Cybersecurity Code of Practice for Critical Information Infrastructure

Cybersecurity Order 2023

CSB
CYBER SECURITY BRUNEI

DOCUMENT REVISION HISTORY

REVISION HISTORY		
Version No.	**Date:**	**DESCRIBTION**
1.0	11/03/2024	Initial Release

CYBERSECURITY CODE OF PRACTICE
FOR CRITICAL INFORMATION INFRASTRUCTURE
CYBERSECURITY ORDER 2023

TABLE OF CONTENTS

In the exercise of the power conferred by Article 83(3) Brunei Cybersecurity Order 2023 ("ORDER"), the Commissioner of Cybersecurity hereby issues the following Code:

1.0 PRELIMINARY

This section sets out the purpose and effect of this Code, compliance requirements and timelines, and definitions of key terms.

1.1 Citation and Commencement

1.1.1 This Code is the Code of Practice for Critical Information Infrastructure and shall take effect from 20th May 2023.

1.2 Glossary and Interpretation

1.2.1 In this Code, unless the context otherwise requires, the following terms shall have the corresponding meaning –

"Order"	Referring to the Cybersecurity Order, 2023
"Business Continuity Plan" ("BCP")	Documented procedures that guide organizations to respond, recover, resume, and restore businesses to a pre-defined level of operation following disruption and cover the resources, services and activities required to ensure the continuity of essential services.
Commissioner of Cybersecurity	The Commissioner of Cybersecurity appointed under section 5(1) of the Order, and includes the Deputy Commissioner and Assistant Commissioner of Cybersecurity appointed under section 5(3) and 5(4) of the Order.
"Critical Information Infrastructure" ("CII")	As defined in section 2 of the Order.
"CII Asset"	The components of an IT or OT system and/or network infrastructure of a CII and includes physical devices and systems, software platforms and applications of the CII.
"CII Designation Date"	Refers to the date on which a computer or computer system was designated as a CII under section 9(1) of the Order.
"CIIO"	Refers to legal owner of the critical information infrastructure and, where the critical information infrastructure is jointly owned by more than one person, includes every joint owner section 2(1) of the Order.
"Code"	This Cybersecurity Code of Practice for Critical Information Infrastructure.

"Compliance Date"	Means: a) In respect of a CII designated on or after the Effective Date, 12 months from the Designation Date; and b) In respect of a Redesignated CII, the date on which the new designation takes effect.
"Cyber Operating Environment"	The operating environment includes systems, applications, networks, physical sites, external interfaces, and access activities.
"Cybersecurity"	As defined in Section 2(1) of the Order.
"Cybersecurity Event"	An observable occurrence of an activity in or through a computer or computer system that may affect the cybersecurity of that or another computer or computer system and includes a cybersecurity incident.
"Cybersecurity Incident"	As defined in Section 2(1) of the Order.
"Cybersecurity Risk"	The potential harm from vulnerabilities or threats in digital systems.
"Cybersecurity Risk Profile"	A profile that outlines a CII's known cybersecurity risks, policy constraints and regulatory obligations for the determination of level risk mitigating controls required.
"Cybersecurity Threat"	As defined in Section 2(1) of the Order.
"Disaster Recovery Plan" ("DRP")	A documented procedure which guides organizations on the steps to recover IT and/or OT capability when a disruption occurs.
"Effective Date"	Means the date this version of the Code takes effect.
"Essential Service"	As defined in Section 2(1) of the Order.
"Indicators of Compromise" ("IOC")	Traces of security breach which can include IP addresses, Uniform Resource Locator (URL), domain, hashes, registry, filename, etc.
"Information technology" ("IT")	An arrangement of interconnected computers that is used in the storing, accessing, processing, analysing and sending of information, for example: computing and telecommunications equipment.
"Kerberos Ticket Granting Ticket Account"	The account is a special hidden account that encrypts all other authentication tokens in the Kerberos authentication protocol. An attacker who has compromised the account can forge a ticket to gain complete access to the entire domain.
"Malware"	Malicious software or firmware intended to perform unauthorized processes that will have adverse impact on the confidentiality, integrity, or availability of a computer system, for example: virus, worm, Trojan horse, spyware and some forms of adware or other code-based entity that infects a host.
"Mechanism"	An automated process that performs a series of activities.

"Operational Technology" ("OT")	An arrangement of interconnected computers that is used in the monitoring and/or control of physical processes, that includes: a) Supervisory control and data acquisition systems, distributed control systems, and other control system configuration such as programmable logic controllers; b) A combination of control components, for example electrical, mechanical, hydraulic, pneumatic, that act together to achieve an industrial objective, for example manufacturing, transportation of matter or energy
"Organizational Structure"	The hierarchical arrangement of roles, lines of authority, and communications of an organization.
"Patch"	A set of changes to software or firmware that addresses its cybersecurity vulnerabilities, or other updates to its functionality, usability, or performance.
"Patch Management"	The process involving one or more of the following actions of acquiring, testing, and installing patches or updates on existing software or firmware, enabling systems to stay updated, addressing vulnerabilities and includes patching applications, anti-malware, and firmware.
"Penetration Testing"	An authorized process of evaluating the security of a computer system, network, or application by finding vulnerabilities attackers could exploit and includes the process of: a. Gathering information about the target; b. Identifying possible entry points; c. Attempting to break in (either virtually or for real); and d. Reporting the findings.
"Periodic"	To perform an activity at a predefined interval.
"Physical Sites"	Primary and secondary locations hosting the CII.
"Purple Teaming"	In the context of an attack simulation means an exercise where the attack activity is revealed and explained to the blue team, and the red and blue teams work together and openly in real time to discuss each attack technique and the corresponding defensive measures, to improve people, process, and technologies.
"Privilege"	The rights assigned to any account including any user, application, service, or system account.
"Privileged Account"	Any account including any user, application, service or system account, that has administrative access privileges.
"Recovery Point Objective"	The amount of data that can be lost within a period most relevant to a business, before significant harm occurs, from the point of a critical event to the most preceding backup.
"Recovery Time Objective"	The quantity of time that an application, system and/or process, can be down for without causing significant damage to the business as well as the time spent restoring the application and its data.

"Redesignated CII"	Means a computer or computer system which is designated as a CII under section 9(1) no later than 3 months after the expiry or withdrawal of a previous designation.
"Remote Access"	Access to a CII by a user, or a process acting on behalf of a user, communicating through an external network.
"Remote Facilities"	Computer or computer system that has remote access capability.
"Residual Risk"	The risk exposure after risk mitigating controls is considered or applied.
"Risk Appetite"	The amount of risk, on a broad level, that CIIO is willing to accept in pursuit of its strategic objectives.
"Scenario-based Cybersecurity Exercise"	An activity to assess and validate an organization's plans and capabilities relating to the handling of simulated cybersecurity incidents (the 'scenario') affecting the organization. The exercise scenario should be based on relevant threats. Depending on the nature of the threats, CIIO may include social engineering and cyber range components in these scenarios.
"Security Architecture"	A set of physical and logical cybersecurity representations that addresses potential cybersecurity risks and gaps in the environment.
"Secured Intermediary Mechanism"	A security hardened agent or device that is used to access and manage a system that resides in a different security zone. Examples include a jump server and bastion host.
"Sensitive Data"	Sensitive data include production data and system configuration information.
"Shall"	In this Code, means that the statement mentioned is a mandatory requirement for compliance.
"Shared User Account"	Accounts that are shared by one or more users and include shared administrative user accounts.
"Should"	In this Code, means that the statement mentioned is a recommended requirement.
"Strong Encryption"	Industry-accepted standard algorithms to scramble data and encrypts/decrypts with key to achieve data confidentiality.
"System Development Lifecycle"	The process of planning, analysis, design, development, testing, implementation, maintenance, and retirement of a computer system.
"Threat Hunting"	The proactive effort to search for signs of malicious activity that has evaded security defences within the CII. It can be triggered by threat intelligence report, security monitoring, incident response, crown jewel analysis, domain expertise and analysis against MITRE ATT&CK, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

"Test Environment"	A setup of computer or computer systems to support test use cases.
"Timely Manner"	To perform an activity as soon as possible.
"Vendor"	Includes both technology suppliers and service providers.
"Vulnerability Assessment"	The process of identifying, assessing and ranking security vulnerabilities in a computer system.

All other words and phrases shall have the same meaning as defined in the Order.

1.2.2 A reference in this Code to a "clause" shall, unless otherwise stated, be construed as a reference to the corresponding clause in this Code and shall include all sub-clauses within that clause.

1.2.3 A reference in this Code to "including" shall not be construed restrictively but shall mean "including without prejudice to the generality of the foregoing" and "including but without limitation."

1.2.4 Use of the singular is deemed to include the plural (and vice versa).

1.2.5 Unless otherwise stated, the provisions of this Code shall apply to all CII. For the avoidance of doubt, references such as "the CII" or "a CII" do not in any way restrict the application of this Code to other CII that the CIIO owns.

1.2.6 Some clauses in this Code are prefaced with a preamble or include illustrations (presented in italicized font and without clause numbers). The preambles and illustrations are intended to provide additional information on the context, purpose, or application of the clauses they relate to. The preambles and illustrations do not form part of the measures that the CIIO is required to take under this Code, and hence need not be included in the scope of any cybersecurity audits carried performed by the CIIO under section 17(1) of the Order.

1.3 Purpose of this Code

1.3.1 This Code is intended to specify the minimum requirements that the CIIO shall implement to ensure the cybersecurity of its CII.

1.3.2 The CIIO is expected to implement measures beyond those stipulated in this Code to further strengthen the cybersecurity of the CII based on the cybersecurity risk profile of the CII.

1.4 Legal Effect of this Code

1.4.1 The CIIO must comply with this Code pursuant to section 13 of the Order. Unless otherwise stated, the provisions of this Code shall apply to all CII.

1.4.2 The CIIO must ensure full compliance with this Code by the Compliance Date.

1.4.3 The CIIO's obligation under this Code are in addition to its other obligation under the Order and other laws, and any relevant written directions or other codes of practice issued by the Commission under the Order.

1.4.4 If any provisions of this Code are held to be unlawful, all other provisions shall remain in full force and effect.

1.4.5 Where the provisions specified in this Code are not met by a CIIO, the commissioner may issue a direction in writing under section 14(1) of the Order to the CIIO for the compliance with the relevant provision.

1.5 Recurring Requirement

1.5.1 This Code includes clauses requiring certain act to be performed on a recurring basis at fixed intervals (e.g., a requirement to perform an act at least once every 24 months) (referred to below as "recurring requirements"). The relevant clauses prescribe the deadline for the first instance of the act. For subsequent instances, the deadline shall be counted from the date the previous instance was performed.

1.5.2 For Redesignated CII, the deadline for the first instance of a recurring requirement after the new designation shall be counted from the date the previous instance was performed, even though it was performed during the previous designation.

1.6 Waiver

1.6.1 The Commissioner may waive the application of any specific provisions of this Code to a CIIO under section 13(7) of the Order.

1.6.2 A CIIO can request for waiver from specific provisions of this Code under section 13(7) of the Order by submitting a written request to the Commissioner with the justifications supporting the request.

1.6.3 Any waiver, if granted by the Commissioner, shall be subject to such terms and conditions as the Commissioner may specify and may, without limitation, be for a fixed period or effective until the occurrence of a specific event.

1.7 Amendment and Revocation

1.7.1 The Commissioner may, at any time, amend or revoke this Code under section 13(1)(b) of the Order.

2.0 AUDIT REQUIREMENTS

This section sets out requirements for remediating findings from audits performed by CIIOs to ensure compliance with the Order and applicable codes of practice and standards of performance.

2.1 Remediation of Audit Findings

Audit findings highlight weaknesses and vulnerabilities in a computer or computer system that can be exploited by a cyber threat actor. Such weaknesses and vulnerabilities should be prioritized and remediated in a timely manner depending on their severity.

2.1.1 Where any audit identifies any non-compliance by a CIIO with the requirements specified in the Order or any Codes of Practice (COP) or Standards of Performance (SOP) issued under the Order, the CIIO shall, unless the Commissioner indicates otherwise in writing, submit an audit finding remediation plan to the Commissioner within 30 working days from the date that the CIIO receives the audit report.

2.1.2 The audit finding remediation plan shall:

a. Detail the remediation actions which the CIIO will take to address each area of non-compliance; and
b. Set out the timeline(s) for implementing the actions stated in sub-clause (a).

2.1.3 The Commissioner may, after consultation with the CIIO and where the Commissioner considers it appropriate, require the CIIO to revise its audit finding remediation plan and resubmit the revised audit finding remediation plan to the Commissioner within such timeframe as may be prescribed by the Commissioner.

2.1.4 The CIIO shall implement the audit finding remediation plan and complete all remediation actions within the timeframe(s) specified in the said plan, to the Commissioner's satisfaction, and at the CIIO's own cost. The CIIO shall update the Commissioner when each remediation action is completed.

3.0 GOVERNANCE REQUIREMENT

Governance involves establishing and maintaining frameworks to ensure that the CIIO's cybersecurity strategies are aligned with its business objectives. It also provides guidance to the CIIO in evaluating, defining, and directing efforts to manage cybersecurity risks.

3.1 Leadership and Oversight

Adequate resources and attention must be devoted to the CIIO's cybersecurity strategy and its application to the CII. Effective leadership from the board of directors and senior management is essential in building the right organizational culture, mindset, and structure towards cybersecurity, and to provide effective and timely business decisions on important cybersecurity matters.

3.1.1 The CIIO shall ensure that the roles relevant to ensuring the CII's cybersecurity are set out in writing, and the responsibility for each of these roles is assigned to a person working in or for the CIIO. This document shall:

a) Specify the organizational structure for persons involved in managing and ensuring the cybersecurity of the CII;
b) Ensure that the organizational structure prevents conflicts of interest from arising in relation to decisions relevant to the cybersecurity of the CII;
c) Specify what each of these roles is authorized to do and/or approve; and
d) Be formally approved by the CIIO personally (where the CIIO consists of one or more natural person) or by the relevant officers responsible for the management of the CIIO (where the CIIO is not a natural person).

3.1.2 The CIIO shall ensure that its board of directors (or equivalent body) includes at least one member that has knowledge and awareness of cybersecurity matters to have oversight of the cybersecurity risks to the CII, and to provide guidance to senior management on how to manage systemic cybersecurity risks.

3.1.3 The CIIO shall ensure that its senior management includes at least one member that has knowledge and awareness of cybersecurity matters to manage the cybersecurity risks to the CII and ensure that cybersecurity measures are implemented.

3.2 Risk Management

Cybersecurity risk management is the process of identifying, analysing, evaluating, and addressing the organization's cybersecurity risks in a cost-effective manner.

With rapid advancement in technology, acceleration in digitalization, and an evolving cybersecurity threat landscape, organizations are exposed to greater cybersecurity risks that may adversely impact their organization and business objectives. Hence it is important for CIIO's to establish and implement a cybersecurity risk management framework. This includes a cybersecurity risk assessment methodology, the organization's cybersecurity risk appetite and a risk register for each CII. In addition, CIIO shall ensure that the cybersecurity risks must be accepted at the appropriate level of senior management in a timely manner.

3.2.1 The CIIO shall establish and implement a cybersecurity risk management framework that provides for the following:

a) Promotion of a "risk culture" that enables the organization and its personnel to have open communications about risk, embrace learning from positive and negative experiences, make

informed decisions about addressing risks, and carry out risk management efforts commensurate with defined risk appetites;
b) The roles and responsibilities of various persons responsible for managing cybersecurity risks to the CII and their governance structure, including their reporting lines and accountabilities;
c) Cybersecurity risk assessment methodology;
d) Processes for the monitoring, communication and reporting of cybersecurity risks in a timely manner – the CIIO's senior management must be given regular reports of cybersecurity risks to the CII so that they are kept aware of the risks and impact, are able to manage the risks, and can ensure that the necessary cybersecurity measures to address the risks are implemented;
e) The organisation's cybersecurity risk appetite and thresholds or limits for residual risk; and
f) Process hazard analysis methodology to reduce or remove the impact on safety due to hazardous events (only for a CII which is an OT system).

3.2.2 The CIIO shall include the following steps in the cybersecurity risk assessment methodology:

a) Risk identification – identification of CII assets and cybersecurity threats, including threats identified from threat modelling[1], threat hunting, post-incident reviews of cybersecurity incidents, and the construction of risk scenarios;
b) Risk analysis – analysis of each risk scenario to determine the likelihood of occurrence and potential impact;
c) Risk evaluation – determining, documenting and prioritizing risks; and
d) Risk response – treatment and monitoring of each risk to keep the risk level within the organization's risk tolerance level.

3.2.3 For CII which are OT systems, the CIIO shall also include non-digital engineering controls as mitigating controls in a cybersecurity risk assessment where applicable.

3.2.4 The CIIO shall maintain and keep updated a risk register for each CII. The risk register shall record information of all cybersecurity risks to the CII, including risks identified through cybersecurity risk assessments. The risk register shall include the following:

a) Risk scenarios;
b) Dates when the risk scenarios are identified;
c) Existing measures in place to address the risk scenario;
d) Current risk ratings;
e) Risk treatment plan;
f) Progress status of the treatment plan;
g) Residual risk ratings; and
h) Risk owner

3.2.5 The CIIO shall ensure that all cybersecurity risks listed in the risk register are reviewed and monitored regularly to ensure that the thresholds or limits for residual risk identified in accordance with clause 3.2.1(e) are not breached.

[1] The threat modelling, the CIIO can refer to CSB's Guideline to Cyber Threat Modelling for Critical Information Infrastructure.

3.3 Policies, Standards, Guidelines and Procedure

Organizations must have governing processes in the form of policies, standards, and guidelines in place. At the top tier of formalized governance are policies, which provide a generalized overview of the organization's security needs and direction. This is followed by mandatory standards for compliance, as well as recommended guidelines for best practice.

The above are distilled into procedures with detailed steps and actions necessary to implement a specific mechanism, control, or solution. Only through such formal documentation can organizations produce a robust and reliable security infrastructure by reducing uncertainty and simplifying complexity. Furthermore, these artefacts need to be communicated to all relevant parties to ensure that relevant parties have a clear understanding on the mitigating controls to reduce the cybersecurity risks. The artefacts need to be reviewed and updated periodically to ensure their relevancy to the organization's cybersecurity threat landscape.

3.3.1 The CIIO shall establish and implement policies, standards, guidelines, and procedures for managing cybersecurity risks and protecting CII against cybersecurity threats. The policies, standards, guidelines, and procedures shall be:

a) Aligned with this Code, sector regulatory cybersecurity requirements, and applicable sectoral or national cybersecurity policies, standards, directions, and procedures; and
b) Published and communicated to all personnel and external parties who act on or have access to a CII.

3.3.2 The CIIO shall review the policies, standards, guidelines and procedures against the current CII cyber operating environment and cybersecurity threat landscape at least once every 12 months. The first instance of this review is to be completed no later than 12 months from the time the policies, standards, guidelines, and procedures were established.

3.3.3 The CIIO shall ensure that actual practices and implementation are consistent with the policies, standards, guidelines, and procedures. Differences, if any, shall be resolved in a timely manner.

3.4 Cybersecurity Design Principles

Cybersecurity design principles underpin the security architecture of the system and network. Adopting these principles and taking proactive steps to integrate security into the design process helps to reduce the overall attack surface of the system and network by various means. Often, this can discourage a cyber-attack as it would significantly increase the time and effort required by a cyber threat actor to compromise the system and network.

3.4.1 The CIIO shall adopt the following principles in relation to its people, process, and technologies to reduce cybersecurity risks to the CII:

a) The defence-in-depth principle to ensure that the security architecture of the CII includes multiple layers of security controls to prevent single point of failure;
b) The least privilege principle to ensure that accounts and users are granted the least extent of access necessary to perform their required functions; and
c) The principle of segregation of duties to ensure that duties and responsibilities for critical functions relating to the CII are divided among different persons.

3.4.2 The CIIO shall also adopt, to the extent possible, the following principles in relation to its people, process, and technologies to reduce cybersecurity risks to the CII:

a) The defence-by-diversity principle to reduce the number of potential attack vectors by having diversity throughout the CII, including diversity in technology, manufacturers and suppliers of assets, communication pathways, etc.; and
b) The zero-trust principle[2] to ensure that each request for access to the CII is authenticated, authorised, and validated for security configuration and posture before access is granted.

3.5 Change Management

Change management is essential for tracking and controlling changes made to the system or network architecture, including to network security design, network connections, configuration settings, and program logic in both hardware and software. Good change management processes ensure that the current design and build state of these systems and networks are known and recorded to support processes such as debugging, audit, and incident response.

3.5.1 The CIIO shall establish a change management process to identify, authorize, implement, and validate all changes made to the CII.

3.6 Use of Cloud Computing Systems and Services

As technologies evolve, organizations may decide to implement parts or the entire computer infrastructure on cloud computing systems. It is important that organizations assess the risks to the CII and impact to both the organization and nation from the outset when considering any such change. This will allow CIIOs to assess the risk trade-offs and to make an informed decision. The risk assessment report needs to be submitted to the Commissioner for review to ensure that all pertinent risks are covered.

3.6.1 The CIIO shall remain responsible and accountable for maintaining oversight of the cybersecurity of the CII and for managing cybersecurity risks to the CII, even when the CII is wholly or partly implemented on cloud computing systems.

3.6.2 The CIIO shall inform the Commissioner of any plans to implement the whole or any part of the CII on cloud computing systems, regardless of the deployment model (e.g., public cloud, private cloud, or hybrid cloud) or service model (e.g., software as a service, platform as a service or infrastructure as a service) being considered.

3.6.3 The CIIO shall not implement the whole or any part of the CII on cloud computing systems unless:

a) It has conducted a cybersecurity risk assessment of the risks relating to and arising from the proposed implementation on cloud computing systems and ensured that the risks identified can be adequately addressed;
b) The completed cybersecurity risk assessment is formally accepted by the CIIO and submitted to the Commissioner for review within 30 days of its completion; and
c) Where it appears to the Commissioner that any part of the cybersecurity risk assessment was not carried out satisfactorily, the CIIO has completed rectification works to the Commissioner's satisfaction at the CIIO's own cost and within the timeframe(s) specified by the Commissioner.

3.6.4 Where the CIIO has already engaged the services of a cloud computing service provider to assist in implementing the whole or any part of the CII on cloud computing systems, the CIIO shall ensure that the

[2] For Cybersecurity White Paper NIST: Planning for a Zero Trust Architecture, the CIIO can refer to the website (https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final)

service provider appoints a person within Brunei Darussalam authorized to accept service of any notice or legal process relating to the provision of services to the CIIO on the service provider's behalf.

3.7 Outsourcing and Vendor Management

A CIIO may engage external parties to perform or assist in performing certain functions, activities, or operations in respect of the CII. Common examples include outsourcing certain business functions to third-party vendors, or having vendors maintain certain assets and systems through contractual agreements. Controls must be implemented to minimize the cybersecurity risks and exposure that may arise from such arrangements to safeguard CII data and operations.

3.7.1 The CIIO shall remain responsible and accountable for the cybersecurity of the CII even if it engages an external party to perform or assist in performing any functions, activities, or operations in respect of the CII (referred to below as "outsourcing").

3.7.2 The CIIO shall establish processes to maintain oversight over all outsourced functions, activities, or operations, to minimize cybersecurity exposure arising from such outsourcing.

3.7.3 The CII shall include terms in its agreement(s) with the external party to help ensure the cybersecurity of the CII and to reduce or mitigate the impact of any cybersecurity risks associated with the outsourcing, including risks associated with the external party's access to the CII and its operations, processing, storage, communications, and other functions. This shall include terms stipulating:

a) The type(s) of access that the external party has to the CII, considering the CIIO's business requirements and the cybersecurity risk profile of the CII;
b) The obligations of the external party to protect the CII against cybersecurity threats and report cybersecurity incidents; and
c) The rights of the CIIO to commission an audit of the external party's cybersecurity posture in relation to the outsourced functions, activities, or operations; or to require that the external party provide a copy of the audit report should the external party commission its own audit for these purposes.

3.7.4 The CIIO shall establish processes for validating the external party's compliance with the terms required under clause 3.7.3 and any other terms in the agreement relating to cybersecurity.

3.7.5 The CIIO shall ensure that it is able to renegotiate the terms of its agreement(s) with external parties in the event of new legal or regulatory requirements.

4.0 IDENTIFICATION REQUIREMENTS

Identification requirements aim to assist the CIIO in understanding and identifying the resources and assets supporting the CIIO's critical business functions in delivering essential services, and the associated cybersecurity risks. It enables the CIIO to focus and prioritize its efforts in protecting these assets.

4.1 Assets Management

Asset management includes creating and maintaining a comprehensive inventory of all CII assets, including hardware, software, assets' dependencies, and connections with any systems or networks. This is a key component in ensuring cybersecurity as it provides visibility of CII assets and allows operators to make informed decisions and prioritize assets for protection. In addition, changes to CII asset or information recorded needs to be updated in the asset inventory in a timely manner to ensure that inventory is up to date.

4.1.1 The CIIO shall establish mechanisms and processes to identify all CII assets and maintain an inventory of the assets. The inventory shall include the following:

a) Owner and/or operator of each CII asset;
b) Name and description of each CII asset;
c) Description of critical functions of each CII asset;
d) Key person(s) responsible for the cybersecurity of each CII asset;
e) The dependencies of each CII asset and the connections between each CII asset and any systems or networks (whether internal or external to the CII);
f) Physical location of each CII asset;
g) Outsourced service providers used to support each CII asset;
h) Cloud services used to support each CII asset.
i) Description of the internet links supporting the CII, including information on the distributed denial-of-service (DDoS) attack mitigation measures in place for these internet links; and
j) CII network topology diagram, including the CII network perimeter, and all external computers and computer systems that the CII interfaces with.

4.1.2 The CIIO shall update the inventory whenever there is any change to any CII asset or to the information to be recorded in the inventory.

5.0 PROTECTION REQUIREMENTS

Protection requirements help the CIIO understand and implement the required people, process, and technology controls to protect the CII and to limit and contain the impact of cybersecurity incidents.

5.1 Access Control

Access control involves safeguarding CII assets from unauthorized access. By deploying access management mechanisms and processes, the CIIO ensures that only authorized parties can access protected systems, information, and applications. Access control includes the steps of Identification, Authentication and Authorization.

5.1.1 The CIIO shall ensure that access to the CII and between parts of the CII is restricted to authorized personnel, activities, processes, and devices.

5.1.2 With respect to the CIIO's obligations under clause 5.1.1, the CIIO shall put in place authorization and authentication controls for any access to the CII and between parts of the CII commensurate with the cybersecurity risk profile of the CII.

5.1.3 The CIIO shall ensure that all vendors' access to the CII are:

a) Documented and pre-approved;
b) Supervised by the CIIO; and
c) Performed on-site.

5.1.4 The CIIO shall implement mechanisms to automatically terminate logon sessions after inactivity for a pre-defined time; if the logon sessions cannot be terminated, the CIIO shall monitor the logon sessions for anomalous activities and trigger an alert for investigation when any anomaly is detected.

5.2 Account Management

Account management is about the requirements in the creation, monitoring, maintenance and retirement of a user, application, service, or system account that has access to the CII. Asset owners should determine appropriate access rights for each specific account while taking into consideration the associated cybersecurity risks. Accounts should not be granted excessive and unnecessary privileges to prevent unauthorized access. In addition, processes need to be established to detect unauthorized activities.

5.2.1 With respect to accounts that have access to the CII, including any user, application, service, or system account, the CIIO shall:

a) Grant to each account only the minimum privileges necessary for its assigned functions and uses;
b) Ensure that rights to install software are granted only to accounts that have been authorized to do so;
c) Ensure that shared user accounts are not created unless necessary for operating the CII;
d) Establish mechanisms and processes to monitor the activities of each account, including behavioural patterns, for any anomalies and to trigger an alert for investigation when any anomaly is detected; and
e) Delete or disable any account that is no longer necessary or is inactive.

5.2.2 The CIIO shall perform a review of all accounts that have access to the CII. The purpose of this review is to evaluate the validity of accounts and to ensure that privileges assigned to each account are up to date. The CIIO shall perform this review at least once every 12 months. The first instance of this review is to be completed no later than 12 months after the Compliance Date.

5.3 Privileged Access Management

Privileged accounts on a network are prime targets for malicious exploitation because they usually have more authority and access to resources. An attacker who has access to these accounts could potentially move about in the network and access privileged resources to gain unauthorized and persistent access to the entire system. Therefore, privileged access must be subject to tighter access control and greater monitoring.

5.3.1 With respect to privileged accounts, the CIIO shall:

a) Ensure that privileged access (i.e., administrative access) is granted only to selected accounts authorized to have such access;
b) Maintain an updated inventory of privileged accounts including details of the permissions and privileges assigned to each account;
c) Implement multi-factor authentication where privileged accounts are used to access the CII, and where privileges are to be escalated to the level of privileged access (e.g., where the user seeks to obtain additional permissions on a system or network after an initial log-in); and
d) Ensure that privileged access is initiated from a cybersecurity hardened environment and transfer of data takes place over authorized connections.

5.4 Domain Controller

Domain controllers are servers that are responsible for authenticating user access to a network. During a cybersecurity incident, the domain controller is one of the primary targets as it contains data that a cyber threat actor could use to cause massive damage. Therefore, it is important to have mechanisms in place to monitor for anomalies.

5.4.1 The CIIO shall implement mechanisms and processes to:

a) Monitor for changes to the trust relationships established between domains; and
b) Identify anomalies in the trust relationships and trigger an alert for investigation when any anomaly is detected.

5.5 Network Segmentation

Network segmentation is the separation of a network into different segments based on their security and risk levels and controlling communication between them. By using data flow control devices or solutions at network intersections and limiting traffic allowed into and out of any given segment, network segmentation makes it difficult for a cyber threat actor to traverse the entire network to perform malicious activities such as reconnaissance work and data theft.

5.5.1 The CIIO shall segment the network architecture of the CII into different network segments based on their different security and risk levels.

5.5.2 The CIIO shall limit any communications between the different network segments of a CII to only the minimum necessary for operating the CII.

5.5.3 The CIIO shall:

a) Implement network security mechanisms between the different network segments of the CII to detect and block malicious network traffic and to secure network communications; and
b) Establish mechanisms and processes to isolate affected network segments of the CII in the event of a cybersecurity incident.

5.6 Network Security

Network security measures exist to restrict traffic flowing between different trust domains such as an organization's internal network and the outside world to protect the network and data from breaches, intrusions, and cybersecurity threats. In addition, the organization should also have boundaries between internal trust domains which must be identified and controlled. Examples include designing and configuring the network in a manner that secures access to and from the CII.

5.6.1 The CIIO shall establish and implement network access control rules for the CII and perform periodic reviews to ensure they remain appropriate and up to date. The frequency of the review shall be commensurate with the cybersecurity risk profile of the CII.

5.6.2 The CIIO shall ensure that the CII is not connected to any network outside of the CII except where necessary for operating the CII. Where such connections are necessary, the CIIO shall:

a) Implement network security mechanisms between the CII and the network to detect and block malicious network traffic and to secure network communications; and
b) Restrict the direction of data flow to only one-way if only one-way data flow is required for the operations.

5.6.3 The CIIO shall ensure that the CII is not connected to the internet except where necessary for operating the CII. Where connection to the internet is necessary, the CIIO shall implement appropriate measures to mitigate and reduce cybersecurity risks arising from any such connection.

5.7 Remote Connection

Remote connection is the access to a non-public computing resource by a user (or a process acting on behalf of a user) communicating through an external network. For example, accessing a network in a CII to perform administration or maintenance from an external network. It is important to secure this access because it acts as a direct conduit into the CII. A secured conduit would make it difficult for a cyber threat actor to gain a foothold in the CII, denying the cyber threat actor the platform to perform reconnaissance for intelligence gathering and to take actions that adversely impact the CII.

5.7.1 The CIIO shall put in place effective cybersecurity measures for all remote connections to the CII to prevent and detect unauthorized access, and to validate that all such remote connections are authorized.

5.7.2 The CIIO shall ensure that:

a) Remote connections to the CII are disabled except where necessary for operating the CII;
b) Multi-factor authentication is required for the establishing a remote connection to the CII;
c) Remote connections to the CII have strong encryption and are made only through secured intermediary mechanisms;
d) Measures are put in place to ensure transmission security and message integrity over the remote connection;
e) Files to be uploaded to the CII are scanned for malware before being uploaded; and
f) Data flows over remote connections to the CII are limited to only the minimum necessary for performing the function required of the connection.

5.8 Wireless Communication

The use of wireless communications may be required within a CII, for example, due to physical constraints. However, this creates an additional attack vector that could be used by a cyber threat actor to gain entry to the network and to exfiltrate information or disrupt services. Moreover, wireless transmission of data presents the risk of data being intercepted. Controls need to be implemented to monitor for and prevent unauthorized access to the wireless network and data.

5.8.1 The CIIO shall ensure that the CII is not connected to any wireless Local Area Network (LAN) except where necessary for operating the CII. Where any such connection is necessary, the CIIO shall ensure that:

a) Only authorized wireless LAN is used.
b) The connection has strong encryption; and
c) Only authorised devices (whether such devices are CII assets or otherwise) are allowed to connect to the wireless LAN.

5.9 System Hardening

A typical CII environment may consist of numerous systems of different makes and models. Servers, consoles, workstations, appliances, network devices and field devices, in their default state, are not secured. Unnecessary services and programs are often left unmonitored, and they are potential avenues for a cyber threat actor to exploit. System hardening measures reduce the likelihood for the cyber threat actor to exploit vulnerabilities on assets that could lead to the compromise of the CII.

5.9.1 In respect of the following types of CII assets as they may be found in the CII, the CIIO shall establish and implement a security configuration baseline for each asset that is commensurate with the cybersecurity risk profile of the CII:

a) Operating systems;
b) Appliances;
c) Consoles and workstations, including Human Machine Interfaces (HMI) and OT engineering workstations;
d) Network devices;
e) Servers, including alarm servers, OT historians and management servers;
f) Software applications; and
g) Any other CII asset or type of asset identified by the Commissioner.

5.9.2 The security configuration baselines shall minimally address the following security practices:

a) Account management - disable or remove default accounts, guest accounts, inactive accounts, and unused accounts;
b) Password and passphrase management – Default passwords shall be changed; passwords and passphrases shall be stored using in their hash forms;
c) Application control – Disable services and remove applications that are not necessary for the operation of the CII;
d) Port(s) and service(s) management – Enable only ports and services that are necessary for the operation of the CII;
e) Physical connection - Enable only external physical connections that are necessary for the operation of the CII;
f) Malware protection – Install and update to the latest version of anti-malware software with the latest anti-malware signatures; and
g) Software upgrade and update - Timely upgrade and update of software and security patches.

5.9.3 The CIIO shall review the security configuration baselines at least once every 12 months to ensure that the baselines remain effective in ensuring the cybersecurity of the CII. The first instance of this review is to be completed no later than 12 months from the time the baselines are established.

5.9.4 The CIIO shall ensure that only authorized computing devices are used for the administration of the CII, and such devices are not used for other, non-administrative purposes.

5.10 Patch Management

Patch management is the process for identifying, obtaining, installing, and verifying updates and upgrades to firmware and software. Timely application of security patches limits the opportunity for a cyber threat actor to exploit vulnerabilities. Hence, it is important for organisations to monitor for new vulnerabilities and their corresponding security patches, and to develop procedures to prioritise and apply the security patches promptly. Furthermore, patches shall be verified and tested prior to installation in the production environment and monitored post-installation.

Management support is critical to ensure there is oversight on the effectiveness of the security patch management process. The management of the CIIO should closely monitor the reporting status to manage the risk exposure arising from unpatched vulnerabilities.

5.10.1 The CIIO shall establish and implement a security patch management process that includes:

a) Monitoring the release of security patches for CII assets;
b) Verifying the integrity of the security patches;
c) Testing security patches in a test environment that is similar to the CII production environment to ensure that the patches do not negatively affect the operations and cybersecurity of the CII;
d) Prioritising the application of security patches based on the level of risk posed to the operations of the CII;
e) Applying security patches in a timely manner to reduce cybersecurity vulnerabilities;
f) Monitoring and tracking the progress of patching;
g) Applying compensating controls to mitigate and reduce cybersecurity risks in cases where a security patch cannot be applied; and
h) Rolling back the application of security patches where necessary.

5.10.2 The CIIO shall ensure that there is management oversight over the effectiveness of the security patch management processes.

5.11 Portable Computing Devices and Removable Storage Media

Portable computing devices and portable media are convenient media to facilitate data transfers but are also an effective means for malware delivery. Organizations that allow the use of portable computing devices and removable storage media in their computing environment run the risk of malware infections through such media. It is therefore crucial that portable computing devices and removable media devices be hardened, verified, and their use be restricted and controlled to reduce the likelihood of a cyber threat actor succeeding in using such media as an attack vector to the CII.

In addition, sensitive information stored in the portable computing devices and removable media devices ought to be encrypted to ensure confidentiality of the data if these devices were compromised or lost.

5.11.1 The CIIO shall establish processes to authorize and track the use of portable computing devices and removable storage media that connect to the CII.

5.11.2 The CIIO shall ensure that all such authorized portable computing devices adhere to a security configuration baseline that minimally addresses the security practices listed in clause 5.9.2, and satisfies any other security standards and requirements which the CIIO may have for such devices.

5.11.3 The CIIO shall ensure that authorized removable storage media are free of malware prior to connecting to the CII.

5.11.4 The CIIO shall ensure that sensitive information relating to the CII (including production data and system configuration information) that is stored in portable computing devices and removable storage media is secured with strong encryption.

5.12 Application Security

As software becomes increasingly complex and connected, the difficulty of achieving application security increases exponentially. Attackers can potentially use many different paths through the applications used in the CII environment to do harm to the CIIO's businesses or organization.

As such, application security which describes cybersecurity measures and practices at the application level should be adopted to secure the application code and data. The Open Web Application Security Project (OWSAP) is one of the effective steps towards producing more secure code and minimise application security risks. To further secure web applications from malicious cyber threat actors, web application firewall (WAF) should be deployed to protect web application systems that are internet-facing to mitigate web vulnerabilities.

In addition, multi-tier architecture should be put in place to separate the application and database tier to improve scalability, security, and resiliency.

5.12.1 The CIIO shall ensure that only applications that are necessary for the operation and cybersecurity of the CII and that have been approved by the CIIO are used in the CII. The CIIO shall establish and maintain a list of such approved applications.

5.12.2 The CIIO shall review the list of approved applications at least once every 12 months. The first instance of this review is to be completed no later than 12 months from the time the list is established.

5.12.3 The CIIO shall verify the integrity of applications before they are used in the CII.

5.12.4 For a CII which is an IT system, the CIIO shall implement multi-tier architecture that separates the application and database tiers and implement security controls at each tier.

5.12.5 For a CII that includes web application systems, the CIIO shall reference the latest Open Web Application Security Project (OWASP) or equivalent application security guidelines when designing, developing, and testing applications to minimise application security risks.

5.12.6 For a CII that includes web application systems that are internet-facing, the CIIO shall also implement a Web Application Firewall (WAF) to monitor for, detect and block web application threats.

5.13 Database Security

Critical data is often stored in a database. While databases are not typically attacked directly, requests for data from applications, malicious or not, is often passed to them. For example, SQL injection or cross-site scripting are attacks that attempt to retrieve data or bypass authentication related to a database. Knowing these types of cyber-attacks are commonplace, measures need to be taken to secure a database.

Database security describes cybersecurity measures that aim to secure the confidentiality, integrity and availability of data stored in a database. For example, granular access control should be applied to the entire database, specific tables, or even in some specific columns or records to ensure only authorised accounts can connect to and query the data in the database. In addition, an individual should not be both a database administrator and system administrator as excessive access could increase the risk of abuse if the access is misused or compromised. Therefore, segregation of duties must be in place to ensure to checks and balances for preventing fraud and errors.

Furthermore, database logging and activity monitoring tools are important in detecting unauthorised access, manipulation, exfiltration, or destruction of data.

5.13.1 The CIIO shall ensure that only authorised accounts can connect to and query databases in a CII.

5.13.2 The CIIO shall ensure that duties relating to system administration and database administration for the CII are segregated and assigned to different persons.

5.13.3 The CIIO shall establish policies to secure databases in a CII, including policies for:

a) Securing data at rest;
b) Preventing data exfiltration; and
c) Restricting access to sensitive data to authorised persons.

5.13.4 The CIIO shall monitor databases in a CII for anomalous activities and trigger an alert for investigation when any anomaly is detected.

5.13.5 The CIIO shall monitor for bulk queries that exceed a predetermined threshold of data to be retrieved and trigger an alert for investigation when any such bulk query is detected.

5.14 Vulnerability Assessment

Vulnerability assessment is a process of identifying, assessing, and discovering security vulnerabilities on a computer system, including IT and OT systems or networks. The systematic approach of identifying, quantifying, and ranking security vulnerabilities enables an organization to select critical vulnerabilities to resolve based on its available resources and the risks posed. To ensure timely remediation of the security vulnerabilities, organizations should conduct vulnerability assessment regularly and when there are major system changes to their systems or networks to identify and mitigate flaws that may be exploited during a cyberattack.

5.14.1 The CIIO shall establish processes to identify and track cybersecurity vulnerabilities of the CII.

5.14.2 The CIIO shall remediate all cybersecurity vulnerabilities in a timely manner, with priority given to vulnerabilities that pose a greater risk to the security or operations of the CII.

5.14.3 The CIIO shall conduct a vulnerability assessment of the CII:

a) For a CII which is an IT system - at least once every 12 months, with the first instance to be completed by the Compliance Date; and

b) For a CII which is an OT system - at least once every 24 months, with the first instance to be completed no later than 12 months after the Compliance Date.

5.14.4 The CIIO shall also conduct a vulnerability assessment for relevant CII assets after implementing any major system changes to the CII. Major system changes include commissioning new systems to be connected to the CII, implementing new application modules, system upgrades and technology refresh.

5.14.5 The CIIO shall, if requested by the Commissioner, submit a copy of the report of any vulnerability assessment, along with the CIIO's plans for remediating each vulnerability, to the Commissioner within 30 working days of receiving the request.

5.15 Penetration Testing

Penetration testing is an authorized and intentional attack on a system to identify security vulnerabilities that could be exploited by a cyber threat actor. This allows organizations to determine exploitable vulnerabilities in their systems and address them.

However, penetration testing services can be intrusive because the penetration testers will gain access to their CIIOs' computer systems and networks and acquire a deep understanding of the systems' vulnerabilities. Such service, if abused, can compromise, and disrupt the systems and networks' operations even after the service provider's job has been completed. As such, CIIOs are required to ensure that the companies they engage to provide penetration testing services are accredited and that the penetration testers performing the tests are certified and competent.

5.15.1 The CIIO shall conduct a penetration test on the CII:

a) For a CII which is an IT system – at least once every 12 months, with the first instance to be completed by the Compliance Date; and
b) For a CII which is an OT system – at least once every 24 months, with the first instance to be completed no later than 12 months after the Compliance Date.

5.15.2 The CIIO shall also conduct penetration tests on relevant CII assets after implementing any major system changes to the CII. Major system changes include commissioning any new systems to be connected to the CII, implementing new application modules, system upgrades and technology refresh.

5.15.3 The CIIO shall ensure that third-party penetration testing service providers and their penetration testers who are performing penetration tests on a CII possess industry-recognized accreditations and certifications respectively, for example CREST[3] or equivalent accreditations and certifications:

a) Penetration testers performing the penetration tests must have industry recognized penetration testing certification to demonstrate assurance of their knowledge and practical skills.
b) Service providers must have industry-recognized accreditation to demonstrate assurance of their policies and procedures in penetration testing service, reporting and data handling, and due diligence in hiring of ethical penetration testers.

5.15.4 The CIIO shall ensure that all penetration tests by third-party service providers are conducted under supervision of the CIIO to ensure that activities carried out by the service providers are within the intended scope of the penetration test and do not disrupt CII operations.

[3] CREST is a not-for-profit organisation registered in the UK that is set-up to serve the needs of the technical information security industry. http://www.crest-approved.org/

5.15.5 The CIIO shall, if requested by the Commissioner, submit a copy of the report of any completed penetration test, along with the CIIO's remediation plans, to the Commissioner within 30 working days of receiving the request.

5.16 Adversarial Attack Simulation

Adversarial attack simulation is a cybersecurity assessment that simulates highly targeted attacks against an organisation's cyber operating environment by sophisticated cyber threat actors. It replicates a cybersecurity attack based on cyber threat actors' tactics, techniques, and procedures. The goal is to assess and enhance the capability of an organization to prevent, detect and respond to cybersecurity incidents.

5.16.1 The CIIO shall establish a red teaming or purple teaming attack simulation plan which identifies, among other things:

a) Objectives to be achieved;
b) Key stakeholders including red team, blue team and management team;
c) Assessment methodology, including planning and attack preparation, attack execution, clean-up and containment, blue team report and reconciliation, recommendations, and remediation;
d) Rules of engagement (only for red teaming);
e) Mitigation measures to minimize potential business impact or disruption; and
f) Recovery plan.

5.16.2 The CIIO shall conduct a red teaming or purple teaming attack simulation on its CII at least once every 24 months to test and validate the effectiveness of its cybersecurity measures against prevalent cybersecurity threats. The first instance of the attack simulation is to be completed no later than 12 months after the Compliance Date.

5.16.3 The CIIO shall, if requested by the Commissioner, submit a copy of the report of any completed red teaming or purple teaming attack simulation, along with the CIIO's remediation plans, to the Commissioner within 30 working days of receiving the request.

5.17 Cryptographic Key Management

The management of cryptographic keys is crucial to the effectiveness of cryptographic techniques. Any compromise to the cryptographic keys could allow a cyber threat actor to decrypt classified information or obtain privileged accesses, which may lead to the failure of the organisation's entire security infrastructure.

5.17.1 The CIIO shall ensure that all cryptographic keys for the CII are protected against unauthorized access.

5.17.2 The CIIO shall establish and implement mechanisms and processes to track and manage the lifecycle of cryptographic keys. The CIIO shall review these mechanisms and processes at least once every 12 months to ensure their continued effectiveness. The first instance of this review is to be completed no later than 12 months from the time the mechanisms and processes are implemented.

6.0 DETECTION REQUIREMENTS

Detection requirements aim to assist the CIIO in understanding and implementing the required people, process, and technology controls to detect and identify any malicious activity or vulnerability that could compromise the CII, including any stepping-stone attacks and attacks against the crown jewels of the system. The CIIO must investigate and identify potential threats and determine the impact, root cause and controls for containing threats and incidents and fortifying CII.

6.1 Logging

Logging is the process of recording events occurring within a system or network and enables an organization to perform investigations and threat hunting. For an organization to establish and maintain successful log management activities, it is vital that polices are developed based on defined goals and requirements, including the logging scope and log generation, transmission, storage, retention, and analysis.

6.1.1 The CIIO shall generate, collect, and store logs of the following:

a) All access and attempts to access the CII and the activities during such access, including application and database activities, and access to data in the CII;
b) Network connections between the CII and networks outside of the CII;
c) Network connections within the CII;
d) Remote connections to the CII; and
e) Connections between the CII and wireless LAN.

6.1.2 The CIIO shall also generate, collect, and store the following categories of logs to provide visibility of network activities within the CII and between the CII and networks outside of the CII:

a) Network Firewall logs;
b) Domain Name System (DNS) logs;
c) Web Proxy logs; and
d) Network Intrusion Detection/Prevention System (NIDS/NIPS) logs.

6.1.3 The CIIO shall provide any such logs referred to in clause 6.1.2 as may be required by the Commissioner for threat monitoring, threat analysis, threat alerts, and incident response.

6.1.4 The CIIO shall ensure that the logs generated, collected, and stored under clauses 6.1.1 and 6.1.2:

a) Use a consistent time source;
b) Are protected against unauthorized access, modification, and deletion;
c) Are stored for a minimum period of 12 months after the date of the event to which the log relates;
d) Have a log file structure (i.e., the arrangement of data fields within each log file) that facilitates analysis and sharing of logs; and
e) Are governed by a log retention policy to facilitate investigations into cybersecurity incidents, the conduct of threat hunting, and any other purposes relating to the cybersecurity of the CII.

6.2 Monitoring and Detection

Monitoring of traffic and logs can help detect cybersecurity threats so that appropriate countermeasures can be deployed. To achieve an effective monitoring regime, it is vital that a baseline of normal operations is established to detect deviations with the use of indicators of compromise. In addition, with the fast-changing cybersecurity landscape, it is critical that the processes and mechanisms are being reviewed consistently.

6.2.1 The CIIO shall establish and implement mechanisms and processes for the purposes of:

a) Monitoring and detecting all cybersecurity events in respect of the CII;
b) Collecting and storing records of all such cybersecurity events (including, where available, logs relating to the cybersecurity event);
c) Analysing all such cybersecurity events, including correlating between cybersecurity events, and determining whether there is or has been any cybersecurity incident; and
d) Triggering applicable incident reporting, response, and recovery plans if there is or has been any cybersecurity incident.

6.2.2 For the purposes of monitoring and detecting cybersecurity events, the mechanisms and processes established by the CIIO shall include:

a) Scanning for indicators of compromise (IOCs), including IP addresses, Uniform Resource Locator (URL), domains and hashes;
b) Establishing the normal day-to-day operational activities and network traffic in the CII, and using this as a baseline against which the CIIO is to monitor for deviations and anomalous activities; and
c) Ensuring that alerts for further investigation are triggered for all deviations and anomalous activities that are detected.

6.2.3 The CIIO shall review the mechanisms and processes established under clause 6.2.1, including the baseline referred to in clause 6.2.2(b), at least once every 12 months to ensure that the mechanisms and processes remain effective for their purposes. The first instance of this review is to be completed no later than 12 months from the time the mechanisms and processes are implemented.

6.3 Threat Hunting

Threat hunting is a proactive effort to search for signs of malicious activity that have evaded security defences within the CII. The objective of threat hunting is to identify previously unknown or ongoing threats within the environment to limit the impact of potential cybersecurity incidents in the evolving cyber threat landscape.

6.3.1 The CIIO shall conduct threat hunting for the CII to search for and identify cybersecurity threats to the CII at least once every 24 months. The first instance of threat hunting is to be completed no later than 12 months after the Compliance Date.

6.3.2 The CIIO shall include cybersecurity threats identified from threat hunting in cybersecurity risk assessments to ensure that the risks derived from the threats are assessed, mitigated, and tracked throughout the CII's system development lifecycle.

6.3.3 The CIIO shall analyse all threats identified from threat hunting to determine if there is or has been any cybersecurity incident in respect of the CII, and shall trigger the applicable incident reporting, response, and recovery plans if there is or has been a cybersecurity incident.

6.4 Cyber Threat Intelligence and Information Sharing

Threat intelligence provides contextual information that enables organizations to take proactive actions to prevent or mitigate cybersecurity incidents. Threat intelligence involves obtaining an understanding of trending threat landscapes, cyber threat actors and their Tactics, Techniques and Procedures (TTPs), and to translate them into actionable contextualized information for early warning and detection. By doing so, organizations will be able to put in place appropriate controls to mitigate cybersecurity threats and vulnerabilities in a timely manner.

Organizations should leverage on collective threat intelligence efforts through sharing and exchanging information on cybersecurity threats and vulnerabilities within the sector and with the Commissioner. This mutual sharing amongst stakeholders develops herd alertness, saves time, reduces duplicate efforts, and allows an organization's identification of threats to become another's prevention.

6.4.1 The CIIO shall establish and implement mechanisms and processes to obtain threat intelligence, and to process and analyse the threat intelligence for relevance and potential impact to the CII. Threat intelligence includes information on the current cybersecurity threat landscape; activities of threat actors; tactics, techniques, and procedures of threat actors; and cybersecurity vulnerabilities.

6.4.2 The CIIO shall establish and implement mechanisms and processes to share information on cybersecurity threats and vulnerabilities, and on measures that can be taken in response to such threats and vulnerabilities, with the Commissioner for threat monitoring and analysis.

6.4.3 The CIIO shall put in place controls to mitigate cybersecurity threats and address vulnerabilities identified from threat intelligence.

7.0 RESPONSE AND RECOVERY REQUIREMENTS

Establishing, managing, and exercising cybersecurity incident response plans and crisis communication plans to prepare the CII for cybersecurity incidents.

7.1 Incident Management

Incident management seeks to minimize the impact of cybersecurity incidents through processes that include the identification, containment and eradication of cybersecurity threats, and the recovery of systems, root-cause analysis, and implementation of corrective actions to prevent recurrence. It is important to have a plan with Cybersecurity Incident Response Team (CIRT) structure that details everyone's roles and responsibilities so that there can be clear lines of accountability and efficient communication channels. Incident response thresholds that are relevant to the business should also be determined so that the incident response plan can be triggered accurately without delays. Communication plans would also allow relevant parties to be updated with accurate situational updates.

When conducting root cause analysis, organizations should also include structural, behavioural, managerial, technical, or systemic factors that could contribute to the cybersecurity incident to address potential underlying issues and prevent a recurrence of similar incidents.

7.1.1 The CIIO shall establish a Cybersecurity Incident Response Plan that sets out how a CIIO should respond to a cybersecurity incident. The CIIO shall ensure that the Plan establishes:

a) A Cybersecurity Incident Response Team (CIRT) structure, including clearly defined roles and responsibilities of each team member and their contact details;
b) An incident reporting structure which sets out how the CIIO will comply with its reporting obligations under the Order and any other laws and regulations that apply to the CII;
c) Communication and coordination structures to ensure the timely escalation of cybersecurity incidents to the Cybersecurity Incident Response Team (CIRT) and to the senior management of the CIIO;
d) Thresholds and procedures to activate the incident response and CIRT;
e) Engagement protocols with relevant external parties, including vendors for forensic or recovery services and law enforcement agencies, and their contact details;
f) A communication plan to communicate information relating to a cybersecurity incident to internal and external stakeholders;
g) Processes and procedures to contain a cybersecurity incident, investigate the cause and impact of the cybersecurity incident, and to restore the CII's operations;
h) Processes and procedures to collect and preserve digital forensic evidence before initiating the recovery process, to support investigations; and
i) A post-incident review process to identify and implement corrective measures to prevent a recurrence.

7.1.2 The CIIO shall ensure that the Cybersecurity Incident Response Team (CIRT) is trained and equipped with the necessary resources to respond to cybersecurity incidents.

7.1.3 The CIIO shall establish procedures to reset the Kerberos Ticket Granting Ticket account for CII assets that use the Kerberos authentication protocol for the domain controller and shall reset the Kerberos Ticket Granting Ticket account if the CII domain controller is compromised.

7.1.4 The CIIO shall establish and implement processes to identify, investigate and address the root causes that contributed to each cybersecurity incident, including any structural, behavioural, managerial, technical,

or systemic factors, to prevent recurrence of similar incidents. This shall include processes to identify, investigate and address:

a) Gaps in the existing cybersecurity governance structure that may have led to ineffective cybersecurity risk management and oversight efforts;
b) Gaps in and failure to comply with policies, standards and procedures which may have contributed to the cybersecurity incident; and
c) Gaps in the audit process and the remediation of audit findings which may have contributed to the cybersecurity incident.

7.1.5 The CIIO shall communicate the Cybersecurity Incident Response Plan to all persons who use, operate, and manage the CII (including external vendors and their personnel), and update these persons whenever there is a change to the Cybersecurity Incident Response Plan.

7.1.6 The CIIO shall review the Cybersecurity Incident Response Plan to ensure that it remains updated and relevant at least once every 12 months. The first instance of this review to be completed no later than 12 months from the time the plan is established.

7.1.7 The CIIO shall also review the Cybersecurity Incident Response Plan when there are material changes to the CII cyber operating environment or incident response requirements.

7.2 Crisis Communication Plan

A crisis communication plan is an important part of an organisation's emergency preparedness and responses. The plan should include vital information including the required processes, mechanisms, and personnel to achieve the goal of ensuring that communications are coordinated and consistent to all stakeholders.

7.2.1 The CIIO shall establish a Crisis Communication Plan to respond to a crisis arising from a cybersecurity incident.

7.2.2 The CIIO shall ensure that the Crisis Communication Plan:

a) Establishes a crisis communication team to be activated during a crisis;
b) Identifies probable cybersecurity incident scenarios and corresponding courses of action;
c) Identifies target audiences and stakeholders for each type of cybersecurity incident scenario, which may include employees, customers, and the public;
d) Identifies spokespersons and technical experts who will represent the organization when addressing the media;
e) Identifies primary and alternate modes of communication for dissemination of information to relevant target audiences and stakeholders;
f) Establishes communication and coordination structures between the crisis communication team, spokespersons, technical experts, and any other relevant persons to ensure coordinated and consistent responses during a crisis; and
g) Provides for crisis communication training to ensure that employees can perform their assigned roles.

7.2.3 The CIIO shall communicate the Crisis Communication Plan to all relevant persons, including the crisis communication team, the spokespersons, and the technical experts, and update these persons whenever there is a change to the Crisis Communication Plan.

7.2.4 The CIIO shall review the Crisis Communication Plan at least once every 12 months to ensure that the Crisis Communication Plan remains effective. The first instance of this review is to be completed no later than 12 months from the time the Crisis Communication Plan is established.

7.3 Cybersecurity Exercise

Conducting cybersecurity exercises allows organizations to assess and validate their planning and operational capabilities, and to surface any areas of improvement. The continuous cycle of assessment, validation and improvement through a regular cyber exercise regime that covers people, process, and technology, improves the operational readiness of the organization, enabling swifter and more effective response to cybersecurity incidents.

7.3.1 The CIIO shall conduct scenario-based cybersecurity exercises to test and validate the effectiveness of the following plans:

a) Cybersecurity Incident Response Plan;
b) Business Continuity Plan;
c) Disaster Recovery Plan; and
d) Crisis Communication Plan.

7.3.2 The CIIO shall conduct the scenario-based cybersecurity exercises referred to at 7.3.1 at least once every 12 months. The first instance of such exercises is to be completed no later than 12 months after the Compliance Date.

7.3.3 In designing the incident response scenarios for the cybersecurity exercises, the CIIO shall include elements that test and validate:

a) Responses to threats and vulnerabilities identified from threat intelligence;
b) Coordination plans with partners and vendors;
c) Continued monitoring for further cybersecurity threats and incidents even during incident response; and
d) Adequacy of the CIIO's resources and capabilities to respond to cybersecurity incidents.

7.3.4 The CIIO shall ensure that the following stakeholders participate in the cybersecurity exercises:

a) Senior management;
b) Crisis management team;
c) Corporate communications and business operation staff;
d) Cybersecurity Incident Response Team (CIRT); and
e) Service providers.

7.3.5 The CIIO shall, if requested by the Commissioner, submit a copy of the report of any completed cybersecurity exercise, along with the CIIO's remediation plans, to the Commissioner within 30 working days of receiving the request.

7.3.6 In relation to cybersecurity exercises conducted by the Commissioner under Part 3 section 18 of the Order, the CIIO shall comply with any request by the Commissioner to provide information relating to the CII, including the relevant Cybersecurity Incident Response Plan and Crisis Communication Plan, for the purpose of planning and conducting such exercises.

8.0 CYBER RESILIENCY REQUIREMENTS

Cyber resilience includes maintaining the ability of the CIIO and CII to withstand cybersecurity incidents, continue the delivery of essential services and recover from cybersecurity incidents.

8.1 Backup and Restoration Plan

Having a sound restoration plan is critical to protect organizations against data loss or data corruption. Backup copies of data, software and systems allow data to be restored from an earlier copy in the event of system disruption or data corruption. Hence, organizations should conduct regular reviews to ensure that the backup copies are reliable. In addition, these backup copies need to be protected from the loss of confidentiality and unauthorized tampering of the data.

8.1.1 The CIIO shall establish a backup and restoration plan to ensure that its CII assets can be recovered in the event of system disruption or data corruption.

8.1.2 The CIIO shall perform periodic backups at a frequency that is commensurate with the CIIO's operational requirements and ensure that the backups are completed successfully.

8.1.3 The CIIO shall ensure that backups are stored on devices that are not connected to any computer or to the internet and are separate from the corresponding CII assets, and are protected from unauthorized access, modification, and deletion.

8.1.4 The CIIO shall test the restoration of the backups periodically to ensure that they can be restored when required. The frequency of the tests shall be commensurate with the cybersecurity risk profile of the CII.

8.1.5 The CIIO shall review the backup and restoration plan at least once every 12 months to ensure that the plan remains relevant. The first instance of this review is to be completed no later than 12 months from the time the plan is established.

8.2 Business Continuity Plan and Disaster Recovery Plan

It is critical for organizations to have effective business continuity and disaster recovery plans to enable them to recover from service disruption and to continue the delivery of products and services. The plans must include processes of creating recovery systems to deal with cyber threats and to ensure process continuity in the wake of a cyber-attack.

To ensure effective business continuity and disaster recovery plans, it is important to include recovery time objective (RTO) and recovery point objective (RPO) when developing the plans. Both metrics help to design the recovery process, define the recovery limits, the frequency of backups and the recovery procedures. The CIIO needs to exercise the plans periodically to ensure that they are effective and relevant personnel are familiar with the plans.

8.2.1 The CIIO shall establish a Business Continuity Plan ("BCP") and a Disaster Recovery Plan ("DRP") to ensure continuous delivery of essential services, in the event of disruption due to a cybersecurity incident.

8.2.2 The CIIO shall ensure that the BCP and DRP include plans for addressing different cybersecurity threat scenarios.

8.2.3 The CIIO shall define the recovery time objective and recovery point objective in the BCP.

8.2.4 For CII assets that use the Kerberos authentication protocol for the domain controller, the CIIO shall exercise the recovery procedures for the compromise of the Kerberos Ticket Granting Ticket as part of the disaster recovery exercise.

8.2.5 The CIIO shall review the BCP and DRP plans at least once every 12 months to ensure their continued effectiveness. The first instance of this review is to be completed no later than 12 months from the time the respective plan is established.

9.0 CYBERSECURITY TRAINING & AWARENESS

Effective security awareness training helps employees understand proper cyber hygiene, the security risks associated with their actions and to identify cybersecurity incidents that they may encounter in their work. Being aware of the evolving cybersecurity threats and being equipped with the essential cybersecurity skillsets enable the CIIO to recognize cybersecurity threats and mitigate them in a timely manner.

9.1 Cybersecurity Awareness Programme

Cybersecurity attacks, such as phishing, are increasingly common, and these attacks often spearheads an attacker's initial entry into an organization. Hence, an effective cybersecurity awareness programme to ensure that employees are aware of and fulfil their cybersecurity responsibilities is paramount. A good cybersecurity awareness programme enhances the cybersecurity vigilance and inculcate the responsible usage of technology of the employees and contractors. This mitigates the cybersecurity risks arising from the human factor.

9.1.1 The CIIO shall establish and implement a cybersecurity awareness programme to educate and develop cybersecurity awareness for all persons who use, operate, and manage the CII (including external vendors and their personnel), including to:

a) Promote awareness of relevant laws, regulations, codes of practice, policies, standards, guidelines, and procedures;
b) Provide regular and timely communication covering general cybersecurity awareness messages and prevailing cybersecurity threats, impacts and mitigations; and
c) Positively shape individual behaviour and the security culture of the organisation.

9.1.2 The CIIO shall measure the effectiveness of the cybersecurity awareness programme in achieving the purposes stated in clause 9.1.1 through means such as quizzes and surveys at least once every 12 months. The first instance of such measuring is to be completed no later than 12 months after the programme is implemented.

9.1.3 The CIIO shall review the cybersecurity awareness programme at least once every 12 months to ensure that the programme remains current and relevant. The first instance of this review is to be completed no later than 12 months from the time the programme is established.

9.2 Cybersecurity Training and Skills

It is important for CIIOs to ensure that the personnel who operate or manage the CII or are involved in ensuring the cybersecurity of the CII have the necessary cybersecurity competencies to perform their roles and responsibilities effectively.

9.2.1 The CIIO shall ensure that all its employees that operate and manage the CII receive training in cybersecurity skills to enable them to perform their roles relating to the CII effectively.

9.2.2 The CIIO shall ensure that any persons other than its employees that operate and manage the CII (including external vendors and their personnel) have the necessary cybersecurity skills to perform their roles relating to the CII effectively.

9.2.3 The CIIO shall ensure that any group of persons tasked with conducting a cybersecurity risk assessment for a CII is supervised by an individual possessing industry-recognised certification, such as Certified in Risk and Information Systems Control (CRISC) or equivalent certification.

9.2.4 The CIIO shall ensure that any group of persons tasked with conducting a cybersecurity audit for a CII is supervised by an individual possessing industry-recognized certification, such as Certified Information Systems Auditor (CISA) or equivalent certification.

10.0 OPERATIONAL TECHNOLOGY (OT) SECURITY REQUIREMENTS

10.1 Application of this Section

10.1.1 This section shall apply to CII which are OT systems ("OT CII").

10.1.2 In this section, the following terms shall have the corresponding meaning:

"Alert suppression"	The act of dismissing a notification.
"fail-safe"	A feature or practice that is designed to handle failure that results in minimal or no harm to equipment, environment, and people.
"Field controller"	Industrial computer (e.g., Programmable Logic Controller (PLC), Remote Terminal Unit (RTU)) in an OT environment used to monitor and/or control physical processes.
"Interlock"	Mechanism, process, or function to prevent operation (e.g., start-up, stoppage, etc) from entering in an undesired state.
"Physical process"	An action or activity denoted by any change of operation states, such as valve movement (open to close status), circuit breaker activated (close to open status) and motor rotation (low to high speed).
"Programme code"	The programmable code (e.g., Supervisory Control and Data Acquisition (SCADA) / Distributed Control System (DCS) function script, ladder diagram, function block diagram, structured text) developed for an application that is used to monitor and control the CII.
"Register block"	A temporary memory space that is used by the field controller to store or manipulate data.
"Safety Instrumented System"	Control systems that take a physical process to a safe state when in conditions that are or may become hazardous.

10.2 OT Architecture and Security

With increased connectivity between IT and OT systems, cyber threat actors are now able to compromise IT enterprise systems connected to the Internet, secure their footholds, and pivot into the OT systems to disrupt industrial processes. Hence, OT CII should not be connected to any enterprise network except where necessary for operating the CII. In addition, control mechanisms implemented in the OT systems and networks should not be shared across different operating environments. By having separate networks and control mechanisms in these networks, the risk of lateral movement between the networks is minimized.

There are several layers of control systems in an OT environment. Examples such as Distributed Control System (DCS) and Supervisory Control and Data Acquisition (SCADA) control the field controllers (e.g. PLC) that connect to the critical operational processes. The design of such control systems is often driven by the need to ensure reliability and safety; cyber security components are usually deprioritized. Hence, these control systems and OT devices tend to be more reliant on perimeter defences and network segregation to ensure that they are protected against cyber threat actors. However, it is important to ensure that these devices are secured to minimize the attack surface.

It is also important to incorporate engineering design concepts such as fail-safe mechanisms to eliminate or reduce the consequences of the affected system with respect to cybersecurity risks.

10.2.1 The CIIO shall ensure that the OT CII is not connected to any enterprise network except where necessary for operating the CII and provided that the direction of data flows is restricted to only one-way from the OT CII to the enterprise network.

10.2.2 The CIIO shall monitor the data flows from the OT CII to any enterprise network for anomalies and trigger an alert for investigation when any anomaly is detected.

10.2.3 The CIIO shall implement separate authentication mechanisms and account credentials for users of the OT CII network and any enterprise network. This is to prevent threat actors from using compromised credentials across different operating environments.

10.2.4 The CIIO shall ensure that the OT CII has fail-safes to ensure the safety and reliability of operations in the event of a cybersecurity incident.

10.2.5 The CIIO shall identify physical processes controlled by the OT CII and shall, to the extent possible, perform the following for each process:

a) Establish a baseline tolerance level for the operation time taken by the physical processes;
b) Monitor the duration of physical processes for deviations from the baseline tolerance level; and
c) Ensure the field controller controlling the physical processes operates in a failsafe state when deviations outside of the tolerance level occur and trigger an alert for investigation.

10.2.6 The CIIO shall ensure that the Safety Instrumented System (SIS) is only connected to authorized field devices[4]. This is to protect the SIS and its functions from being compromised in the event of a cybersecurity incident affecting other computers or computer systems.

10.2.7 The CIIO shall periodically assess whether it is possible to replace CII assets (including legacy assets) with more secure versions and make such replacements where possible to improve the cybersecurity of the CII.

[4] Field devices include actuator, sensor, or circuit relay and breaker. The CIIO may refer to level 0 of the Purdue Enterprise Reference Architecture (PERA).

10.3 Secure Coding

Codes determine how digital devices behave and could be compromised to perform unintended actions that impact the operations of the system. It is thus important to implement security mechanisms and processes to secure the codes.

10.3.1 The CIIO shall verify the integrity of all embedded firmware of OT CII assets before they are used in the CII, and shall periodically verify the integrity of all embedded firmware in the OT CII.

10.3.2 The CIIO shall verify the integrity of the programme codes in a field controller before use, and shall periodically verify the integrity of all programme codes in field controllers.

10.3.3 With regard to field controllers that are intended to have a fail-safe state, the CIIO shall identify and include interlocks in the field controllers' programme codes.

10.3.4 The CIIO shall establish mechanisms to validate the input values to the field controller to ensure that they are within a valid operational range.

10.3.5 The CIIO shall ensure that no unauthorized changes are made to the programme code or input values of a field controller.

10.3.6 The CIIO shall assign a separate and designated register block each for reading, writing, validating writes, calculation, and any other relevant function of the field controller, in order to facilitate data verification, prevent buffer overflows, prevent unauthorized writes and protect controller data.

10.3.7 The CIIO shall identify programme codes in a field controller that function independently of other programme codes within the field controller, and modularize such programme codes to facilitate the detection of malicious codes.

10.4 Field Controllers

Field controllers are usually insecure by design and are potentially vulnerable to communication interception and modification. In addition, the processing unit within the field controller is susceptible to modification thus affecting the control functions. Therefore, it is necessary to verify that both the field controller itself and the communication to and from the field controller are secured to achieve integrity of the communication.

10.4.1 The CIIO shall establish mechanisms and processes to reduce and manage cybersecurity risks relating to connections between a field controller and any network or device, including:

a) Establishing a separate communication module when connecting the field controller to an external network or device, to prevent unauthorized access to the OT CII through the field controller;
b) Implementing authentication processes for data transmission between the field controller and any network or device;
c) Preventing unauthorized data transmission, including unauthorized write functions, to ensure the safety and reliability of the operations;
d) Preventing data transmission between the field controller and the network or device when the field controller is in a fault or error state, except were doing so would adversely affect the safety and reliability of operations; and
e) Enabling security features such as password-protection.

10.4.2 The CIIO shall ensure that all alerts, errors, and warnings from the field controllers are investigated in a timely manner.

10.4.3 The CIIO shall establish mechanisms to monitor for alert suppression in the field controllers and trigger an alert for investigation when any unauthorized alert suppression is detected.

10.4.4 The CIIO shall establish baselines for normal day-to-day operational activities of field controllers, including baselines for cycle time, operational uptime, stop state, and memory usage, against which the CIIO is to monitor for deviations and anomalous activities, and trigger an alert for investigation when any deviation or anomaly is detected.

10.4.5 The CIIO shall review the baselines referred to in clause at least once every 12 months. The first instance of this review is to be completed no later than 12 months from the time the baseline is established.

11.0 DOMAIN-SPECIFIC PRACTICES

11.1 Application of this Section

11.1.1 This section applies only to CII which CII assets include internet-facing Domain Name System (DNS) servers.

11.2 Domain Name System Security Extension (DNSSEC)

DNS is the phone book of the Internet. It enables access to internet websites and services using user-friendly domain names rather than IP address. It translates domain names to IP address and back, telling computers where to send and retrieve information.

Unfortunately, it also accepts any address given to it, without verification and validation. This makes it vulnerable to cyber-attacks like spoofing, and DNS cache poisoning, that focus on corrupting or altering the DNS records and placing false information in a DNS resolver cache. To address such attacks, DNSSEC should be enabled.

DNSSEC is a security feature of DNS which validates DNS information (e.g. IP address) for a given domain name (e.g. csb.gov.bn), by adding cryptographic signatures to existing DNS records. This allows for the validation of the authenticity and message content integrity of DNS records.

11.2.1 The CIIO shall enable DNSSEC validation for its DNS resolvers, or implement any equivalent or better methods of validating the integrity of DNS records, to prevent DNS attacks such as DNS cache poisoning and DNS spoofing.

11.2.2 The CIIO shall ensure that all domain names under its control and used in connection with the CII, including in the operation of the CII and in the delivery of services, are DNSSEC signed on the corresponding DNS Authoritative Server for each domain name.

ANNEX A – GUIDANCE FOR STRENGTHENING ORGANISATIONAL CYBERSECURITY POSTURE

An organisation's cybersecurity is only as strong as its weakest link. Even as measures are taken under this code to ensure the cybersecurity of the CII, it is vital that CIIOs ensure cybersecurity throughout its organisation. This Annex A seeks to provide guidance for strengthening the cybersecurity posture of the organisation. CIIOs are highly encouraged to implement these measures.

For the avoidance of doubt, the matters in this Annex need not be included in the scope of cybersecurity audits conducted under section 17 of the Order.

Domain	Guidance
Cybersecurity Design Principles	1. The CIIO should adopt the defence-in-depth principle to ensure that the security architecture of a computer or computer system used by the organisation includes multiple layers of security controls to prevent single point of failure. 2. The CIIO should adopt the least privilege principle to ensure that accounts and users are granted the least extent of access necessary to perform their required functions. 3. The CIIO should adopt the principle of segregation of duties to ensure that duties and responsibilities for critical functions relating to a computer or computer system used by the organisation are divided among different persons. 4. The CIIO should also adopt, to the extent possible, the following principles in relation to its people, process, and technologies to reduce cybersecurity risks to a computer or computer system used by the organisation: a) The defence-by-diversity principle to reduce the number of potential attack vectors by having diversity throughout a computer or computer system used by the organisation, including diversity in technology, manufacturers and suppliers of assets, communication pathways, etc.; and b) The zero-trust principle to ensure that each request for access to any computer or computer system used by the organisation is authenticated, authorised, and validated for security configuration and posture before access is granted.

Wireless Communication	1. The CIIO should ensure that a computer or computer system used by the organisation is not connected to any wireless Local Area Network (LAN) except where necessary for authorised operations. Where any such connection is necessary, the CIIO should ensure that: a) Only authorised wireless LAN is used; b) The connection has strong encryption; and c) Only authorised devices are allowed to connect to the wireless LAN.
Threat Hunting	1. The CIIO should conduct threat hunting for a computer or computer system used by the organisation to search for and identify cybersecurity threats to the systems at least once every 24 months. 2. The CIIO should include cybersecurity threats identified from threat hunting in cybersecurity risk assessments to ensure that the risks derived from the threats are assessed, mitigated, and tracked throughout the system development lifecycle of a computer or computer system used by the organisation. 3. The CIIO should analyse all threats identified from threat hunting to determine if there is or has been any cybersecurity incident in respect of a computer or computer system used by the organisation, and should trigger the applicable incident reporting, response, and recovery plans if there is or has been a cybersecurity incident.
Domain Name System	1. The CIIO should ensure that all domain names under its control and used in connection with any computer or computer system used by the organisation, including in the delivery of services, are DNSSEC signed on the corresponding DNS Authoritative Server for each domain name. 2. The CIIO should enable DNSSEC validation, or implement any equivalent or better methods of validating the integrity of DNS records, for DNS resolver to prevent DNS attacks such as DNS cache poisoning and DNS spoofing.

QUERIES AND FEEDBACK

Questions and feedback on this document may be submitted to:

CII_feedback@csb.gov.bn