්‍ෂණය කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනය අනිෂ්ට ක්‍රියාකාරකම් හඳුනාගැනීම සඳහා ජාල, පද්ධති හෝ වෙනත් තොරතුරු තාක්‍ෂණ වත්කම් අධීක්‍ෂණය කළ යුතු අතර, ඒ සඳහා අනවසර ඇතුළුවීම් හඳුනාගැනීමේ පද්ධතියක් සහ අනවසර ඇතුළුවීම් වැළැක්වීමේ පද්ධතියක් (Intrusion Prevention and Detection Systems) ස්ථාපනය කිරීම මගින් එවන් අනිෂ්ට ක්‍රියාකාරකම්වලට එරෙහිව කටයුතු කළ යුතුය.

තවද, ආයතනය සඳහා ආරක්‍ෂක තොරතුරු සහ සිදුවීම් කළමනාකරණ (Security Information and Event Management) පද්ධති හඳුන්වා දීම තුළින් සයිබර් ආරක්‍ෂක අධීක්‍ෂණය සහ තර්ජන හා සිද්ධි හඳුනාගැනීම් සිදු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය තීරණාත්මක තොරතුරු යටිතල පහසුකම් සපයන ආයතන සඳහා අදාළ වේ.

4.4.4 ආරක්‍ෂණයට බලපාන සිදුවීම් ශ්‍රී ලංකා සර්ටි ආයතනය වෙත වාර්තා කිරීම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයේ තොරතුරු ආරක්‍ෂණ කමිටුව විසින් තීරණය කරනු ලබන පරිදි, තීරණාත්මක තොරතුරු ආරක්‍ෂණ සිදුවීම් ශ්‍රී ලංකා සර්ටි ආයතනයට වාර්තා කර ඒවා කළමනාකරණය කිරීම සඳහා අවශ්‍ය උපදෙස් සහ තාක්‍ෂණික සහය ලබාගත යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.5 ආරක්‍ෂණයට බලපාන සිදුවීම්වලට ප්‍රතිචාර දැක්වීම



තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම්වලට වඩා කාර්යක්ෂම ලෙස ප්‍රතිචාර දැක්වීම සඳහා, ආයතනය විසින් ආරක්ෂණ සිද්ධි සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් සකස් කළ යුතු අතර, යම් සිද්ධියකදී එම සැලැස්ම ක්‍රියාත්මක කළ යුතුය. තොරතුරු සහ සයිබර් ආරක්ෂණ සිදුවීම් සඳහා කාර්යක්ෂම ලෙස ප්‍රතිචාර දැක්වීම සම්බන්ධයෙන් ආයතනය අනුගත විය යුතු ප්‍රතිපත්තීන් පහත දැක්වේ.

4.5.1 ආරක්ෂණයට බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සඳහා වන ප්‍රතිපත්තිය

ආයතනයේ වත්කම්වලට එරෙහිව ක්‍රියාත්මක වන තොරතුරු සහ සයිබර් ආරක්ෂණ සිද්ධියක් හඳුනා ගැනීමට, ප්‍රතිචාර දැක්වීමට, එහි අනිටු ප්‍රතිඵල සීමා කිරීමට සහ එම සිදුවීම් නිසා හානියට පත් වන්නම් නැවත ඵලදායී ලෙස යථා තත්වයට පත් කිරීමට අවශ්‍ය උපදෙස් සහ ක්‍රියා පටිපාටියකින් සමන්විත සිදුවීම් සඳහා වන ප්‍රතිචාර සැලැස්මක් (Incidents Response Plan) ආයතනය විසින් සකස් කළ යුතුය.

එම සැලැස්මේ අවම වශයෙන්, සිදුවීම් වාර්තා කිරීමේ ක්‍රියා පටිපාටිය, සිදුවීම් හඳුනාගැනීමේ උපාය මාර්ග, සිදුවීම් විශ්ලේෂණ ක්‍රමවේද සහ එම සිදුවීම්වලින් වන බලපෑම සීමා කිරීමේ ක්‍රමවේද සහ හානි වූ වත්කම් ප්‍රතිසාධනය කිරීමට අවශ්‍ය ක්‍රියාකාරකම් අඩංගු විය යුතුය. තවද, විශේෂයෙන්ම, එම සැලැස්ම ක්‍රියාත්මක කිරීම සඳහා අදාළ කාර්ය මණ්ඩල නිලධාරීන් සතු වගකීම් සහ එම සිදුවීම් පසුපිටරම් කිරීම සඳහා අදාළ ක්‍රමවේද ද ඇතුළත් විය යුතුය.

සිද්ධි ප්‍රතිචාර සැලැස්ම ආයතනය තුළ ක්‍රියාත්මක කර එහි ක්‍රියාකාරීත්වය වරින් වර පරීක්ෂා කළ යුතු අතර එම සැලැස්ම සම්බන්ධයෙන් ආයතනයේ සියලුම කාර්ය මණ්ඩල සාමාජිකයින් දැනුවත් කළ යුතුය.

ආරක්ෂණ සිද්ධි සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් නිර්මාණය කිරීම සඳහා වන ක්‍රමවේදය තොරතුරු සහ සයිබර් ආරක්ෂණ මාර්ගෝපදේශයෙහි ඉදිරිපත් කර ඇත.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.5.2 ආරක්ෂණයට බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සක්‍රීය කිරීම සඳහා වන ප්‍රතිපත්තිය

තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීමක දී, ආයතනික මෙහෙයුම්වලට ඇති බලපෑම අවම කිරීම සහ එම මෙහෙයුම් නැවත යථා තත්වයට පත් කිරීම පිණිස, ආයතනයේ බලයලත් නිලධාරියා විසින් සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සක්‍රීය කළ යුතුය.

ආයතනය විසින් තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් ලේඛනගත කිරීම සඳහා සිදුවීම් පිළිබඳ ලේඛණයක් (Incidents Register) පවත්වාගෙන යා යුතුය. සිදුවීම් ලේඛනයේ අවම වශයෙන් පහත සඳහන් තොරතුරු පවත්වා ගත යුතුය. ඒවා නම්, සිදුවීම වූ දිනය සහ වේලාව, සිදුවීම වාර්තා කළ සේවකයාගේ නම සහ තනතුර, සිදුවීම පිළිබඳ විස්තරය, බලපෑමේ ස්වභාවය, සිදුවීමෙහි වර්ගීකරණය, සිදුවීමට ප්‍රතිචාර වශයෙන් ගන්නා ලද ක්‍රියාමාර්ග, සිදුවීම භාරව කටයුතු කරන නිලධාරියා, සිදුවීමේ වත්මන් තත්වය යනාදිය වේ.

යම් සිදුවීමක් සඳහා ප්‍රතිචාර දැක්වීම සඳහා ආයතනය ගතයුතු ක්‍රියාමාර්ග, තොරතුරු හා සයිබර් ආරක්‍ෂණ මාර්ගෝපදේශයෙහි දක්වා ඇත. ආයතනය විසින් තොරතුරු හා සයිබර් ආරක්‍ෂණ සිදුවීමකදී, විධිමත් වෝභාරික පරීක්‍ෂණයක් සිදු කිරීමට අවශ්‍ය සාක්ෂි ලෙස භාවිතා කළ හැකි තොරතුරු හඳුනා ගැනීම, රැස් කිරීම සහ සංරක්‍ෂණය කිරීම සඳහා සුදුසු ක්‍රමවේදයක් භාවිතා කළ යුතුය. වෝභාරික පරීක්‍ෂණය සිදු කළ යුතු ආකාරය දැක්වෙන ප්‍රතිපත්ති අංක 4.5.3 යටතේ ඉදිරිපත් කර ඇත.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.5.3 වෝභාරික පරීක්‍ෂණ පිළිබඳ ප්‍රතිපත්තිය



වෝභාරික පරීක්‍ෂණයක් ආයතනය තුළ සිදු කිරීමට අවශ්‍ය වූ විට, ඒ සඳහා විධිමත් ක්‍රියාවලියක් අනුගමනය කළ යුතුය. මෙවන් පරීක්‍ෂණ සඳහා අවශ්‍ය සාක්ෂි භෞතික ලේඛන, දෘඩ තැටිවල දත්ත, මෙවලම්, ලොග් සටහන්, ආරක්‍ෂිත කැමරා දර්ශන, විද්‍යුත් තැපැල් පණිවුඩ, හඬපට සහ වෙනත් විද්‍යුත් ලේඛන ආදියෙන් ලබා ගත හැකිය.

ඉලෙක්ට්‍රොනික සාක්ෂි භෞතික ස්වභාවයෙන් නොපැවතීම, පිටපත් කිරීමේ හැකියාව සහ ඒවායේ නෂ්‍යතාවය (volatility) සම්බන්ධයෙන් ගත්විට ඒවා සම්ප්‍රදායික වෝභාරික සාක්ෂිවලට වඩා වෙනස් වන බැවින්, එවැනි සාක්ෂි විශ්ලේෂණය කිරීම සඳහා විශේෂඥ දැනුමක් අත්‍යවශ්‍ය වේ. ආයතනය එවැනි සාක්ෂි විශ්ලේෂණය කිරීම සඳහා ශ්‍රී ලංකා සර්ව ආයතනය හෝ අදාළ තාක්‍ෂණික හැකියාවන් සහිත ආයතනයක් මගින් තාක්‍ෂණික සහාය ලබා ගත යුතුය.

ආයතනය විසින් සිදු කරන වෝහාරික පරීක්ෂණයකදී, සාක්ෂිවල භාරකාර දාමය (chain of custody) පවත්වාගෙන යෑම සඳහා අවම වශයෙන් පහත සඳහන් තොරතුරු ලේඛන ගත කළ යුතුය. ඒවා නම්, සිද්ධිය සහ ඊට අදාළ සාක්ෂි පිළිබඳ විස්තර, සාක්ෂි එකතු කරන ලද දිනය සහ වේලාව, සාක්ෂි ලබාදුන් නිලධාරියාගේ නම සහ තනතුර සහ සාක්ෂි එක් එක් නිලධාරීන්ගේ (හෝ ආයතනවල) භාරකාරීත්වයට පත් වූ අයුරු ආදිය වේ. යම් විමර්ශනයකදී ඉදිරිපත් කළ යුතු භාරකාර දාමය නිසි පරිදි පවත්වාගෙන යාම ආයතනයේ තොරතුරු ආරක්ෂණ නිලධාරීගේ වගකීමක් වේ.

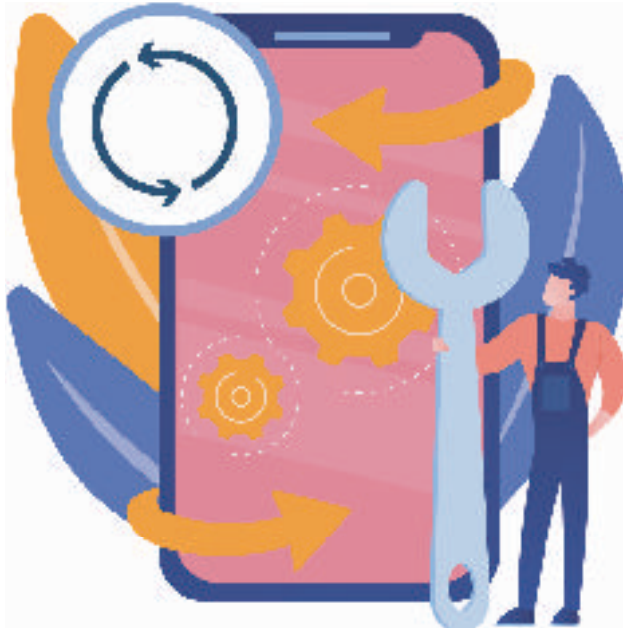
දැනට ගෙන ඇති සහ ඉදිරියට ගැනීමට අපේක්ෂිත ක්‍රියාමාර්ග සම්බන්ධයෙන් අවශ්‍ය විය හැකි සියලු සාක්ෂි රඳවා තබා ගැනීමේ සහ සංරක්ෂණය කිරීමේ වගකීම ආයතනයේ තොරතුරු ආරක්ෂණ නිලධාරී සතු වේ. සාක්ෂි ලෙස භාවිතා කළ හැකි ලේඛන, ඉලෙක්ට්‍රොනික මාධ්‍යයෙන් ඇති තොරතුරු හෝ ඒවා අඩංගු මෙවලම් නැතිවීම, විනාශ කිරීම හෝ වේතනාත්මකව වෙනස් කිරීම ආදියෙන් වැළැක්වීමේ වගකීම් ද මෙයට ඇතුළත් වේ.

වෝහාරික පරීක්ෂණ ක්‍රියාත්මක කිරීමේදී පෞද්ගලික දත්ත ආරක්ෂණය, පරිගණක අපරාධ, ගෙවීම් මෙවලම් වංචා සහ විද්‍යුත් ගණුදෙනු සම්බන්ධව පවතින නීති හෝ වෙනත් අදාළ නීතිමය රාමුවලට යටත්ව සිදු කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.6 මෙහෙයුම් ප්‍රතිසාධනය කිරීම

ආපදාවක් හේතුවෙන් හානියට හෝ බිඳ වැටීමකට ලක් වූ ඕනෑම සේවාවක් ප්‍රතිස්ථාපනය කිරීම සඳහා එලදායි ක්‍රියාකාරී සැලැස්මක් ආයතනය විසින් සකස් කර ක්‍රියාවට නැංවිය යුතුය. තොරතුරු සහ සයිබර් ආරක්‍ෂණ සිදුවීමකින් පසුව ආයතනයේ මෙහෙයුම් යථා තත්වයට පත් කිරීම සම්බන්ධයෙන් ආයතනය අනුගත විය යුතු ප්‍රතිපත්තීන් පහත දැක්වේ.



4.6.1 ආපදා ප්‍රතිසාධන සැලැස්ම පිළිබඳ ප්‍රතිපත්තිය

ආයතනයක් සතුව යම් ආපදාවකදී (හෝ සිදුවීමකදී), බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් යථා තත්වයට පත් කිරීම සඳහා සකස් කරන ලද ආපදා ප්‍රතිසාධන සැලැස්මක් (Disaster Recovery Plan) තිබිය යුතුය.

එවන් සැලැස්මක, එම ආපදා අවස්ථාවේදී බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් නැවත යථා තත්වයට පත් කිරීම සඳහා කළ යුතු ක්‍රියාකාරකම් ද එක් එක් නිලධාරියාට අදාළ භූමිකාවන් සහ වගකීම් ද අඩංගු විය යුතුය.

ආපදා ප්‍රතිසාධන සැලැස්මක් සකස් කිරීමේදී, වත්කම් සඳහා වන අවදානම් තක්සේරුවක් සහ හානි පිළිබඳ විශ්ලේෂණයක් සිදු කොට එවන් හානියකදී බිඳ වැටුණු (හෝ අඩපණ වූ) දත්ත ප්‍රතිසාධනයට ගත යුතු අවම කාලය සහ වත්කම් ප්‍රතිසාධනය කර මෙහෙයුම් නැවත ආරම්භ කිරීමට ගත යුතු අවම කාලය සලකා බැලිය යුතුය. ආයතනය එහි ආපදා ප්‍රතිසාධන සැලැස්මේ ක්‍රියාකාරීත්වය වරින් වර පරීක්ෂා කර යාවත්කාලීන කිරීම කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.6.2 ආපදා ප්‍රතිසාධන සැලැස්ම සක්‍රීය කිරීම පිළිබඳ ප්‍රතිපත්තිය

යම් ආපදාවකදී, අදාළ බලයලත් නිලධාරියා විසින් ආයතනයේ බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් යථා තත්වයට පත් කර ආයතනයේ මෙහෙයුම් නැවත ක්‍රියාත්මක කිරීමට ආපදා ප්‍රතිසාධන සැලැස්ම ක්‍රියාත්මක කළයුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

4.6.3 තීරණාත්මක ආපදා හෝ සිදුවීම් සන්නිවේදනය පිළිබඳ ප්‍රතිපත්තිය

සංකීර්ණ ආපදාවකදී හෝ ආරක්ෂණයට බලපාන සිදුවීමකදී (උදාහරණ ලෙස තීරණාත්මක ආපදාවක් සයිබර් ප්‍රහාරයක් නිසා ඇතිවූ සිදුවීමකදී වැනි) ආයතනය ප්‍රධානියා විසින් තීරණය කරන පරිදි අදාළ රේඛීය අමාත්‍යාංශය, ශ්‍රී ලංකා සර්ව ආයතනය, සිදුවීමට අදාළ වින්දිතයන්, ජනමාධ්‍යයන්, සේවාදායකයින් සහ නීතිය ක්‍රියාත්මක කරන බලධාරීන් වැනි අභ්‍යන්තර සහ බාහිර පාර්ශ්ව සමඟ සැලැස්මකට අනුව සුදුසු ලෙස එම අර්බුදය පිළිබඳව සන්නිවේදනය කළ යුතුය. අර්බුදය අදාළ පාර්ශ්වකරුවන් වෙත සන්නිවේදනය කිරීම සඳහා ආයතනය විසින් එහි ජ්‍යෙෂ්ඨ මට්ටමේ වගකිව යුතු නිලධාරියෙකු පත් කළ යුතුය.

අනුකූලතාව: සියලුම රාජ්‍ය ආයතන සඳහා අදාළ වේ.

5. ප්‍රමුඛතා පදනමින් ක්‍රියාත්මක කළ යුතු ප්‍රතිපත්තිමය කරුණු

තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ආයතනය තුළ ක්‍රියාත්මක කිරීම සඳහා පහත දැක්වෙන ප්‍රතිපත්තිමය කරුණු ප්‍රමුඛතා මට්ටමින් ක්‍රියාත්මක කළ යුතු වේ.

ප්‍රතිපත්ති අංශය	ප්‍රතිපත්ති අංකය	ප්‍රමුඛතා පදනමින් ක්‍රියාත්මක කළ යුතු ප්‍රතිපත්තිමය කරුණු	සියලුම ආයතන	ඊ.ජී.පී. නො.ය.ප. පවතින ආයතන
තොරතුරු සහ සයිබර් ආරක්‍ෂණ පාලනය	4.1.1	තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම සඳහා ආයතන ප්‍රධානියා විසින් නායකත්වය සැපයීම	✓	✓
	4.1.2	තොරතුරු හා සයිබර් ආරක්‍ෂණ ආයතනික ව්‍යුහයක් ස්ථාපන කිරීම	✓	✓
	4.1.2 (අ)	තොරතුරු ආරක්‍ෂණ නිලධාරියකු පත්කර තොරතුරු හා සයිබර් ආරක්‍ෂණ වගකීම් පැවරීම		✓
	4.1.2 (ආ)	තොරතුරු ආරක්‍ෂණ නිලධාරියකු නොමැති අවස්ථාවකදී, ප්‍රධාන නව්‍යකරණ නිලධාරියා වෙත තොරතුරු හා තොරතුරු තාක්‍ෂණ වත්කම් ආරක්‍ෂා කිරීමට වගකීම් පැවරීම	✓	
	4.1.2 (ඇ)	තොරතුරු හා සයිබර් ආරක්‍ෂණ විගණන සම්බන්ධයෙන් කටයුතු කිරීම සඳහා (ප්‍රධාන) අභ්‍යන්තර විගණක වෙත වගකීම් පැවරීම	✓	✓
	4.1.3	තොරතුරු ආරක්‍ෂණ කමිටුවක් පත් කිරීම	✓	✓
	4.1.4	අවදානම් කළමනාකරණ කමිටුවක් පත් කිරීම		✓
	4.1.5	පරිශීලකයන්ගේ වගකීම් හඳුනාගෙන ඒවා ප්‍රකාශයට පත් කිරීම	✓	✓
	4.1.6	තොරතුරු හා සයිබර් ආරක්‍ෂණය සම්බන්ධයෙන් වගකිව යුතු නිලධාරීන්ගේ ධාරිතා සංවර්ධනය කිරීම	✓	✓
	4.1.7	රහසිගත හෝ ඉතා රහසිගත ලෙස වර්ගීකරණය කර ඇති තොරතුරු හෝ තීරණාත්මක ජාතික යටිතල පහසුකම් භාවිතා කරන කාර්යමණ්ඩලයේ ආරක්‍ෂණ නිෂ්කාගත සහ පසුබිම් පරීක්ෂාවක් කිරීම		✓

ප්‍රතිපත්ති අංශය	ප්‍රතිපත්ති අංකය	ප්‍රමුඛතා පදනමින් ක්‍රියාත්මක කළ යුතු ප්‍රතිපත්තිමය කරුණු	සියලුම ආයතන	ෆ.කී.ජා. තො.ස.ප. පවතින ආයතන
	4.1.8	තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරකම්, එහි ආයතනික දැක්ම, මෙහෙවර සහ අරමුණ සමඟ පෙළ ගැස්වීම	✓	✓
	4.1.9	තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරී සැලසුම් සකස්කර ක්‍රියාත්මක කිරීම	✓	✓
වත්කම් හිමිකරුවන් සහ අවදානම් හඳුනා ගැනීම	4.2.1	තොරතුරු, තොරතුරු තාක්ෂණ වත්කම් හා තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් හඳුනා ගැනීම.	✓	✓
	4.2.3	වත්කම් හිමිකරුවන් සහ භාරකරුවන් හඳුනා ගෙන ඔවුන්ට ඒවා ආරක්ෂා කිරීමට වගකීම් පැවරීම	✓	✓
	4.2.4	තොරතුරු වත්කම් සහ තොරතුරු තාක්ෂණ වත්කම් රෙජිස්තර පවත්වාගෙන යාම	✓	✓
	4.2.5	තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සඳහා අවදානම් තක්සේරු කිරීම		✓
	4.2.6	තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් ඒවායේ වටිනාකම් සහ සංවේදීතාවය මත වර්ගීකරණය කිරීම	✓	✓
	වත්කම් ආරක්ෂා කිරීම	4.3.1	නිශ්චලව පවතින දත්ත ආරක්ෂා කිරීම	✓
4.3.2		සංවරණය වන දත්ත ආරක්ෂා කිරීම	✓	✓
4.3.3		තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම් සඳහා වන භෞතික ආරක්ෂාව සහතික කිරීම	✓	✓
4.3.4		තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට ඇති පරිශීලක ප්‍රවේශ පාලනය කිරීම	✓	✓
4.3.5		ගක්කිමින් සත්‍යාපනයන් සහතික කිරීම	✓	✓
4.3.6		දත්තවල ස්වෛරීභාවය සුදුසු පරිදි සහතික කිරීම	✓	✓
4.3.7		විලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතා කර ඒවායේ සර්මා යාවත්කාලීන කිරීම	✓	✓
4.3.8		ප්‍රති-අනිෂ්ට මෘදුකාංග භාවිතා කිරීම	✓	✓

ප්‍රතිපත්ති අංශය	ප්‍රතිපත්ති අංකය	ප්‍රමුඛතා පදනමින් ක්‍රියාත්මක කළ යුතු ප්‍රතිපත්තිමය කරුණු	සියලුම ආයතන	ෆනි.ජා. තො.ය.ප. පවතින ආයතන
	4.3.9	නිල සන්නිවේදන කටයුතු සඳහා නිල විද්‍යුත් තැපැල් භාවිතා කිරීම	✓	✓
	4.3.10	විද්‍යුත් තැපැල් වල ආරක්‍ෂාව සහතික කිරීම	✓	✓
	4.3.11	සුදුසු පරිදි ඩිජිටල් අත්සන් භාවිතා කිරීම	✓	✓
	4.3.12	පරිමිති ආරක්‍ෂණ පාලනයන් සිදු කිරීම	✓	✓
	4.3.13	ආරක්‍ෂිත දුරස්ථ ප්‍රවේශය ක්‍රමවේද භාවිතා කිරීම	✓	✓
	4.3.14	උපස්ථ සඳහා උපාය මාර්ගයක් භාවිතා කිරීම	✓	✓
	4.3.16	ආරක්‍ෂාව තහවුරු කරගත් මාදුකාංග සංවර්ධනය හා භාවිතය සහතික කිරීම	✓	✓
	4.3.17	වත්කම් සුරක්‍ෂිතව බැහැර කිරීම	✓	✓
	4.3.18	අභ්‍යන්තර තොරතුරු ආරක්‍ෂණ විගණන ක්‍රියාවලියක් පවත්වාගෙන යාම.	✓	✓
	4.3.19	ඕනෑම වෙබ් අඩවියක්, වෙබ් යෙදුමක් හෝ පද්ධතියක් නිල වශයෙන් දියත් කිරීමට පෙර අවදානම් තක්සේරු කිරීම සහ විනිවිද යාමේ පරීක්‍ෂණ සිදු කිරීම	✓	✓
	4.3.20	තොරතුරු තාක්‍ෂණ වත්කම් වල ආරක්‍ෂණ ප්‍රතිරෝධීය ශක්තිමත් කිරීම	✓	✓
	4.3.21	නිවසේ සිට රාජකාරි කටයුතු වල නිරතවීම සඳහා වන ආරක්‍ෂණ මාර්ගෝපදේශ අනුගමනය කිරීම.	✓	✓
	4.3.23	අනාරක්‍ෂිත ජාල භාවිතයෙන් වැළකී සිටීම	✓	✓
	4.3.24	සැපයුම්කරුවන් කළමනාකරණය කිරීම	✓	✓
	4.3.25	වෙනස්වීම් කළමනාකරණය කිරීම	✓	✓

ප්‍රතිපත්ති අංශය	ප්‍රතිපත්ති අංකය	ප්‍රමුඛතා පදනමින් ක්‍රියාත්මක කළ යුතු ප්‍රතිපත්තිමය කරුණු	සියලුම ආයතන	ෆ.කී.ජා. නො.ය.ප. පවතින ආයතන
ආරක්‍ෂණයට බලපාන තොරතුරු හා සයිබර් ආරක්‍ෂණ සිදුවීම් හඳුනා ගැනීම	4.4.1	ආරක්‍ෂණ සිදුවීම් වාර්තා කරන ලෙස කාර්ය මණ්ඩලයට උපදෙස් ලබාදීම	✓	✓
	4.4.2	ආරක්‍ෂණයට බලපාන සිදුවීම් හඳුනා ගැනීම සඳහා ලොග් සටහන් සමාලෝචනය කිරීම	✓	✓
	4.4.3	ආරක්‍ෂණයට බලපාන සිදුවීම් අඛණ්ඩව අධීක්‍ෂණය කරමින් සිදුවීම් හඳුනා ගැනීම		✓
	4.4.4	ආරක්‍ෂණයට බලපාන සිදුවීම් ශ්‍රී ලංකා සර්ට් ආයතනය වෙත වාර්තා කිරීම	✓	✓
ආරක්‍ෂණයට බලපාන සිදුවීම්වලට ප්‍රතිචාර දැක්වීම	4.5.1	සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් සකස් කිරීම	✓	✓
	4.5.2	සිදුවීමකදී, සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම ක්‍රියාත්මක කිරීම	✓	✓
	4.5.3	ආරක්‍ෂණ සිදුවීම් සඳහා චෝභාරික පරීක්‍ෂණ සිදු කිරීම	✓	✓
මෙහෙයුම් ප්‍රතිසාධනය කිරීම	4.6.1	ආපදා ප්‍රතිසාධනය සැලැස්මක් නිර්මාණය කිරීම	✓	✓
	4.6.2	ආපදා අවස්ථාවකදී ආපදා ප්‍රතිසාධනය සැලැස්ම ක්‍රියාත්මක කිරීම	✓	✓
	4.6.3	කීර්ණාත්මක ආපදාවක් හෝ සිදුවීමක් සන්නිවේදනය කිරීම සඳහා සැලැස්මක් නිර්මාණය කිරීම	✓	✓

ෆ. කී. ජා. නො. ය. ප. පවතින ආයතන : කීර්ණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් පවතින ආයතන

6. තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය අධීක්‍ෂණය කිරීමේ සහ ඇගයීමේ ක්‍රමවේදය

- 6.1 තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාවට නැංවීමට පෙර ආයතනයේ තොරතුරු හා සයිබර් ආරක්‍ෂණ සුදානම හඳුනා ගැනීම සඳහා සහ ප්‍රතිපත්තිය ක්‍රියාත්මක කරමින් තොරතුරු හා තොරතුරු තාක්‍ෂණ වත්කම් ආරක්‍ෂා කිරීමට රාජ්‍ය ආයතන ගෙන ඇති ක්‍රියාමාර්ගවල කාර්යසාධනය අධීක්‍ෂණය සහ ඇගයීම සඳහා ක්‍රමවේදයක් නිර්මාණය කර ඇත.
- 6.2 ඒ අනුව ශ්‍රී ලංකා සර්ව ආයතනය අංක 6.6 හි දක්වා ඇති ප්‍රශ්නාවලියෙහි අඩංගු කරුණු පදනම් කර ගනිමින් ආයතනයේ තොරතුරු හා සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේ සුදානම පිළිබඳ මූලික තක්සේරුවක් ලබා ගන්නා අතර එම තක්සේරුව පදනම් කර ගනිමින් එම ආයතන වල මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම සඳහා අවශ්‍ය මගපෙන්වීම ලබා දෙනු ඇත.
- 6.3 ශ්‍රී ලංකා සර්ව ආයතනය වාර්ෂිකව ආයතනවල තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේ කාර්ය සාධනය ඇගයීමට ලක් කරනු ලබන අතර එක් එක් ආයතනය ප්‍රතිපත්තියට අනුගත වී ඇති අයුරු තොරතුරු සහ සයිබර් ආරක්‍ෂණ දර්ශකයක (Information and Cyber Security Index) ඉදිරිපත් කරනු ඇත. තවද මෙම ඇගයීමේ ප්‍රතිඵල මත පදනම්ව ආයතනයේ සමස්ත තොරතුරු සහ සයිබර් ආරක්‍ෂණ සුදානම වැඩිදියුණු කිරීමට අවශ්‍ය නිර්දේශ ශ්‍රී ලංකා සර්ව ආයතනය විසින් ඉදිරිපත් කරනු ඇත.
- 6.2.4 ආයතනවල තොරතුරු සහ සයිබර් ආරක්‍ෂණ ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේ කාර්ය සාධනය හෝ සුදානම ඇගයීමට මෙම ලේඛනයේ අංක 6.6 පරිච්ඡේදයේ සඳහන්ව ඇති ප්‍රශ්න 50 කට ආසන්න සංඛ්‍යාවකින් යුත් ප්‍රශ්නාවලිය භාවිතා කළ යුතු අතර ආයතනයේ තොරතුරු ආරක්‍ෂණ නිලධාරියා, ප්‍රධාන නවීකරණ නිලධාරියා හෝ තොරතුරු තාක්‍ෂණ විෂය භාර නිලධාරියා විසින් මෙම ප්‍රශ්නාවලිය සම්පූර්ණ කළ යුතු අතර, එය සෑම වසරකම ඔක්තෝබර් 30 වැනි දිනට පෙර හෝ ඊට පෙර ආයතන ප්‍රධානියාගේ අත්සන සහිතව ශ්‍රී ලංකා සර්ව ආයතනය වෙත යොමු කළ යුතුය.
- 6.5 පිළිතුරු සපයන නිලධාරියා විසින් අදාළ ප්‍රශ්න සඳහා විස්තරාත්මක ප්‍රතිචාරයක් සැපයීමට අවශ්‍ය විටදී, ඒ සඳහා ප්‍රශ්නාවලිය අවසානයේ ඇති සටහන් තීරුවේ (Remarks) විස්තර සැපයිය හැකිය. තවද, මෙම ප්‍රශ්නාවලියේ භාවිතා වී ඇති පදමාලාව පිළිබඳ පැහැදිලි කිරීම් සඳහා මෙම ප්‍රතිපත්තියේ සඳහන්ව ඇති අර්ථ දැක්වීම් (Definitions) භාවිතා කළ හැක.
- 6.6 ඇගයීමේ ප්‍රශ්නාවලිය සියළුම රාජ්‍ය ආයතන සිය දැනුවත්භාවය මත සෑම ප්‍රශ්නයකටම ඔවුන්ගේ ප්‍රතිචාරය දැක්වීමට අවශ්‍ය වේ.

ප්‍රතිපත්ති යොමුව	තක්සේරු නිර්ණායක	ප්‍රතිපත්ති අංකය	ආයතනය අනුගතද		සටහන්
			ඔව්	නැත	
තොරතුරු සහ සයිබර් ආරක්ෂණ පාලනය					
ආරක්ෂණ ආයතනික ව්‍යුහය	1. ආයතනය සඳහා තොරතුරු ආරක්ෂණ නිලධාරියෙකු පත් කර තිබේද?	4.1.2			
	2. ආයතනය සිය තොරතුරු ආරක්ෂණ නිලධාරියා වෙත තොරතුරු හා සයිබර් ආරක්ෂණ වගකීම් පවරා තිබේද?	4.1.2			
	3. තොරතුරු ආරක්ෂණ නිලධාරියකු පත් කර නොමැති නම්, ප්‍රධාන නව්‍යකරණ නිලධාරී හෝ තොරතුරු තාක්ෂණ විෂය භාර නිලධාරියාට තොරතුරු ආරක්ෂණ වගකීම් පවරා තිබේද?	4.1.2			
	4. ආයතනය සිය (ප්‍රධාන) අභ්‍යන්තර විගණන නිලධාරී වෙත තොරතුරු හා සයිබර් ආරක්ෂණ විගණන වගකීම් පවරා දී තිබේද?	4.1.2			
	5. තොරතුරු හා සයිබර් ආරක්ෂාව පිළිබඳ තීරණ ගැනීමට ආයතනයේ කමිටුවක් පිහිටුවා තිබේද?	4.1.3			
	6. ආයතනයේ තොරතුරු හා සයිබර් ආරක්ෂණ අවදානම් සම්බන්ධයෙන් තීරණ ගැනීම සඳහා අවදානම් කළමනාකරණ කමිටුවක් පිහිටුවා තිබේද?	4.1.4			

ප්‍රතිපත්ති යොමුව	තක්සේරු නිර්ණායක	ප්‍රතිපත්ති අංකය	ආයතනය අනුගතද		සටහන්
			ඔව්	නැත	
පරිශීලකයන්ගේ වගකීම්	7. තොරතුරු හා සයිබර් ආරක්‍ෂාව සම්බන්ධයෙන් වන වගකීම් ඔබ ආයතනයේ කාර්ය මණ්ඩලයට පැහැදිලි කොට දී තිබේද?	4.1.5			
ධාරිතා සංවර්ධනය	8. තොරතුරු හා සයිබර් ආරක්‍ෂණය සම්බන්ධ වගකීම් දරන නිලධාරීන්ගේ තොරතුරු ආරක්‍ෂණ හැකියාව වර්ධනය කිරීම සඳහා පුහුණු හා දැනුවත් කිරීම් කර තිබේද?	4.1.6			
පසුබිම් පරීක්‍ෂාව	9. ඔබේ ආයතනය "ඉතා රහසිගත" හෝ "රහසිගත" තොරතුරු වත්කම් හෝ නිර්ණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් සහිත පද්ධති සම්බන්ධයෙන් කටයුතු කරන නිලධාරීන්ගේ පසුබිම් පරීක්‍ෂණ සහ ආරක්‍ෂක නිෂ්කාගත සිදු කර තිබේද?	4.1.7			
උපායමාර්ගික පෙළගැස්වීම	10. ආයතනයේ කාර්යයන්, ප්‍රතිපත්ති, උපාය මාර්ග හෝ ව්‍යාපෘති සැලසුම් කිරීමේදී සහ ක්‍රියාත්මක කිරීමේදී, තොරතුරු හා සයිබර් ආරක්‍ෂාව සැලකිල්ලට ගෙන තිබේද?	4.1.8			

ප්‍රතිපත්ති යොමුව	තක්සේරු නිර්ණායක	ප්‍රතිපත්ති අංකය	ආයතනය අනුගතද		සටහන්
			මිච්චි	නැත	
ක්‍රියාකාරී සැලසුම්	11. තොරතුරු හා සයිබර් ආරක්ෂණ ක්‍රියාකාරකම් සඳහා ආයතනය මූල්‍ය ප්‍රතිපාදන වෙන් කර තිබේද?	4.1.9			
	12. ආයතනය එහි තොරතුරු හා සයිබර් ආරක්ෂණ අරමුණු සාක්ෂාත් කර ගැනීම සඳහා වන ව්‍යාපෘති ක්‍රියාකාරී සැලසුම්වලට ඇතුළත් කර තිබේද?	4.1.10			
වත්කම්, හිමිකරුවන්, පරිශීලකයන් සහ අවදානම් හඳුනා ගැනීම					
වත්කම් හඳුනා ගැනීම	13. ආයතනය සතු වටිනාකමක් ඇති තොරතුරු වත්කම් හඳුනාගෙන තිබේද?	4.2.1			
	14. ආයතනය සතු තොරතුරු වත්කම් හා සම්බන්ධ අවදානම් තක්සේරු කර තිබේද?	4.2.5			
	15. ආයතනයේ තොරතුරු වත්කම්වල සංවේදීතාව හෝ වෙනත් ක්‍රමවේදයක් මත පදනම්ව තොරතුරු වත්කම් වර්ගීකරණය (classification of information assets) කර තිබේද?	4.2.1			
	16. ආයතනය තොරතුරු වත්කම් ලේඛනයක (information assets) සටහන්කර තිබේද?	4.2.5			
	17. ආයතනය තොරතුරු තාක්ෂණ වත්කම් (IT assets) හඳුනාගෙන තිබේද?	4.2.6			

	18. ආයතනය තොරතුරු තාක්ෂණ වත්කම්, ලේඛනයක ලේඛනගත කර තිබේද?	4.2.1			
	19. ආයතනය තොරතුරු තාක්ෂණ වත්කම් ඒවායේ තීරණාත්මකභාවය (criticality) මත වර්ගීකරණය කර තිබේද?	4.2.5			
	20. ආයතනයේ වත්කම්වල හිමිකරුවන් හඳුනාගෙන තිබේද?	4.2.6			

වත්කම් ආරක්ෂා කිරීම

දත්ත කේතනය	21. ගබඩා කිරීමට පෙර ආයතනයේ සංවේදී තොරතුරු කේතනය (encrypt) කෙරේද?	4.2.4			
	22. ආයතනයේ සංවේදී තොරතුරු පරිගණක ජාල සහ වෙනත් වැනලයන් හරහා ගමන් කිරීමට පෙර කේතනය කෙරේද?	4.2.1			

භෞතික ආරක්ෂාව	23. ආයතනයේ සංවේදී තොරතුරු සකසන්නේ හෝ ගබඩා කරන්නේ භෞතික වශයෙන් ආරක්ෂිත ස්ථානවල ද?	4.2.4			
	24. ගිනි ගැනීම්, ජල ගැලීම්, ආර්ද්‍රතාව වෙනස් වීම් සහ උෂ්ණත්ව වෙනස් වීම් වැනි තත්වයන්ගෙන් ආයතනයේ ආරක්ෂිත ස්ථාන ආරක්ෂා කිරීමට සුදුසු පියවර ගෙන තිබේද?	4.2.6			
	25. ආයතනයේ ආරක්ෂිත ස්ථාන වලට අනවසර ඇතුළුවීම් වැලැක්වීමට ක්‍රමවේද සකසා තිබේද?	4.2.3			

ප්‍රතිපත්ති යොමුව	තක්සේරු නිර්ණායක	ප්‍රතිපත්ති අංකය	ආයතනය අනුගතද		සටහන්
			ඔව්	නැත	
	26. ආයතනයේ අන්‍යෝන්‍ය කළමනාකරණ සහ ප්‍රවේශ පාලන ක්‍රමවේදයක් (Identity Management and Access Control) තිබේද?	4.3.1			
	27. ආයතනයේ ශක්තිමත් සත්‍යාපන (strong authentication) ක්‍රමවේද භාවිතා කරන්නේද?	4.3.2			
දත්ත ස්වෛරීභාවය	28. ආයතනය සිය දත්ත වල ස්වෛරීභාවය (Data Sovereignty) සැලකිල්ලට ගෙන තිබේද?	4.3.3			
	29. මේසගත සේවා ලබා ගැනීමට පෙර ආයතනය එහි අවදානම සැලකිල්ලට ගෙන තිබේද?	4.3.3			
	30. ආයතනය වලංගු බලපත්‍ර සහිත පරිගණක මෙහෙයුම් පද්ධති පමණක් භාවිතා කරන්නේද?	4.3.3			
වලංගු බලපත්‍ර සහිත මෘදුකාංග භාවිතය සහ සර්වා යාවත්කාලීන කිරීම	31. ආයතනයේ පරිගණක මෙහෙයුම් පද්ධති සැපයුම්කරු විසින් සපයන ලද නවතම සර්වා මගින් යාවත්කාලීන කර තිබේද?	4.3.4			
	32. සැපයුම්කරු විසින් සපයන ලද තීරණාත්මක සර්වා ස්ථාපනය කිරීමට පෙර නිසි ඇගයීමකට භාජනය කරන්නේද?	4.3.5			

ප්‍රතිපත්ති යොමුව	තක්සේරු නිර්ණායක	ප්‍රතිපත්ති අංකය	ආයතනය අනුගතද		සටහන්
			ඔව්	නැත	
ප්‍රති අනිෂ්ට මෘදුකාංග	33. ආයතන සියලුම පරිගණක සහ අදාළ උපාංගවල වලංගු බලපත්‍රයක් සහිත ප්‍රති අනිෂ්ට මෘදුකාංග ස්ථාපනය කර තිබේද?	4.3.6			
විද්‍යුත් තැපැල්	34. ආයතනයේ නිල සන්නිවේදන කටයුතු සඳහා පුද්ගලික විද්‍යුත් තැපැල් භාවිතය වැලැක්වීමට අවශ්‍ය ක්‍රියාමාර්ගයන් ගෙන තිබේද?	4.3.6			
	35. විද්‍යුත් තැපැල් ලිපිවල අමුණා ඇති අනිෂ්ට මෘදුකාංග හඳුනා ගෙන ඒවා ඉවත් කිරීමට ආයතනයේ විද්‍යුත් තැපැල් පෙරහන් සක්‍රීය කොට තිබේද?	4.3.7			
	36. ආයතනය විද්‍යුත් තැපැල මගින් සංවේදී තොරතුරු හුවමාරු කරන විට කේතනය භාවිතා කරයිද?	4.3.7			
පරිමිති ආරක්‍ෂණ පාලනයන්	37. ආයතනයේ ගිනිපවුරක් ස්ථාපනය කර තිබේද?	4.3.7			
ආරක්‍ෂිත දුරස්ථ ප්‍රවේශය	38. ආයතනය දුරස්ථ ප්‍රවේශය සඳහා ආරක්‍ෂිත තත්‍යසම පුද්ගලික ජාල (virtual private networks) භාවිතා කරන්නේද?	4.3.8			

ප්‍රතිපත්ති යොමුව	තක්සේරු නිර්ණායක	ප්‍රතිපත්ති අංකය	ආයතනය අනුගතද		සටහන්
			ඔව්	නැත	
	39. ආයතනයේ දුරස්ථව සම්බන්ධ වන සියලුම පරිශීලකයින් ආරක්ෂිත තනාසම පුද්ගලික ජාල භාවිතා කරන්නේද?	4.3.9			
උපස්ථ උපාය මාර්ග	40. ආයතනය දත්ත උපස්ථ (backup) කරන්නේද?	4.3.10			
	41. ආයතනය සිය උපස්ථ ගබඩා කර ඇත්තේ දත්ත සැකසුම් ස්ථානයෙන් භෞතිකව දුරස්ථ, ගිනිගැනීම් ආදියෙන් ආරක්ෂිත ස්ථානයකද?	4.3.10			
වත්කම් සුරක්ෂිතව බැහැර කිරීම	42. සංවේදී තොරතුරු අඩංගු දත්ත ගබඩා මාධ්‍ය බැහැර කිරීමට ඔබ ආයතනය පහත සඳහන් කිසිවක් අනුගමනය කරන්නේද? (ඉරා දැමීම, සිදුරු කිරීම භෞතිකව හානි කිරීම යනාදිය)	4.3.12			
අභ්‍යන්තර තොරතුරු ආරක්ෂණ විගණන වැඩසටහන	43. ආයතනය සතුව අභ්‍යන්තර තොරතුරු හා සයිබර් ආරක්ෂණ විගණන වැඩසටහනක් තිබේද?	4.3.13			
	44. ආයතනය ඕනෑම වෙබ් අඩවියක්, වෙබ් යෙදුමක් හෝ පද්ධතියක් නිල වශයෙන් දියත් කිරීමට පෙර ශ්‍රී ලංකා සර්ව ආයතනය මගින් අවදානම් තක්සේරු කිරීම සහ විනිවිදයාමේ පරීක්ෂණ සිදු කරන්නේද?	4.3.13			

ප්‍රතිපත්ති යොමුව	තක්සේරු නිර්ණායක	ප්‍රතිපත්ති අංකය	ආයතනය අනුගතද		සටහන්
			ඔව්	නැත	
	45. ආයතනයේ පරිගණක ජාල සඳහා අවදානම තක්සේරු කිරීම සහ විනිවිදයාමේ පරීක්ෂණ සිදු කර තිබේද?	4.3.14			
නිවසේ සිට රාජකාරි කටයුතුවල නිරතවීම	46. රජය විසින් නිකුත් කරන ලද උපදෙස්වලට අනුකූලව ශ්‍රී ලංකා සර්ව ආයතනය විසින් නිකුත් කරන ලද නිවසේ සිට වැඩ කිරීම සඳහා වන තොරතුරු හා සයිබර් ආරක්ෂණ මාර්ගෝපදේශ ඔබ ආයතනය පිළිපදින්නේද?	4.3.14			
රාජකාරි කටයුතු සඳහා නම පෞද්ගලික මෙවලම් භාවිතය	47. රාජකාරි කටයුතු සඳහා පෞද්ගලික මෙවලම් භාවිතා කිරීමට පෙර ඒවා ලියාපදිංචි කිරීමට ආයතනය විධිමත් ක්‍රියා පටිපාටියක් අනුගමනය කරන්නේද?	4.3.17			
	48. ආයතනය රාජකාරි කටයුතු සඳහා පෞද්ගලික මෙවලම් භාවිතා කරන විට, ඒවායේ සංවේදී දත්ත සැකසීමට හෝ ගබඩා කිරීමට ඉඩ දෙන්නේද?	4.3.18			

තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් හඳුනා ගැනීම

ආරක්ෂණ සිදුවීම් වාර්තා කිරීම	49. තොරතුරු සහ සයිබර් ආරක්ෂණය සම්බන්ධයෙන් කිසියම් සැක කටයුතු ක්‍රියාකාරකමක්, සම්බන්ධතාවක්, සොරකමක්, වෛරසයක්, අවදානමක්, අනවසර ප්‍රවේශයක්, ලිපිගොනු විකෘති කිරීම හෝ මෙම ප්‍රතිපත්තිය උල්ලංඝනය කිරීමක් ආයතනයේ තොරතුරු ආරක්ෂාව හා නිලධාරියාට වාර්තා කරන ලෙස කාර්ය මණ්ඩලයට උපදෙස් දී තිබේද?	4.3.19			
	50. ආයතනය තොරතුරු හා සයිබර් ආරක්ෂණ සිදුවීම් ශ්‍රී ලංකා සර්ව ආයතනය වෙත හෝ වෙනත් අදාළ ආයතනයකට වාර්තා කර තිබේද?	4.3.19			

ප්‍රතිපත්ති යොමුව	තක්සේරු නිර්ණායක	ප්‍රතිපත්ති අංකය	ආයතනය අනුගතද ඔව් නැත		සටහන්
ආරක්‍ෂණ සිදුවීම්වලට ප්‍රතිචාර දැක්වීම					
ආරක්‍ෂණයට බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සහ එය ක්‍රියාත්මක කිරීම	51. ආරක්‍ෂණයට අහිතකර ලෙස බලපාන සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්මක් (Incidents Response Plan) තිබේද?	4.3.21			
	52. තොරතුරු හා සයිබර් ආරක්‍ෂණ සිදුවීමක දී, ආයතනය සමග සිය මෙහෙයුම්වලට ඇති බලපෑම අවම කිරීම සහ එම මෙහෙයුම් නැවත යථා තත්වයට පත් කිරීම පිණිස, සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමේ සැලැස්ම සක්‍රීය කරන්නේද?	4.3.22			
මෙහෙයුම් යථා තත්වයට පත් කිරීම					
ආපදා ප්‍රතිසාධන සැලැස්ම සහ එය ක්‍රියාත්මක කිරීම	53. යම් ආපදාවකදී (හෝ සිදුවීමකදී), බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් යථා තත්වයට පත් කිරීම සඳහා සකස් කරන ලද ආපදා ප්‍රතිසාධන සැලැස්මක් (Disaster Recovery Plan) ආයතනයට තිබේද?	4.3.22			
	54. යම් ආපදාවකදී (හෝ සිදුවීමකදී), බිඳ වැටුණු හෝ අඩපණ වූ සේවාවන් යථා තත්වයට පත් කිරීම සඳහා ආයතනය සිය ආපදා ප්‍රතිසාධන සැලැස්මක් ක්‍රියාත්මක කරන්නේද?	4.4.1			

අර්ථ දැක්වීම

ප්‍රති - අනිෂ්ට මෘදුකාංග
(Anti-malware)

ප්‍රති- අනිෂ්ට මෘදුකාංග යනු අනිෂ්ට මෘදුකාංග හඳුනා ගැනීමට හෝ එම මෘදුකාංග පරිගණක පද්ධති හෝ ඉලෙක්ට්‍රොනික උපාංගවලට ආසාදනය වීම වැළැක්වීමට නිර්මාණය කර ඇති මෘදුකාංගයකි. අනිෂ්ට මෘදුකාංග (malware) යනු පරිගණක-යකට, සේවාදායකයක පරිගණකයකට හෝ පරිගණක ජාලයකට (උදා: වෙබර්ස්, චර්ම්, රැන්සම්වෙයා) හානි කිරීමේ අරමුණින් නිර්මාණය කර ඇති ඕනෑම ආකාරයක මෘදුකාංගයකි.

වත්කම් වර්ගීකරණය
(Assets Classification)

වත්කම් වර්ගීකරණය යනු ආයතනයට වටිනාකමක් ඇති වත්කම් ඒවායේ සංවේදීතා මට්ටම සහ වටිනාකම මත පදනම්ව වර්ගීකරණය කිරීමේ ක්‍රියාවලියයි. මෙහි මූලික පරමාර්ථය වන්නේ ආයතනයට එම වත්කමේ ඇති වටිනාකමට අනුකූලව සුදුසු මට්ටමේ ආරක්‍ෂාවක් ලබා දීම සහතික කිරීමයි. මේ ආකාරයට තොරතුරු හා තොරතුරු තාක්‍ෂණ වත්කම් වර්ගීකරණය කළ හැකිය.

වත්කම් භාරකරු
(Assets Custodian)

තොරතුරු වත්කම් හිමිකරු විසින් අනුමත කරන ලද ආරක්‍ෂක අවශ්‍යතාවලට අනුව වත්කමේ ජීවන චක්‍රය පුරා තොරතුරු වත්කමක් ආරක්‍ෂා කිරීමේ වගකීම ඇති නිලධාරියෙකු හෝ ආයතනයක් වේ.

වත්කම් හිමිකරු
(Assets Owner)

වත්කම් හිමිකරු යනු වත්කම්වල දෛනික කලමනාකරණය සඳහා වගකිව යුතු විධායක මට්ටමේ නිලධාරියෙකු වේ. වත්කම් හිමිකරු විසින් අදාළ වත්කමෙහි මුළු ජීවන චක්‍රයම පාලනය කරනු ලබන අතර වත්කම්වලට ඇති අවදානම හඳුනාගෙන ඒවා ආරක්‍ෂා කිරීම සඳහා සුදුසු ආරක්‍ෂණ ක්‍රමවේදයන් යෝජනා කළ යුතුය.

තොරතුරුවල උපයෝජ්‍යතාවය
(Availability of Information)

උපයෝජ්‍යතාවය යනු තොරතුරු අවසරලත් පුද්ගලයන් සඳහා අවශ්‍ය ඕනෑම අවස්ථාවකදී ප්‍රවේශ වීම සහ භාවිත කිරීමේ හැකියාව තහවුරු කිරීමයි.

තොරතුරුවල රහස්‍යභාවය
(Confidentiality of Information)

රහස්‍යභාවය යනු අනවසර පුද්ගලයන්ට සහ ආයතනවලට තොරතුරු හෙළි නොකරන බවට තහවුරු කිරීමයි.

සංවේදී තොරතුරු වත්කම්
(Sensitive Information Assets)

සංවේදී තොරතුරු වත්කම් යනු අස්ථානගත වීමක්, වෙනස් කිරීමක්, අවහානිතයක්, අනවසර හෙළිදරව් කිරීමක් හෝ බිඳ වැටීමක් නිසා ආයතනයකට හෝ පුද්ගලයකුට අහිතකර බලපෑමක් ඇති කළ හැකි තොරතුරු වේ. මේවා “ඉතා රහසිගත” (Secret), “රහසිගත” (Confidential) සහ සීමිත හුවමාරුව (Limited Sharing) ලෙස වර්ගීකරණය කරනු ඇත.

තීරණාත්මක තොරතුරු තාක්ෂණ වත්කම්
(Critical IT Assets)

තීරණාත්මක තොරතුරු තාක්ෂණ වත්කම් යනු අනවසර ඇතුල්වීමක්, අවහා විනයක් හෝ බිඳ වැටීමක් නිසා එහි ඇති දත්තවලට, ආයතනයට හෝ පුද්ගලයකුට අහිතකර බලපෑමක් ඇති කළ හැකි පද්ධති වේ. මේවා ඉතා තීරණාත්මක (Very Critical) සහ තීරණාත්මක (Critical) තොරතුරු තාක්ෂණ වත්කම් ලෙස වර්ගීකරණය කළ හැකිය. මෙම පද්ධති සඳහා ඉහළ මට්ටමේ ආරක්ෂාවක් අවශ්‍ය වන අතර ඒවා පහත අර්ථ දක්වා ඇති තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් යන ආකාරයෙන් ද පැවතිය හැකිය.

තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම්
(Critical National Information Infrastructure)

තීරණාත්මක ජාතික තොරතුරු යටිතල පහසුකම් යනු බිඳ වැටීමකදී හෝ අසාහරණයකදී ජාතික ආරක්ෂාව, පාලනය, ආර්ථිකය, සෞඛ්‍ය සහ සමාජ යහපැවැත්ම කෙරෙහි සාමාන්‍යමය බලපෑමක් ඇති කරන තොරතුරු හා තොරතුරු තාක්ෂණ වත්කම් වේ.

ඩිජිටල් අත්සන්
(Digital Signatures)

ඩිජිටල් අත්සන් යනු ඩිජිටල් පණිවිඩ හෝ ලේඛනවල සත්‍යතාවය තහවුරු කිරීම සඳහා යොදා ගැනෙන තාක්ෂණයකි. එය යචන්තාගේ සත්‍යතාව (අන්‍යතාවය), පණිවිඩ නිරවද්‍යතාවය (අනවසර වෙනස් කිරීම) සහ ප්‍රතික්ෂේප කිරීම (යචන්තාට පසුව ලේඛනය ජනනය කිරීම ප්‍රතික්ෂේප කළ නොහැක) සපයයි.

සංකේතනය
(Encryption)

සංකේතනය යනු පණිවිඩයක් ආරක්ෂිත- කේත සහිත පෙළකට පරිවර්තනය කිරීමේ ක්‍රියාවලියයි. එය විකේතනය හරහා නැවත පරිවර්තනය නොකර තේරුම් ගත නොහැක.

රාජ්‍ය ආයතන
(Government Organizations)

රාජ්‍ය ආයතන යනු 2016 අංක 12 දරන තොරතුරු දැනගැනීමේ අයිතිය පිළිබඳ පනතේ අර්ථ දක්වා ඇති පොදු අධිකාරීන්ය.

ආරක්ෂක පාලන
(Information Security Controls)

ආරක්ෂක පාලන යනු තොරතුරු සහ තොරතුරු තාක්ෂණ වත්කම්වලට ආරක්ෂක අවදානම් වළක්වා ගැනීම, හඳුනා ගැනීම, ප්‍රතික්‍රියා කිරීම හෝ අවම කිරීම සඳහා වන ආරක්ෂක ක්‍රියාකාරකම් වේ. මෙවන් පාලනයන්, තොරතුරු වත්කම් ආරක්ෂා කිරීම සඳහා ස්ථාපනය කර ඇති තාක්ෂණයන්, ප්‍රතිපත්ති, ක්‍රියා පටිපාටි හෝ වෙනත් ක්‍රමවේද වේ.

තොරතුරු ආරක්ෂක නිලධාරී
(Information Security Officer)

තොරතුරු ආරක්ෂණ නිලධාරියා යනු තොරතුරු වත්කම් ප්‍රමාණවත් ලෙස ආරක්ෂා කිරීම සහතික කිරීම සඳහා සංවිධාන අරමුණු, උපාය මාර්ග සහ ක්‍රියාකාරී සැලසුම් ස්ථාපිත කිරීම සහ පවත්වාගෙන යාම සඳහා වගකිව යුතු ජ්‍යෙෂ්ඨ මට්ටමේ නිලධාරියෙකි..

තොරතුරු ආරක්ෂණ කමිටුව
(Information Security Committee)

ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීමේදී, තොරතුරු ආරක්ෂණ නිලධාරී විසින් සිදු කරනු ලබන සියලුම තොරතුරු ආරක්ෂණ පාලන, ක්‍රියාකාරී සැලසුම්, වත්කම් වර්ගීකරණ යෝජනා ක්‍රම, සිද්ධි ප්‍රතිචාර සැලසුම් සහ ආපදා ප්‍රතිසාධන සැලසුම් සහ අනෙකුත් ක්‍රියාකාරකම් සමාලෝචනය කිරීම සහ අනුමත කිරීම සඳහා මෙම කමිටුව වගකිව යුතුය.

ආරක්‍ෂක තොරතුරු සහ සිදුවීම් කළමනාකරණ පද්ධති (Security Information and Event Management Systems)

ආරක්‍ෂක තොරතුරු සහ සිදුවීම් කළමනාකරණ පද්ධති යනු ලොග් සටහන් වලින් එකතු කරන දත්ත විශ්ලේෂණය කර, ආරක්‍ෂක තර්ජන සහ සිදුවීම් තත්‍ය කාලීනව හඳුනාගෙන ඒවාට නිසි ක්‍රියාමාර්ග ගැනීම සඳහා පද්ධති පරිපාලකයන් වෙත දැනුම්දීම සඳහා නිර්මාණය කර ඇති පද්ධති වේ.

තොරතුරු හා සයිබර් ආරක්‍ෂාව (Information and Cyber Security)

තොරතුරු හා සයිබර් ආරක්‍ෂාව යනු තොරතුරු වල රහස්‍යභාවය, නිරවද්‍යතාවය සහ උපයෝජ්‍යතාවය සහතික කිරීම සඳහා එම තොරතුරු වත්කම් වෙත අනවසරයෙන් වන ප්‍රවේශ වීම්, හාවිත කිරීම්, වෙනස් කිරීම්, හෝ විනාශ කිරීම් වලින් තොරතුරු වත්කම් ආරක්‍ෂා කිරීමයි. මේ යටතේ තොරතුරු වත්කම් අඩංගු හෝ භාවිතා වන තොරතුරු තාක්‍ෂණ මෙවලම් පුද්ගලයන් විසින් ද්වේශසහගව සයිබර් තාක්‍ෂණය හෝ වෙනත් ක්‍රමවේදයන් භාවිතා කොට සිදු කරන හානිදායී ක්‍රියා වලින් ආරක්‍ෂා කර ගැනීම හෝ ජල ගැලීම්, ගිනිගැනීම් වැනි වෙනත් ස්වභාවික විපත් මගින් සිදු වන හානි වලින් ආරක්‍ෂා කර ගැනීමත් ඇතුළත් වේ.

තොරතුරු වත්කම් (Information Assets)

තොරතුරු තාක්‍ෂණ වත්කම් යනු ආයතනයට වටිනාකමක් ඇති තොරතුරු හෝ දත්ත වේ. විද්‍යුත් ආකෘතියකින් ලබා ගත හැකි ලේඛන, දත්තසමුදා වාර්තා මෙන්ම කඩදාසි ආකෘතියෙන් ලබා ගත හැකි ලේඛන මෙයට ඇතුළත් වේ. තොරතුරු වත්කම් සඳහා උදාහරණ : වචන ගොනුව, රූප, දත්ත ගබඩාවක සේවකයින්ගේ පුද්ගලික වාර්තාව

තොරතුරු තාක්‍ෂණ වත්කම් (IT Assets)

තොරතුරු තාක්‍ෂණ වත්කම් යනු ආයතනයට වටිනාකමක් ඇති ඕනෑම තොරතුරු තාක්‍ෂණ උපකරණ තොරතුරු පද්ධතිය, මෘදුකාංග, ගබඩා මාධ්‍ය වේ. තොරතුරු තාක්‍ෂණ වත්කම් සඳහා උදාහරණ වන්නේ පරිගණක, සේවාදායක පරිගණක, රවුටර, දෘඪ තැටි, ජාල, මෘදුකාංග, තොරතුරු පද්ධති සහ එහි සංරචක වේ.

ආක්‍රමණ හඳුනාගැනීමේ පද්ධති හා ආක්‍රමණය වැළැක්වීමේ පද්ධති (Intrusion Detection and Prevention Systems)

ආක්‍රමණ හඳුනාගැනීමේ පද්ධති (Intrusion Detection Systems) යනු, සයිබර් ප්‍රහාර හඳුනා ගැනීම සඳහා ජාල විශ්ලේෂණය කරන මෙවලම් වේ. ආක්‍රමණය වැළැක්වීමේ පද්ධති :ඔබ්එරම්සදබ ජරුඩැබඑසදබ්*ගිඑෆ්පී* යනු සයිබර් ප්‍රහාර හඳුනා ගැනීම සඳහා ජාල විශ්ලේෂණයකර ඒ මත පදනම්ව සයිබර් ප්‍රහාර වලක්වනු ලබන මෙවලම් වේ.

තොරතුරුවල නිරවද්‍යතාවය (Integrity of Information)

නිරවද්‍යතාවය යනු නුසුදුසු වෙනස් කිරීම්වලට එරෙහිව තොරතුරු ආරක්‍ෂා කිරීමයි. මෙමගින් තොරතුරු එහි මුල් ස්වරූපයෙන් පවතින බව සහතික කරයි.

නිල විද්‍යුත් තැපෑල (Official Email)

නිල විද්‍යුත් තැපෑල යනු "gov.lk" යන වසම් නාමය සහිත රජය විසින් සපයන ලද විද්‍යුත් තැපෑලේ ගිණුම් වේ.

<p>පෞද්ගලික මේසය (Private Cloud)</p>	<p>තෝරාගත් පරිශීලකයින් සඳහා පමණක් අන්තර්ජාලය හරහා හෝ පුද්ගලික අභ්‍යන්තර ජාලයක් හරහා ලබාදෙන සේවාවන්. උදා: ලංකා රාජ්‍ය මේසය</p>
<p>පොදු මේසය (Public Cloud)</p>	<p>මේසගත සේවා යනු ඒවා මිලදී ගැනීමට කැමති ඕනෑම කෙනෙකුට ලබා ගත හැකි සේවා වේ.</p>
<p>ප්‍රතිසාධන ලක්ෂ්‍ය අරමුණ (Recovery Point Objective: RPO)</p>	<p>ප්‍රතිසාධන ලක්ෂ්‍ය අරමුණ යනු ආයතනය කොපමණ වාරයක් උපස්ථ ගත යුතුද යන්න පිළිබඳ මිනුමක් වන අතර, එය ප්‍රතිසාධන දත්ත යාවත්කාලීන කරන්නේ කෙසේද යන්න පිළිබඳ අගමීමක් ලබා දෙයි. එය දත්ත ප්‍රතිසාධනය කිරීමට පිළිගත හැකි මුල්ම කාලය (earliest possible time) පෙන්වනු ලබයි. උදාහරණයක් ලෙස, උපස්ථ අතර ව්‍යසනයක් සිදුවුවහොත්, ආයතනය විනාඩි 2 ක දත්ත හෝ පැය 2 ක දත්ත හෝ සම්පූර්ණ දිනයක දත්ත අහිමි කර ගත හැකිද යන්න පිළිබඳ මිනුමක් වේ.</p>
<p>ප්‍රතිසාධන කාල අරමුණ (Recovery Time Objective: RTO)</p>	<p>ප්‍රතිසාධන කාල අරමුණ යනු ආයතනයකට දරාගත හැකි බිඳවැටීම් කාලයයි.</p>
<p>පද්ධති ශක්තිමත් කිරීම (Systems Hardening)</p>	<p>පද්ධති ශක්තිමත් කිරීම යනු තොරතුරු තාක්ෂණ අවදානම සහ අනවසර පුද්ගලයන්ට නතු වීමේ හැකියාව අවම කිරීම සඳහා පෙරනිමි වින්‍යාසය සහ සැකසුම් වෙනස් කිරීම මගින් පද්ධතියක් සුරක්ෂිත කිරීමේ ක්‍රියාවලියයි.</p>
<p>තනාසම පෞද්ගලික ජාල (Virtual Private Network)</p>	<p>තනාසම පෞද්ගලික ජාල යනු අන්තර්ජාලය හරහා දත්ත සන්නිවේදනය කිරීම සඳහා සංකේතාත්මක වැනලයක් භාවිතා කිරීමෙන් ආරක්ෂිත සම්බන්ධතාවයක් ස්ථාපිත කිරීමයි.</p>

භාවිත ලේඛන

1. තොරතුරු හා සයිබර් ආරක්‍ෂණ මාර්ගෝපදේශය, ශ්‍රී ලංකා සර්ව ආයතනය විසින් 2002 දී ප්‍රකාශයට පත්කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.
2. අවම තොරතුරු ආරක්‍ෂණ ප්‍රමිතීන්, ශ්‍රී ලංකා සර්ව ආයතනය විසින් 2021 දී ප්‍රකාශයට පත් කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.
3. ශ්‍රී ලංකාවේ තොරතුරු සහ සයිබර් ආරක්‍ෂණ උපායමාර්ගය (2019:2023) ශ්‍රී ලංකා සර්ව ආයතනය විසින් 2019 දී ප්‍රකාශයට පත් කරන ලදී. මෙය <https://cert.gov.lk/documents/NCSStrategy.pdf> යන වෙබ් අඩවියෙන් බාගත කළ හැක.
4. සයිබර් ආරක්‍ෂණ රාමුව, එක්සත් ජනපද ජාතික ප්‍රමිති සහ තාක්‍ෂණ ආයතනය විසින් ප්‍රකාශයට පත් කරන ලදී. මෙම ලේඛනය <https://www.nist.gov/cyberframework/online-learning/five-functions> යන වෙබ් ලිපිනය මගින් බාගත කළ හැක.
5. නිවසේ සිට වැඩ කිරීම සඳහා තොරතුරු ආරක්‍ෂණ මාර්ගෝපදේශය, ශ්‍රී ලංකා සර්ව ආයතනය විසින් ප්‍රකාශනය කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් ලිපිනය මගින් බාගත කළ හැක.
6. රාජ්‍ය ආයතන සඳහා සම්පාදිත වෙබ් අඩවි ආරක්‍ෂක මාර්ගෝපදේශය ශ්‍රී ලංකා සර්ව ආයතනය විසින් 2022 දී ප්‍රකාශයට පත් කරන ලදී. මෙය www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.
7. රාජ්‍ය ආයතන සඳහා සම්පාදිත වෙබ් යෙදවුම් ආරක්‍ෂණ මාර්ගෝපදේශය ශ්‍රී ලංකා සර්ව ආයතනය විසින් 2022 දී ප්‍රකාශයට පත් කරන ලදී. www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.
8. වෙබ් යෙදවුම් ආරක්‍ෂාව සඳහා සම්පාදිත තාක්‍ෂණික මාර්ගෝපදේශය ශ්‍රී ලංකා සර්ව ආයතනය විසින් 2022 දී ප්‍රකාශයට පත් කරන ලදී. www.onlinesafety.lk යන වෙබ් අඩවියෙන් බාගත කළ හැක.
9. ජාත්‍යන්තර ප්‍රමිති සංවිධානය : 27002 (2013) : තොරතුරු තාක්‍ෂණය - ආරක්‍ෂක ශිල්පීය ක්‍රම - තොරතුරු ආරක්‍ෂණ කළමනාකරණ පද්ධති - අවශ්‍යතා. මෙය <https://www.iso.org>



அரசாங்க
நிறுவனங்களுக்கான
தகவல் மற்றும் இணைய
பாதுகாப்பு கொள்கை

(உ) இலங்கை சேர்ட் 2022. முழுப் பதிப்புரிமை உடையது.

அரசாங்க முகவராண்மைக்கான தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கை
- தமிழ் பதிப்பு

முதலாவது பதிப்பு : 2023 ஜனவரி

அமைச்சரவையானது 2022 ஆகஸ்ட் 22 ஆம் திகதியிலிருந்து பயனுறுதியாகும் வகையில் இந்தக் கொள்கையினை அமுல்படுத்துவதற்கும் வலுவூட்டுவதற்குமான அங்கீகாரத்தினை வழங்கியுள்ளது.

ஆவண வகையீடு : பொது

வெளியீடு:

ஆராய்ச்சி, கொள்கை மற்றும் கருத்திட்டப் பிரிவு

இலங்கை சேர்ட்

அறை 4-112இ பண்டாரநாயக்க ஞாபகார்த்த சர்வதேச மாநாட்டு மண்டபம்,

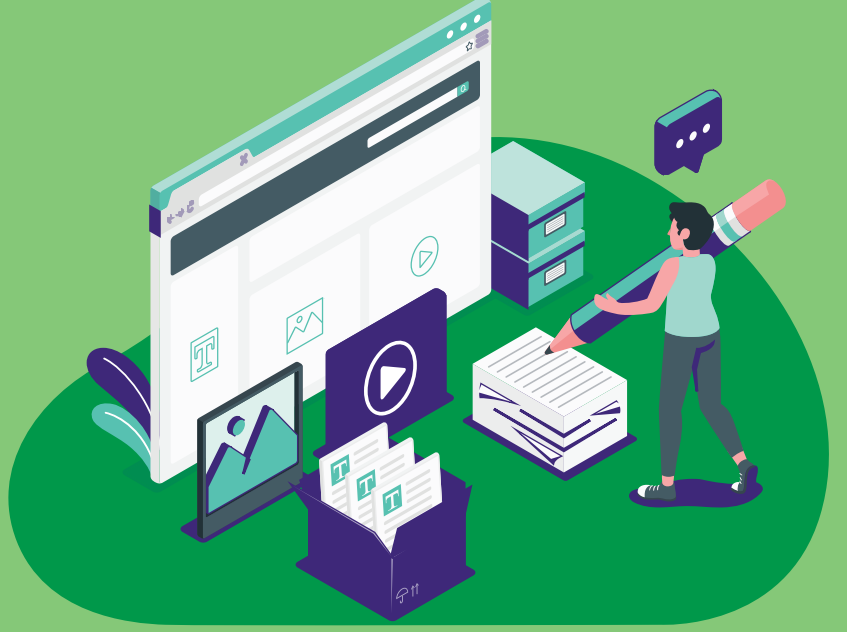
பௌத்தாலோக மாவத்தை, கொழும்பு 7.

இலங்கை

தொலைபேசி : +94 11 269 1692, **தொலைநகல் :** +94 11 269 1064

மின்னஞ்சல் : cert@cert.gov.lk

இணையத்தளம் : www.cert.gov.lk | www.onlinesafety.lk



பொருளடக்கம்

1.	.அறிமுகம்	147
2.	தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கை கட்டமைப்பு	149
3.	தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கை	152
3.1	அறிமுகம்	153
3.2	கொள்கையின் நோக்கம்	158
4.	கொள்கை கூற்றுக்கள்	158
4.1	தகவல் பாதுகாப்பு நிருவாக முறைமை	158
4.1.1.	தலைமைத்துவம் மீதான கொள்கை	159
4.1.2.	பாதுகாப்பு நிறுவன கட்டமைப்பு மீதான கொள்கை	159
(அ)	தகவல் பாதுகாப்பு உத்தியோகத்தர்	
	தொழிற்பாடு மீதான கொள்கை	162
4.1.4.	இடர் முகாமைத்துவ குழு மீதான கொள்கை	161
4.1.5.	இறுதிப் பயனர் பொறுப்புக்கள் மீதான கொள்கை	161
4.1.6.	திறன் விருத்தி மீதான கொள்கை	162
4.1.7.	பதவியினரின் பாதுகாப்பு ஆனமதி மீதான கொள்கை	162

	4.1.8.	மூலோபாய சீரமைப்பு மீதான கொள்கை	163
	4.1.9.	செயல்திட்டங்கள் மீதான கொள்கை	163
4.2.		சொத்துக்கள், உரிமையாளர்கள், பயனர்கள் மற்றும் இடர்களை அடையாளங் காணுதல்	164
	4.2.1.	தகவல் சொத்துக்கள் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை அடையாளங் காணுதல் மீதான கொள்கை	164
	4.2.2.	முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு அடையாளங் காணுதல் மீதான கொள்கை	165
	4.2.3.	சொத்து உரிமையாளர்கள்இ பாதுகாவலர்கள் மற்றும் பயனர்களின் பொறுப்புக்கள் மீதான கொள்கை.	166
	4.2.4.	தகவல் சொத்துக்கள் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்கள பதிவேட்டினை பேணுவது மீதான கொள்கை	166
	4.2.5.	இடர் மதிப்பீடுகள் மீதான கொள்கை	167
	4.2.6.	சொத்துக்களின் வகையீடு மீதான கொள்கை.	168
4.3.		சொத்துக்களின் பாதுகாப்பு	168
	4.3.1.	ஓய்விலுள்ள தரவினைப் பாதுகாத்தல் மீதான கொள்கை	169
	4.3.2.	பரிமாற்றப்படுகின்ற தரவினைப் பாதுகாத்தல் மீதான கொள்கை	169
	4.3.3.	பௌதீக ரீதியான பாதுகாப்பு மீதான கொள்கை	169
	4.3.4.	இனங் காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடு மீதான கொள்கை	171
	4.3.5.	வலுவான உறுதிப்படுத்தல் மீதான கொள்கை	172
	4.3.6.	கணனி கிளவுட் மற்றும் கணினி தரவு இறையாண்மை மீதான கொள்கை.	173
	4.3.7.	உரிமம் பெற்ற மென்பொருள் மற்றும் இணைப்புக்களை இற்றைப்படுத்தல் மீதான கொள்கை	174
	4.3.8.	தீம்பொருள் எதிர்ப்பு மீதான கொள்கை.	172
	4.3.9.	உத்தியோகபூர்வ மின்னஞ்சல்கள் மீதான கொள்கை	176
	4.3.10.	மின்னஞ்சல்களின் பாதுகாப்பு மீதான கொள்கை	176
	4.3.11.	டிஜிட்டல் கையொப்பங்கள் மீதான கொள்கை	176
	4.3.12.	சுற்றுவட்ட பாதுகாப்பு கட்டுப்பாடகன் மீதான கொள்கை	177
	4.3.13.	தொலைபேசி அணுகலைப் பெறுவது தொடர்பான கொள்கை	177
	4.3.14.	காப்பு மூலோபாயம் மீதான கொள்கை	178
	4.3.15.	அரசாங்க நிறுவனங்களால் வழங்கப்பட்ட சொத்துக்களின் பாதுகாப்பு மீதான கொள்கை	179
	4.3.16.	வடிவமைப்பு மூலமான பாதுகாப்பு தொடர்பான கொள்கை	182
	4.3.17.	சொத்துக்களைப் பாதுகாப்பாக அகற்றுவது மீதான கொள்கை	181
	4.3.18.	உள்ளக தகவல், இணைய பாதுகாப்பு கணக்காய்வுத் திட்டம் மீதான கொள்கை	182

4.3.19.	பயன்படுத்துவதற்கு முன்னரான கணக்காய்வு தொடர்பான கொள்கை	182
4.3.20.	முறைமைகளினைக் கடினமாக்குவது மீதான கொள்கை	183
4.3.21.	வீட்டிலிருந்து பணியாற்றுவது தொடர்பான கொள்கை	184
4.3.22.	உத்தியோகபூரவ வேலைக்காக தமது சொந்த வாகனத்தினைப் பயன்படுத்துதல்	184
4.3.23.	பாதுகாப்பற்ற வலையமைப்புக்களினைப் பயன்படுத்துவது மீதான கொள்கை	185
4.3.24.	வழங்குனர் முகாமைத்துவம் மீதான கொள்கை.	185
4.3.25.	பதிவுகளை மீளாய்வு செய்வது தொடர்பான கொள்கை.	186
4.4.3.	நிகழ்வுகள் தொடர்பான நிகழ்வுகளை கண்காணித்தல் மீதான கொள்கை	189
4.4.4.	இலங்கை சேர்ட்டிற்கு நிகழ்வுகளை அறிக்கையிடுவது மீதான கொள்கை	189
4.5.	நிகழ்வுகளுக்குப் பதிலளித்தல்	189
4.5.1.	நிகழ்விற்குப் பதிலளிக்கும் திட்டம் மீதான கொள்கை	190
4.5.2.	நிகழ்வுக்குப் பதிலளிக்கும் திட்டத்தைச் செயற்படுத்துவது மீதான கொள்கை	190
4.5.3.	தடையவியல் விசாரணைகள் மீதான கொள்கை	191
4.6.	இயல்பான நடவடிக்கைகளினை மீட்டெடுப்பது தொடர்பான கொள்கை	92
4.6.1.	அனர்த்த மீட்புத் திட்டம் மீதான கொள்கை.	93
4.6.2.	அனர்த்த மீட்புத்திட்டத்தை செயற்படுத்தவது மீதான கொள்கை	93
4.6.3.	நெருக்கடி நிலையின் தொடர்பாடல் மீதான கொள்கை	93
5.	முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டிய கொள்கைகள்	94
6.	தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கையினை கண்காணித்தல் மற்றும் மதிப்பாய்வு செய்வதற்கான முறை	98
	சொற்களஞ்சியம்	209
	உசாத்துணைகள்	213





1. அறிமுகம்

- 1.1. இலங்கையில் உள்ள பல அரசாங்க நிறுவனங்கள் தற்போது டிஜிட்டல் முறைமைகள் மற்றும் உட்கட்டமைப்புகளின் நம்பகமான செயற்பாடுகளில் தங்கியுள்ளன. எவ்வாறாயினும், தீங்கிழைக்கும் நபர்கள் இத்தகைய டிஜிட்டல் அமைப்புகளைப் பயன்படுத்தி முக்கியமான தகவல் திருட்டு நடவடிக்கைகளிலும், நாளாந்த செயற்பாடுகளில் இடையூறு விளைவிப்பதிலும் ஈடுபட்டு வருவதுடன், நிறுவனங்களின் நற்பெயருக்கும் களங்கம் விளைவிக்கின்றனர். இது பொதுமக்களின் நம்பிக்கையையும் அரசாங்க நிறுவனங்களின் மீதான நம்பிக்கையையும் இழக்க வழிவகுப்பதுடன் தேசத்தின் பாதுகாப்பு, பொருளாதாரம், உள்ளக பாதுகாப்பு மற்றும் பொது மக்களின் நல்வாழ்விலும் ஆபத்தினை ஏற்படுத்துகின்றன.
- 1.2. இந்தத் தகவல் மற்றும் சைபர் பாதுகாப்பு அபாயங்களைத் திறம்பட நிவர்த்தி செய்வதற்கும், பல்வேறு அச்சுறுத்தல்களிலிருந்து அரசாங்க நிறுவனங்களின் தகவல், டிஜிட்டல் அமைப்புகள் மற்றும் உட்கட்டமைப்பு (இனி, தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்கள்) ஆகியவற்றைப் பாதுகாப்பதற்கும், இலங்கை கணினி அவசரநிலைத் தயார்நிலை அணியானது (Sri Lanka Computer Emergency Readiness Team) இலங்கை சேர்ட் நிறுவனம் (Sri Lanka CERT) என்றும் அழைக்கப்படுகிறது, இலங்கையின் இணையவெளியைப் பாதுகாப்பதற்கான ஆணையைக் கொண்டுள்ளதுடன், அரசாங்க நிறுவனங்களின் பயன்பாட்டிற்காக தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையை உருவாக்கியுள்ளது. நிறுவன மட்டத்தில் தகவல் மற்றும் சைபர் பாதுகாப்புத் திட்டத்தைச் செயற்படுத்துவதற்கான ஆபத்து அடிப்படையிலான அணுகுமுறையை இந்தக் கொள்கை

வழங்குகிறது. சொத்துக்களைக் கண்டறிந்து பாதுகாப்பதற்கும், தகவல் பாதுகாப்பு சம்பவங்களை சரியான நேரத்தில் கண்டறிவதற்கும், சம்பவங்களுக்கு பதிலளிப்பதற்கும், திறமையான மற்றும் பயனுள்ள முறையில் இணைய தாக்குதல்களில் இருந்து மீள்வதற்கும் நிறுவனங்கள் செயல்படுத்த வேண்டிய செயல்களின் தொகுப்பையும் இது வழங்குகிறது.

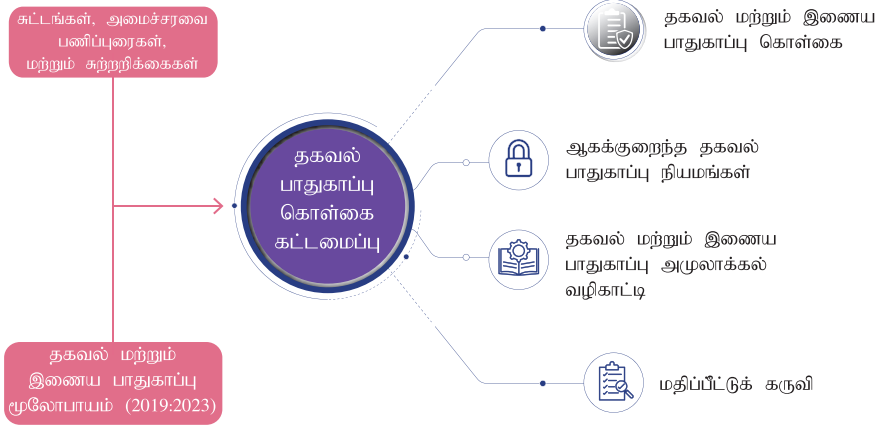
- 1.3. அரசாங்க நிறுவனங்களுக்கான தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கையானது இலங்கையின் தகவல் மற்றும் இணைய பாதுகாப்பு மூலோபாயத்தின் (2019: 2023) நடைமுறைக்கு இணங்க உருவாக்கப்பட்டுள்ளது. இது சர்வதேச நியமங்கள் மற்றும் தரநிலைப்படுத்தலுக்கான சர்வதேச அமைப்பு (International Organization for Standardization) மற்றும் அமெரிக்காவின் தேசிய தரநிலைகள் மற்றும் தொழில்நுட்ப நிறுவனம் (National Institute of Standards and Technology) போன்ற சிறந்த நடைமுறைகளின் அடிப்படையில் உருவாக்கப்பட்டது, மேலும் அரசாங்கத்தின் தகவல் பாதுகாப்பு நிபுணர்கள் மற்றும் மூத்த அதிகாரிகளால் விரிவாக மீளாய்வு செய்யப்பட்டது.
- 1.3. 2016 ஆம் ஆண்டின் 12 ஆம் இலக்க தகவல் அறியும் உரிமைச் சட்டத்தில் "பகிரங்க அதிகாரசபை' என வரையறுக்கப்பட்டுள்ள அனைத்து அரசு நிறுவனங்களும் இந்தக் கொள்கைக்கு இணங்குதல் வேண்டும். அரசாங்க நிறுவனங்களின் தலைவர்கள் தங்கள் நிறுவனங்களுக்குள் பாதுகாப்பான மற்றும் திறமையான சேவையை வழங்குவதை உறுதி செய்வதற்கான கொள்கையை செயற்படுத்துவதற்கு பொறுப்பாகவும் இருத்தல் வேண்டும். இலங்கை சேர்ட் நிறுவனம் கொள்கையை நடைமுறைப்படுத்துவதில் அனைத்து அரசாங்க நிறுவனங்களுக்கும் சிபாரிசுகளை எளிதாக வழங்குவதுடன், வருடாந்த அடிப்படையில் கொள்கையை நடைமுறைப்படுத்துவது தொடர்பில் நிறுவனங்களின் செயல்திறனை மதிப்பீடு செய்யும்.





2. தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கை கட்டமைப்பு

- 2.1. தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கைக் கட்டமைப்பானது, தகவல் மற்றும் இணைய பாதுகாப்புத் திட்டங்களைத் திறமையான மற்றும் பயனுள்ள முறையில் செயற்படுத்துவதற்கு அரசாங்க நிறுவனங்களுக்குத் தேவையான வழிகாட்டுதல்களினைக் கொண்ட உள்ளடக்கத்தை அறிமுகப்படுத்துகிறது. இது அரசாங்க நிறுவனங்களுக்கான (அ) தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கை (Information and Cyber Security Policy) (ஆ) குறைந்தபட்ச தகவல் பாதுகாப்புத் தரநிலைகள் (Minimum Information Security Standards) (இ) தகவல் மற்றும் சைபர் பாதுகாப்பு நடைமுறைப்படுத்தல் வழிகாட்டி (Information and Cyber Security Implementation Guide) மற்றும் (ஈ) தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கையின் அமுலாக்கத்தைக் கண்காணித்து மதிப்பாய்வு (Monitoring and Evaluation Methodology) செய்வதற்கான ஒரு முறை ஆகியவற்றினை உள்ளடக்குகின்றது. உரு - 1 ஆனது தகவல் பாதுகாப்பு கொள்கை கட்டமைப்பின் கண்ணோட்டத்தினை வழங்குகின்றது.



உரு:1 தகவல் பாதுகாப்பு கொள்கை கட்டமைப்பு

2.2. தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கை கட்டமைப்பில் பின்வருவன உள்ளடங்குகின்றன:

- அ. தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கை (Information and Cyber Security Policy): கொள்கை கட்டமைப்பின் முக்கிய அங்கமாக தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கை விளங்குகின்றது. இது அரசாங்க நிறுவனங்கள் இணங்க வேண்டிய கொள்கைகளின் தொகுப்பை வழங்குகிறது. அத்தியாவசிய கட்டுப்பாடுகளை கோட்டுக் காட்டுவதுடன் தகவல் பாதுகாப்பு நிகழ்வுகளிலிருந்து தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாப்பதில் அரசாங்க நிறுவனங்களுக்கு வழிகாட்டுதல்களையும் வழங்குகிறது.
- ஆ. குறைந்தபட்ச தகவல் பாதுகாப்பு நியமங்கள் (Minimum Information Security Standards): அரசு நிறுவனங்களால் கடைபிடிக்கப்படும் தகவல் பாதுகாப்பு கட்டுப்பாடுகளின் குறைந்தபட்ச ஏற்றுக் கொள்ளக்கூடிய நியமங்களை இந்த ஆவணம் கோட்டுக் காட்டுகிறது. இலங்கை சேர்ட்டினது www.onlinesafety.lk இணையத்தளத்தில் உசாத்துணைக்காக குறைந்தபட்ச தகவல் பாதுகாப்பு நியமங்கள் உள்ளன.
- இ. தகவல் மற்றும் இணைய பாதுகாப்பு அமுலாக்கல் வழிகாட்டி (Information and Cyber Security Implementation Guide): இது கொள்கையை செயல்படுத்துவதில் குறிப்பிட்ட விவரங்கள் தேவைப்படும் ஊழியர்கள் மற்றும் அக்கறைதாரர்களுக்கு விரிவான வழிமுறைகளை வழங்குகிறது. இந்த வழிகாட்டியில் தகவல் பாதுகாப்பு நிருவாகக் கட்டமைப்பை நிறுவுதல், சொத்துக்களின் வகைப்பாடு, இடர் மேலாண்மை, சொத்துக்களின் பாதுகாப்பு, பேரிடர் மீட்பு மற்றும் காப்பு

பிரதிகள், சம்பவங்களை நிருவகித்தல், அடையாளம் மற்றும் அணுகல் கட்டுப்பாடு மற்றும் பலவற்றின் வழிமுறைகள் உள்ளன. இந்த ஆவணம் இலங்கை சேர்ட் நிறுவனத்தின் www.onlinesafety.lk எனும் இணையத்தளத்தில் உடனடியாகக் காணப்படும் உள்ளது.

ஈ. கண்காணிப்பு மற்றும் மதிப்பீட்டு முறை (Monitoring and Evaluation Methodology): இது கொள்கையை ஏற்றுக் கொள்வதில் அரசு நிறுவனங்களின் தயார நிலையை மதிப்பிடுவதற்கும், அதன் செயலாக்கத்தின் முன்னேற்றத்தை மதிப்பிடுவதற்கும் மதிப்பீட்டு அளவுகோல்களை வழங்குகிறது. இலங்கை சேர்ட் நிறுவனம், இந்த ஆவணத்தின் 6 ஆவது பிரிவில் குறிப்பிடப்பட்டுள்ள வழிமுறைகளைப் பயன்படுத்தி, அரசாங்க நிறுவனங்களின் தகவல் மற்றும் இணைய பாதுகாப்பு நடவடிக்கைகளின் முதிர்ச்சியை முன் வரையறுக்கப்பட்ட காலக்கெடுவிற்குள் மதிப்பீடு செய்கிறது.

2.3. தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கை கட்டமைப்பானது தொடர்புடைய சட்டங்கள் மற்றும் ஒழுங்குமுறைகள், இலங்கையின் தகவல் மற்றும் இணைய பாதுகாப்பு மூலோபாயம், இ-அரசாங்க கொள்கைகள் மற்றும் அமைச்சரவை உத்தரவுகளால் நிருவகிக்கப்படுகிறது.





3. தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கை

3.1. அறிமுகம்

3.1.1. தகவல் மற்றும் இணைய பாதுகாப்பு என்பது தகவல்களின் ரகசியத்தன்மை (Confidentiality) நேர்மைத்தன்மை (Integrity) மற்றும் கிடைக்கும் தன்மையை (Availability) உறுதி செய்வதற்காக அங்கீகரிக்கப்படாத அணுகல், பயன்பாடு, மாற்றுதல், மற்றும் அழித்தல் ஆகியவற்றிலிருந்து தகவல் சொத்துக்களைப் பாதுகாப்பதைக் குறிக்கிறது. இணைய தொழில்நுட்பம் அல்லது ஏனைய வழிகளைப் பயன்படுத்தி தனிநபர்களின் தீங்கிழைக்கும் செயல்களிலிருந்து தகவல் சொத்துக்களைக் கொண்ட தகவல் சொத்துக்களைப் பாதுகாத்தல் மற்றும் வெள்ளம் மற்றும் தீ போன்ற ஏனைய இயற்கை பேரழிவுகளிலிருந்து சொத்துக்களைப் பாதுகாத்தல் ஆகியவை இதில் உள்ளடங்கும்.

3.1.2. இந்தச் சூழலில், தனிநபர்களின் தீங்கிழைக்கும் செயற்பாடுகள் மற்றும் இயற்கை பேரிடர்களால் ஏற்படும் சேதங்களிலிருந்து தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாப்பதற்கு அரசு நிறுவனங்கள் பின்பற்ற வேண்டிய விதிகள் மற்றும் வழிகாட்டுதல்களின் தொகுப்பை அறிமுகப்படுத்துவதே தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கையின் முக்கிய நோக்கமாகும்.

3.1.3 கொள்கையின் ஏனைய நோக்கங்கள்

- அ. பொதுத் துறை முழுவதும் பொதுவான தகவல் மற்றும் இணைய பாதுகாப்பு நியமத்தினை நிறுவுதல்,
- ஆ. தகவல் அமைப்புகள் மற்றும் டிஜிற்றல் உட்கட்டமைப்பின் வடிவமைப்பு, செயல்படுத்தல், பயன்பாடு மற்றும் செயல்பாடுகள் தொடர்பான பாதுகாப்பு தரநிலைகள், விதிகள் மற்றும் செயல்முறைகளை கட்டாயப்படுத்துவதன் மூலம் தகவல் மற்றும் சைபர் பாதுகாப்பு நிகழ்வுகளுக்கு அரசாங்க நிறுவனங்களின் பின்னடைவை வலுப்படுத்துதல்,
- இ. தகவல் மற்றும் இணைய பாதுகாப்பு சம்பவங்களை சரியான நேரத்தில் கண்டறிவதற்கான ஒரு பொறிமுறையை நிறுவுதல், நிறுவனங்களுக்கு இதுபோன்ற சம்பவங்களின் தாக்கத்தை குறைத்தல் மற்றும் இதுபோன்ற சம்பவங்களால் பாதிக்கப்பட்ட எந்தவொரு திறன்கள் அல்லது சேவைகளை திறமையாக மீட்டெடுக்கவும், மற்றும்
- ஈ. தகவல் மற்றும் இணைய பாதுகாப்பின் விதிகள், சிறந்த நடைமுறைகள், நியமங்கள் மற்றும் செயல்முறைகள் குறித்து ஊழியர்களுக்குக் கற்பித்தல் மற்றும் நிறுவனத்தின் பாதுகாப்பு நிலை குறித்த ஊழியர்களுக்கு நம்பிக்கையை ஏற்படுத்துதல்.

3.1.4. இந்தக் கொள்கை எளிய மொழியில் எழுதப்பட்டுள்ளது. அனைத்து ஊழியர்களும் தொடர்புடைய மூன்றாம் தர்ப்பு சேவை வழங்குநர்களும், அவர்கள் பாடம் பற்றிய அறிவைப் பொருட்படுத்தாமல், கொள்கையைச் செயற்படுத்துவது தொடர்பாக அவர்களின் பொறுப்புகள் மற்றும் கடமைகளைப் புரிந்து கொள்ள முடியும்.

3.1.5. நல்ல தகவல் பாதுகாப்பு நடைமுறைகளை ஆதரிப்பதற்கு அரசு நிறுவனங்களுக்கு தொழில்நுட்ப மற்றும் பாதுகாப்பு வழிகாட்டுதலை வழங்க இந்த ஆணை அவ்வப்போது புதுப்பிக்கப்படும்.

3.2. கொள்கையின் நோக்கம்

3.2.1. இந்தக் கொள்கையானது அமைச்சுக்கள், திணைக்களங்கள், பொதுக் கூட்டுத்தாபனங்கள், உள்ளூராட்சி நிறுவனங்கள் மற்றும் 2016 ஆம் ஆண்டின் 12 ஆம் இலக்க தகவலறியும் உரிமைச் சட்டத்தில் “பகிரங்க அதிகாரசபை” என வரையறுக்கப்பட்டுள்ள எந்தவொரு அரசு நிறுவனத்திற்கும் பொருந்தும். இந்தக் கொள்கையானது அரசு நிறுவனங்களின் சார்பில் தகவல் தொழில்நுட்ப சேவைகளை நிருவகிக்கும் உரிய மூன்றாம் தர்ப்பு சேவை வழங்குநர்களுக்கும் ஏற்புடையதாகத் வேண்டும்.

3.2.2. இங்கு வழங்கப்பட்ட கொள்கைகள் இரண்டு நிலைகளின் அடிப்படையில் உருவாக்கப்பட்டுள்ளன. அவை, (அ) அனைத்து அரசு நிறுவனங்களுக்கும் பொருந்தும் கொள்கைகள், மற்றும் (ஆ) முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கு பொருந்தும் கொள்கைகள். முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்கள் இந்தக் கொள்கையில் குறிப்பிடப்பட்டுள்ள அனைத்து கொள்கைகளுக்கும் இணங்குதல் வேண்டும். ஏனைய நிறுவனங்கள் அனைத்து அரசு நிறுவனங்களுக்கும் ஏற்புடையதான கொள்கைகளுடன் இணங்கி நடத்தல் வேண்டும். எவ்வாறாயினும், சிறந்த பாதுகாப்பிற்காக முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கு பொருந்தக்கூடிய கொள்கைகளுக்கு இணங்கும் வகையில் ஏனைய நிறுவனங்களுக்கு பரிந்துரைக்கப்படுகிறது.

- 3.2.3 முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்கள், தேசிய பாதுகாப்பு, நிருவாகம், பொருளாதாரம், சுகாதாரம் மற்றும் சமூக நல்வாழ்வு ஆகியவற்றில் பலவினமான தாக்கத்தை ஏற்படுத்தும் தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை பராமரிக்கும் நிறுவனங்களாக வரையறுக்கப்படுகின்றன. முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களின் பட்டியல் இலங்கை சேர்ட் நிறுவனத்தினால் வெளியிடப்படும்.
- 3.2.4. இந்தக் கொள்கையானது தகவல் மற்றும் இணைய பாதுகாப்பு நிருவாகக் கோட்பாடுகள் மற்றும் அமெரிக்காவின் தேசிய நியமங்கள் மற்றும் தொழில்நுட்ப நிறுவனத்தினால் முன்மொழியப்பட்ட பல ஒரே நேரத்தில் மற்றும் தொடர்ச்சியான தகவல் பாதுகாப்பு செயற்பாடுகளின் அடிப்படையில் உருவாக்கப்பட்டது. இந்த செயற்பாடுகளில் (அ) நிறுவனத்தின் தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை அடையாளம் காணுதல் (உதாரணம். தரவு, தகவல், கணினிகள் மற்றும் ஏனைய டிஜிற்றல் உட்கட்டமைப்பு), (ஆ) சொத்துக்களைப் பாதுகாக்க தேவையான நடவடிக்கைகளை எடுத்தல், (இ) தகவல் மற்றும் இணைய பாதுகாப்பு சம்பவங்களைக் கண்டறிதல், (ஈ) சம்பவங்களுக்கு பதிலளிப்பது, மற்றும் (இ) ஒரு சம்பவத்தால் பாதிக்கப்பட்ட சேவையை மீட்டெடுத்தல். அரசாங்க நிறுவனத்திற்குள் தகவல் மற்றும் இணைய பாதுகாப்பு தொடர்பான நடவடிக்கைகளை இயக்குவதற்கும் கட்டுப்படுத்துவதற்கும் தகவல் மற்றும் இணைய பாதுகாப்பு நிருவாக பொறிமுறையும் இந்தக் கொள்கையில் அடங்கும். தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாக்க அரசு நிறுவனங்கள் பின்பற்ற வேண்டிய செயற்பாடுகளை படம் 2 காட்டுகிறது.





உரு - 2 - தகவல் மற்றும் இணைய பாதுகாப்புக்கான படிமுறைகள்

3.2.5. தகவல் பாதுகாப்பு செயற்பாடுகளின் அடிப்படையில் உருவாக்கப்பட்டுள்ள 3.2.4 இல் குறிப்பிடப்பட்டுள்ளபடி, இந்தக் கொள்கையைச் செயல்படுத்துவதன் மூலம் சொத்துக்களைப் பாதுகாப்பதற்காக ஒருநிறுவனத்தால் எடுக்கப்படும் நடவடிக்கைகள் கீழே விவரிக்கப்பட்டுள்ளன.

- அ. தகவல் மற்றும் இணைய பாதுகாப்பு நிருவாகம் (Information and Cyber Security Governance): தகவல் மற்றும் இணைய பாதுகாப்பு நிருவாகம் என்பது பொதுவாக ஒரு நிறுவனத்தின் தகவல் மற்றும் இணைய பாதுகாப்பை இயக்கும் மற்றும் கட்டுப்படுத்தும் நிருவாக பொறிமுறையை குறிப்பிடுகின்றது. தகவல் மற்றும் இணைய பாதுகாப்பு நிருவாகத்தை செயற்படுத்த, நிறுவனங்கள் ஒரு பாதுகாப்பு நிறுவன கட்டமைப்பை நிறுவுதல் வேண்டும் என்பதுடன் தகவல் பாதுகாப்பிற்கு பொறுப்பு வாய்ந்த அதிகாரிகளை நியமித்தலும் வேண்டும். அத்தகைய அதிகாரிகளின் திறனை மேம்படுத்துதல், நிறுவனங்களின் தகவல் மற்றும் இணைய பாதுகாப்பு நோக்கங்களை வரையறுத்தல், செயல் திட்டங்களை உருவாக்குதல். மற்றும் தொடர்புடைய நடவடிக்கைகளுக்கான ஆதாரங்களை ஒதுக்குதல். (பிரிவு 4.1 இணைப் பார்க்கவும்).
- ஆ. செயற்பாடுகளை அடையாளம் காணுதல் (Identify Function): தரவு, தகவல், கணினிகள், அமைப்புகள் மற்றும் டிஜிற்றல் உட்கட்டமைப்பு போன்ற சொத்துக்களை அடையாளம் காணவும், அந்த சொத்துக்களுடன் தொடர்புடைய அபாயங்களைக் கண்டறிந்து திறம்பட நிருவகிக்கவும் இது அரசாங்க நிறுவனங்களுக்கு உதவுகிறது (பிரிவு 4.2 இணைப் பார்க்கவும்).
- இ. பாதுகாப்பு செயற்பாடு (Protect Function): தடையற்ற சேவைகளை வழங்குவதற்காக தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களின் பாதுகாப்பை உறுதி செய்ய தேவையான பொருத்தமான கட்டுப்பாடுகளை பாதுகாக்கும் செயற்பாடு கோடிட்டுக் காட்டுகிறது. பாதுகாப்புச் செயற்பாட்டிற்கு இணங்க, நிறுவனங்கள் சொத்துக்களுக்கான பயனர் அணுகலை நிருவகித்தல், .பயர்வால்கள் மற்றும் ஆண்டிமால்வேர் மென்பொருளை நிறுவுதல், அமைப்புகளின் கணக்காய்வுகளை நடாத்துதல், காப்புரிமை உத்தியை நிறுவுதல் மற்றும் பிரிவு 4.3 இல் குறிப்பிடப்பட்டுள்ள கொள்கைகளைச் செயற்படுத்துதல் போன்ற பொருத்தமான கட்டுப்பாடுகளை செயற்படுத்துதல் வேண்டும்.
- ஈ. கண்டறிதல் செயற்பாடு (Detect Function): கண்டறிதல் செயற்பாடு, சரியான நேரத்தில் தகவல் மற்றும் இணைய பாதுகாப்பு சம்பவங்கள் நிகழ்வதை அடையாளம் காண தேவையான செயற்பாடுகளை வரையறுக்கின்றது. கணினிகள் மற்றும் தொடர்புடைய சாதனங்கள் மூலம் உருவாக்கப்படும் பதிவுகளை ஆய்வு செய்ய நிறுவனங்கள் தகுந்த கருவிகளைப் பயன்படுத்தி சம்பவங்களை திறமையான முறையில் கண்டறிதல் வேண்டும் (பிரிவு 4.4 இணைப் பார்க்கவும்).
- உ. பதிலளிக்கும் செயற்பாடு (Respond Function): கண்டறியப்பட்ட சம்பவத்திற்கு பதிலளிக்கும் வகையில் எடுக்கப்பட வேண்டிய நடவடிக்கைகளை பதிலளிக்கும் செயற்பாடு வரையறுக்கிறது. ஒரு சம்பவத்திற்கு திறமையான மற்றும் பயனுள்ள முறையில் பதிலளிப்பதற்காக, பிரிவு 4.5 இல் வரையறுக்கப்பட்டுள்ளபடி நிறுவனங்கள் ஒரு சம்பவ பதிலளிக்கும் திட்டத்தை உருவாக்கி செயற்படுத்துதல் வேண்டும்.

ஊ. மீட்டெடுக்கும் செயற்பாடு (Recover Function): தகவல் மற்றும் இணைய பாதுகாப்புச் சம்பவத்தால் பாதிக்கப்பட்ட எந்தத் திறன்கள் அல்லது சேவைகளை மீட்டெடுப்பதற்கான பொருத்தமான செயற்பாடுகளை மீட்டெடுப்பு செயற்பாடு அடையாளம் காட்டுகின்றது. மீட்புச் செயற்பாட்டிற்கு இணங்க, நிறுவனம் பேரழிவு மீட்புத் திட்டத்தை உருவாக்கி, ஒரு சம்பவத்தின் போது இயல்பான செயற்பாடுகளை மீட்டெடுப்பதற்கான திட்டத்தை செயற்படுத்துதல் வேண்டும் (பிரிவு 4.6 இணைப் பார்க்கவும்).





4. கொள்கை கூற்றுக்கள்

அரசாங்க நிறுவனங்களுக்கான தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கையானது ஆறு முக்கிய கொள்கை விடயப் பரப்புக்களைக் கொண்டுள்ளது, அதாவது (அ) நிறுவனத்திற்குள் ஒரு தகவல் மற்றும் இணைய பாதுகாப்பு நிர்வாக அமைப்பை நிறுவுதல், (ஆ) சொத்துக்கள், சொத்து உரிமையாளர்கள், பாதுகாவலர்கள் மற்றும் இடர்களை அடையாளம் காணுதல், (இ) சொத்துக்களைப் பாதுகாத்தல், (ஈ) தகவல் மற்றும் இணைய பாதுகாப்பு சம்பவங்களை அடையாளம் காணுதல் (உ) பாதுகாப்புச் சம்பவங்களுக்குப் பதிலளிப்பது, மற்றும் (ஊ) ஒரு சம்பவத்தால் சீர்குலைந்து போன செயற்பாடுகளை மீட்டெடுத்தல். மேற்குறித்த ஆறு விடயங்கள் தொடர்பாக அரசு நிறுவனங்கள் கடைப்பிடிக்க வேண்டிய கொள்கை விடயப் பரப்புக்கள் கீழே தரப்பட்டுள்ளன.

4.1. தகவல் பாதுகாப்பு நிர்வாக முறைமை

தகவல் பாதுகாப்பு நிர்வாக முறைமையானது நிறுவனமொன்றில் தகவல் பாதுகாப்பினை நெறிமுறைப்படுத்துவதற்கும் கட்டுப்படுத்துவதற்குமான பொறிமுறை யொன்றினை முன்மொழிகின்றது. இது தகவல் பாதுகாப்பு நடவடிக்கைகள் உரிய முறையில் நிருவகிக்கப்படுவதனை உறுதி செய்வதற்குத் தேவையான தலைமைத்துவம் மற்றும் பொறுப்புக் கூறல் கட்டமைப்பு குறித்து விதித்துரைக்கின்றது. தகவல் மற்றும் சைபர் பாதுகாப்புச்

செயற்பாடுகளை நிறுவனத்தின் தொலைநோக்குப் பார்வை மற்றும் நோக்கத்துடன் சீரமைக்க வேண்டியதன் அவசியத்தையும், பொறுப்பான மற்றும் பொறுப்புள்ள அதிகாரிகளின் திறன் தகவல் மற்றும் இணைய பாதுகாப்புத் திட்டமிடல் மற்றும் இந்தக் கொள்கையை ஏற்றுக்கொள்ளும் அரசு நிறுவனங்களின் முக்கியத்துவம் ஆகியவற்றையும் இது எடுத்துக்காட்டுகின்றது.

4.1.1. தலைமைத்துவம் மீதான கொள்கை

நிறுவனத்தின் தலைமைத்துவமானது தாபனத்தின் தகவல் பாதுகாப்பு நடவடிக்கைகளுக்கான தலைமைத்துவத்தினை வழங்குவதுடன் தாபனத்தின் தகவல் மற்றும் சொத்துக்களைப்பாதுகாப்பதற்கான இறுதிப் பொறுப்புக்கும் பொறுப்புக் கூறலுக்கும் பொறுப்பு வாய்ந்ததாகும். நிறுவனத்தின் தலைமைத்துவமானது நிறுவனத்தின் நோக்கு மற்றும் செயற்பணியினை ஆதரிக்கும் தகவல் பாதுகாப்பு இலக்குகள் மற்றும் முன்னுரிமைகளை அமைக்கும் நிறுவனத்தின் தகவல் மற்றும் இணைய பாதுகாப்பு நிகழ்ச்சித்திட்டமொன்றினைத் தாபிப்பதுடன் தகவல் பாதுகாப்பு நடவடிக்கைகளை ஆதரவளிப்பதற்கும் அதனை வெற்றிகரமாக முன்னெடுப்பதற்கும் கிடைக்கக்கூடிய மூலவளங்களையும் உறுதி செய்யும்.



பயனர்கள் தகவல் பாதுகாப்புக் கொள்கைகள் மற்றும் வழிகாட்டுதல்களுக்கு இணங்க, அவர்கள் பயன்படுத்தும் தகவல் மற்றும் முறைமைகளைப் பாதுகாப்பதில் முனைப்புடன் செயற்படும் நிறுவனத்திற்குள் ஒரு தகவல் பாதுகாப்பு கலாச்சாரத்தை உருவாக்குவதற்கான தலைமைத்துவத்தை நிறுவனத்தின் தலைவர் வழங்குவார்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.1.2. பாதுகாப்பு நிறுவன கட்டமைப்பு மீதான கொள்கை

நிறுவனமானது தகவல் பாதுகாப்பு நிறுவனசார் கட்டமைப்பொன்றினைத் தாபித்தல் வேண்டும். முறைமையின் தகவல் பாதுகாப்பு நடவடிக்கைகளை இயக்கவும், வழிகாட்டவும் மற்றும் நிருவகிக்கவும், தகவல் மற்றும் இணைய பாதுகாப்பு மீறல்கள், ஊடுருவல்கள் மற்றும் குறுக்கீடுகளுக்கு எதிராக நிறுவனத்தைப் பாதுகாக்கவும் இந்த முறைமை அவசியமாகும்.

பயனுறுதி வாய்ந்த தகவல் பாதுகாப்பு நிறுவனசார் கட்டமைப்பானது (அ) தகவல் பாதுகாப்பு உத்தியோகத்தர், (ஆ) பிரதான புத்தாக்க உத்தியோகத்தர் மற்றும் (இ) (பிரதம) உள்ளக கணக்காய்வாளர் போன்ற பிரதான பதவிகளினை உள்ளடக்குகின்றது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

(அ) தகவல் பாதுகாப்பு உத்தியோகத்தர் தொழிற்பாடு மீதான கொள்கை

நிறுவனமானது தகவல் பாதுகாப்பு உத்தியோகத்தர் ஒருவரை நியமித்தல் வேண்டும். அத்தகைய தகவல் பாதுகாப்பு உத்தியோகத்தரானவர், நிறுவன தலைமை அதிகாரியுடன் கலந்தாலோசித்து நிறுவனத்தின் தகவல் பாதுகாப்பு நோக்கங்களை நிறுவுதல், தகவல் பாதுகாப்பு அபாயங்களை நிருவகித்தல் மற்றும் தகவல் பாதுகாப்பு மூலோபாயங்கள், கொள்கைகள் மற்றும் செயல்திட்டங்களைச் செயல்படுத்துதல் ஆகியவற்றின் மூலம் நிறுவனத்தின் தகவல் மற்றும் சொத்துக்கள் போதுமான அளவு பாதுகாக்கப்படுவதை உறுதி செய்யும் வகையில் ஒரு சிரேட் தரத்திலான உத்தியோகத்தராக இருத்தல் வேண்டும்.

தகவல் பாதுகாப்பு உத்தியோகத்தரின் தொழிற்பாடானது த.தொ. தொழிற்பாட்டிலிருந்து வேறுபட்டதாக இருத்தல் வேண்டும் என்பதுடன் தகவல் பாதுகாப்பு உத்தியோகத்தரானவர் தகவல் பாதுகாப்பு தொடர்பான நடவடிக்கைகள் தொடர்பில் நிறுவனத்தின் தலைவரிடம் நேரடியாக அறிக்கையிடலும் வேண்டும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்படையதாகும்.

(ஆ) பிரதான புத்தாக்க உத்தியோகத்தரின் தொழிற்பாடு மீதான கொள்கை

பிரதான புத்தாக்க உத்தியோகத்தர் (அல்லது தகவல் தொழில்நுட்ப விடயத்துக்குப் பொறுப்பான அலுவலர்) தகவல் மற்றும் ஏனைய தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாப்பதற்கும், நிறுவனத்தின் வர்த்தகச் செயற்பாடுகளின் தொடர்ச்சியை உறுதி செய்வதற்கும் தகுந்த நடவடிக்கைகளை எடுப்பதற்குப் பயிற்றுவிக்கப்பட்டு பொறுப்புகள் வழங்கப்படுதல் வேண்டும். குறிப்பு: தகவல் பாதுகாப்பு உத்தியோகத்தரினை நியமிப்பதற்குத் தகுந்த அதிகாரி இல்லாத நிறுவனத்தில், பிரதான புத்தாக்க உத்தியோகத்தர் அல்லது தகவல் தொழில்நுட்ப விடயத்திற்குப் பொறுப்பான உத்தியோகத்தர் ஒருவர் தகவல் பாதுகாப்பு உத்தியோகத்தரின் பாத்திரத்தை வகிக்க அதிகாரம் அளிக்கப்படுவார்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

(இ) (பிரதம) உள்ளக கணக்காய்வாளரின் தொழிற்பாடு மீதான கொள்கை

உள்ளக கணக்காய்வாளருக்கு (பிரதம), நிறுவனத்தின் தகவல் பாதுகாப்பு கணக்காய்வுகளை ஆரம்பித்தல் மற்றும் மேற்பார்வை செய்தல், தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கையை ஏற்றுக் கொள்வதன் முன்னேற்றத்தை மதிப்பிடுதல் மற்றும் தகவல் பாதுகாப்பு தொடர்பான கண்டுபிடிப்புக்களை கணக்காய்வு மற்றும் முகாமைத்துவக் குழுவுக்கு (புரணவை யனெ ஆயயெபநஅநவெ ஊழஅஅவைவநந) அறிக்கையிடுதல் போன்ற பொறுப்புகள் உரித்தளிக் கப்பட்டுள்ளன.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்படையதாகும்.

4.1.3. தகவல் பாதுகாப்புக் குழு மீதான கொள்கை

நிறுமானது தகவல் பாதுகாப்பு தொடர்பான நடவடிக்கைகளுக்கு மூலோபாய வழிகாட்டுதல்களை வழங்கும் நோக்குடன் தகவல் பாதுகாப்புக் குழுவை தாபித்தல் வேண்டும். தகவல் பாதுகாப்பு உத்தியோகத்தினால் உருவாக்கப்பட்ட அனைத்து தகவல் பாதுகாப்பு கட்டுப்பாடுகள், செயல் திட்டங்கள், சொத்து வகையீட்டுத் திட்டங்கள், பாதுகாப்பு கொள்கைகள், சம்பவ மறுமொழி திட்டங்கள் மற்றும் பேரழிவு மீட்பு திட்டங்கள் ஆகியவற்றை மதிப்பாய்வு செய்து அங்கீகாரம் அளிப்பதற்கு இந்த குழு பொறுப்பு வாய்ந்ததாகும். மேலும், அத்தகைய திட்டங்களின் அமுலாக்கங்களினையும் கண்காணிக்கும். நிறுவனத்தின் தலைவர், குழுவின் தலைவராக இருப்பதுடன், மேலும் குழுவானது தகவல் பாதுகாப்பு உத்தியோகத்தர், பிரதம புத்தாக்க உத்தியோகத்தர், (பிரதம) உள்ளக கணக்காய்வாளர் மற்றும் சொத்து உரிமையாளர்களையும் கொண்டிருக்கும். சொத்து உரிமையாளர்கள் மீதான கொள்கையானது பிரிவு 4.2.3 இல் தரப்பட்டுள்ளது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.1.4. இடர் முகாமைத்துவ குழு மீதான கொள்கை

நிறுவனமானது இடர் முகாமைத்துவக் குழுவொன்றினைத் தாபித்தல் வேண்டும். இந்தக் குழு, நிறுவனத்தின் தலைவருக்கு நேரடியாக முறைப்பாடு செய்யும் ஒரு சுயாதீனக் குழுவாக இருக்கும், மேலும் தகவல் மற்றும் தகவல் தொழில்நுட்பச் சொத்துக்கள் தொடர்பாக நிறுவனத்தின் இடர் முகாமைத்துவத்தினை மேற்பார்வையிடும் பொறுப்பைக் கொண்டுள்ளது.

இடர் முகாமைத்துவ குழுவானது சொத்துக்கள் தொடர்பான இடர்களைக் கண்டறிந்து மதிப்பீடு செய்யும், மேலும், இடர்களைக் குறைப்பதற்குத் தேவையான நடவடிக்கைகளை எடுக்க தகவல் பாதுகாப்புக் குழுவுக்கு பொருத்தமான கட்டுப்பாடுகளை முன்மொழிகிறது. இந்தக் குழுவில் பிரிவுத் தலைவர்கள், சொத்து உரிமையாளர்கள் மற்றும் தகவல் பாதுகாப்பு உத்தியோகத்தர் ஆகியோர் உள்ளடங்குகின்றனர். நிறுவனத்தின் பிரதித் தலைவர் குழுவின் தலைவராக இருப்பார்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்படையதாகும்.

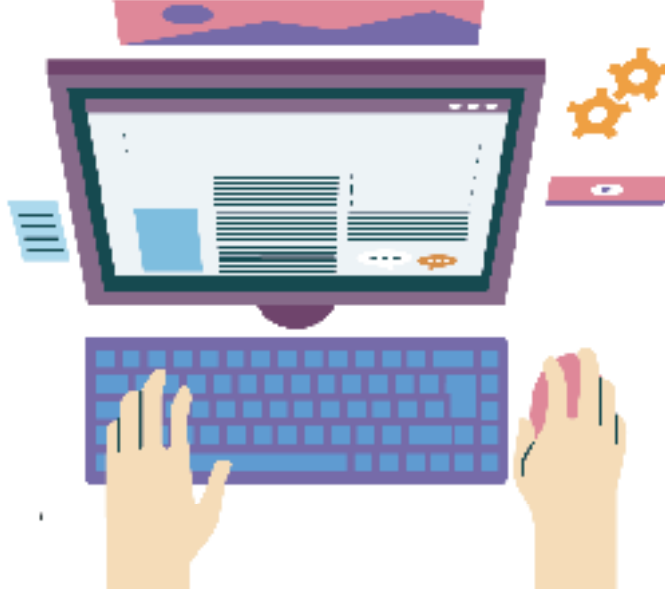
4.1.5. இறுதிப் பயனர் மீதான பொறுப்புக் கொள்கை

தகவல் பாதுகாப்பானது ஒவ்வொருவரினதும் பொறுப்பாகும். அனைத்து இறுதி பயனர்களும் பொறுப்புடன் நடந்து கொள்ளுதல் வேண்டும் என்பதுடன் அவர்கள் அணுகக்கூடிய தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துகளின் பாதுகாப்பு தொடர்பான நிறுவனக் கொள்கைக்கு இணங்குதலும் வேண்டும்.

இறுதிப் பயனர் பொறுப்புகளில் தகவல், கணினி சாதனங்கள், மின்னஞ்சல்கள், இணையம், சமூக ஊடகங்கள், தொலைபேசிகள் மற்றும் தொலைநகல்களின் சரியான பயன்பாடு ஆகியவை அடங்கும். ஆனால் அவை மட்டுப்படுத்தப்படவில்லை.

அனைத்து பயனர்களும் தகவல் மற்றும் இணைய பாதுகாப்பு அமலாக்கல் வழிகாட்டியில் குறிப்பிட்டுக் காட்டப்பட்டுள்ள இறுதிப் பயனர் பொறுப்புகள் மற்றும் இந்தக் கொள்கையால் தேவைப்படும் பொருந்தக்கூடிய தகவல் பாதுகாப்பு நடைமுறைகளைப் புரிந்து கொண்டு கடைப்பிடித்தல் வேண்டும். அத்தகைய வளங்களை தவறாகப் பயன்படுத்தினால், தாபன விதிக் கோவையில் குறிப்பிடப்பட்டுள்ள ஒழுங்கு நடவடிக்கைகளுக்கும், கணினி குற்றச் சட்டம் அல்லது வேறு ஏதேனும் பொருந்தக்கூடிய சட்டவாதிகளின் சட்டங்களின் கீழும் சட்ட நடவடிக்கைகள் மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.



4.1.6. திறன் விருத்தி மீதான கொள்கை

தகவல் பாதுகாப்பு விழிப்புணர்வு மற்றும் பயிற்சியை நடத்துவதன் மூலம் பொறுப்பான தனிநபர்கள் (தகவல் பாதுகாப்பு உத்தியோகத்தர், பிரதம புத்தாக்க உத்தியோகத்தர், பிரதம உள்ளக கணக்காய்வாளர், சொத்துகளின் உரிமையாளர்கள், முதலியன) மற்றும் இறுதி பயனர்களின் தகவல் பாதுகாப்பு திறனை நிறுவனம் உருவாக்குகிறது. சம்பந்தப்பட்ட அதிகாரிகளின் இத்தகைய திறன் மேம்பாட்டு நடவடிக்கைகள் சரியான முறையில் மேற்கொள்ளப்படுதல் வேண்டும், மேலும், இது போன்ற நடவடிக்கைகள் அமைப்பின் வருடாந்த பயிற்சித் திட்டத்தில் சேர்க்கப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.1.7. பதவியினரின் பாதுகாப்பு அனுமதி மீதான கொள்கை

மிக இரகசியமான அல்லது இரகசியமானது என வகைப்படுத்தப்பட்ட தகவலைக் கையாளும் ஒரு பதவிக்கு ஒதுக்கப்பட்ட அல்லது மாற்றப்பட்ட அல்லது முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுடன் அணுகல் உள்ளவர்கள் எந்தவொரு நபரும், நியமனம் அல்லது அந்தப் பதவிக்கு மாற்றுவதற்கு முன் பாதுகாப்பு அனுமதிச் சோதனைக்கு உட்படுத்தப்படுதல் வேண்டும்.

அவர்களின் சேவையின் போது பின்னணி சோதனைகள் மற்றும் அவ்வப்போது பாதுகாப்பு அனுமதி சோதனைகள் மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்படையதாகும்.

இலங்கை சேர்ட் நிறுவனம் இணங்கும் நிலையைத் தீர்மானிக்க வருடாந்தத் தகவல் பாதுகாப்புத் தயார்நிலை மதிப்பீடுகளை மேற்கொள்ளும், மேலும் அத்தகைய மதிப்பீடுகளை நாடாத்துவதற்கு தாபனமானது இலங்கை சேர்ட்டுக்கு வசதிகளின்னை ஏற்படுத்திக் கொடுத்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.2. சொத்துக்கள், உரிமையாளர்கள், பயனர்கள் மற்றும் இடர்களை அடையாளங் காணுதல்.

நிறுவன சொத்துக்களுக்கான தகவல் பாதுகாப்பு அபாயங்களை நிருவகிப்பதற்கு அவர்களின் செயற்பாட்டு சூழலைப் பற்றிய புரிதலை நிறுவனம் உருவாக்குதல் வேண்டும். நிறுவனத்திற்கு மதிப்புள்ள தகவல், முறைமைகள் மற்றும் தகவல் தொழில்நுட்ப சாதனங்கள் (சொத்துக்கள்), சொத்துக்களின் உரிமையாளர்கள் மற்றும் சொத்துக்களின் பாவனையாளர்கள் அவர்களின் தொழிற்பாடுகள் மற்றும் பொறுப்புகள் மற்றும் சொத்துகளுடன் தொடர்புடைய தற்போதைய அபாயங்கள் ஆகியவற்றை நிறுவனம் அடையாளம் காணுதல் வேண்டும். இது தொடர்பில், நிறுவனமானது பின்வரும் கொள்கைகளின்னை கடைப்பிடித்தல் வேண்டும்.



4.2.1. தகவல் சொத்துக்கள் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை அடையாளங் காணுதல் மீதான சொத்துக்கள்

நிறுவனம் அதன் முக்கியமான தகவல் சொத்துக்களை (கெழ்ச்சியுவழையெ யளநவன) அடையாளம் காணுதல் வேண்டும். ஒரு தகவல் சொத்து என்பது அதன் நிறுவன செயற்பாடுகளை நிறைவேற்றுவதில் நிறுவனத்திற்கு உதவுகின்ற மதிப்புமிக்க எத்தகைய தகவலுமாகும்.

வர்த்தக ரகசியங்கள், கேள்வி மனு ஆவணங்கள், வரவு செலவுத் தாள்கள் மற்றும் ஊழியர்களின் தனிப்பட்ட பதிவுகள், நிறுவனத்தால் வழங்கப்படும் சேவைகள் தொடர்பான பயன்பாட்டு

மென்பொருள் மூலம் சேகரிக்கப்பட்ட தரவு போன்றவை தகவல் சொத்துக்களுக்கான எடுத்துக்காட்டுகளாகும். தகவல் சொத்துக்கள் காகித ஆவணம், டிஜிட்டல் ஆவணம், தரவுத்தளம், கடவுச்சொல் அல்லது குறியாக்க விசை (encryption key) அல்லது வேறு ஏதேனும் டிஜிட்டல் கோப்பு போன்ற பல்வேறு வடிவங்களில் வரலாம்.

தாபனமானது தகவல் தொழில்நுட்ப சொத்துக்களையும் (IT assets) அடையாளம் காணும். தகவல் தொழில்நுட்ப சொத்து என்பது ஒரு தகவல் தொழில்நுட்ப சூழலிலுள்ள ஒரு மென்பொருள் (உதாரணம். இயக்க முறைமை, சம்பள முறைமை, முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு) அல்லது வன்பொருள் (உதாரணம். கணினிகள், வன்தட்டுகள், சர்வர்கள், ரவுட்டர்கள், .பயர்வால்கள்) வலையமைப்புக்கள் அல்லது ஏனைய டிஜிட்டல் உட்கட்டமைப்பு வசதிகள் குறிப்பிடுகின்றது.

சொத்துக்களை அடையாளம் காணுதல் (தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்கள்) அங்கீகரிக்கப்படாத அணுகல், பயன்பாடு, வெளிப்படுத்துதல், இடையூறு, மாற்றம் அல்லது அழித்தல் ஆகியவற்றிலிருந்து சொத்துக்களைப் பாதுகாக்கும் நோக்கத்துடன் ஒருமைப்பாடு (integrity), ரகசியத்தன்மை (confidentiality) மற்றும் சொத்துகளின் கிடைக்கும் தன்மையினை (availability) உறுதிசெய்யும் நோக்கத்துடன் மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.2.2. முக்கிய உட்கட்டமைப்பு வசதிகளை அடையாளம் காணுதல் மீதான கொள்கை.

முக்கியமான தேசிய தகவல் உட்கட்டமைப்புக்கள் என்பது தேசிய பாதுகாப்பு, நிருவாகம், பொருளாதாரம், சுகாதாரம் மற்றும் ஒரு நாட்டின் சமூக நல்வாழ்வில் பேரழிவுகரமான தாக்கத்தை ஏற்படுத்தும் தோல்வி அல்லது அழிவினை ஏற்படுத்துகின்ற முறைமைகள் அல்லது வசதிகளைக் குறிப்பிடுகின்றது.

முக்கியமான தேசிய தகவல் உட்கட்டமைப்பினைப் பராமரிக்கும் நிறுவனங்கள் இந்தக் கொள்கையில் குறிப்பிடப்பட்டுள்ள அத்தகைய உட்கட்டமைப்பைப் பாதுகாக்க தகுந்த நடவடிக்கைகளை எடுத்தல் வேண்டும். குறிப்பாக, தேசிய தகவல் உட்கட்டமைப்பினை அடையாளம் காண்பதானது இலங்கை கணினி அவசர தயார்நிலை அணியினால் மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்படையதாகும்.



4.2.3. சொத்து உரிமையாளர்கள், பாதுகாவலர்கள் மற்றும் பயனர்களின் பொறுப்புக்கள் மீதான கொள்கை.

நிறுவனமானது உரிமையாளர்கள் மற்றும் பாதுகாவலர்களை அடையாளம் கண்டு கொள்ளுதல் வேண்டும். சொத்து உரிமையாளர் ஒரு சிரேட் நிறைவேற்றுத் தரத்திலான அதிகாரி அல்லது ஒரு சொத்தின் வாழ்க்கைச் சுழற்சியைக் கட்டுப்படுத்தும் அங்கீகரிக்கப்பட்ட நிருவாகப் பொறுப்பைக் கொண்ட ஒரு தாபனமாக இருத்தல் வேண்டும். சொத்து உரிமையாளர் சொத்துக்களுக்கான இடர்களைப் புரிந்து கொள்ளுதல் வேண்டும் என்பதுடன் அத்தகைய சொத்துக்களைப் பாதுகாப்பதற்கான சொத்து உருவாக்கப்படும்போது அல்லது நிறுவனத்திற்கு சொத்துக்கள் மாற்றப்படும்போது அல்லது தாபனத்தால் கையகப்படுத்தப்படும் போது அதன் உரிமையை முறையாக ஒதுக்குவது அவசியமாகும்.

தகவல் சொத்தின் பாதுகாவலர், என்பவர் சொத்தின் பாதுகாப்பிற்கு பொறுப்பான ஒரு நபர் அல்லது ஒரு நிறுவனம் மற்றும் சொத்தின் பாதுகாப்பு தொடர்பான கட்டுப்பாடுகளை (தகவல் சொத்தின் உரிமையாளரால் அடையாளம் கண்டு அங்கீகரிக்கப்பட்ட) செயற்படுத்துவதற்கான பொறுப்பாளியாவார்.

சொத்து உரிமையாளரும் பாதுகாவலரும் சொத்துக்களுக்கான பதிவேடுகளை விருத்தி செய்தல், சொத்துக்களை வகைப்படுத்துதல் மற்றும் சொத்துக்களைப் பாதுகாத்தல், சொத்துக்களுக்கான அணுகல் கட்டுப்பாடுகளை வரையறுத்தல் மற்றும் மறுபரிசீலனை செய்தல், சொத்து நீக்கப்படும் போது அல்லது அழிக்கப்படும் போது சரியான கையாளுதலை உறுதி செய்தல் ஆகியவற்றுக்கும் பொறுப்பாளிகளாவார்.

நிறுவனம் அதன் சொத்துக்களைப் பயன்படுத்தும் பயனர்களையும் அடையாளம் காண வேண்டும். உத்தியோகபூர்வ நோக்கங்களுக்காக சொத்துக்களைப் பயன்படுத்தும் பணியாளர்கள், பயனர்கள், உத்தியோகபூர்வ நோக்கங்களுக்காக சொத்துக்களைப் பயன்படுத்த வேண்டிய பயனர்களை சொத்து உரிமையாளர்கள் துல்லியமாக அடையாளம் காணுதல் வேண்டும், மேலும் பிரிவு 4.3.4 மற்றும் 4.3.5 இல் குறிப்பிடப்பட்டுள்ளபடி அந்த சொத்துக்களுக்கான அணுகலைக் கட்டுப்படுத்துதலும் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.2.4. தகவல் சொத்துக்கள் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்கள் பதிவேடுகளைப் பேணுவது மீதான கொள்கை

நிறுவனமானது தகவல் சொத்துக்களை தகவல் சொத்து பதிவேட்டில் (Information Assets Register) பதிவு செய்தல் வேண்டும். ஒரு தகவல் சொத்துக்கள் பதிவு என்பது ஒரு தாபனம் வைத்திருக்கும் மற்றும் செயலாக்கும் தகவல் சொத்துக்களின் முறையான இருப்பு ஆகும்.

குறைந்தபட்சம், ஒரு தாபனமானது, தகவல் சொத்தின் பெயர், தகவல் சொத்தின் அமைவிடம், தகவல் சொத்தின் உரிமையாளர் மற்றும் பாதுகாவலர், வகைப்படுத்தப்பட்ட திகதி, சொத்துக்களை செயலாக்கும் கணினி முறைமை, வகைப்படுத்துவதற்கான காரணம், அகற்றல் தேவைகள், வகைப்படுத்தல் மீளாய்வு திகதி, இழப்பு .: இணக்கப்பாடு அல்லது வெளிப்படுத்துதல் ஆகியவற்றின் தாக்கம் என்பவற்றினைப் பதிவு செய்யும். தகவல் சொத்துக்கள் பதிவேடு துல்லியமாகவும், புதுப்பித்ததாகவும், சீரானதாகவும் மற்ற சர்க்குகளுடன் சீரமைக்கப்பட்டதாகவும் இருத்தல் வேண்டும்.



நிறுவனமானது தகவல் தொழில்நுட்ப சொத்துகள் பதிவேட்டில் (IT Assets Register) தகவல் தொழில்நுட்ப சொத்துகளின் விவரங்களை பதிவு செய்யும். தகவல் தொழில்நுட்ப சொத்துப் பதிவேட்டில் குறைந்தபட்சம், சொத்துகளின் வகை (உதாரணம். வன்பொருள், மென்பொருள், சர்வர்), சொத்தின் இருப்பிடம், இயக்க முறைமை, உரிம விவரங்கள், பயனர்கள், ஆபத்து, வகைப்பாடு நிலை, மதிப்பிடப்பட்ட மதிப்பு மற்றும் பலவற்றைக் கொண்டிருத்தல் வேண்டும். தகவல் தொழில் நுட்பசொத்துப் பதிவேடானது துல்லியமாகவும், புதுப்பித்ததாகவும், மற்ற இருப்புகளுடன் சீரானதாகவும் இருத்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.2.5. இடர் மதிப்பீடுகள் மீதான கொள்கை

நிறுவனத்தின் சொத்துக்களுக்கு ஏற்படும் அச்சுறுத்தல்கள் மற்றும் பாதிப்புகள் மற்றும் சொத்துக்களின் மீதான அவற்றின் தாக்கம் ஆகியவற்றைத் தீர்மானிக்க தாபனமானது இடர் மதிப்பீட்டை மேற்கொள்ளும்.

இடர் மதிப்பீட்டின் நோக்கம், சொத்துக்களுக்கு (தரவு, கணினி அமைப்புகள் அல்லது ஏனைய டிஜிட்டல் உட்கட்டமைப்பு) ஏற்படும் பாதிப்புகள் மற்றும் அச்சுறுத்தல்களைக் கண்டறிவது மற்றும் ஏற்றுக் கொள்ளக்கூடிய அளவிற்கு ஆபத்தை குறைப்பதற்கு எத்தகைய பாதுகாப்பு நடவடிக்கைகள் எடுக்கப்பட வேண்டும் என்பதை தீர்மானிப்பதுமேயாகும். இடர் மதிப்பீட்டின் அடிப்படையில், தாபனமானது இடர் பதிவேட்டில் இடர்களுக்கு முன்னுரிமை அளித்து இடர்களை பதிவு செய்தல் வேண்டும்.

பிரிவு 4.3 இல் குறிப்பிடப்பட்டுள்ள கொள்கைப் பரிசீலனைகளை கவனத்தில் கொண்டு, இடர் பதிவேட்டில் (Risk Register) பதிவு செய்யப்பட்ட இடர்களுக்கான தகுந்த பாதுகாப்பு முன்னெச்சரிக்கைகளை நிறுவனம் எடுத்தல் வேண்டும். இடர் மதிப்பீடு தாபனத்தின் இடர் முகாமைத்துவ குழுவினால் மேற்கொள்ளப்படும். தாபனமானது பொருத்தமான

திறன்களைக் கொண்டிருக்கவில்லை என்றால், இந்த நோக்கத்திற்காக ஒரு தகுதி வாய்ந்த மற்றும் அனுபவம் வாய்ந்த நிறுவனமொன்று பணியில் அமர்த்தப்படும். இலங்கை கணினி அவசரதயார் நிலை அணியானது முக்கியமான தேசிய தகவல் உட்கட்டமைப்புகளுக்கு இடர் மற்றும் பாதிப்பு மதிப்பீடுகளை மேற்கொள்வதற்கு உதவியளிக்கும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்படையதாகும்.

4.2.6. சொத்துக்களின் வகையீடு மீதான கொள்கை

நிறுவனமானது சொத்துக்களை வகைப்படுத்தி, சொத்துக்களின் உணர்திறனை தீர்மானிக்க வேண்டும்.

ஒரு சொத்தானது தாபனத்திற்கான அதன்மதிப்பு மற்றும் அதன் உணர்திறன் ஆகியவற்றிற்கு ஏற்ப பொருத்தமான அளவிலான பாதுகாப்பைப் பெறுவதை உறுதி செய்வதே வகைப்படுத்தலின் பிரதான நோக்கமாகும். தகவல் சொத்து வகையீடானது ஏற்றுக் கொள்ளப்பட்ட வழிகாட்டுதல்களின் அடிப்படையில் மேற்கொள்ளப்படுதல் வேண்டும்.

தகவல் சொத்துக்களுக்கான வகையீட்டு மட்டங்கள் "மிக இரகசியமானவை" (secret) "இரகசியமானவை" (confidential) "வரையறுக்கப்பட்ட பகிர்வு" (limited sharing), "பொது" (public) மற்றும் "வகைப்படுத்தப்படாத" (unclassified) என்பனவாகும்.

தகவல் தொழில்நுட்பச் சொத்துக்களானவை "மிகவும் முக்கியத்துவம் வாய்ந்த" (very critical) "முக்கியத்துவம் வாய்ந்த" (critical) "முக்கியத்துவம் அல்லாத" (non-critical) மற்றும் "வகைப்படுத்தப்படாத" (unclassified) என நான்கு நிலைகளாக வகைப்படுத்தப்படும்.

தகவல் தகவல் தொழில்நுட்ப சொத்துக்கள் வகைப்படுத்தல் திட்டத்தின் விபரணமானது "தகவல் மற்றும் சைபர் பாதுகாப்பு அமலாக்கல் வழிகாட்டி" இல் உள்ளது. (பிரிவு 2.2 (இ) இணைப் பார்க்கவும்).

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3. சொத்துக்களின் பாதுகாப்பு



சொத்துக்களை இனங்காண்பதன் பேரில், அந்த நிறுவனமானது, சாத்தியமான தகவல் பாதுகாப்பு நிகழ்வு அல்லது சம்பவத்தின் தாக்கத்தைத் தடுப்பதற்கு, மட்டுப்படுத்துவதற்கு அல்லது கட்டுப்படுத்துவதற்கு பொருத்தமான கட்டுப்பாடுகளை நடைமுறைப்படுத்துதல் வேண்டும். பிரயோகிக்கப்படுகின்ற கட்டுப்பாடுகள் ஒவ்வொரு சொத்தின் வகையீட்டின் அடிப்படையில் அமைந்திருத்தல் வேண்டும்.

கொள்கையுடன் ஒத்திணங்குவதற்காக, இந்த நிறுவனம், சொத்தை அடைவதனைக் கட்டுப்படுத்தும், தரவைப் பாதுகாப்பதற்கு நடைமுறையிலுள்ள செயல்முறைகளை செயற்படுத்தும், தரவு அனுப்பப்படுகின்ற போது மற்றும் தரவு ஓய்விலுள்ள போது தரவுக்கான பாதுகாப்பு கட்டுப்பாடுகளை வரையறுக்கும், உரிமம் பெற்ற, அதிகாரமளிக்கப்பட்ட மென்பொருளைப் பயன்படுத்தும், நிறுவனத்தின் கொள்கைகள் கீழே தரப்பட்டுள்ளவற்றுடன் இணங்குதல் வேண்டும்.

4.3.1. ஓய்விலுள்ள தரவினைப் பாதுகாப்பது தொடர்பான கொள்கை

நிறுவனமானது, ஓய்விலுள்ள தரவினைப் பாதுகாத்தல் வேண்டும். ஓய்விலுள்ள தரவு என்பது சாதனத்திலிருந்து சாதனம் அல்லது வலைப்பின்னலிலிருந்து வலைப்பின்னலுக்கு தீவிரமாக நகராத தரவு (உ.ம். சேவையகம், கிளவுட், வன்செலுத்தி, மடிக்கணினி, டிவிடர்ஸ்) அல்லது காப்பகப்படுத்தப்பட்ட சேமிக்கப்பட்ட தரவு ஆகும். சேமிப்பதற்கு முன்னர் "மிக இரகசியமானது" (confidential) அல்லது "இரகசியமானது" (secret) என வகைப்படுத்தப்படுகின்ற எந்தவொரு தரவினையும் (தகவல் ஆதனங்கள்) குறியாக்கம் (encrypt) செய்வதும் சொத்துக்களுக்குப் பௌதீக ரீதியான பாதுகாப்பு, இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடு வழங்குவதும் அத்தியாவசியமானதாகும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3.2. பரிமாற்றப்படுகின்ற தரவினைப் பாதுகாத்தல் மீதான கொள்கை.

நிறுவனமானது பரிமாற்றப்படுகின்ற தரவினைப் பாதுகாத்தல் வேண்டும். பரிமாற்றப்படுகின்ற தரவு என்பது இணையம் முழுவதும் அல்லது ஒரு தனிப்பட்ட வலையமைப்பினூடாக போன்ற அத்தகையதொரு இடத்திலிருந்து பிறிதொரு இடத்திற்கு தீவிரமாக நகரும் தரவு (உ.ம். தரவு ஒரு நிறுவனத்திற்கு சொந்தமான வை.பை உள்ளடங்கலாக தனிப்பட்ட வலையமைப்பினூடாக தளம் 'அ' இலிருந்து தளம் 'ஆ' க்கு மாற்றப்படுகின்றது) ஆகும்.

பரிமாற்றப்படுகின்ற தரவினைப் பாதுகாக்கும்நோக்கில், நிறுவனம், தரவு பரிமாற்றத்திற்காக நகர்த்துவதற்கும், பாதுகாப்பான இணைப்புகளை (HTTPS, TLS, SFTP போன்றன) பயன்படுத்துவதற்கு முன்னர் உணர்வுபூர்வமான தகவல்களை ("மிக இரகசியமானது" அல்லது "இரகசியமானது" என்று தகவல்களை வகைப்படுத்தி) குறியாக்கம் செய்தல் வேண்டும். மேலும், தாபனமானது, வை.பை ஏற்பாடுகள் தொடர்பில் பாதுகாப்பு அளபுருக்களை (security parameters) மேற்கொண்டுள்ளது என்பதை உறுதி செய்தலும் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3.3. பௌதீக ரீதியான பாதுகாப்பு மீதான கொள்கை

நிறுவனமானது, பௌதீகதலையீடு மற்றும் அதிகாரமற்ற அணுகலைத் தடுப்பதற்காக சொத்துக்களுக்கு பௌதீகரீதியான பாதுகாப்பை வழங்குதல் வேண்டும்.

சொத்துக்களின் பாதுகாப்பு தேவைகளின் அடிப்படையில், ஒவ்வொரு நிறுவனமும் அதற்கு முக்கியமான ஆதனங்களை சேமிப்பதற்கு அல்லது செயல்முறைக்கு பாதுகாப்பான பகுதிகளை வரையறுத்தல் வேண்டும். "மிக இரகசியமானது" மற்றும் "இரகசியமானது" என்று வகைப்படுத்தப்பட்ட தகவல் ஆதனங்கள் குறிப்பிடப்பட்ட பாதுகாப்பான பகுதிகளில் சேமிக்கப்பட்டு, செயற்படுத்தப்படுதல் வேண்டும்.



மேலும், "மிகவும்" முக்கியமானவை" என வகைப்படுத்தப்படும் தகவல் தொழில்நுட்ப சொத்துக்கள் பாதுகாப்பான பகுதிகளில் சேமிக்கப்பட்டு செயற்படுத்தப்படும். பாதுகாப்பான பகுதிகள் இயற்பொருள் சார்ந்தசுமர்கள், பூட்டக்கூடிய கதவுகள் மற்றும் பல் ஆக்கக்கூறு பதிவு முறைமைகளால் (multi-factor entry systems) பாதுகாக்கப்படுதல் வேண்டும் என்பதுடன், பௌதீக தலையீடுகள் மற்றும் அதிகாரமற்ற அணுகலைத் தடுப்பதற்கு தொடர்ந்து இரகசிய கமராக்கள் (CCTV) மூலம் கண்காணிக்கப்படுதல் வேண்டும்.

தீ, வெள்ளம், ஈரப்பதம், மின்காந்த துறைகள் மற்றும் வெப்பநிலை ஆகியவற்றிலிருந்து அச்சுறுத்தல்களைத் தடுப்பதற்கு பாதுகாப்புப் பகுதிகள் பாதுகாக்கப்படுதல் வேண்டும். இதற்கு மேலதிகமாக, தாபனம், தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்களைப் பயன்படுத்துபவர் அணுகுவதைக் கட்டுப்படுத்துவதற்கு பல்வேறு தொழில்நுட்பங்களைப் பயன்படுத்துதல் வேண்டும். அத்தகைய தொழில்நுட்பங்கள், பயன்படுத்துபவரின் அடையாளம், கடவுச்சொற்கள், அணுகல் அட்டைகள், தனிப்பட்ட அடையாள எண் மற்றும் மரபணுக்கள் ஆகியவற்றை உள்ளடக்குகின்றது, ஆனால் அதற்குள் மட்டுப்படுத்தப்படவில்லை.

இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடுச் செயல்முறையை (கொள்கைக் கூற்று 4.3.4 இணைப் பார்க்கவும்) நடைமுறைப்படுத்துவதன் மூலம் கணினிகள், முறைமைகள் அல்லது ஏதேனும் சாதனங்களை அணுகுவதனை கட்டுப்படுத்தப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3.4. இனங்காணல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடு மீதான கொள்கை

நிறுவனமானது, பயன்படுத்துபவர் தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்கள் இரண்டினையும் அணுகுவதைக் கட்டுப்படுத்துதல் வேண்டும். இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்துதல் என்பது தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்களை பாதுகாப்பாக வைத்திருப்பதற்காக அணுகுவதை முகாமை செய்கின்ற அணுகுமுறையொன்றாகும். இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்துதல் என்பது, முறைமைகளையும் தகவல்களையும் அவர்கள் அணுகுவதற்கு அனுமதிப்பதற்கு முன்னர் பயன்படுத்துபவரின் அடையாளத்தையும் அவர்கள் அணுகுகின்ற அளவையும் சரி பார்ப்பதில் கவனம் செலுத்துகின்றது. பயன்படுத்துபவர் தங்கள் பணி இலக்குகளை (தெரிந்து கொள்ள வேண்டியவை) ஆற்றுவதற்குத் தேவையான ஆதனங்களை மட்டுமே அணுகுவதற்கும் மற்றும் பணி இலக்குகளை (பயன்படுத்த வேண்டிய தேவையுள்ள)



ஆற்றுவதற்கும் அனுமதி வழங்கப்படுதல் வேண்டும். பயன்படுத்துபவர் அவர்களின் வகியாகத்திற்கு ஏற்ப தேவையான முறைமைகளும், தகவல்களுக்கும் எப்போதும் குறைந்தபட்ச அணுகல் வழங்கப்படுதல் வேண்டும். கொடுக்கப்பட்ட கொள்கைகளின் அடிப்படையில், நிறுவனமானது அதன் பயன்பாட்டிற்கான இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாட்டுச் செயன்முறையினை விருத்தி செய்தல் வேண்டும்.

இலங்கை சேர்ட் நிறுவனமானது, நிறுவனத்தால் தனிப் பயனாக்கக் கூடியதும், பின்பற்றக் கூடியதுமான அரசு நிறுவனங்களுக்கான "இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்தும் செயன்முறை" இனை வரைந்துள்ளது. நிறுவனத்தால் செயற்படுத்தப்படும் இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்தும் செயன்முறை போதுமானதாகவும் புதுப்பித்ததாகவும் இருப்பதை நிறுவனம் உறுதி செய்ய வேண்டும். மேலும், அனைத்து ஊழியர்களும், மூன்றாம் தரப்பு சேவை வழங்குநர்களும் அரசு நிறுவனத்தால் செயற்படுத்தப்படும் இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்தும் செயன்முறையை கடைப்பிடித்தல் வேண்டும்

இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகுவதைக் கட்டுப்படுத்தும் செயன்முறையின் ஏதேனும் மீறல்கள், ஏற்படுமிடத்து தேவையான நடவடிக்கைக்காக தகவல் பாதுகாப்பு செயற்குழுவிடம் தெரிவிக்கப்படும். ஒரு தகவல் பாதுகாப்பு செயற்குழு நிறுவப்படாத சூழ்நிலையில், அத்தகைய மீறல்கள் சர்வதேச தர நிர்ணய அமைப்பு மூலம் நிறுவன தலைமைத்துவத்திற்கு தெரிவிக்கப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.5. வலுவான உறுதிப்படுத்தல் மீதான கொள்கை

அதிகாரமளித்தலானது பயனரொருவரின் இனங்காணல் செயல்முறையாகும். அதிகாரமளித்தலானது சான்றின் மூலம் பயனர் அதிகாரமளித்தல் செயல்முறையானது (இனங்காணுதல்) மற்றும் பயனர் உறுதிப்படுத்தல் (அடையாளத்தினை உறுதிப்படுத்துதல்) என்பவற்றினூடாக நிறுவனத்தின்



சொத்துக்களுக்கு அணுகலினை வழங்குகின்றது.

கொள்கையின் 4.6.4 இல் குறிப்பிடப்பட்டவாறு நிறுவனத்தின் இனங்காணல் முகாமைத்துவ மற்றும் அணுகல் கட்டுப்பாட்டுச் செயல் முறைக்கமைவாக, பயனர் அடையாளத்தினை உறுதிப்படுத்துவதற்கு நிறுவனமானதும் வலுவானதுமான அதிகாரத்தினைப் பயன்படுத்துதல் வேண்டும்.

பயன்படுத்துபவரின் பெயர் மற்றும் கடவுச்சொல் சேர்க்கை மற்றும் பல் காரணி அங்கீகாரத்தினை (multi-factor authentication) பயன்படுத்துதல் ஆகியவை பயன்படுத்துபவரின் அடையாளத்தை உறுதிப்படுத்துவதற்கு பரிந்துரைக்கப்படுகின்றன.

ஒரு வலுவான உறுதிப்படுத்தல் செயல்முறையை உறுதி செய்வதற்கு, பின்வரும் காரணிகளை, (ஆனால் மட்டுப்படுத்தப்படவில்லை) நிறுவனத்தின் இனங்காணுதல் முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாட்டுக் கொள்கையினை உருவாக்குவதில் கவனம் செலுத்துதல் வேண்டும்.

(அ) வலுவானகடவுச்சொல்:

- கடவுச்சொற்கள் குறைந்தபட்சம் 8 எழுத்துக்களைக் கொண்ட நீளத்திலும், மற்றும் மேல், மற்றும் கீழ் நிலை எழுத்துக்கள் ஆகிய இரண்டையும் (உ.ம். ய-ணு).இலக்கங்கள் (0,9),மற்றும் சிறப்பு எழுத்துக்கள் (!@\$/+) கொண்டிருத்தல் வேண்டும்.
- அனைத்து கடவுச் சொற்களையும் வழக்கமான அணுகலுக்கு 90 நாட்கள் என்று முன்கூட்டியே தீர்மானிக்கப்பட்ட இடைவெளிகளுக்குப் பின்னர் மாற்றப்படுதல் வேண்டும். சிறப்புரிமை அணுகலானது (privileged access) ஒரு தேவையொன்றின் அடிப்படையில் மட்டுமே வழங்கப்படுதல் வேண்டும்..

(ஆ) பல்காரணி அங்கீகாரம் (ஆகிய)

- மிக இரகசிய மற்றும் இரகசியத் தகவல்களை அணுகக்கூடிய பயனர் கணக்களைப் பாதுகாப்பதற்காக பல்காரணி அங்கீகார அணுகலை நிறுவனம் செயற்படுத்தும்.
- பல்காரணி அங்கீகாரத்தினை வடிவமைப்பதில், நிறுவனம் குறைந்த பட்சம் பயனரின் அறிவு (உங்களுக்குத் தெரிந்தது: what you know உ.ம். கடவுச்சொல்), உடைமை (உங்களிடம் என்ன உள்ளது: றாயவ லழர றாயந உ.ம். குறி அடையாளம், அணுகல்அட்டை) அல்லது உள்ளார்ந்தவை (ரொநச-நடெந) (உங்கள் உள்ளார்ந்த தன்மையாக இருப்பது:what you are,உ.ம். மரபணுக்கேரேகை)

ஆகியவற்றின் சேர்க்கையினை கவனத்தில் எடுத்துக் கொள்ளுதல் வேண்டும். நிறுவனத்தை விட்டு வெளியேறுகின்றபணியாளர் ஒருவருக்கு வழங்கப்பட்ட கடவுச்சொற்கள் மற்றும் பிற வேறு உறுதிப்படுத்தல் சான்றுகளும், மேலும் பணியாளர் அணுகுவதைத் தடுப்பதற்கு அனைத்து சொத்துக்களிலிருந்தும் திரும்பப் பெறப்பட்டு அகற்றப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3..6. கணனி கிளவுட் மற்றும் தரவு இறையாண்மை மீதான கொள்கை

தரவு இறையாண்மை (data sovereignty) என்பது நாட்டிற்குள் உள்ள சட்டங்கள் மற்றும் நிருவாக கட்டமைப்புகளுக்கு உட்பட்ட தரவுகளை குறிக்கிறது, அத்தகைய தரவு சேகரிக்கப்பட்டு, செயலாக்கப்பட்டு சேமிக்கப்படுகிறது. இந்தச் சூழலில், சேகரிக்கப்பட்ட தரவைச் சேமித்து செயலாக்க மற்ற நாடுகளிலிருந்து கிளவுட் சேவைகள் பெறப்படும் போது, குறிப்பாக தரவு இறையாண்மையில் அரசாங்க நிறுவனம் அதிக கவனம் செலுத்துதல் வேண்டும்.



கிளவுட் கணினி என்பது பொதுவாக தகவல் தொடர்பாடல் தொழில்நுட்ப ஆதாரங்களைக் குறிக்கிறது (உதாரணம். சேமிப்பகம், செயலாக்கம், பயன்பாட்டு மேம்பாட்டு தளங்கள் போன்றவை) பயனரின் நேரடி முகாமை இல்லாமல் தேவைக்கேற்ப பயனர்களுக்குக் கிடைக்கும்.. இப்போதெல்லாம் பல நிறுவனங்கள் செலவீன சேமிப்பு, அளவிடுதல் மற்றும் அதிகரித்த செயல்திறன் காரணமாக கிளவுட் சேவைகளுக்கு நகர்கின்றன.

இருப்பினும், நிறுவனமானது, கிளவுட் சேவைகளைப் பயன்படுத்துவதன் ஆபத்து பற்றி குறிப்பாக, பொது கிளவுட்டைப் (பொது கிளவுட் என்பது, அவற்றை வாங்க விரும்பும் எவருக்கும் கிடைக்கப் பெறுகின்ற கிளவுட் சேவையொன்றாகும்) பயன்படுத்தும் போது மிகவும் எச்சரிக்கையாக இருத்தல் வேண்டும். வெவ்வேறு அதிகார வரம்புகளில் செயற்படுவதால் கிளவுட் மீது வரையறுக்கப்பட்ட கட்டுப்பாடு, கட்டிடக் கலைஞர்களின் வரையறுக்கப்பட்ட தெரிவுநிலை மற்றும் செயல்பாடுகளின் வரையறுக்கப்பட்ட வெளிப்படைத்தன்மை, சேவை மட்ட ஒப்பந்தங்களில் சாத்தியமான குறிப்பிடத்தக்க பொருத்தமின்மைகள் ஆகியவை பொதுவான கிளவுட் அபாயங்கள் ஆகும்.

தங்கள் கிளவுட் சேவைத் தேவைகளைப் பூர்த்தி செய்வதில், நிறுவனங்கள் லங்கா அரசு கிளவுட் (Lanka Government Cloud) மூலம் சேவைகளைப் பெறுவதற்கு முன்னுரிமை அளிக்க வேண்டும். லங்கா அரசு கிளவுட் என்பது அரசாங்கத்திற்குச் சொந்தமான தனியார் கிளவுட் சேவையாகும், இது தகவல் மற்றும் தொடர்பாடல் தொழில்நுட்ப நிறுவனத்தால் இயக்கப்படுகிறது, இது அரசாங்கத்தின் கிளவுட் சேவைத் தேவைகளைப் பூர்த்தி செய்யும் வகையில் வடிவமைக்கப்பட்டுள்ளது. எவ்வாறாயினும், எந்தவொரு கிளவுட் சேவை வழங்குநரிடமிருந்தும் சேவைகளைப் பெறுவதற்கு முன், சரியான இடர் மதிப்பீட்டைச் செய்ய நிறுவனங்களுக்கு கண்டிப்பாக பரிந்துரைக்கப்படுகிறது.

மேலும், தரவுகளை சேகரித்தல், சேமித்தல் மற்றும் செயலாக்குதல் அல்லது பிற அதிகார வரம்புகளில் மென்பொருள் பயன்பாடுகளை ஹோஸ்ட் செய்தல் தொடர்பான அமைப்பின் அனைத்து நடவடிக்கைகளும் தரவு பாதுகாப்பு தொடர்பாக இலங்கையில் உள்ள தொடர்புடைய சட்டங்கள் மற்றும் ஒழுங்குமுறைகளுக்கு இணங்க மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.7. உரிமம் பெற்ற மென்பொருள் மற்றும் இணைப்புக்களின் இற்றைப்படுத்தல்கள் மீதான கொள்கை.

நிறுவனமானது, செல்லுபடியாகும் இற்றைப்படுத்தல்களுடன் உரிமம் பெற்ற மென்பொருளைப் பயன்படுத்துதல் வேண்டும். இது முறைமை மென்பொருள், பயன்பாட்டு நிரல்கள் மற்றும் பிரயோக மென்பொருள் (உதாரணம். வார்த்தை செயலாக்க பொதிகள்: word processing packages, தரவுத்தளங்கள்: databases, உலாவிகள்: browsers, தீம்பொருள் எதிர்ப்பு: யவெலையுடறயசந போன்றவை) ஆகியவற்றை உள்ளடக்குகின்றது, ஆனால் அதற்குள் மட்டுப்படுத்தப்படவில்லை



விற்பனையாளர் வழங்கிய சமீபத்திய இணைப்புகள் மற்றும் திருத்தங்களுடன் இயக்க முறைமைகள் மற்றும் ஏனைய தொடர்புடைய மென்பொருள்களை நிறுவனம் புதுப்பித்தல் வேண்டும். மேலும், நிறுவனங்கள் தானியங்கி புதுப்பிப்புகளை இயக்குதல் வேண்டும். முன்னதாக, அவற்றினை நிறுவுவதால் ஏற்படும் உள்ளார்ந்த பாதிப்பு குறித்து உரிய வகையில் மதிப்பீடு செய்யப்படுதல் வேண்டும். (குறிப்பாக மிகவும் சிக்கல் வாய்ந்த மற்றும் சிக்கலான முறையில் வகைப்படுத்தப்பட்ட தகவல் தொழில்நுட்ப சொத்துக்களுக்கானவை)

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.8. தீம்பொருள் எதிர்ப்பு மீதான கொள்கை

நிறுவனமானது, செல்லுபடியாகும் உரிமத்துடன் தீம்பொருள் எதிர்ப்பு மென்பொருளை நிறுவுதல் வேண்டும். தீம்பொருள் எதிர்ப்பு கருவிகள், எந்த சாத்தியமான நுழைவு புள்ளியிலும் செயலில் இருக்கும் என்பதுடன், மிகப் புதிய தீம்பொருள் கையொப்பங்கள் நாளாந்தம் வரைப்படுத்தப்படுவதுடன், தானியங்கி முறையில் இறறைப்படுத்தல்கள் செயற்படுத்தப்படுதலும் வேண்டும்.

கோப்புகளைபதிவிறக்கம்செய்தல் அல்லது திறத்தல், அகற்றக்கூடிய அல்லது தொலைநிலை சேமிப்பகத்தில் உள்ள கோப்புறைகள் மற்றும் வலைப் பக்க ஸ்கானிங் உள்ளடங்கலாக அணுகுகின்ற போதான பரிசோதனைக்கு ஏற்ப தீம்பொருள் கண்டறிதல் கட்டமைக்கப்படுதல் வேண்டும்.

அரசாங்க நிறுவனமொன்று இன்னொரு நிறுவனத்துடன் அல்லது பொது மக்களுடன் இலத்திரனியல் முறையினூடாக தொடர்பு கொள்ளும் போது, அனுப்புவர் தகவலானது தீம்பொருள் தாக்கத்திலிருந்து விடுபட்டது என்பதனை உறுதி செய்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.9. உத்தியோகபூர்வ மின்னஞ்சல்கள் மீதான கொள்கை

நிறுவனம், உத்தியோகபூர்வ தகவல் தொடர்புகளுக்கு உத்தியோகபூர்வ மின்னஞ்சல்களைப் பயன்படுத்துதல் வேண்டும். ஊழியர்கள் தனிப்பட்ட தொடர்பாடல்களுக்கு உத்தியோகபூர்வ மின்னஞ்சல்களைப் பயன்படுத்துதலாகாது.

உத்தியோகபூர்வ மின்னஞ்சல்கள் என்பது "gov.lk" என்ற தளப் பெயருடன் அரசாங்கத்தால் வழங்கப்பட்ட மின்னஞ்சல் ஆகும். உத்தியோகபூர்வ மின்னஞ்சல் கணக்குகள், உத்தியோகபூர்வ தளங்கள் என்பதுடன், நிறுவனம், கணக்கை அணுகுவதற்கு, மின்னஞ்சல்களைப் படிப்பதற்கு அல்லது கணக்கை நீக்குவதற்கான உரிமையைக் கொண்டுள்ளது.

அனைத்து மின்னஞ்சல் இணைப்புகளும், மூலம் அல்லது உள்ளடக்கத்தைப் பொருட்படுத்தாது, எந்தவொரு அரசாங்க நிறுவனத்தின் கணினி முறைமையில் திறக்கப்படுவதற்கு அல்லது சேமிக்கப்படுவதற்கு முன்பு வைரஸ்கள் மற்றும் பிற அழிவுத் திட்டங்களுக்காக ஸ்கான் செய்யப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்

4.3.10. மின்னஞ்சல்களின் பாதுகாப்பு மீதான கொள்கை

நிறுவனமானது, பொருந்தக்கூடிய அனைத்து பாதுகாப்பு அம்சங்களுடன் அவர்களது மின்னஞ்சல் கணக்குகளை கட்டமைத்தல் வேண்டும். தகவல் பாதுகாப்பை உறுதிப்படுத்துவதற்கு, மின்னஞ்சல் சேவையகமானது, தரவு பாதுகாப்பு தொடர்பான உரிய சட்டங்களுடன் இணங்கி ஒழுக்குதல் வேண்டும்.

தீம்பொருள் இணைக்கப்பட்டுள்ளதாக அறியப்பட்ட மின்னஞ்சல்களை அகற்றவும், கோரப்படாத மற்றும் விரும்பத்தகாத ("ஸ்பாம்") மின்னஞ்சல் மூலம் இன்பாக்ஸ் குழப்பப்படுவதைத் தடுப்பதற்கும் தாபனம் மின்னஞ்சல் வடிகட்டிகளை அமைத்தல் வேண்டும். மேலும், மின்னஞ்சல்கள் மூலம் உணர்திறன் மிக்க தகவல்களை அனுப்புகின்ற போது, அது குறியாக்கம் செய்யப்படுதல் வேண்டும்.

இலங்கை அரசாங்கவலையமைப்பினால் வழங்கப்பட்ட மின்னஞ்சல்கணக்குகளைப் பொறுத்தவரையில், மின்னஞ்சல் சேவை பாதுகாப்பாக உருவாக்கப்படுவதை உறுதிப்படுத்துவதற்கு தகவல் மற்றும் தொடர்பாடல் தொழில்நுட்ப முகவரான்மை தேவைப்படுவதுடன், மேற்பார்வை அல்லது ஒழுங்குபடுத்தும் தேவைப்பாடுகளுக்கு காலமுறை அடிப்படையில் பாதுகாப்பு ஆய்வு அறிக்கைகள் இலங்கை சேர்ட் இடமிருந்து பெறப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.11. டிஜிட்டல் கையொப்பங்கள் மீதான கொள்கை

பொருத்தமானவிடத்து, நிறுவனமானது டிஜிட்டல் கையொப்பங்களை நடைமுறைப்படுத்துதல் வேண்டும். அதேபோன்று, நம்பகத்தன்மை (authenticity), நேர்மை (integrity), மற்றும் மறுதலிப்பு (nonrepudiation) ஆகியவற்றை உறுதி செய்வதற்கு மின்னஞ்சல்களுக்கு டிஜிட்டல் கையொப்பங்கள் பயன்படுத்தப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.12. சுற்றுவட்ட பாதுகாப்புக் கட்டுப்பாடுகள் மீதான கொள்கை

இணைய தாக்குதல்களுக்கு எதிராக ஆதனங்களுக்கு (தகவல், கணினிகள், வலையமைப்புகள் மற்றும் முறைமைகள் ஆதனங்கள்) பாதுகாப்பை வழங்கவும், தீங்கிழைக்கும் மென்பொருள் இணையம் வழியாக ஆதனங்களை அணுகுவதிலிருந்து தடுப்பதற்கும் தாபனமானது, .பயர்வால்ஸ், ஊடுருவலைக் கண்டறியும் முறைமைகள் (intrusion detection systems) மற்றும் ஊடுருவலை தடுக்கும் முறைமைகள் (intrusion prevention systems) போன்ற அத்தகைய சுற்றுவட்டப் பாதுகாப்பு கட்டுப்பாடுகளை நிறுவுதல் வேண்டும்.

நிறுவனமானது, சுற்றுவட்டப் பாதுகாப்பு அச்சுறுத்தல் தரவுத்தளத்தை (threat databases) கிரமமாக இற்றைப்படுத்துதல் வேண்டும், தானியங்கி இற்றைப்படுத்தல் ஏற்பாடுகளுடன் தீம்பொருள் எதிர்ப்பு நிறுவப்படுதல் வேண்டும், பொருத்தமான கட்டமைப்புகளுடன் இயல்புநிலை அமைப்புகளை (default settings) இற்றைப்படுத்துதல் வேண்டும், மற்றும் அத்தகைய சாதனங்களுக்கும், முறைமைகளுக்குமாக வழங்கப்பட்ட பயன்படுத்துபவரின் கணக்குகளின் இயல்பு நிலையை விற்பனையாளர் முடக்குதல் வேண்டும்..

தகவல் மற்றும் சைபர் பாதுகாப்பு நடைமுறைப்படுத்தல் வழிகாட்டியில் வழங்கப்பட்டுள்ள சாதனங்களைக் கட்டுப்படுத்தும் பாதுகாப்பு கட்டமைப்பு விபரங்கள் பற்றிய கண்டே-ணாட்டமொன்றை வழங்குகின்றது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.1.13. தொலையியக்கி அணுகலைப் பெறுதல் மீதான கொள்கை

நிறுவனமானது, புவியியல் ரீதியாக தொலைதூர அமைவிடங்களிலுடாக அதிகாரமளிக்கப்படாத அணுகலைத் தடுப்பதற்கு உள் வலையமைப்புகளுக்கு தொலையியக்கி அணுகலைப் பெறுதல் வேண்டும்.



தொலையியக்கி அணுகலானது, நிறுவனத்திற்கு பல தகவல் பாதுகாப்பு அச்சுறுத்தல்களை கொண்டு வருகின்றது. பொது இணையத்தில் தகவல்கள் செல்கின்ற போது ஒட்டுக்கேட்கும் ஆபத்து, முறைமைகள் அல்லது தரவினை அதிகாரமின்றி அணுகுதல் மற்றும் தரவு மற்றும் தீம்பொருள் தொற்றுக்களை

கண்காணித்தலும் கையாளுதலும் ஆகியவை தொலையியக்கி அணுகலுடன் இணைந்து காணப்படுகின்ற பொதுவான பாதுகாப்பு அபாயங்களாகும்.

தொலையியக்கி அணுகல் அபாயத்தைக் குறைப்பதற்கு, தாபனம் பாதுகாப்பான மெய்நிகர் தனியார் வலையமைப்புகளைப் (Virtual Private Networks) பயன்படுத்துதல் வேண்டும், அதிகாரமளிக்கப்பட்டு பயன்படுத்துபவர்கள் மட்டுமே தாபனத்தின் இனங்காணும் முகாமைத்துவத்தின் மற்றும் அணுகல் கட்டுப்பாட்டு கொள்கையின் அடிப்படையில் முறைமைகளை அணுகுவதற்கு அனுமதித்தல் வேண்டும், பல் காரணி உறுதிப்படுத்தலை நடைமுறைப்படுத்துதல் வேண்டும், வாடிக்கையாளர் சாதனங்களில் இருந்து தொலைநிலை அணுகலை பாதுகாக்க வேண்டும் என்பதுடன், நம்பகமான வலையமைப்புகளைப் பயன்படுத்துதலும் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.14. காப்பு மூலோபாயத்தின் மீதான கொள்கை

நிறுவனமானது, அனர்த்தமொன்று ஏற்படுகின்ற சந்தர்ப்பத்தில், வழமையான செயற்பாடுகளை மீண்டும்கொண்டு வருவதற்குத் தேவையான காப்புத் தரவு, பதிவுகள், முறைமைகள், மென்பொருள், உருவாக்க விபரங்கள் மற்றும் ஏனைய தகவல்களை மீட்டெடுக்க மூலோபாயமொன்றைக் கொண்டிருத்தல் வேண்டும். இந்த மூலோபாயம் தாபனத்தின் அனர்த்த மீட்பு திட்டத்துடன் இணைக்கப்படுதல் வேண்டும் (பிரிவு 4.6.1 இணைப் பார்க்கவும்).

நிறுவனமானது எவையேனும் சீர்குலைந்த சேவைகளினை முழுமையாக மீளமைப்பதற்கு அல்லது மீட்பதற்கு காப்பு ஊடகங்கள் பயன்படுத்தப்பட முடியுமென்பதனை உறுதி செய்தல் வேண்டும்..

அரசாங்கத்தின் ஒழுங்குமுறைப்படுத்தும் தேவைப்பாடுகளின்படி, காப்பு ஊடகத்தில் எழுதப்பட்ட தரவானது பாதுகாக்கப்படுதல் வேண்டும்.

நிறுவனமானது, காப்புஅதிர்வேண்ணைத் தீர்மானிப்பதற்கு மீட்பு நேரம் நோக்கம் (Recovery Time Objective: RTO) மற்றும் மீட்பு புள்ளி நோக்கம் (Recovery Point Objective: RPO) ஆகியவற்றையும் வரையறுத்தல் வேண்டும்.

இது, ரன்சம்வெயர் மென்பொருள் உள்ளடங்கலாக எந்தவொரு தீங்கிழைக்கும் தாக்குதல்களிலிருந்தும் நேரடித் தரவினைப் பாதுகாப்பதற்காக நேரடித் தரவு மற்றும் காப்பு தரவுக்கு இடையே காற்று இடைவெளியொன்று (air gap) இருத்தல் வேண்டும் என்று பரிந்துரைக்கின்றது.



இது, காப்பு தரவு செயலாக்க தளத்தில் இருந்து பௌதீக ரீதியில் தொலைவிலிருக்கின்ற தீப்பற்றாத, பாதுகாப்பான அமைவிடத்தில் சேமிக்கப்படுதல் வேண்டும் என்று மேலும் பரிந்துரைக்கின்றது. இது ஒரு தீ ஆதாரம், பாதுகாப்பான இடத்தில் சேமிக்கப்படும் என்று காப்புப் பிரதிகளில் ஏதேனும் மாற்றங்கள் மேற்கொள்ளப்பட்டுள்ளனவா என்பதைக் கண்டறிவதற்கான பொறிமுறையொன்றும் நடைமுறைப்படுத்தப்படுதல் வேண்டும். "மிக இரகசியமானது" மற்றும் "இரகசியமானது" என்று பெயரிடப்பட்ட தகவல் ஆதனங்களைக் கொண்ட காப்புப்பிரதிகள், ஆதனங்கள் பதிவேட்டில் குறிப்பிடப்பட்டுள்ள பாதுகாப்பு தேவைப்பாடுகளுக்கு ஏற்ப சேமிக்கப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3.15. அரசாங்க நிறுவனங்களால் வழங்கப்பட்ட சொத்துக்களின் பாதுகாப்பு மீதான கொள்கை

இன்று பல அரசு மற்றும் அரசாங்க நிறுவனங்கள் அரசாங்கத்தால் வழங்கப்படும் தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களில் (டிஜிட்டல் உள்ளகட்டமைப்பு, இலத்திரனியல் சேவைகள், பயன்பாடுகள்) செயல்படுகின்றன. இச்சூழலில், தகவல் தொடர்பாடல் தொழில்நுட்ப நிறுவனம் (Information Communication Technology Agency: ICTA) அல்லது ஏனைய அரசு நிறுவனங்கள் தங்களால் உருவாக்கப்பட்ட தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களின் பாதுகாப்பு, நம்பகத்தன்மை (reliability), நேர்மைத்துவம் (integrity) மற்றும் துல்லியம் (accuracy) ஆகியவற்றை உறுதி செய்ய வேண்டும். உதாரணமாக, லங்கா அரசு வலையமைப்பு (Lanka Government Network) லங்கா அரசு கிளவுட் (Lanka Government Cloud) மின்னஞ்சல் சேவை (Email Service) லங்கா அரசு கட்டணமுறை (Lanka Government Payment System), குறுஞ் செய்தி சேவை (Short Message Service) ஆகியவை முகாமைத்துவ முறைமை

(Document Management System) அல்லது ஏனைய சேவைகளின் பாதுகாப்பு, அத்தகைய உட்கட்டமைப்பை உருவாக்கிய தொடர்புடைய நிறுவனத்தால் உத்தரவாதம் அளிக்கப்படுதல் வேண்டும். இந்த உட்கட்டமைப்புகளுக்கு தேவையான பாதுகாப்பு சான்றிதழ்கள் இலங்கை சேர்ட் இலிருந்து அல்லது வேறு ஏதேனும் தகுதி வாய்ந்த நிறுவனத்திடம் இருந்து சம்பந்தப்பட்ட நிறுவனங்களால் பெறப்படுதல் வேண்டும்.

மேற்கொள்ளப்படும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

4.3.16. வடிவமைப்பு மூலமான பாதுகாப்பு தொடர்பான கொள்கை

இந்த அமைப்பு மென்பொருள் பெறுகைகள் மற்றும் உள்ளக மென்பொருள் உருவாக்கத்தில் வடிவமைப்பு மூலம் பாதுகாப்பு என்ற அணுகுமுறையைப் பின்பற்றுவதல் வேண்டும். வடிவமைப்பு மூலம் பாதுகாப்பு என்ற அணுகுமுறை மென்பொருள் வளர்ச்சி வாழ்க்கை சுழற்சியின் ஒவ்வொரு கட்டத்திற்கும் பாதுகாப்பு அவதானிப்புகளை சேர்ப்பதன் மூலம் பாரம்பரிய மென்பொருள் வளர்ச்சி அணுகுமுறையை நீடிக்கின்றது.

மென்பொருளை உருவாக்குவதில் (அல்லது மென்பொருளைப் பெறுவதில்), நிறுவனம், பாதுகாப்பு திட்டமிடல் மற்றும் கருத்திட்ட திட்டமிடல் நிலையில் ஆபத்து பற்றிய மதிப்பீடுகளை நடத்துதல், விலைமனு ஆவணங்களில் பாதுகாப்பு தேவைப்பாடுகளை வரையறுத்தல்.

வடிவமைப்பில், அபிவிருத்திக் கட்டத்தில் பாதுகாப்பு கட்டிடமைப்பை மதிப்பாய்வு செய்தல், பாதுகாப்பு தொடர்பான பலவீனங்களை (குறைபாடுகள்) கண்டறிவதற்கான வளர்ச்சி கட்டத்தில் குறியீட்டை மதிப்பாய்வு செய்தல் மற்றும் அமைப்புகளில் உள்ள பாதுகாப்பு பலவீனங்களை அடையாளம் காண செயற்படுத்தும் கட்டத்தில் பாதிப்பு மதிப்பீடுகளைச் செய்தல்.

இறுதியில், முறைமை நீக்கப்படுகின்ற நிலையில், அமைப்புகள் அதன் தரவு மற்றும் பிற தகவல் ஆதனங்களை அனுமதியளிக்கப்படாத தனிநபர்களால் அணுகவும் மீட்கவும் முடியாது என்பதை உறுதி செய்வதற்கு முறைமைகள் பாதுகாப்பாக அகற்றப்படுதல் வேண்டும்.

”தகவல் மற்றும் சைபர் பாதுகாப்பினை நடைமுறைப்படுத்தும் வழிகாட்டி” பாதுகாப்பான பிரயோகத்தை விருத்தி செய்யும் வாழ்க்கை சுழற்சி பற்றிய விபரங்களை வழங்குகின்றது.”

இந்த நிறுவனம் சைபர் பிரயோகங்களை விருத்தி செய்கின்ற போது, இலங்கை ‘சேர்ட்’ இனால் வழங்கப்பட்ட அரசு நிறுவனங்களுக்கான ”இணைய தள பாதுகாப்பு வழிகாட்டுதல்கள், இணைய பிரயோக பாதுகாப்புக்கான வழிகாட்டல்கள்”, என்பவற்றை பின்பற்றுவதல் வேண்டும்.

இந்த வழிகாட்டுதல்களை www.onlinesafety.lk எனும் இணைய தளத்திலிருந்து பதிவிறக்கம் செய்யலாம்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.17. சொத்துக்களை பாதுகாப்பாக அகற்றுதல் தொடர்பான கொள்கை

சொத்துக்கள் இதற்குமேலும் தேவைப்படாத போது முறையான நடைமுறையைப் பயன்படுத்தி பாதுகாப்பாக அகற்றப்படுதல் வேண்டும். கட்புல ஊடகங்கள் (இறுவட்டுக்கள் அல்லது டிவிடிகள்), காந்த ஊடகம் (நாடாக்கள் அல்லது இறுவட்டுக்கள்), வட்டு இயக்கிகள் (வெளிப்புற, சிறிய அல்லது தகவல் முறைமைகளிலிருந்து அகற்றுதல்), ‘.பிளா’ ஞாபக சேமிப்பு சாதனங்கள் (எஸ்எஸ்டி கள் அல்லது யுஎஸ்பி ‘.பிளா’ டிரைவ்கள்) மற்றும் ஆவணங்கள் (காகித ஆவணங்கள், காகித வெளியீடு அல்லது புகைப்பட ஊடகம்) ஆகியவற்றை உள்ளடக்குகின்ற, ஆனால் அதற்குள் வரையறுக்கப்படாத நிறுவனங்க



ளின் சேமிப்பு ஊடகம் பாதுகாப்பாக அகற்றப்படுதல் வேண்டுமென்று தேவைப்படுத்தப்படுகின்றது. இனி தேவைப்படாத தகவல்கள் ஊடகத்தில் இருந்தால், அசல் தகவலை மீட்டெடுப்பதைத் தடுப்பதற்கு, தகவல் மீட்க முடியாத முறையில் நீக்கப்படுதல் வேண்டும்.. துறைசார் வடிவமைப்பு (sector-based formatting) என்பது ஊடகங்களில் உள்ள தகவல் ஆதனங்களை அகற்றுவதற்கான சாத்தியமான முறையாகும். தகவல் ஆதனங்களைக் கொண்ட ஊடகங்களை நிரந்தரமாக அழிப்பதற்கான சாத்தியமான வழிகள் துண்டாக்குதல் அல்லது குத்துதல் ஆகும். சேமிப்பு ஊடகத்தில் உள்ள ஆதனங்கள் "மிக இரகசியமானது" அல்லது "இரகசியமானது" என வகைப்படுத்தப்பட்டால், தகவல் பாதுகாப்பு குழுவிடமிருந்து அகற்றும் நடவடிக்கைக்கு முறையான அனுமதியைப் பெற்றதன் பின்னர், ஊடகங்களை பௌதீக ரீதியாக அழிப்பதே பாதுகாப்பான முறையாகும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3.18. உள்ளக தகவல் இணைய பாதுகாப்பு கணக்காய்வு திட்டம் மீதான கொள்கை.

நிறுவனமானது, தகவல் தொழில்நுட்ப பாதுகாப்பு கட்டுப்பாட்டு ஆய்வுகள், பிரயோகப் பாதுகாப்பு கட்டுப்பாட்டு மீளாய்வுகள், வலையமைப்பு நிருமாண மீளாய்வுகள், தகவல் தொழில்நுட்ப செயல்முறை ஆய்வுகள், பாதுகாப்பு இணக்க மீளாய்வுகள், உள்ளக மற்றும் வெளிப்புற பாதிப்பு பற்றிய மதிப்பீடுகள் (vulnerability assessments) ஊடுருவல் பற்றிய சோதனை மற்றும் வலையமைப்பு பிரயோக ஊடுருவல் சோதனை (penetration tests) ஆகியவற்றை உள்ளடக்கிய, ஆனால் அதற்குள் மட்டுப்படுத்தப்படாத வழக்கமான ஆய்வுகளை நடத்துவதற்கு நிறுவனம் முறையானதொரு உள்ளக தகவல் பாதுகாப்பு ஆய்வுத் திட்டத்தைக் கொண்டிருத்தல் வேண்டும்.

மதிப்பீடுகளானவை, சம்பவமொன்று நிகழ்ந்ததன் பின்னர், மாற்றமொன்று அறிமுகப்படுத்தப்பட்டதன் பின்னர் (பிரயோகத்திற்கு அல்லது பேணுகின்ற சூழலுக்கு), நியமத்தில் அல்லது வழிகாட்டல்களில் மாற்றங்கள் ஏற்பட்டதன் பின்னர், வைரஸ் அல்லது தீம்பொருள் பரவியதன் பின்னர், அல்லது தகவல் பாதுகாப்பு குழுவினால் தீர்மானிக்கப்பட்டதன் பின்னர், காலத்திற்குக் காலம் (குறைந்தபட்சம் ஆண்டு தோறும்) மேற்கொள்ளப்படுதல் வேண்டும்.

நிறுவனத்தின் (பிரதான) உள்ளக கணக்காய்வாளர் ஆய்வினை ஒருங்கிணைத்தல் வேண்டும் என்பதுடன், ஒவ்வொரு அமைச்சினதும் பிரதம உள்ளக கணக்காய்வாளர் அதன் அதிகாரத்தின் கீழ் தாபனங்களின் தகவல் பாதுகாப்பு ஆய்வுகளை ஒருங்கிணைத்தல் வேண்டும்.

கணக்காய்வு அறிக்கைகளில் எழுப்பப்பட்ட பரிந்துரைகளை நடைமுறைப்படுத்துவதை பார்வையிடுவதற்காக முறைசார் செயல்முறை நிறுவனத்தால் நிறுவப்படவுள்ளது. முறைமையினை (பிரதம) உள்ளக கணக்காய்வாளர் தலைமையை எடுத்து இந்த செயல்முறையினைப் பொறுப்பேற்றல் வேண்டும்.

அத்தகைய ஆய்வுகளை மேற்கொள்வதற்கு தகைமை வாய்ந்த தரப்பொன்றினால் ஆய்வுகள் மேற்கொள்ளப்படுதல் வேண்டும் அல்லது இலங்கை சேர்ட் இன் சேவையைப் பெறுதல் வேண்டும். ஆய்வுகள் மூன்றாம் தரப்பினரால் மேற்கொள்ளப்பட வேண்டுமாயின், தாபனத்தின் ஆதனங்களின் இரகசியத்தன்மையை உறுதிசெய்வதற்கு, வெளிப்படுத்தல் அல்லாத ஒப்பந்தம் (Non Disclosure Agreement) கைச்சாத்திடப்படுதல் வேண்டும் என்பது எ அத்தியவசியமானகும்

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.19. பயன்படுத்துவதற்கு முன்னரான கணக்காய்வு மீதான கொள்கை

உள்ளக தகவல் பாதுகாப்பு ஆய்வுத் திட்டத்திற்கு இணையாக, தாபனமானது, நேரடி சூழலில் எந்தவொரு இணையத்தளத்தை, இணையப் பயன்பாட்டை அல்லது முறைமையைப் பயன்படுத்துவதற்கு முன்னர் பாதிப்புப் பற்றிய மதிப்பீடுகள் மற்றும் ஊடுருவல் சோதனைகளை (vulnerability assessment and penetration tests) மேற்கொள்ளுதல் வேண்டும்.

இந்த மதிப்பீடுகளை, இலங்கை சேர்ட் உடன் கலந்தாலோசித்து தகுதியான மூன்றாம் தரப்பினரால் நடத்தப்படுவதற்கு அல்லது இலங்கை சேர்ட் இனது சேவையை இந்நிறுவனம் பெறுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3.20. முறைமைகளைக் கடினமாக்குதல் மீதான கொள்கை

நிறுவனமானது, சாத்தியமான தாக்குதல் வெக்டர்கள் நீக்குவதன் மூலம் மற்றும் முறைமைகளின் தாக்குதல் மேற்பரப்பினை ஒடுக்குவதன் மூலம் அவற்றின் மேற்பரப்பின்பாதிப்பினைக் குறைப்பதற்கு தகவல் தொழில்நுட்ப ஆதனங்களை கடினப்படுத்துதல் (hardening) வேண்டும்.. உதாரணமாக, இயக்க அமைப்புகள், சேவையகங்கள், வலையமைப்புகள் மற்றும் வலையமைப்பு சாதனங்கள், தரவுத் தளங்கள், மற்றும் மெய்நிகர் தனியார் வலையமைப்புகளை நிறுவனமானது கடினப்படுத்துதல் வேண்டும். கணினிகள் கடினப்படுத்துதல் பற்றிய வழிகாட்டுதல்கள் தகவல் பாதுகாப்பு செயலாக்க வழிகாட்டியில் வழங்கப்பட்டுள்ளன.



அனுபவம் வாய்ந்த மற்றும் திறமையான பணியாளர்களின் ஆதரவுடன் மட்டுமே கடினப்படுத்தும் முறைமைகள் மேற்கொள்ளப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3.21. வீட்டிலிருந்து பணியாற்றுவதில் மீதான கொள்கை

வீட்டிலிருந்து பணியாற்றுவதற்கு மாறுகின்ற போது (அல்லது தொலைதூர இடங்களில் இருந்து வேலை செய்யும் பொழுது), தகவல் பாதுகாப்பு அச்சுறுத்தல்கள் அதிகரித்துள்ளன. ஆகவே, பணியாளர்கள், தொலைதூரத்திலிருந்து வேலை செய்கின்ற போது சிறந்த பாதுகாப்பு நடைமுறைகளின் தொகுப்பை எடுத்துக்காட்டுகின்ற இலங்கை சேர்ட் இனால் வெளியிடப்பட்ட, "வீட்டிலிருந்து பணியாற்றுவதற்கான தகவல் பாதுகாப்பு வழிகாட்டுதல்களை" கடைப்பிடித்தல் வேண்டும். இதுதொலைவிலிருந்து வேலை செய்வதற்கு அனுமதிக்கப்படுகின்றபோது நிறுவனத்தின் தகவல் தொழில்நுட்ப ஆதனங்களை பாதுகாப்பாக அணுகுவதை உறுதி செய்வதற்கு இலங்கை சேர்ட் இனால் வழங்கப்பட்ட "தகவல் தொழில்நுட்ப நிருவாகிகளுக்கான குறைந்தபட்ச வழிகாட்டல்களை" தகவல் தொழில்நுட்ப நிருவாகிகள் பின்பற்றுவதில் வேண்டும்.

இதனை www.onlinesafety.lk எனும் இணைய தளத்திலிருந்து பதிவிறக்கம் செய்யலாம்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.3.22. உத்தியோகபூர்வ வேலைக்காக தங்களது சொந்த சாதனத்தைப் பயன்படுத்துதல்.

நிறுவனமானது, பணியாளர்கள் தமது தனிப்பட்ட மடிக் கணினிகள், ஸ்மார்ட் போன்கள் மற்றும் 'டப்டுகளைப் பயன்படுத்தி உத்தியோகபூர்வ கடமைகளை மேற்கொள்வதற்கான அனுமதி தவிர்க்கப்படுதல் வேண்டும்.

எனினும், தகவல்பாதுகாப்புமுவினால் தீர்மானிக்கப்பட்ட குறிப்பிட்ட சூழ்நிலைகளில், தாபனமானது, தகவல் பாதுகாப்பு உத்தியோகத்தின் மேற்பார்வையின் கீழ், தேர்ந்தெடுக்கப்பட்ட பணியாளர்களை உத்தியோகபூர்வ கடமைகளை ஆற்றுவதற்கு தமது தனிப்பட்ட சாதனங்களைப் பயன்படுத்துவதற்கு அனுமதிக்கலாம்.

இதுபோன்ற சூழ்நிலைகளில், சாதனங்கள் நிறுவனத்தில் சரியான முறையில் பதிவு செய்யப்படுவதும், அத்தகைய சாதனங்கள் இந்தக் கொள்கைக்கு இணங்குவதை உறுதி செய்வதும் அவசியமாகும்.



எந்த சந்தர்ப்பத்திலும் "மிக இரகசியமானது" (Confidential) மற்றும் "இரகசியமானது" (Secret) என்று வகைப்படுத்தப்பட்ட தகவலை செயற்படுத்த அல்லது சேமிக்க பணியாளர்களின் தனிப்பட்ட சாதனங்கள் பயன்படுத்தப்படுதலாகாது.

உத்தியோகபூர்வ கடமைகளை ஆற்றுவதற்கு ஊழியர்களது தனிப்பட்ட சாதனங்கள் பயன்படுத்தப்படும் போது, தாபனமானது, பயன்படுத்துபவர்களின் கணக்குகள் வரையறுக்கப்பட்ட சிறப்புரிமைகளைக் கொண்டவை, கணக்குகள் வலுவான கடவுச்சொற்கள் மற்றும் பல் ஆக்கக்கூற்று உறுதிப்படுத்தப்படுதலுடன் பாதுகாக்கப்படுகின்றன, தீம்பொருள் எதிர்ப்பு மென்பொருள் நிறுவப்பட்டு, தானியங்கி இற்றைப்படுத்தல்கள் செயற்படுத்தப்படுகின்றன, இயக்க முறைமைகள், பயன்பாட்டு மென்பொருள் மற்றும் பயன்படுத்தப்படுகின்ற ஏனைய பிரயோக மென்பொருள் தேவையான இணைப்பு இற்றைப்படுத்தல்களுடன் செல்லுபடியாகும் உரிமங்களைக் கொண்டுள்ளன என்பவற்றை உறுதிப்படுத்துதல் வேண்டும்.

மேலும், உத்தியோகபூர்வ வேலைக்கு தனிப்பட்ட சாதனங்களில் தனிப்பட்ட மற்றும் நிறுவனத் தகவல்களை மதிப்பாய்வு செய்ய அல்லது தக்க வைத்துக்கொள்ள அல்லது விசாரணை அல்லது சட்டத் தேவையின் போது அரசாங்க முகவர் அல்லது மூன்றாம் தரப்பினருக்கு தகவலை வெளியிடுவதற்கான உரிமையை நிறுவனம் கொண்டுள்ளது.

தனிப்பட்ட சாதனத்தின் பாதுகாப்பானது, சாதனத்தின் உரிமையாளரின் பொறுப்பாகும். சாதனத்தின் பயன்பாட்டின் காரணமாக தனிப்பட்ட தரவை இழப்பது உள்ளடங்கலாக சாதனத்திற்கு ஏற்படும் இழப்பு அல்லது சேதத்திற்கு தாபனம் பொறுப்பேற்காது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.3.23. பாதுகாப்பற்ற வலையமைப்புக்களின் பயன்படுத்துவது தொடர்பான கொள்கை.

நிறுவனத்தின் ஊழியர்கள், உத்தியோகபூர்வ மின்னஞ்சல் மற்றும் உத்தியோகபூர்வ மென்பொருள் தீர்வுகளை அணுகுவதற்கு நம்பமுடியாதவை .பைவலையமைப்புகள் (உ.ம். ஹோட்டல்கள், உணவகங்கள், பேருந்து தரிப்பிடங்களில் கிடைப்பவை) மற்றும் ஏனைய பொதுவில் பகிரப்பட்ட தனிப்பட்ட கணினிகள், கியோஸ்க்குகள் (kiosks) மற்றும் ஏனைய தொடர்புடைய சாதனங்கள் போன்ற பாதுகாப்பற்ற வலையமைப்புகளைப் பயன்படுத்துவதைத் தவிர்த்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்..

4.3.24. வழங்குனர் முகாமைத்தவம் மீதான கொள்கை

தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை உருவாக்கி நிருவகிப்பதில் வெளிப்புறத் தரப்பினர் (வன்பொருள், மென்பொருள், வலையமைப்புகள், ஹோஸ்டிங் மற்றும் நிருவகிக்கப்பட்ட சேவைகள் போன்றவை) ஈடுபடும் போது தகுந்த நடவடிக்கைகள் எடுக்கப்படுவதை நிறுவனம் உறுதி செய்யும்.

தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்களை அபிவிருத்தி செய்வதிலும் முகாமைசெய்வதில் வெளித் தரப்பினர் ஈடுபடுகின்ற போது பொருத்தமான நடவடிக்கைகள் எடுக்கப்படுவதை நிறுவனம் உறுதி செய்யும். இது வன்பொருள், மென்பொருள் மற்றும் பேணுதல் சேவை வழங்குநர்களுக்கு மட்டுமே ஏற்படையது, ஆனால் அதற்குள் மட்டுப்படுத்தப்பட்டதல்ல.

வற்பனையாளர் முகாமைத்துவத்தை மேற்கொள்வதில், தாபனம் குறைந்தபட்சம் பின்வருவனவற்றைக் கவனத்தில் கொள்ள வேண்டியிருக்கின்றது: (அ) காப்பு, சேமிப்பு, மீட்டும் மற்றும் இடைநேர் ஏற்பாடுகள், பாதுகாப்பு கட்டமைப்புகள், தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்கள் போன்றவற்றை அணுகுதல் ஆகியன உள்ளடங்கலாக, ஆனால் இதற்குள் மட்டுப்படுத்தப்படாத ஒப்பந்தத் தரப்பினரின் பொறுப்புகள் மற்றும் கடமைகளை இனங்காணுதல், (ஆ) அரசாங்கத்தால் தெளிவுபடுத்தப்பட்டவாறு தாபனத்தால் உருவாக்கப்பட்ட தகவல் பாதுகாப்பு நடைமுறைகளைப் பின்பற்றுதல், (இ) ஒப்பந்தத்துடன் தொடர்புபட்டுள்ள ஒப்பந்த தரப்பின் செயல்முறைகளையும், கட்டுப்பாடுகளையும் ஆய்வு செய்யும் உரிமை மற்றும் (ஈ) ஒப்பந்த நியதிகள் மற்றும் நிபந்தனைகளை பின்பற்றாது பற்றிய கண்காணிப்பும் அறிக்கையிடலும். ஒப்பந்ததரப்புகளுடனான உறவுகளை முகாமை செய்கின்ற பொறுப்பு, நிறுவனத்தின் தலைமை உத்தியோகத்தரினால் தீர்மானிக்கப்பட்டவாறு, நியமிக்கப்பட்ட சொத்து உரிமையாளர்கள், நியமிக்கப்பட்ட அதிகாரிகள் அல்லது நிறுவனங்களுக்கு ஒதுக்கப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்..

4.3.25. மாற்றல் முகாமைத்துவம் மீதான கொள்கை

நிறுவனமானது, அனைத்து மாற்றங்களையும் கட்டுப்படுத்துதல் வேண்டும். முகாமை செய்யப்படாத மாற்றங்கள் தகவல் மற்றும் தகவல் தொழில்நுட்ப சாதனங்களுக்கு அபாயங்களை ஏற்படுத்துகின்றன என்பதுடன், செயல்பாட்டு இடையூறுகளை ஏற்படுத்தும் திறனையும் கொண்டுள்ளன. உதாரணமாக, கட்டுப்பாடற்ற நிறுவல்கள் (அல்லது நிறுவல் நீக்கங்கள்), உட்புகுத்தல்கள், நீக்குதல்கள் மற்றும் முறைமைகளுக்கான மாற்றங்கள், இரகசியத்தன்மை, நேர்மை மற்றும் தரவு கிடைக்கும் பண்புக்கூறுகளை பாதிக்கலாம் அல்லது முறைமையின் தொகுப்பிற்கு வழிவகுக்கும் முறைமைக்கு பாதிப்புகளை ஏற்படுத்தலாம்.

மேலும், மாற்றங்களில் ஈடுபட்டுள்ள ஊழியர்கள், செயற்பாட்டுத் தகவலின் இரகசியத்தன்மைக்கு அச்சுறுத்தல்களை ஏற்படுத்தலாம். ஆகவே, முறைமைக்கான ஒட்டுமொத்த பாதுகாப்பு ஆபத்தைக் குறைப்பதற்கு தகவல் பாதுகாப்பு குழு முறையானதொரு மாற்ற முகாமைச் செயல்முறையை அமுல்படுத்த வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்..

4.4. தகவல் பாதுகாப்பு சம்பவங்களை கண்டறிதல்.



நிறுவனமானது, தகவல் மற்றும் இணைய பாதுகாப்பு சம்பவங்களை சரியான நேரத்தில் அடையாளம் காண பொருத்தமான நடவடிக்கைகளை செயற்படுத்துதல் வேண்டும். எந்தவொரு இணைய பாதுகாப்பு சம்பவங்கள், பாதிப்புகள் அல்லது கொள்கை மீறல்களை சம்பந்தப்பட்ட அதிகாரிகளுக்கு தெரிவிக்குமாறு அமைப்பு ஊழியர்களுக்கு அறிவுறுத்தும். மேலும், நிகழ்வுகளை அடையாளம் காண பதிவுகளை பகுப்பாய்வு செய்வதற்கான வழிமுறைகளை அமைப்பு வரிசைப்படுத்துகிறது மற்றும் தொடர்ச்சியான கண்காணிப்பு தீர்வுகளை பின்பற்றுகிறது, இது ஒழுங்கற்ற செயல்பாடுகள் மற்றும் செயல்பாட்டு தொடர்ச்சிக்கான பிற அச்சுறுத்தல்களைக் கண்டறியும்.

4.4.1. சம்பவங்களை அறிக்கையிடுதல் மீதான கொள்கை

சந்தேகத்திற்கிடமான நடவடிக்கை அல்லது ஏதேனும் பாதுகாப்பு மீறல் குறித்து உடனடியாக தகவல் பாதுகாப்பு உத்தியோகத்தருக்கு தெரிவிக்குமாறு பணியாளர்களுக்கு தெளிவாக ஆலோசனையளிக்கப்படுதல் வேண்டும். பாதுகாப்பு மீறல்களானவை, வலையமைப்பு, தொலைத்தொடர்பு அல்லது கணினி முறைமைகளுக்கு அதிகாரமளிக்கப்படாத அணுகல், கணினிகளில் வைரஸ் வெளிப்படையாக இருப்பது, நிறுவனங்களால் தடைசெய்யப்பட்ட எந்தவொரு சொத்தின் வெளிப்படையான இருப்பு, அதிகாரமளிக்கப்படாத பயன்படுத்துதலால் எந்தவொரு கோப்பிலும் வெளிப்படையான மோசடி, மற்றும் பிறதொரு பயன்படுத்துதல் அல்லது ஒப்பந்தக்காரரால் இந்த வழிகாட்டல்கள் அல்லது பாதுகாப்புக் கொள்கை மீறப்படுதல் ஆகியவற்றை உள்ளடக்குகின்றன, ஆனால் அதற்குள் அவை மட்டுப்படுத்தப்படவில்லை. தகவல் தொழில்நுட்ப சொத்துக்களில் தற்போதுள்ள ஏதேனும் பாதிப்புகள் பற்றி தெரிவிக்குமாறு பயன்படுத்துபவர்களுக்கு ஆலோசனை வழங்கப்படுதல் வேண்டும்.



நிறுவனமானது, சம்பவங்களைக் கண்டறிதல், கண்டறியப்பட்ட தகவல் பாதுகாப்பு நிகழ்வுகளை அறிக்கையிடுதல் மற்றும் ஆதாரங்களைப் பாதுகாத்தல் போன்றவை பற்றி பணியாளர்களுக்கு போதுமான விழிப்புணர்வு மற்றும் பயிற்சிகளை வழங்குதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்..

4.4.2. பதிவுகளை மீளாய்வு செய்தல் மீதான கொள்கை

நிறுவனமானது, முறைமைகள் மற்றும் நிகழ்வுகளை கண்டறிவதற்கு இணைக்கப்பட்டுள்ள கூறுகள் மூலம் உருவாக்கப்பட்ட பதிவுகளைப் (அணுகல் பதிவுகள் (access logs), பிழையான பதிவுகள் (error logs) சேவையக பதிவுகள் (server logs), ஆய்வுப் பதிவுகள் (audit logs), பாதுகாப்புச் சுவர் பதிவுகள் (firewall logs) மற்றும் தீம்பொருள் எதிர்ப்பு பதிவுகளினைப் (antivirus logs) பேணுதல் மற்றும் மீளாய்வு செய்தல் வேண்டும்.

நிறுவனமானது, முறைமைகள் மீது தீங்கிழைக்கும் தாக்குதல்களைக் கண்டறிவதற்கும், பிழைகள் அல்லது பாதுகாப்பு மீறல்களுக்கான காரணங்களைத் தீர்மானிப்பதற்கும் கிரமமாக பதிவுகளை மீளாய்வு செய்தல் வேண்டும்.

பதிவுகள், மோசடி மற்றும் அதிகாரமளிக்கப்படாத அணுகலுக்கு எதிராக பாதுகாக்கப்படுதல் வேண்டும். முக்கியமான மற்றும் தனிப்பட்ட முறையில் அடையாளம் காணக்கூடிய தகவல்களைக் கொண்ட பதிவுகளைப் பொறுத்தவரை, சேமித்து பகுப்பாய்வு செய்வதற்கு முன்னர் பொருத்தமான தனியுரிமை பாதுகாப்பு நடவடிக்கைகள் எடுக்கப்படுதல் வேண்டும்.

பதிவுகளானவை, 12 மாத காலத்திற்கு அல்லது தகவல் பாதுகாப்பு குழுவினால் தீர்மானிக்கப்பட்டவாறு வைத்திருக்கப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்..

4.4.3. நிகழ்வுகளைத் தொடர்ந்து கண்காணிப்பது மீதான கொள்கை

நிறுவனமானது, தீங்கிழைக்கும் நடவடிக்கைகளைக் கண்டறிவதற்கான வலையமைப்புகள் அல்லது முறைமைகளைக் கண்காணித்தல் வேண்டும் என்பதுடன், ஊடுருவலைக் கண்டறியும் முறைமைகள் மற்றும் ஊடுருவலைத் தடுக்கும் முறைமையை (ஊடுருவலைக் கண்டறியும்

முறைமைகள் ∴ ஊடுருவலைத் தடுக்கும் முறைமைகள்) நடைமுறைப்படுத்துவதன் ஊடாக அத்தகைய நடவடிக்கைகளை எதிர்கொள்ளுதல் வேண்டும்.

நிறுவனமானது, பாதுகாப்பு கண்காணிப்பு மற்றும் அதிகளவான அச்சுறுத்தல் மற்றும் சம்பவத்தைக் கண்டறிவதற்கான பாதுகாப்பு தகவல் மற்றும் நிகழ்வு முகாமைத்துவ முறைமைகளைப் பயன்படுத்த முடியும்.

இணக்கம்: அனைத்து முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களுக்கும் ஏற்புடையதாகும்.

4.4.4. இலங்கை சேர்ட்டுக்கு நிகழ்வுகளை அறிக்கையிடுவது தொடர்பான கொள்கை

தகவல் பாதுகாப்பு குழு தீர்மானித்ததன்படி, தொழில்நுட்ப ஆலோசனை மற்றும் கையாளுதல் ஆகியவற்றிற்காக முக்கியமான தகவல் பாதுகாப்பு சம்பவங்களை உடனடியாக இலங்கை சேர்ட்டிற்கு அறிக்கையிடுமாறு நிறுவனத்திற்கு ஆலோசனை வழங்கப்படுகின்றது.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்..

4.5. சம்பவங்களுக்குப் பதிலளித்தல்



தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவங்களுக்கு திறம்பட பதிலளிப்பதற்காக, நிறுவனம் ஒரு சம்பவ மறுமொழி திட்டத்தை உருவாக்கி, ஒரு சம்பவம் நடந்தால் திட்டத்தை செயல்படுத்த வேண்டும். தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவங்களுக்கு பதிலளிப்பதில் நிறுவனம் இணங்க வேண்டிய கொள்கைகள் கீழே கொடுக்கப்பட்டுள்ளன.

4.5.1. சம்பவத்திற்குப் பதிலளிக்கும் திட்டம் மீதான கொள்கை

ஒரு நிறுவனத்தின் சொத்துக்களுக்கு எதிரான தகவல் மற்றும் இணையப் பாதுகாப்பு சம்பவத்தின் எதிர்மறையான விளைவுகளைக் கண்டறிந்து, பதிலளிப்பதற்கு மற்றும் கட்டுப்படுத்துவதற்கு, முன்னரே தீர்மானிக்கப்பட்ட அறிவுறுத்தல்கள் மற்றும் நடைமுறைகளின் தொகுப்பைக் கொண்ட ஒரு சம்பவ மறுமொழித் திட்டத்தை நிறுவனம் உருவாக்கும். சம்பவத்திலிருந்து திறம்பட மீள்வதற்கான தெளிவான வழிமுறைகள் மற்றும் நடைமுறைகளும் இதில் அடங்கும்.

சம்பவத்திற்கு பதிலளிக்கும் திட்டமானது (Incident Response Plan), குறைந்தபட்சம், சம்பவத்தை அறிக்கையிடும் நடைமுறைகள், கண்டறிதல், பகுப்பாய்வுக்கான உபாயங்கள் மற்றும் சம்பவங்களைக் கட்டுப்படுத்துதல் (ஒழிப்பு அல்லது மீட்டி), நியமிக்கப்பட்ட பதவியினர்க்கு தகவல் பாதுகாப்பு பொறுப்புகளை ஒதுக்குதல் மற்றும் சம்பவங்களுக்கு பின்னரான மீளாய்வுகள் தொடர்பான நடைமுறைகள் ஆகியவற்றைக் கொண்டிருத்தல் வேண்டும்.

சம்பவத்திற்கு பதிலளிக்கும் திட்டமானது, அவ்வப்போது சோதிக்கப்பட்டு, நிறுவனத்தின் அனைத்து பதவியினருக்கும் தெரிவிக்கப்படுதல் வேண்டும்.

ஒரு சம்பவ மறுமொழித் திட்டத்தை உருவாக்குவதற்கான வழிகாட்டுதல்கள் தகவல் மற்றும் இணைய பாதுகாப்பு நடைமுறைப்படுத்தல் வழிகாட்டியில் வழங்கப்பட்டுள்ளன.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்.

4.5.2. சம்பவத்திற்குப் பதிலளிக்கும் திட்டத்தினைச் செயற்படுத்தும் மீதான கொள்கை.

ஒரு தகவல் பாதுகாப்பு சம்பவம் ஏற்பட்டால், நியமிக்கப்பட்ட அங்கீகரிக்கப்பட்ட நபர், நிறுவன நடவடிக்கைகளில் தாக்கத்தை குறைக்க, சம்பவத்திற்குப் பிறகு இயல்பான செயற்பாடுகளை மீண்டும் ஆரம்பிப்பதற்கு, சம்பவ மறுமொழித் திட்டத்தை செயற்படுத்துதல் வேண்டும்.

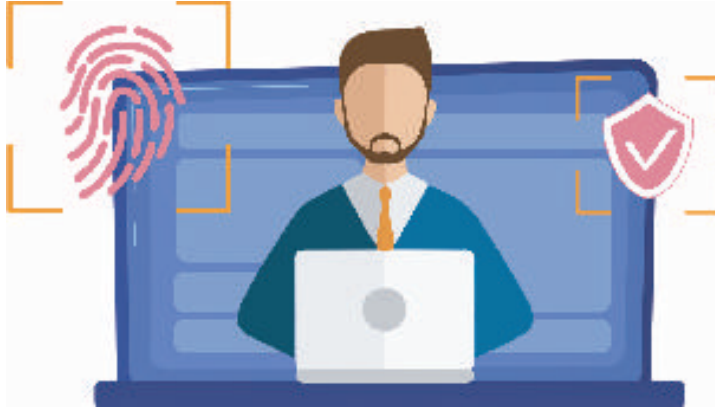
சம்பவங்கள் தொடர்பான தகவல்களைப் பதிவு செய்ய ஒரு சம்பவப் பதிவேட்டை (Incidents Register) நிறுவனம் பேணுதல் வேண்டும். சம்பவப் பதிவேட்டில் குறைந்தபட்சம் பின்வரும் தகவல்கள் இருக்க வேண்டும்: சம்பவத்தின் தேதி மற்றும் நேரம், சம்பவத்தைப் பற்றி முறைப்பாடு செய்த ஊழியரின் பெயர் மற்றும் பதவி, சம்பவத்தின் விளக்கம், தாக்கத்தின் தன்மை, சம்பவத்தின் வகைப்பாடு, சம்பவத்திற்கு பதிலளிக்கும் வகையில் எடுக்கப்பட்ட நடவடிக்கை சம்பவம், சம்பவத்தை கையாளும் உத்தியோகத்தர், சம்பவத்தின் தற்போதைய நிலை மற்றும் ஏனைய விடயங்கள்.

சம்பவங்களுக்கு பதிலளிப்பதற்கான வழிகாட்டுதல்கள் தகவல் மற்றும் சைபர் பாதுகாப்பு அமுலாக்கல் வழிகாட்டியில் வழங்கப்பட்டுள்ளன.

ஒரு தகவல் மற்றும் சைபர் பாதுகாப்பு சம்பவம் நடந்தால், தடயவியல் விசாரணைகளில் பயன்படுத்தக்கூடிய ஆதாரமாக செயல்படக்கூடிய தகவலை அடையாளம் காணவும், சேகரிக்கவும் மற்றும் பாதுகாக்கவும் அமைப்பு நடைமுறைகளை தொடங்க வேண்டும். தடயவியல் விசாரணை தொடர்பான கொள்கைகள் பிரிவு 4.5.3 இல் வழங்கப்பட்டுள்ளன.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்..

4.5.3. தடயவியல் விசாரணைகள் மீதான கொள்கைகள்



தடயவியல் விசாரணை (Forensic Investigation) தேவைப்படும் பட்சத்தில், அமைப்பு முறையான விசாரணை செயல்முறையை பின்பற்றுதல் வேண்டும். தடயவியல் விசாரணை தொடர்பான ஆதாரங்களை இயற்பியல் ஆவணங்கள், வன் இறுவட்டுக்களில் உள்ள தரவு, சாதனப் பதிவுகள், CCTV காட்சிகள், மின்னஞ்சல் பதிவுகள், குரல் பதிவுகள் மற்றும் ஏனைய மின்னணு பதிவுகள் போன்ற பரந்த அளவிலான மின்னணு வழிமுறைகள் மூலம் கைப்பற்ற முடியும்.

இலத்திரனியல் சான்றுகள் பாரம்பரிய ஆதாரங்களில் இருந்து வேறுபட்டதாக இருப்பதால், அதன் இயல்பு, நிலையற்ற தன்மை (volatility) மற்றும் பிரதிபலிப்பு (intangibility) அத்தகைய ஆதாரங்களைக் கையாள நிபுணத்துவ அறிவு அவசியம். அத்தகைய தொழில்நுட்ப திறன்களைக் கொண்ட இலங்கை சேர்ட் அல்லது தொடர்புடைய நிறுவனத்திடம் இருந்து இந்த அமைப்பு தொழில்நுட்ப உதவியைப் பெறுதல் வேண்டும்.

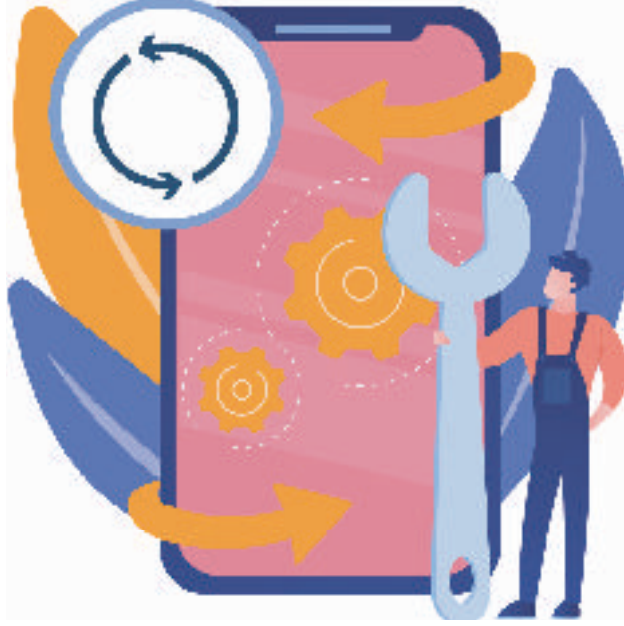
தடயவியல் விசாரணையில், குறைந்தபட்சம் பின்வரும் தகவல்கள் தேவைப்படும். நிறுவனத்தால் காவலில் (chain of custody) வைக்கப்படும் போது பயன்படுத்தப்பட்ட சங்கிலி: சம்பவம் மற்றும் சேகரிக்கப்பட்ட ஆதாரங்களின் விவரங்கள், சேகரிக்கப்பட்ட ஆதாரங்களின் திகதி மற்றும் நேரம், ஆதாரம் பெறப்பட்ட பெயர் மற்றும் பதவி மற்றும் ஆதாரங்களை மாற்றிய வரலாறு. விசாரணையில் அளிக்கப்படும் காவலில் இருக்கும் சங்கிலியை தகவல் பாதுகாப்பு உத்தியோகத்தர் பராமரித்தல் வேண்டும்.

நடப்பு, நிலுவையில் உள்ள அல்லது எதிர்பார்க்கக்கூடிய உரிமைகோரல்களைப் பற்றிய அனைத்து ஆதாரங்களையும் தக்கவைத்து பாதுகாக்கும் பொறுப்பை நிறுவனத்தின் தகவல் பாதுகாப்பு உத்தியோகத்தர் கொண்டுருத்தல் வேண்டும். ஆதாரமாகப் பயன்படுத்தக்கூடிய ஆவணங்கள், மின்னணுப் பதிவுகள் அல்லது ஒத்த கருவிகளை இழக்கவோ, அழிக்கவோ அல்லது வேண்டுமென்றே மாற்றவோ கூடாது என்ற பொறுப்பும் இதில் உள்ளடங்கும்.

தடயவியல் விசாரணையில், தனிப்பட்ட தரவு பாதுகாப்பு, கணினி குற்றங்கள், பணம் செலுத்தும் சாதன மோசடிகள் மற்றும் மின்னணு பரிவர்த்தனைகள் தொடர்பான சட்ட கட்டமைப்புகள் பயன்படுத்தப்படும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்படையதாகும்..

4.6. இயல்பான செயற்பாடுகளை மீட்டெடுத்தல் மீதான கொள்கை



நிறுவனமானது, அனர்த்தத்தின் காரணமாக பாதிக்கப்பட்ட எந்தவொரு இயலுமைகளையும் அல்லது சேவைகளையும் வழமைக்குக் கொண்டு வருவதற்குரிய பயனுள்ள நடவடிக்கைகளின் திட்டமொன்றை உருவாக்கி நடைமுறைப்படுத்துதல் வேண்டும். பேரழிவுகள் அல்லது தகவல் மற்றும் இணைய பாதுகாப்பு சம்பவங்களில் இருந்து மீள்வதில் நிறுவனம் இணங்க வேண்டும் என்ற கொள்கை அறிக்கைகள் கீழே தரப்பட்டுள்ளன.ஹ

4.6.1. அனர்த்த மீட்புத் திட்டம் மீதான கொள்கை

நிறுவனமானது, அனர்த்தமொன்று (அல்லது சம்பவம்) ஏற்படுகின்ற சந்தர்ப்பத்தில், அத்தகைய அனர்த்தத்திலிருந்து (அல்லது சம்பவம்) மீள்வதற்கு வசதியாக அனர்த்த மீட்புத் திட்டமொன்றை (Disaster Recovery Plan) கொண்டிருத்தல் வேண்டும்.

அனர்த்த மீட்புத் திட்டமானது, அனர்த்தத்திலிருந்து மீள்வதற்கு மேற்கொள்ள வேண்டிய செயற்பாடுகள் மற்றும் திட்டத்தில் உள்ள ஒவ்வொரு குழு உறுப்பினரினதும் வகிபாகத்தையும், பொறுப்புகளையும் கொண்டிருத்தல் வேண்டும்.

அனர்த்த மீட்புத் திட்டமானது இடர் மதிப்பீடொன்றையும், தகவல் மற்றும் தகவல் தொழில்நுட்ப ஆதனங்களின் வணிக தாக்கம் பற்றிய பகுப்பாய்வையும் நடத்துவதன் மூலம் வடிவமைக்கப்படுதல் வேண்டும் என்பதுடன், மீட்பு நடவடிக்கைகளானவை தரவுகளை (மீட்பு நேர நோக்கம்) மீட்டெடுப்பதற்கு ஏற்றுக்கொள்ளக் கூடிய காலத்தின் ஆரம்ப புள்ளிமற்றும் அனர்த்தமொன்றுக்குபின்னர் (மீட்பு புள்ளி நோக்கம்) தரபனத்தின் தொழிற்பாடுகள் மற்றும் முறைமைகளையும்ஆரம்பிக்க வேண்டிய முன்னைய புள்ளியைக் கருத்தில் கொண்டு வடிவமைக்கப்படுதல் வேண்டும்.

இந்த அனர்த்த மீட்புத் திட்டமானது, காலாந்தர அடிப்படையில் பரிசோதிக்கப்பட்டு இற்றைப்படுத்தப்படுதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்..

4.6.2. அனர்த்த மீட்புத் திட்டத்தைச் செயற்படுத்துதல் மீதான கொள்கை

அனர்த்தமொன்று ஏற்படுகையில், நியமிக்கப்பட்ட அதிகாரமளிக்கப்பட்ட நபர், நிறுவனத்தின் செயற்பாடுகளில் தாக்கத்தைக் குறைப்பதற்கும், நிகழ்வொன்றுக்குப் பின்னர் வழமையான நடவடிக்கைகளை மீள ஆரம்பிப்பதற்கும் அனர்த்த மீட்புத் திட்டத்தைச் செயற்படுத்துதல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்.

4.6.3. நெருக்கடியின் போதான தொடர்பாடல் மீதான கொள்கை

நிறுவனத்தின் தலைமைத்துவத்தினால் தீர்மானிக்கப்பட்டபடி பாரியதொரு நெருக்கடி (முக்கியமான பேரழிவு, ணைய பாதுகாப்பு சம்பவம்) ஏற்படுகின்றவிடத்து திட்டமொன்றின்படி, நிறுவனத்தின் பொறுப்பான அமைச்சுகள், இலங்கை சேர்ட், பாதிக்கப்பட்டவர்கள், ஊடகங்கள், சேவை நாடுநர்கள் மற்றும் சட்டத்தை நடைமுறைப்படுத்தும் அதிகாரிகள் போன்ற அத்தகைய உள்ளக மற்றும் வெளியகத் தரப்புகளுடன் தொடர்பு கொள்ளுதல் வேண்டும்.

இந்த நிறுவனம், நெருக்கடியை உரிய அக்கறைதாரர்களுக்குத் தெரிவிப்பதற்கு பொறுப்புடையவாற்ற சிரேட் அதிகாரியை நியமித்தல் வேண்டும்.

இணக்கம்: அனைத்து அரசாங்க நிறுவனங்களுக்கும் ஏற்புடையதாகும்..

5. முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டிய கொள்கைகள்

நிறுவனத்தின் தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கையினை அமுல்படுத்தும் பொருட்டு, பின்வரும் கொள்கைகள் முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டியுள்ளன.

கொள்கை விடயம்	கொள்கை இல.	முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டிய கொள்கைகள்	அனைத்து நிறுவனங்கள்	மு.தே.மு.உ. முடிவழங்குனர்கள்
தகவல் மற்றும் இணையப் பாதுகாப்பு நிருவாக முறைமை	4.1.1	நிறுவனத் தலைவரினால் தகவல் மற்றும் சைப்ர் பாதுகாப்பு கொள்கையினை அமுல்படுத்துவதற்கான தலைமைத்துவத்தினை வழங்குதல்.	✓	✓
	4.1.2	தகவல் மற்றும் இணைய பாதுகாப்பு நிருவாக கட்டமைப்பொன்றினைத் தாபித்தல்.	✓	✓
	4.1.2 (அ)	தகவல் பாதுகாப்பு உத்தியோகத்தர் மற்றும் தகவல் மற்றும் தகவல் பாதுகாப்பு பொறுப்புக்கள் குழுவொன்றினை நியமித்தல்		✓
	4.1.2 (ஆ)	தகவல் பாதுகாப்பு உத்தியோகத்தர் இல்லாவிடின், தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களைப் பாதுகாப்பதற்கு பிரதம தகவல் உத்தியோகத்தரிடம் பொறுப்புக்களைக் கையளித்தல்.	✓	
	4.1.2 (இ)	தகவல் மற்றும் இணைய பாதுகாப்பு கசனக்காய்வுகளை ஒருங்கிணைப்பதன் மூலம் தகவல் மற்றும் இணைய பாதுகாப்பு கணக்காய்வுகளை ஒருங்கிணைப்பதற்கு (பிரதம) பொறுப்புக்களைக் கையளித்தல்.	✓	✓
	4.1.3	தகவல் பாதுகாப்புக் குழு ஒருவரை நியமித்தல்.	✓	✓
	4.1.4	இடர்முகாமைத்துவகுழுஒருவரை நியமித்தல்.		✓
	4.1.5	பயனர் பொறுப்புக்களை அடையாளங் காணுதலும் பயனர்களுடன் தொடர்பு கொள்ளுதலும்.	✓	✓
	4.1.6	தகவல் மற்றும் சைப்ர் பாதுகாப்புக்கான உத்தியோகபூர்வ பொறுப்பின் திறன் விருத்தி.	✓	✓
	4.1.7	முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குநர்களை அல்லது மிக இரகசியமான மற்றும் இரகசியமான தகவல் சொத்துக்களைக் கையாளும் பதவியினர் மீது பாதுகாப்பு அனுமதி மற்றும் பின்னணி சோதனைகளை நிறைவேற்றுதல்.		✓

கொள்கை விடயம்	கொள்கை இல.	முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டிய கொள்கைகள்	அனைத்து நிறுவனங்கள்	மு.தே.மு.உ. முவழங்குனர்கள்
	4.1.8	நிறுவனத்தின் நோக்கு, செயற்பணி மற்றும் நோக்கங்களுடன் தகவல் மற்றும் சைப்ர் பாதுகாப்பு நடவடிக்கைகளை ஒழுங்குமுறைப்படுத்துதல்.	✓	✓
	4.1.9	தகவல் மற்றும் சைப்ர் பாதுகாப்பு செயல்திட்டங்களை விருத்தி செய்வதும் அமுல்படுத்துதலும்.	✓	✓
சொத்துக்கள், சொத்து உரிமையாளர்கள் மற்றும் இடர்களை அடையாளங் காணுதல்.	4.2.1	தகவல், தகவல் தொழில்நுட்ப சொத்துக்கள் மற்றும் முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வழங்குனர்கள் என்பவற்றினை அடையாளங் காணுதல்.	✓	✓
	4.2.3	சொத்து உரிமையாளர்கள், பாதுகாவலர்களை அடையாளங் காணுதலும் சொத்துக்களைப் பாதுகாப்பதற்கான பொறுப்பினை கையளித்தலும்.	✓	✓
	4.2.4	தகவல் மற்றும் தகவல் சொத்துப் பதிவேடுகளைப் பேணுதல்.	✓	✓
	4.2.5	தகவல் மற்றும் தகவல் சொத்துக்களுக்கான இடர் மதிப்பீடுகளை மேற்கொள்ளுதல்.		✓
	4.2.6	தகவல் மற்றும் தகவல் தொழில்நுட்ப சொத்துக்களை அவற்றின் பெறுமதி மற்றும் உணர்திறனின் அடிப்படையில் வகைப்படுத்துதல்.	✓	✓
	சொத்துக்களைப் பாதுகாத்தல்	4.3.1	இறுதியில் தரவினைப் பாதுகாத்தல்	✓
4.3.2		இடைத்தங்கலில் தரவினைப் பாதுகாத்தல்	✓	✓
4.3.3		தகவல் மற்றும் தகவல் சொத்துக்களின் பௌதீக ரீதியான பாதுகாப்பினை உறுதி செய்தல்.	✓	✓
4.3.4		தகவல் மற்றும் தகவல் சொத்துக்களுக்கான பயனர் அணுகலினை கட்டுப்படுத்துதல்.	✓	✓
4.3.5		உறுதியான அதிகாரத்தினை உறுதி செய்தல்.	✓	✓
4.3.6		பொருத்தமான முறையில் தரவு இறைமையினை உறுதி செய்தல்.	✓	✓
4.3.7		வலிதான உரிமம் பெற்ற மென்பொருட்களைப் பயன்படுத்துதலும் புதிய பொருட்களை இறைப்படுத்துதலும்.	✓	✓
4.3.8		யுவைஅயு. டிபிசுநமென்பொருளை நிறுவுதல்.	✓	✓

கொள்கை விடயம்	கொள்கை இல.	முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டிய கொள்கைகள்	அனைத்து நிறுவனங்கள்	மு.தே.மு.உ முவழங்குனர்கள்
	4.3.9	உத்தியோகபூர்வ தொடர்பாடல்களுக்கு உத்தியோகபூர்வ மின்னஞ்சலினைப் பயன்படுத்துதல்.	✓	✓
	4.3.10	மின்னஞ்சல்களின் பாதுகாப்பினை உறுதி செய்தல்.	✓	✓
	4.3.11	பொருத்தமான முறையில் டிஜிற்றல் கையெப்பங்களைப் பயன்படுத்துதல்.	✓	✓
	4.3.12	சுற்றளவு பாதுகாப்பு கட்டுப்பாடுகளை செயல்படுத்துதல்.	✓	✓
	4.3.13	தொலைவிலிருந்து அணுகும் பாதுகாப்பு முறைகளைப் பயன்படுத்துதல்.	✓	✓
	4.3.14	காப்பு மூலோபாயத்தைப் பயன்படுத்துதல்	✓	✓
	4.3.16	மென்பொருள் விருத்தி மற்றும் கொள்ளல் நடவடிக்கைகளின் போது வடிவமைப்பு கோட்பாடுகளின் மூலமாக பாதுகாப்பினை உறுதி செய்தல்.	✓	✓
	4.3.17	சொத்துக்களின் விற்பனைப் பாதுகாப்பினை உறுதி செய்தல்.	✓	✓
	4.3.18	உள்ளக தகவல் பாதுகாப்பு கணக்காய்வு செயல்முறையொன்றினை அமுல்படுத்துதல்.	✓	✓
	4.3.19	இடர் மதிப்பீடுகளை மேற்கொள்ளுதல், உத்தியோகபூர்வ இணையத்தளத்தினை ஆரம்பிப்பதற்கு முன்பாக ஊடுருவல் சோதனைகளை மேற்கொள்ளுதல், சைபர் பயன்பாடுகள் அல்லது வேறு ஏதேனும் முறைமையினை மேற்கொள்ளுதல்.	✓	✓
	4.3.20	தகவல் தொழில்நுட்ப சொத்துக்களின் பாதுகாப்பு கண்காணிப்பினை வலுப்படுத்துதல்	✓	✓
	4.3.21	தொலைவிலிருந்து வேலை செய்யும்போது வீட்டிலிருந்து வேலை செய்வதற்கான வழிகாட்டுதல்களைப் பின்பற்றவும்.	✓	✓
	4.3.23	நட்பகமற்ற வலையமைப்புகளைப் பயன்படுத்துவதை தடுத்தல்	✓	✓
	4.3.24	வழங்குனர்களை முகாமை செய்தல்	✓	✓
	4.3.25	மாற்றங்களை முகாமை செய்தல்.	✓	✓

கொள்கை விடயம்	கொள்கை இல.	முன்னுரிமை அடிப்படையில் அமுல்படுத்தப்பட வேண்டிய கொள்கைகள்	அனைத்து நிறுவனங்கள்	மு.தே.மு.உ முடிவங்களுக்கள்
சம்பவங்களைக் கண்டறிதல்	4.4.1	சம்பவங்கள் தொடர்பில் அறிக்கையிடுமாறு பதவியினருக்கு அறிவுறுத்துதல்.	✓	✓
	4.4.2	சம்பவங்களை அடையாளங் காண்பதற்கு குறிப்பீடுகளை மீளாய்வு செய்தல்	✓	✓
	4.4.3	நிகழ்வுகளை தொடர்ச்சியாக கண்காணிப்பதன் மூலம் சம்பவங்களை அடையாளங் காணுதல்		✓
	4.4.4	இலங்கை சேர்ட்டிற்கு நிகழ்வுகளை அறிக்கையிடல்.	✓	✓
நிகழ்வுகளுக்குப் பதிலளித்தல்	4.5.1	நிகழ்வு பதிலளிப்பு திட்டமொன்றினை விருத்தி செய்தல்.	✓	✓
	4.5.2	சம்பவ நிகழ்வொன்றில் சம்பவ பதிலளிப்பு திட்டத்தினைச் செயற்படுத்துதல்.	✓	✓
	4.5.3	சம்பவங்கள் மீதான தடயவியல் விசாரணைகளை மேற்கொள்ளுதல்.	✓	✓
சாதாரண தொழிற்பாடுகளை மீட்டல்	4.6.1	பேரழிவு மீட்புத் திட்டமொன்றினை விருத்தி செய்தல்.	✓	✓
	4.6.2	பேரழிவு நிகழ்வின் போது பேரழிவு பேரழிவு மீட்புத் திட்டமொன்றினை செயற்படுத்துதல்.	✓	✓
	4.6.3	நெருக்கடித் தொடர்பாடல் திட்டத்தினை விருத்தி செய்தல்	✓	✓

6. தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கையினை கண்காணித்தல் மற்றும் மதிப்பாய்வு செய்வதற்கான முறை.

- 6.1 தகவல் மற்றும் இணைய பாதுகாப்புக் கொள்கையை நடைமுறைப்படுத்துவதற்கு முன்பாக, அரசாங்க வளங்களைப் பாதுகாப்பதற்காக தகவல் பாதுகாப்பினைக் கடைப்பிடிப்பது தொடர்பில் அரசு நிறுவனங்களின் தற்போதைய நிலையைக் கண்டறிவது அவசியமானதொன்றாகும். எனவே இத்தகைய மதிப்பீட்டுக் கருவியானது, தகவல் மற்றும் இணைய பாதுகாப்புத் தயார் நிலையை அமுல்படுத்துவதில் அரசாங்க தாபனத்தின் தற்போதைய தகுதி நிலையைக் கண்டுபிடிக்கும் வகையில் வடிவமைக்கப்பட்டுள்ளது.
- 6.2 அதற்கிணங்க இலங்கை சேர்ட் ஆனது பிரிவு 6.6 இல் தரப்பட்டுள்ள வினாக்களின் அடிப்படையில் கொள்கையினை அமுல்படுத்துவது தொடர்பில் அரசாங்க நிறுவனங்களின் தயார் நிலை குறித்து பூர்வாங்க மதிப்பீட்டினை மேற்கொள்ளும். காண்புகளின் அடிப்படையில், கொள்கையினை அமுல்படுத்துவது தொடர்பில் அரசாங்க நிறுவனங்களுக்கு பரிந்துரைகள் வழங்கப்படும்.
- 6.3 இலங்கை சேர்ட் ஆனது வருடாந்த அடிப்படையில் ஒவ்வொரு அரசாங்க நிறுவனத்தின் மூலமாகவும் கொள்கை இணக்கப்பாட்டு மட்டத்தினை மதிப்பாய்வு செய்து தகவல் மற்றும்சைப் பாதுகாப்பு சுட்டெண் (ஐகெழசஅயவழை யெனெ ஊலடிநச னூநஉரசவைல ஐனெநஓ) மீதான இணக்கப்பாட்டு மட்டத்தினை வழங்கும். இலங்கை சேர்ட் ஆனது நிறுவனத்தின் ஒட்டுமொத்த தகவல் மற்றும் இணைய பாதுகாப்பு தயார்நிலையை மேம்படுத்துவதற்கான பரிந்துரைகள் வழங்கும்.
- 6.4 நிறுவனத்தில் கொள்கை அமுலாக்கலினை செயலாற்றுகையினை (அல்லது தயார்நிலை) மதிப்பாய்வு செய்வதற்கு, ஏறக்குறைய50 வினாக்கொத்துக்களைக் கொண்டுள்ள பிரிவு 6.6 இல் சமர்ப்பிக்கப்பட்ட வினாக்கொத்தானது பயன்படுத்தப்படும்.தகவல் பாதுகாப்பு உத்தியோகத்தர், பிரதான புத்தாக்க உத்தியோகத்தர், அல்லது தகவல் தொழில்நுட்ப பாடத்திற்குப் பொறுப்பான உத்தியோகத்தர், இந்த மதிப்பீட்டை பூர்த்தி செய்து, ஒவ்வொரு வருடமும் அக்டோபர் 30 ஆம் திகதி அல்லது அதற்கு முன்னதாக நிறுவன தலைவரின் கையொப்பத்துடன் இலங்கை சேர்ட்டுக்கு அனுப்பி வைக்கப்படுதல் வேண்டும்.
- 6.5 ஒவ்வொரு வினாவுக்கும் விரிவாக பதிலளிக்க விரும்பும் பதிலளிப்பவர் மதிப்பீட்டு வினாக் கொத்தின் இறுதியில் குறிப்புக்கள் பிரிவில் விரிவாக பதிலளிக்க முடியும். பதிலளிப்பவர் உரிய பதங்களின் விரிவான விளக்கத்திற்காக இந்த ஆவணத்தின் சொற்களஞ்சியத்தினைப் பார்க்கலாம்.
- 6.1. மதிப்பீட்டு வினாக் கொத்து அனைத்து அரசாங்க நிறுவனங்களும் அவற்றின் அறிவுக்கு எட்டிய வரையில் ஒவ்வொரு வினாவுக்கும் விடையளிக்குமாறு கேட்டுக் கொள்ளப்படுகின்றன.

கொள்கை உசாத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை	குறிப்புகள்	
தகவல் மற்றும் இணைய பாதுகாப்பு முறைமை					
பாதுகாப்பு நிறுவன கட்டமைப்பு	1. நிறுவனம் தகவல் பாதுகாப்பு உத்தியோகத்தர் ஒருவரை நியமித்துள்ளதா?	4.1.2 (அ)			
	2. தாபனம் தகவல் பாதுகாப்பு உத்தியோகத்தருக்கு பொறுப்புக்களை உரித்தளித்துள்ளதா?	4.1.2 (அ)			
	3. தகவல் பாதுகாப்பு உத்தியோகத்தர் நியமிக்கப்பட்டிருக்கா விட்டால், நிறுவனமானது தகவல் தொழில்நுட்பம் உரித்தளிக்கப்பட்ட தகவல் பாதுகாப்பு பொறுப்புகள் விடயத்திற்குப் பொறுப்பான உத்தியோகத்தரோ அல்லது பிரதான புத்தாக்க உத்தியோகத்தரினையோ கொண்டுள்ளதா?	4.1.2 (அ)			
	4. நிறுவனமானது (பிரதான) உள்ளக கணக்காய்வாளருக்கு தகவல் பாதுகாப்பு கணக்காய்வு பொறுப்புகளை வழங்கியுள்ளதா?	4.1.2 (இ)			
	5. நிறுவனமானது தகவல் பாதுகாப்பு அல்லது தகவல் தொழில்நுட்பம் குறித்த தீர்மானங்களை மேற்கொள்வதற்கான குழுவினைக் கொண்டுள்ளதா?	4.1.3			
	6. நிறுவனமானது தகவல் சைபர் பாதுகாப்பு தொடர்பான இடர்கள் குறித்த தீர்மானங்களை மேற்கொள்வதற்கான குழுவினைக் கொண்டுள்ளதா?	4.1.4			

கொள்கை உசாத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை	குறிப்புகள்
இறுதிப் பயனர் பொறுப்புகள்	7. நிறுவனமானது பயனர்களுக்கு இறுதிப் பயனர் பொறுப்புகளை குறித்து விளக்கமளித்துள்ளதா?	4.1.5		
திறன் விருத்தி	8. பொறுப்புக்கூறும் நபர்களின் தகவல் பாதுகாப்பு திறனை மேம்படுத்துவதற்கு நிறுவனம் ஏதேனும் நடவடிக்கை எடுத்திருக்கிறதா?	4.1.6		
பின்னணி செவ்வை பார்த்தல்கள்	9. "மிகஇரகசியம்" மற்றும் "இரகசியம்", தகவல் சொத்துக்கள் அல்லது முக்கியமானதேசியதகவல் உட்கட்டமைப்பு வழங்குநர்கள் அணுகல் ஆகியவற்றைக் கையாளும் அதிகாரிகளின் பின்னணிச் சோதனைகள் மற்றும் பாதுகாப்பு அனுமதியை தங்களின் நிறுவனம் மேற்கொள்கிறதா?	4.1.7		
மூலோபாய வரிசை	10. நிறுவனத்தின் செயல்பாடுகள், கொள்கைகள், உத்திகள் அல்லது திட்டங்களை வடிவமைத்து செயல்படுத்துவதில், உங்கள் நிறுவனம் தகவல் பாதுகாப்பை கணக்கில் எடுத்துள்ளதா?	4.1.8		

கொள்கை உட்காத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை	குறிப்புக்கள்
செயல் திட்டம்	11. தங்களது நிறுவனம் தகவல் பாதுகாப்பு நடவடிக்கைகளுக்கான நிதி ஏற்பாடுகளைக் கொண்டுள்ளதா?	4.1.9		
	12. தங்களது நிறுவனம் அதன் தகவல் பாதுகாப்பு நோக்கங்களை அடைவதற்கு விருத்தி செய்யப்பட்ட செயல்திட்டங்களை வைத்துள்ளதா?	4.1.10		

சொத்துக்கள், உரிமையாளர்கள், பயனர்கள் மற்றும் இடர்களினை அடையாளங் காணுதல்

சொத்துக்களை அடையாளங் காணுதல்	13. நிறுவனத்திற்கு பெறுமதி சேர்க்கும் தகவல் சொத்துக்களை உங்களின் நிறுவனம் அடையாளங் கண்டு வைத்துள்ளதா?	4.2.1		
	14. உங்களின் நிறுவனமானது தகவல் சொத்துக்களுடன் இணைந்துள்ள இடரினை மதிப்பீடு செய்துள்ளதா?	4.2.5		
	15. உங்களின் நிறுவனம் தகவல் தொழில்நுட்பச் சொத்துக்களை அடையாளங் கண்டுள்ளதா?	4.2.6		
	16. உங்களின் நிறுவனமானது தகவல் சொத்து பதிவேட்டில் தகவல் சொத்துக்களைப் பதிவு செய்துள்ளதா?	4.2.4		
	17. உங்களின் நிறுவனம் தகவல் தொழில்நுட்பச் சொத்துக்களை அடையாளங் கண்டுள்ளதா?	4.2.1		

கொள்கை உசாத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை		குறிப்புகள்
	18. உங்களின் நிறுவனம் தகவல் தொழில்நுட்ப சொத்துப் பதிவேட்டொன்றில் தகவல் தொழில்நுட்பச் சொத்துக்களைப் பதிவு செய்துள்ளதா?	4.2.4			
	19. உங்களின் நிறுவனம் தகவல் தொழில்நுட்ப சொத்துக்களை அவற்றின் முக்கியத்துவத்தின் அடிப்படையில் வகையீடு செய்துள்ளதா?	4.2.6			
	20. உங்களின் நிறுவனம் சொத்துக்களின் உரிமையாளர்களை அடையாளங் கண்டுள்ளதா?	4.2.3			
குறியாக்கம்	21. உங்கள் நிறுவனம் முக்கியமான தகவலை சேமிப்பிற்கு முன் குறியாக்கம்(நடெசலிவ) செய்கிறதா?	4.3.1			
	22. இலத்திரனியல் அலைவரிசைகள் மூலம் நகரும் முன் உங்கள் நிறுவனம் முக்கியமான தகவல்களை குறியாக்கம் செய்கிறதா?	4.3.2			
பௌதீகப் பாதுகாப்பு	23. உங்கள் நிறுவனம் பாதுகாப்பான பகுதிகளில் முக்கியமான தகவல்களைச் செயலாக்குகிறதா அல்லது சேமிக்கிறதா?	4.3.3			
	24. தீ, வெள்ளம், ஈரப்பதம் மற்றும் வெப்பநிலை ஆகியவற்றிலிருந்து பாதுகாப்பான பகுதிகளைப் பாதுகாக்க உங்கள் நிறுவனம் தகுந்த நடவடிக்கைகளை எடுத்திருக்கிறதா?	4.3.3			
	25. பாதுகாப்பான பகுதிகளுக்கு அங்கீகரிக்கப்படாத நுழைவை உங்கள் நிறுவனம் தடுக்கின்றதா?	4.3.3			

கொள்கை உசாத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை	குறிப்புகள்
சொத்துக்களைப் பாதுகாத்தல்				
அடையாள முகாமைத்துவமும் அணுகுமுறைக் கட்டுப்பாடும்.	26. உங்கள் நிறுவனத்திற்கு அடையாள முகாமைத்துவம் மற்றும் அணுகல் கட்டுப்பாடு கொள்கை (Identity and Access Management) உள்ளதா?	4.3.4		
	27. உங்கள் நிறுவனம் வலுவான அங்கீகாரத்தைப் (strong authentication) பயன்படுத்துகிறதா?	4.3.5		
தரவு இறையாண்மை	28. தங்களின் நிறுவனம் தரவு இணையாண்மையினை (data sovereignty) உறுதி செய்கின்றதா?	4.3.6		
	29. கிளவுட் சேவையைப் பெறுவதற்கு முன் உங்கள் நிறுவனம் ஆபத்தை மதிப்பிடுகிறதா?	4.3.6		
உரிமம் பெற்ற மென்பொருள் மற்றும் இணைப்புகளின் இற்றைப்படுத்தல்கள்	30. நிறுவனம் செல்லுபடியாகும் உரிமம்(கள்) கொண்ட இயக்க முறைமைகளை பயன்படுத்துகிறதா?	4.3.7		
	31. விற்பனையாளர் வழங்கிய சமீபத்திய இணைப்புகள் மற்றும் திருத்தங்களுடன் நிறுவனத்தின் இயக்கமுறைமை(கள்) புதுப்பிக்கப்பட்டுள்ளனவா?	4.3.7		
	32. விற்பனையாளருக்கு வழங்கப்பட்ட முக்கியமான இணைப்புகள் நிறுவப்படுவதை உறுதி செய்வதற்கான நடைமுறை உங்கள் நிறுவனத்திடம் உள்ளதா?	4.3.7		

கொள்கை உட்காத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை	குறிப்புக்கள்
தீம்பொருள்	33. நிறுவனம் அனைத்து இயந்திரங்களிலும் செல்லுபடியாகும் உரிமத்துடன் தீம்பொருள்எதிர்ப்பு (Antimalware) மென்பொருளை நிறுவியுள்ளதா?	4.3.8		
மின்னஞ்சல்	34. உத்தியோகபூர்வ தகவல் தொடர்புகளுக்காக தனிப்பட்ட மின்னஞ்சல்களைப் பயன்படுத்தும் பயனர்களை உங்கள் நிறுவனம் கட்டுப்படுத்துகிறதா?	4.3.9		
	35. தீம்பொருள் இணைக்கப்பட்டுள்ள மின்னஞ்சல்களை அகற்ற தங்கள் நிறுவனம் மின்னஞ்சல் வழிபாடுகளை அமைக்கிறதா?	4.3.10		
	36. மின்னஞ்சல் வழியாக முக்கியமான தகவலை அனுப்பும்போது தங்களின் நிறுவனம் குறியாக்கத்தைப் பயன்படுத்துகிறதா?	4.3.10		
சுற்றளவுப் பாதுகாப்பு சாதனங்கள்	37. உங்கள் கணினி வலையமைப்பில் உங்கள் நிறுவனத்திடம் பயர்வால் உள்ளதா?	4.3.12		
தொலைநிலை அணுகல் பாதுகாப்பு	38. தொலைநிலை அணுகலுக்கு உங்கள் நிறுவனம் பாதுகாப்பான வேர்ச்சுவல் தனியார் வலையமைப்புக்களை (Virtual Private Network) பயன்படுத்துகிறதா?	4.3.13		
	39. தொலைதூரத்தில் இணைக்கும் அனைத்து பயனர்களும் வேர்ச்சுவல் தனியார் வலையமைப்புக்களைப் பயன்படுத்துகிறார்களா?	4.3.13		

கொள்கை உசாத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை	குறிப்புகள்
காப்புப் பிரதி மூலோபாயம்	40. உங்கள் நிறுவனம் தரவை காப்புப் பிரதி (டியஉமரி) எடுக்கிறதா?	4.3.14		
	41. காப்புப் பிரதிகள் தரவுச் செயலாக்கத் தளத்திலிருந்து உடல் ரீதியாக தொலைவில் உள்ள தீ தடுப்பு, பாதுகாப்பான இடத்தில் சேமிக்கப்பட்டுள்ளதா?	4.3.14		
சொத்துக்களின் பாதுகாப்பான அகற்றல்	42. முக்கியமான தகவல்களைக் கொண்ட மின்னணு ஊடகங்களை அப்புறப்படுத்த உங்கள் நிறுவனம் பின்வருவனவற்றில் ஏதேனும் ஒன்றைப் பின்பற்றுகிறதா? - துண்டாக்குதல், குத்துதல், உடல்ரீதியாக சேதப்படுத்துதல், தேய்த்தல்.	4.3.17		
உள்ளக தகவல் பாதுகாப்பு கணக்காய்வு நிகழ்ச்சித்திட்டம்	43. தங்களின் நிறுவனம் உள்ளக தகவல் பாதுகாப்பு கணக்காய்வு நிகழ்ச்சித்திட்டமொன்றினை வைத்திருக்கின்றதா?	4.3.18		
	44. உங்கள் நிறுவனம் பாதிப்பு மதிப்பீடு மற்றும் ஊடுருவல் சோதனைகளை இலங்கை சேர்ட் மூலம் மென்பொருள் பயன்பாடுகளை வரிசைப்படுத்துவதற்கு முன் செயல்படுத்துகிறதா?	4.3.19		
	45. தங்களின் கணினி வலையமைப்புகளுக்கு பாதிப்பு மதிப்பீடு மற்றும் ஊடுருவல் சோதனையினைச் செயற்படுத்துகிறதா?	4.3.19		

கொள்கை உசாத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை	குறிப்புகள்
வீட்டிலிருந்து வேலை	46. உங்களின் நிறுவனமானது இலங்கை சேர்ட்டினால் வழங்கப்பட்ட வீட்டிலிருந்து வேலைக்குரிய வழிகாட்டுதல்களை பின்பற்றுகின்றதா?	4.3.21		
சொந்த சாதனங்களை அலுவலக தேவைகளுக்குப் பயன்படுத்துதல்.	47. சொந்த சாதனங்களைப் பதிவு செய்வதற்கான முறையான நடைமுறை எதனையும் தங்களின் நிறுவனம் கொண்டுள்ளதா?	4.3.22		
	48. முக்கியமான தரவினை செயல்முறைப்படுத்துவதற்கு அல்லது களஞ்சியப்படுத்துவதற்கு சொந்த சாதனங்களைப் பயன்படுத்துவதற்கு தங்களின் நிறுவனம் அனுமதியளிக்கின்றதா?	4.3.22		
தகவல் பாதுகாப்பு நிகழ்வினைக் கண்டறிதல்				
நிகழ்வுகளை அறிக்கையிடுதல்	49. சந்தேகத்திற்கிடமான செயல்பாடு, தொடர்பு, திருட்டு, வைரஸ், பாதிப்பு, அங்கீகரிக்கப்படாத அணுகல், கோப்புகளை சேதப்படுத்துதல் அல்லது பாதுகாப்புக் கொள்கையை மீறுதல் ஆகியவற்றை தகவல் பாதுகாப்புக்கு பொறுப்பான நபரிடம் தெரிவிக்குமாறு ஊழியர்களுக்கு தங்களின் நிறுவனம் அறிவுறுத்தியுள்ளதா?	4.4.1		
	50. நீங்கள் எப்போதாவது இலங்கை சேர்ட்டிற்கு அல்லது வேறு ஏதேனும் தரப்புக்கு இணைய பாதுகாப்பு நிகழ்வுகள் குறித்து அறிவித்துள்ளீர்களா?	4.4.4		

கொள்கை உசாத்துணை	மதிப்பீட்டு வகையீடு	கொள்கை	இணக்கம் ஆம் இல்லை	குறிப்புகள்
நிகழ்வகளுக்கப் பதிலளித்தல்				
நிகழ்வுப் பதிலளிப்பு திட்டமும் திட்டத்தினைச் செயற்படுத்துதலும்.	51. உங்களின் நிறுவனம் நிகழ்வுப் பதிலளிப்புத் திட்டமொன்றினை (Incidents Response Plan) விருத்தி செய்துள்ளதா?	4.5.1		
	52. தகவல் மற்றும் சைபர் பாதுகாப்பு நிகழ்வொன்றில், அதன் தொழிற்பாடுகளின் தாக்கத்தினைக் குறைப்பதற்கு அல்லது அத்தொழிற்பாட்டினை மீளச் சேமிப்பதற்கு நிகழ்வு பதிலளிக்கும் திட்டமொன்றினை நிறுவனம் செயற்படுத்தியுள்ளதா?	4.5.2		
நிகழ்வகளுக்கப் பதிலளித்தல்				
பேரிடர் மீட்புத் திட்டமும் திட்டத்தினைச் செயற்படுத்துதலும்.	53. உங்களின் நிறுவனம் பேரிடர் நிகழ்வொன்றில் மீட்பினை வசதிப்படுத்துவதற்கு விருத்தி செய்யப்பட்ட பேரிடர் மீட்புத் திட்டமொன்றினை (Disaster Recovery Plan) வைத்துள்ளதா?	4.6.1		
	54. பேரிடர் நிகழ்வில் (அல்லது நிகழ்வு), தங்களின் நிறுவனமானது சீர்குலைந்த சேவைகளினை மீளமைப்பதற்கு அதன் பேரிடர் மீட்பு திட்டமொன்றினை செயற்படுத்துன்றதா?	4.6.2		

சொற் களஞ்சியம்

தீம்பொருள் எதிர்ப்பு
(Antimalware)

தீம்பொருள் எதிர்ப்பு என்பது சாதனங்களில் உள்ள தீம்பொருளைக் கண்டறிய அல்லது கணினி முறைமைகள் அல்லது மின்னணு சாதனங்களில் தீம்பொருளைத் தாக்குவதைத் தடுக்க வடிவமைக்கப்பட்ட மென்பொருளாகும். மால்வேர் என்பது கணினி, சேர்வர் அல்லது கணினி வலையமைப்பிற்கு (உதாரணம் - வைரஸ்கள், புழுக்கள், ransomware) சேதம் விளைவிப்பதற்காக வேண்டுமென்றே வடிவமைக்கப்பட்ட மென்பொருளாகும்.

சொத்துக்களின் வகையீடு
(Assets Classification)

வகைப்படுத்தல் என்பது தகவல் சொத்துக்களை அதன் உணர்திறன் நிலை, சிக்கலான நிலை மற்றும் அந்த தகவலைப் பகிர்வதால் ஏற்படும் தாக்கம் ஆகியவற்றின் அடிப்படையில் வகைப்படுத்தும் செயல்முறையாகும். நிறுவனத்திற்கு அதன் முக்கியத்துவத்திற்கு ஏற்ப தகவல் பொருத்தமான அளவிலான பாதுகாப்பைப் பெறுவதை உறுதி செய்வதே முதன்மை நோக்கமாகும்.

சொத்துக்களின் பாதுகா-
வலர்(Assets Custodian)

தகவல் சொத்து உரிமையாளரால் வரையறுக்கப்பட்ட தேவைகளுக்கு ஏற்ப, சேமித்து வைத்து, கொண்டு செல்லப்படும் அல்லது செயலாக்கப்படுவதால், வாழ்க்கைச் சுழற்சி முழுவதும் ஒரு தகவல் சொத்தைப் பாதுகாக்கும் பொறுப்பைக் கொண்ட நிறுவனத்தில் உள்ள நபர்.

சொத்துக்களின் உரிமை-
யாளர்(Assets Owner)

ஒரு சொத்து உரிமையாளர் என்பவர் சொத்துக்களின் அன்றாட நிருவாகத்திற்கு பொறுப்பாகவுள்ள ஆளொருவராவார்.

தகவலின் கிடைப்ப-
னவு(Availability of
Information)

கிடைப்பனவானது சரியான நேரத்தில், நம்பகமான அணுகல் மற்றும் தகவலைப் பயன்படுத்துவதை உறுதி செய்கிறது.

தகவல் சொத்துக்களின்
இரகசியத் தன்மை(Confidentiality of Information)

இரகசியத்தன்மை என்பது அங்கீகரிக்கப்படாத நபர்களுக்கும் நிறுவனங்களுக்கும் தகவல் வெளியிடப்படாது என்ற உத்தரவாதத்தைக் குறிக்கின்றது.

உணர்திறன் மிக்க
தகவல் சொத்துக்கள்
(Sensitive Information
Assets)

எந்தவொரு தகவல் இழப்பு, மாற்றம், தவறாகப் பயன்படுத்துதல், வெளிப்படுத்துதல் அல்லது தோல்வி ஆகியவை நிறுவனம் அல்லது தொடர்புடைய தனிநபர்கள் அல்லது நிறுவனங்களின் நலன்களை மோசமாக பாதிக்கலாம். இந்த தகவல் சொத்துக்களை அரசு நிறுவனத்தால் "மிக ரகசியம்", "ரகசியம்" மற்றும் "வரையறுக்கப்பட்ட பகிர்வு" என வகைப்படுத்தலாம்.

முக்கியமான ∴ உணர்தி-
றன் மிக்க தகவல்
சொத்துக்கள் (Critical IT
Assets)

முக்கியமான தகவல் தொழில்நுட்ப சொத்துக்கள் அமைப்பு எனப்படுவது அங்கீகரிக்கப்படாத அணுகல், தவறான பயன்பாடு அல்லது தகர்வு ஆகியவை தகவல் ∴ அமைப்பு அல்லது தனிநபர்களை மோசமாக பாதிக்கலாம். இந்த அமைப்புகளுக்கு உயர் மட்ட பாதுகாப்பு தேவைப்படுகிறது மேலும் கீழே வரையறுக்கப்பட்டுள்ளபடி முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு வடிவத்திலும் இருக்கலாம். இந்த தகவல் பாதுகாப்பு சொத்துக்களை நிறுவனத்தால் "முக்கியத்துவம் வாய்ந்த" மற்றும் "மிகவும் முக்கியமான" என வகைப்படுத்தலாம்.

முக்கியமான தேசிய தகவல் உட்கட்டமைப்பு(Critical National Information Infrastructure)

முக்கியமான தகவல் உட்கட்டமைப்பு என்பது அமைப்புகள் அல்லது வசதிகளைக் குறிப்பிடுகின்றது. அதன் இயலாமை அல்லது அழிவானது தேசிய பாதுகாப்பு, நிருவாகம், பொருளாதாரம், சுகாதாரம் மற்றும் ஒரு தேசத்தின் சமூக நலனில் பலவினமான தாக்கத்தை ஏற்படுத்தும்.

டிஜிட்டல் கையொப்பங்கள்(Digital Signatures)

டிஜிட்டல் கையொப்பங்கள் என்பது டிஜிட்டல் செய்திகள் அல்லது ஆவணங்களின் நம்பகத் தன்மையை சரி பார்க்கும் கணித ரீதியான முறைமையாகும். இது அனுப்புநரின் நம்பகத்தன்மை (பயனர்களின் அடையாளம்), செய்தி ஒருமைப்பாடு (முறையற்ற மாற்றம் அல்லது அழிவுக்கு எதிராக பாதுகாப்பு) மற்றும் நிராகரிப்பு (உரிமை கோரப்பட்ட அனுப்புநர் பின்னர் ஆவணத்தை உருவாக்குவதை மறுக்க முடியாது) ஆகியவற்றை வழங்குகிறது.

குறியாக்கம்(Encryption)

மறைகுறியாக்கம் என்பது ஒரு எளிய உரைச் செய்தியை பாதுகாப்பான-குறியீடு செய்யப்பட்ட உரை வடிவமாக மாற்றும் செயல்முறையாகும். மறைகுறியாக்கம் மூலம் அதனை மீண்டும் மாற்றாமல் புரிந்து கொள்ள முடியாது.

அரசாங்க நிறுவனங்கள்(Government Organizations)

2016 ஆம் ஆண்டின் 12 ஆம் இலக்க தகவலுக்கான உரிமைச்சட்டத்தில் வரையறுக்கப்பட்ட பகிரங்க அதிகார சபைகள் அரசாங்க நிறுவனங்களாகும்.

தகவல் பாதுகாப்பு கட்டுப்பாடுகள்(Information Security Controls)

பாதுகாப்புக் கட்டுப்பாடுகள் என்பது தகவல் மற்றும் தகவல் தொழில்நுட்பச் சொத்துக்களுக்கான பாதுகாப்பு அபாயங்களைத் தவிர்ப்பதற்கான, கண்டறிவதற்கான, எதிர்ப்பதற்கான அல்லது குறைப்பதற்கான பாதுகாப்பு அல்லது எதிர் நடவடிக்கைகளாகும். கட்டுப்பாடுகள் என்பது தொழில்நுட்பங்கள், கொள்கைகள், நடைமுறைகள் அல்லது தகவல் சொத்துக்களைப் பாதுகாக்க வைக்கப்படும் செயலிகளாக இருக்கும்.

தகவல் பாதுகாப்பு உத்தியோகத்தர் (Information Security Officer)

தகவல் பாதுகாப்பு உத்தியோகத்தர் என்பவர் என்பது நிறுவனத்தின் குறிக்கோள்கள், மூலோபாயம் மற்றும் தகவல் சொத்துக்கள் போதுமான அளவு பாதுகாக்கப்படுவதை உறுதி செய்வதற்கான செயல் திட்டங்களை நிறுவுதல் மற்றும் பராமரிப்பதற்கு பொறுப்பான ஒரு சிரீட் நிலையிலான நிருவாகி ஆவார்.

தகவல் பாதுகாப்பு குழு (Information Security Committee)

தகவல் பாதுகாப்புக் குழுவானது, தகவல் பாதுகாப்புத் திட்டமிடல், நிதியளித்தல், செயற்படுத்துதல் மற்றும் தகவல் பாதுகாப்பு நடவடிக்கைகள் செயற்படுத்தப்படுவதைக் கண்காணித்தல் உள்ளிட்ட தகவல் பாதுகாப்பு தொடர்பான அனைத்து நடவடிக்கைகளையும் நிறுவனத்திற்குள் வழி நடாத்தும் மற்றும் நிருவகிக்கும் குழுவினைக் குறிப்பிடுகின்றது..

தகவல் மற்றும் நிகழ்வு முகாமைத்துவ முறைமைகள்(Security Information and Event Management Systems)

தகவல் மற்றும் நிகழ்வு முகாமைத்துவ முறைமைகள் என்பது பதிவுக் கோப்புகளிலிருந்து சேகரிப்புத் தரவை பகுப்பாய்வு செய்தல் மற்றும் பாதுகாப்பு அச்சுறுத்தல்கள் மற்றும் நிகழ்வுகள் பற்றிய அறிக்கைகள் மற்றும் நிகழ்நேர கணினி கண்காணிப்பை ஒருங்கிணைத்து, முக்கியமான சிக்கல்களைப் பற்றி வலையமைப்பு நிருவாகிகளுக்குத் தெரிவிக்கின்றதுடன் பாதுகாப்பின் நிகழ்நேர பகுப்பாய்வை வழங்க பாதுகாப்பு நிகழ்வுகளுக்கிடையே வலையமைப்பு வன்பொருள் மற்றும் பிரயோகங்கள் மூலம் உருவாக்கப்பட்ட விழிப்புட்டல்கள் தொடர்புகளை ஏற்படுத்துகிறது.

தகவல் மற்றும் இணைய பாதுகாப்பு (Information and Cyber Security)

தகவல் பாதுகாப்பு என்பது ஒருமைப்பாடு, ரகசியத்தன்மை மற்றும் கிடைக்கும் தன்மையை உறுதி செய்வதற்காக அங்கீகரிக்கப்படாத அணுகல், பயன்பாடு, வெளிப்படுத்தல், இடையூறு, மாற்றம் அல்லது அழிவிலிருந்து சொத்துகளைப் பாதுகாப்பதனைக் குறிப்பிடுகின்றது. இது வெள்ளப் பெருக்கு தீ போன்ற ஏனைய இயற்கை பேரழிவுகளிலிருந்தும், சைபர் தொழில்நுட்பம் அல்லது வேறு ஏதேனும் வழிகளிலான பயன்பாட்டுடன் நனிநபர்களின் கேடு விளைவிக்கும் நடவடிக்கைகளிலிருந்து தகவல் சார்ந்த சொத்துக்களினைக் கொண்டிருக்கின்ற அல்லது பயன்படுத்துகின்ற தகவல் தொழில்நுட்ப சொத்துக்களின் பாதுகாப்பினை உள்ளடக்குகின்றது.

தகவல் சொத்துக்கள் (Information Assets)

தகவல் சொத்து என்பது நிறுவனத்திற்கு மதிப்புள்ள தகவல் அல்லது தரவினைக் குறிப்பிடுகின்றது.மின்னணு வடிவத்தில் கிடைக்கும் ஆவணங்கள், தரவுத்தள பதிவுகள் மற்றும் காகித வடிவத்தில் கிடைக்கும் ஆவணங்கள், தகவல் சொத்துகளுக்கான எடுத்துக்காட்டுகள்: சொற் கோப்புக்கள், படங்கள், தரவுத்தளத்தில் பணியாளர்களின் தனிப்பட்ட பதிவு என்பன இதில் உள்ளடங்கும்.

தகவல் தொழில்நுட்ப சொத்துக்கள்(IT Assets)

தகவல் தொழில்நுட்பசொத்து என்பது நிறுவனத்திற்கு மதிப்புள்ள எந்தவொரு தகவல் தொழில்நுட்ப உட்கரணங்கள், தகவல் அமைப்பு, மென்பொருள், சேமிப்பு ஊடகம்.கணினிகள், சேவையகங்கள், திசைவிகள், வட்டுகள், வலையமைப்புகள், மென்பொருள், தகவல் அமைப்புகள் மற்றும் அதன் கூறுகள் ஆகியவை தகவல் தொழில்நுட்ப சொத்துகளுக்கான எடுத்துக்காட்டுகளாகும்.

ஊடுருவலைக் கண்டறியும் முறைமைகள் ∴ ஊடுருவலைத் தடுக்கும் வழிமுறைமைகள் (IPS/IDS)

ஊடுருவல் கண்டறிதல் அமைப்புகள் என்பது அறியப்பட்ட சைபர் தாக்குதல்களை அடையாளம் காண வலையமைப்பு போக்குவரத்தை பகுப்பாய்வு செய்யும் சாதனங்கள். ஊடுருவல் தடுப்பு அமைப்புகள் சாதனங்கள் வலையமைப்பு நெரிசலினை பகுப்பாய்வு செய்து அறியப்பட்ட சைபர் தாக்குதல்களை அடையாளம் காணுவதனைக் குறிப்பிடுகின்றது. இருப்பினும், அது கண்டறியும் தாக்குதல்களின் வகையின் அடிப்படையில் பாக்கெட் வழங்கப்படுவதைத் தடுப்பதன் மூலம் தாக்குதல்களை நிறுத்த முடியும்.

<p>தகவலின் நேர்மைத் தன்மை(Integrity of Information)</p>	<p>தகவலின் நேர்மைத்துவம் என்பது தவறான மாற்றம் அல்லது அழிவுக்கு எதிராக தகவல்கள் பாதுகாக்கப்படுவதனைக் குறிப்பிடுகின்றது. தகவலானது அதன் மூல வடிவத்தில் இருப்பதை இது உறுதி செய்கிறது.</p>
<p>உத்தியோகபூர்வ மின்னஞ்சல்கள் (Official Email)</p>	<p>அதிகாரபூர்வ மின்னஞ்சல்கள் என்பது “பழஎ.டம” என்ற டொமைன் பெயருடன் அரசாங்கத்தால் வழங்கப்பட்ட மின்னஞ்சல்கணக்குகள் ஆகும்.</p>
<p>தனிப்பட்ட கிளவுட்(Pri- vate Cloud)</p>	<p>தேர்ந்தெடுக்கப்பட்ட பயனர்களுக்கு மட்டுமே இணையம் அல்லது தனிப்பட்ட உள்ளக வலையமைப்பு மூலம் வழங்கப்படும் சேவைகள்.உதாரணம் - லங்கா அரசு கிளவுட்</p>
<p>பொது கிளவுட்(Public Cloud)</p>	<p>பொதுகிளவுட் சேவையினை வாங்க விரும்பும் எவருக்கும் கிடைக்கக் கூடியதாக இருக்கும்.</p>
<p>மீட்பு புள்ளி நோக்கம் (Recovery Point Objective: RPO)</p>	<p>மீட்பு புள்ளி நோக்கம் (சீழு) என்பது நிறுவனம் எவ்வளவு அடிக்கடி காப்புப்பிரதிகளை எடுக்க வேண்டும் என்பதற்கான அளவீடு ஆகும், மேலும் மீட்டெடுக்கப்பட்ட தரவு எவ்வளவு புதுப்பிக்கப்படும் என்பதைக் குறிக்கிறது.தரவை மீட்டெடுப்பதற்கு ஏற்றுக் கொள்ளக்கூடிய ஆரம்ப காலத்தை இது குறிக்கிறது .உதாரணமாக, காப்புப்பிரதிகளுக்கு இடையில் ஒரு பேரழிவு ஏற்பட்டால், நிறுவனத்தால் 2 நிமிட மதிப்புள்ள தரவு அல்லது 2 மணிநேரம் அல்லது முழு நாளையும் இழக்க நேரிடும்.</p>
<p>மீட்பு நேர நோக்கம் (Recovery Time Objective: RTO)</p>	<p>ஒரு வர்த்தகம் பொறுத்துக் கொள்ளக்கூடிய வேலையில்லா நேரத்தை சுவுமுகுறிக்கிறது.ஒரு பேரழிவிற்குப் பிறகு நிறுவனத்தின் செயல்பாடுகள் மற்றும் அமைப்புகளை மீண்டும் தொடங்குவதற்கான ஆரம்ப கட்டம் இதுவாகும்.</p>
<p>முறைமைகள் கடினப்படு- த்துதல் (System Hardening)</p>	<p>கணினி கடினப்படுத்துதல் என்பது தகவல் தொழில்நுட்ப பாதிப்பு மற்றும் சமரசம் செய்யப்படுவதற்கான சாத்தியக் கூறுகளைக் குறைக்க இயல்புநிலை உள்ளமைவு மற்றும் முறைமைகளினை மாற்றுவதன் மூலம் ஒரு கணினியைப் பாதுகாப்பதற்கான செயன்முறையாகும்.தாக்குதல் மேற்பரப்பைக் குறைப்பதன் மூலமும், தீங்கிழைக்கும் செயற்பாட்டின் நோக்கத்திற்காக தாக்குபவர்கள் தொடர்ந்து பயன்படுத்த முயற்சிக்கும் திசையன்களைத் தாக்குவதன் மூலமும் இதனைச் செய்யலாம்.</p>
<p>மெய்நிகர் தனிப்பட்ட வலையமைப்பு (Virtual Private Network)</p>	<p>விரச்சுவல் பிரைவேட் நெட்வொர்க், இணையத்தில் தரவுத் தொடர்புக்காக மறை குறியாக்கப்பட்ட சுரங்கப் பாதையைப் பயன்படுத்தி பாதுகாப்பான இணைப்பை ஏற்படுத்துகிறது.</p>

உசாத்துணைகள்

1. தகவல் பாதுகாப்பு அமுலாக்க வழிகாட்டி. இலங்கை சேர்ட்டின் ஆராய்ச்சி, கொள்கை மற்றும் திட்டப் பிரிவினால் 2022 இல் வெளியிடப்பட்டது. இந்த ஆவணத்தை www.onlinesafety.lk மூலம் அணுகலாம்.
2. ஆகக்குறைந்த தகவல் பாதுகாப்பு வழிகாட்டிகள். இலங்கை சேர்ட் நிறுவனத்தின் ஆராய்ச்சி, கொள்கை மற்றும் கருத்திட்டப் பிரிவினால் பிரசுரிக்கப்பட்டது. இதனை <https://www.onlinesafety.lk> எனும் இணைப்பினூடாக அணுக முடியும்.
3. இலங்கை தகவல் மற்றும் இணைய பாதுகாப்பு மூலோபாயம். (2019:2023), இலங்கை சேர்ட் நிறுவனத்தின் ஆராய்ச்சி, கொள்கை மற்றும் கருத்திட்டப் பிரிவினால் 2019 நவம்பரில் பிரசுரிக்கப்பட்டது. இந்த ஆவணத்தினை https://cert.gov.lk/documents/NCS_Strategy.pdf எனும் இணைப்பினூடாக அணுகலாம்.
4. NIST இணைய பாதுகாப்பு கட்டமைப்பு. தேசிய கட்டளைகள் மற்றும் தொழில்நுட்ப நிறுவனத்தினால் பிரசுரிக்கப்பட்டது, ஐக்கிய அமெரிக்க வர்த்தக திணைக்களம். மூலத் தரவுகள் <https://www.nist.gov/cyberframework/online-learning/five-functions> எனும் இணைப்பினூடாக பெற்றுக் கொள்ள முடியும்.
5. வீட்டிலிருந்து வேலைக்கான தகவல் பாதுகாப்பு வழிகாட்டிகள். இலங்கை சேர்ட்டினால் பிரசுரிக்கப்பட்டது. இந்த ஆவணத்தினை <https://www.onlinesafety.lk/> எனும் இணைப்பினூடாக அணுக முடியும்.
6. அரசு நிறுவனங்களுக்கான இணையத்தள பாதுகாப்பு வழிகாட்டுதல்கள். இலங்கை சேர்ட்டின் ஆராய்ச்சி, கொள்கை மற்றும் திட்டப் பிரிவினால் 2022 இல் வெளியிடப்பட்டது. இந்த ஆவணத்தை <https://www.onlinesafety.lk> எனும் இணைப்பின் மூலம் அணுகலாம்.
7. வலையமைப்பு பயன்பாடு மற்றும் இணையத்தள பாதுகாப்புக்கான தொழில்நுட்ப வழிகாட்டுதல்கள். 2022 இல் இலங்கை சேர்ட்டின் ஆராய்ச்சி, கொள்கை மற்றும் திட்டப் பிரிவினால் வெளியிடப்பட்டது. இந்த ஆவணத்தை <https://www.onlinesafety.lk> எனும் இணைப்பினூடாக அணுக முடியும்.
8. சைபர் விண்ணப்ப பாதுகாப்புக்கான தொழில்நுட்ப வழிகாட்டிகள். இலங்கை சேர்ட் நிறுவனத்தின் ஆராய்ச்சி, கொள்கை மற்றும் கருத்திட்டப் பிரிவினால் பிரசுரிக்கப்பட்டது. இந்த ஆவணத்தினை <https://www.onlinesafety.lk/> எனும் இணைப்பினூடாக அணுக முடியும்.
9. ஐசூ 27002 (2013):தகவல் தொழில்நுட்பம் – பாதுகாப்பு உபாயங்கள் – தகவல் பாதுகாப்பு முகாமைத்துவ முறைமைகள் – தேவைப்பாடுகள், சர்வதேச நியமன்கள் நிறுவனம், சர்வதேச கட்டளைகள் நிறுவனத்தினால் பிரசுரிக்கப்பட்டது. இந்த ஆவணத்தினை <https://www.iso.org> எனும் இணைப்பினூடாக அணுக முடியும்.



Ministry of Technology



Funded by the European Union

