CYBERSECURITY ACT 2018
(ACT 9 OF 2018)
CYBERSECURITY CODE OF PRACTICE FOR CRITICAL INFORMATION INFRASTRUCTURE
(FIRST EDITION – SEPTEMBER 2018)

ADDENDUM NO. 1– DECEMBER 2019

This addendum ("Addendum") shall be read in conjunction with the Cybersecurity Code of Practice for Critical Information Infrastructure (First Edition – September 2018) and shall form part of the Code of Practice. This Code of Practice shall take effect from 20 December 2019.

S/No	Part / Page No	Amendments / Corrections
1	3	Clause 1.1.1 of the Code of Practice is amended by inserting, immediately after the words "under the Act.", the words "Compliance to ANNEX A shall be effective from 19 June 2020."
2	3	Clause 1.2 of the Code of Practice is amended (a) by inserting, immediately after the definition of "network security assessment", the following definition: "network zone" means a logical segmented section of a network that contains computer or computer systems which have been grouped in accordance with specific security requirements set; (b) by inserting, immediately after the definition of "organisation structure", the following definition: "patch" means a set of changes to a software/firmware in addressing its cybersecurity vulnerabilities, or other updates to its functionality, usability or performance; (c) by inserting, immediately after the definition of "organisational structure", the following definition: "patch management" means the process involving one or more of the following actions of acquiring, testing and installing patches/updates on existing software/firmware, enabling systems to stay updated, addressing vulnerabilities and includes patching applications, anti-malware, and firmware; (d) by inserting, immediately after the definition of "personnel", the following definition: "privilege account" means any user or system account that has administrative access privileges; (e) by inserting, immediately after the definition of "risk appetite", the following definition: "role-based access control" means a method of granting the appropriate access and permissions in accordance with the roles of individual users within an organisation;

		(f) by inserting, immediately after the definition of "shall", the following definition: "shared user account" means accounts that are shared by one or more users and includes shared administrative user accounts; (g) by inserting, immediately after the definition of "system development lifecycle", the following definition: "test environment" means one or more computer or computer systems that is used for the purposes of determining if the requirements of a specification or contract of a software is met, and is usually not part of the production environment; and (h) by inserting, immediately after the definition of "vulnerability assessment", the following definition: "wireless lan" means a wireless computer network that links two or more devices using wireless communication to form a local area network within a limited area.
3	7	The Code of Practice is amended by inserting, immediately after clause 1.4.1, the following clause: "Without prejudice to Clause 1.4.1, ANNEX A shall also apply to any CII, which is an OT system"
4	20	Clause 12 of the Code of Practice is amended by inserting, immediately after the words "1. Cybersecurity Agency of Singapore, "Security By Design Framework", 2017", the words "2. Cybersecurity Agency of Singapore, "Industrial Control Systems Cybersecurity Guidelines", 2018"
5	22	The Code of Practice is amended by inserting, immediately after the words "9. "Security and Privacy Controls for Federal Information Systems and Organisations, NIST Special Publication 800-53 Revision 4", NIST, 2013", the section, ANNEX A: OT SYSTEMS REQUIREMENTS.

CYBERSECURITY ACT 2018
(ACT 9 OF 2018)
CYBERSECURITY CODE OF PRACTICE FOR CRITICAL INFORMATION INFRASTRUCTURE

In exercise of the powers conferred by section 11(1)(a) of the Cybersecurity Act ("the Act"), the Commissioner of Cybersecurity hereby issues the following Code:

1. PRELIMINARY

1.1 Citation and Commencement

1.1.1 This Code may be cited as the "Cybersecurity Code of Practice for Critical Information Infrastructure", and shall come into effect from 1st September 2018 and compliance to this Code shall be nine (9) months from the date of designation of a critical information infrastructure ("CII") under the Act. Compliance to ANNEX A shall be effective from 19 June 2020.

1.2 Interpretation

1.2.1 In this Code, unless the context otherwise requires –

"Act" means Cybersecurity Act 2018;

"architecture review" means a process of reviewing and analysing the design of the application and network architecture to identify critical assets, network design weaknesses, sensitive data stores and business critical interconnections for potential attack vectors and potential vulnerabilities in the network and application architectures;

"authorised" means the official management decision given by a senior officer working in or for the CIIO to operate and to explicitly accept the risk to the CIIO on the implementation of an agreed-upon set of security controls;

"Assistant Commissioner" means "Assistant Commissioner" as defined in section 2 of the Act;

"business continuity plan" ("BCP") means documented procedures that guide organisations to respond, recover, resume and restore businesses to a pre-defined level of operation following disruption and covers the resources, services and activities required to ensure the continuity of essential services;

"Commissioner" means the Commissioner of Cybersecurity appointed under section 4(1)(a) of the Act, and includes the Deputy Commissioner and Assistant Commissioners appointed under section 4(1)(b) of the Act as well as Assistant Commissioners appointed under section 4(2) of the Act;

"critical information infrastructure" ("CII") means "critical information infrastructure" as defined in section 2 of the Act and in this Code, this term refers to all CII owned by a CIIO where the CIIO owns more than one CII;

"CII asset" means the components of an IT/OT system and/or network infrastructure of a CII and includes physical devices and systems, software platforms and applications of the CII;

"CIIO" means the owner of a CII; "owner" in this respect, means "owner" defined in section 2 of the Act;

"cybersecurity" means "cybersecurity" as defined in section 2 of the Act;

"cybersecurity event" means 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;

"cyber operating environment" means the operating environment that includes systems, applications, networks, physical sites, external interfaces and access activities;

"cybersecurity risk" means "cybersecurity risk" as defined in section 6 of the Cybersecurity (Critical Information Infrastructure) Regulations of the Act;

"cybersecurity risk profile" means 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" means "cybersecurity threat" as defined in section 2 of the Act;

"cybersecurity incident" means "cybersecurity incident" as defined in section 2 of the Act;

"disaster recovery plan" ("DRP") means a documented procedure which guides organisations to recover IT/OT capability when a disruption occurs;

"essential services" means "essential services" as defined in section 2 of the Act;

"external computer or computer system" means computer and computer system that is external to a CII and includes remote facilities that have connection to the CII;

"host security assessment" means a process of security assessment on a host to assess the host security configuration that cannot be seen from the network, to identify additional exposures and configuration weaknesses. It checks if the host's systems and applications are hardened effectively. Host, in this context, includes operating system, database server, firewall, router/switch, virtualisation implementation, load balancer, IDS, web proxy, web server, application server, mail server and wireless devices;

"information technology" ("IT") refers to arrangement of interconnected computers that is used in the storing, accessing, processing, analysing and sending of information, for example: computing and telecommunications equipment;

"malware" means malicious software or firmware intended to perform unauthorised 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;

"network security assessment" means a process to identify and evaluate security weaknesses of the network and the network perimeter of a computer or computer system;

"network zone" means a logical segmented section of a network that contains computer or computer systems which have been grouped in accordance with specific security requirements set;

"operational technology" ("OT") refers to an arrangement of interconnection 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;

"organisational structure" means the hierarchical arrangement of roles, lines of authority, and communications of an organisation;

"patch" means a set of changes to a software/firmware in addressing its cybersecurity vulnerabilities, or other updates to its functionality, usability or performance;

"patch management" means the process involving one or more of the following actions of acquiring, testing and installing patches/updates on existing software/firmware, enabling systems to stay updated, addressing vulnerabilities and includes patching applications, anti-malware, and firmware;

"penetration testing" means an authorised 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;

"personnel" means any person who use, operate or act on a CII including employees, contractors and third party service providers;

"privilege account" means any user or system account that has administrative access privileges;

"process interface" means a process acting on behalf of a computer or computer system;

"remote access" means access to a CII by a user, or a process acting on behalf of a user, communicating through an external network;

"remote facilities" means computer or computer system that have remote access capability;

"residual risk" means the risk exposure after risk mitigating controls are considered or applied;

"risk acceptance" means the informed decision to knowingly take a particular risk;

"risk appetite" means the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives and it is often taken as a forward looking view of risk acceptance;

"role-based access control" means a method of granting the appropriate access and permissions in accordance with the roles of individual users within an organisation;

"security by design framework" means a framework for incorporating security into an IT/OT system throughout its life-cycle, from creation to disposal and includes the identification, protection, detection, response and recovery capabilities for the cyber resiliency of the IT/OT systems;

"security baseline configuration standards" means a documented set of specifications for a IT/OT system, or a set of configuration parameters within a system, that has been formally reviewed and agreed on at a given point in time;

"shall", in this Code, means that the statement mentioned is a mandatory requirement for compliance;

"shared user account" means accounts that are shared by one or more users and includes shared administrative user accounts;

"should", in this Code, means that the statement mentioned is a recommended requirement;

"system development lifecycle" means the approach to creating and maintaining an IT/OT system from inception till retirement and includes the process of planning, analysis, design, testing, implementation, maintenance and retirement;

"test environment" means one or more computer or computer systems that is used for the purposes of determining if the requirements of a specification or contract of a software is met, and is usually not part of the production environment;

"vendor" includes both technology suppliers and service providers;

"vendor service application" means application that the vendor use for the purpose of diagnosis or maintenance of the CII and include application that is installed on the vendor's computer;

"vulnerability assessment" means the process of identifying, assessing and discovering security vulnerabilities in a system and comprises of host security assessment, network security assessment and architecture review;

"wireless lan" means a wireless computer network that links two or more devices using wireless communication to form a local area network within a limited area.

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.

1.3 Purpose of this Code

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

1.3.2 A CIIO is expected to take further measures beyond measures required to be taken under this Code, to further strengthen the cybersecurity of its CII based on its cybersecurity risk profile.

1.4 Scope and Applicability

1.4.1 Unless otherwise stated, the provisions of this Code shall apply to all CII.

1.4.2 Without prejudice to clause 1.4.1, ANNEX A shall also apply to any CII, which is an OT system.

1.5 Legal effect of this Code

1.5.1 Subject to sections 11(4) and 11(7) of the Act, a CIIO must comply with this Code under section 11(6) of the Act.

1.5.2 A CIIO's obligations under this Code are in addition to its other obligations under this and other Acts, as well as any relevant written directions or other codes of practice issued by the Commissioner under this Act.

1.5.3 If any provision of this Code is held to be unlawful, all other provisions shall still remain in full force and effect.

1.5.4 Where the provisions specified in this Code are not met by a CIIO, the Commissioner may issue a direction in writing under section 12(1) to the CIIO for compliance with the relevant provision.

1.6 Waiver

1.6.1 The Commissioner may waive the application to a CIIO from any specific provisions of this Code under section 11(7) of the Act.

1.6.2 A CIIO can request for waiver from specific provisions of this Code under section 11(7) of the Act 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 on a one-time basis, temporary, permanent, for a fixed period, or effective until the occurrence of a specific event.

1.7 Variation and Revocation

1.7.1 The Commissioner may, at any time, amend or revoke this Code under section 11(1)(b) of the Act.

2. COMPLIANCE REQUIREMENTS

2.1 Obligation for CIIO to meet specified requirements

2.1.1 Pursuant to section 15(1)(a) of the Act, a CIIO shall carry out an independent cybersecurity audit of the CII at least once every 2 years or at such higher frequency as may be directed by the Commissioner in the case of its CII.

2.1.2 The scope of the audit shall include:

(a) All CII owned by the CIIO; and

(b) Compliance with the Act and this Code, and any applicable codes of practice, codes of standards of performance and directions that the Commissioner may have issued.

2.1.3 A CIIO shall submit the audit report to the Commissioner within 30 days after the completion of the audit as required under section 15(2) of the Act.

2.1.4 The Commissioner may by order under section 15(4)(a) of the Act require an audit in respect of a CII to be carried out by an auditor appointed by the Commissioner, for the purpose of ascertaining the CIIO's compliance with the Act and with this or any other applicable codes of practice. The cost of such audit must be borne by the CIIO.

2.1.5 In the event an order is made by the Commissioner under section 15(4)(a) of the Act to require an audit to be carried out on a CII, its CIIO shall render full co-operation to Commissioner's appointed auditor, and provide all necessary support, access, information and assistance to the auditor conducting the audit.

2.2 Rectification plan

2.2.1 Where an audit conducted under section 15(4)(a) of the Act identifies any non-compliance by a CIIO with the requirements specified in the Act or any codes of practice or standards of performance issued under the Act, the CIIO shall unless the Commissioner indicates otherwise in writing, submit a rectification plan to the Commissioner within thirty (30) working days from the date of the CIIO receives the audit report.

2.2.2 The rectification plan shall:

(a) Detail the actions which the CIIO will take to address all non-compliance; and

(b) Set out the timeline(s) for implementing the actions stated in sub-clause (a).

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

2.2.4 Upon the approval of the rectification plan or revised rectification plan by the Commissioner, the CIIO shall implement the said plan and complete all rectification works within the timeframe(s) as specified therein to the satisfaction of the Commissioner, at the CIIO's own cost.

3. GOVERNANCE REQUIREMENTS

3.1 Authorities, Roles and Responsibilities

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 relevant officer working in or for the CIIO. This document shall:

(a) Specify the organisational structure for the management of the CII's cybersecurity;

(b) Specify what each of these officers are authorised to do and/or approve;

(c) Specify which person is ultimately responsible for ensuring the CII is compliant with the Act, any subsidiary legislation made under the Act as well as all codes of practice or standards of performance issued by the Commissioner under section 11 of the Act; 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).

3.2 Risk Management

3.2.1 The CIIO shall establish in writing, a cybersecurity risk management framework. The framework shall include:

(a) Roles and responsibilities in managing cybersecurity risk, including reporting lines and accountabilities;

(b) Identification and prioritisation of CII assets;

(c) Organisation's cybersecurity risk appetite, as well as thresholds or limits for residual risk;

(d) Cybersecurity risk assessment methodology; and

(e) Treatment and monitoring of cybersecurity risk.

3.2.2 Additionally, the CIIO shall maintain a list of all cybersecurity risk identified, by way of a risk register in respect of each CII. The CIIO shall ensure all identified cybersecurity risks listed are monitored regularly with a view to ensure that the thresholds or limits identified in clause 3.2.1(c) are not breached. The risk register shall be updated after every cybersecurity risk assessment. A risk register shall document the following:

(a) Date the risk is identified;

(b) Description of the risk;

(c) Likelihood of occurrence;

(d) Severity of the occurrence;

(e) Risk treatment;

(f) Risk owner;

(g) Status of risk treatment; and

(h) Residual risk.

3.3 Policies, Standards and Guidelines

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

(a) Aligned with this Code, sector regulatory cybersecurity requirements, and applicable sectoral or national cybersecurity policies, standards and directions; 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 and guidelines against the current CII cyber operating environment and cybersecurity threat landscape at least once a year, starting from the date of the last review or the effective date of each policy, standard or guideline.

3.4 Security By Design

3.4.1 The CIIO shall adopt Security By Design Framework established by CSA[1] to the extent that it applies to the CII's system development lifecycle. Where there are parts of the Framework which do not apply to the CII's system development lifecycle, the CIIO shall explain how and why these parts are not applicable as such.

4. IDENTIFICATION REQUIREMENTS

4.1 Asset Management

4.1.1 The CIIO shall, for its CII, identify all CII assets and maintain an inventory of CII assets identified. For each CII asset, this inventory shall include the following information:

(a) Name/Description of each CII asset;

(b) Critical functions of each CII asset;

(c) Owner and/or operator of each CII asset;

[1] CSA's SBD Framework can be found at https://www.csa.gov.sg/legislation/cybersecurity-act

(d) Physical location of each CII asset; and

(e) CII asset dependencies on internal and/or external systems/networks.

4.1.2 The CIIO shall also identify the CII network perimeter and all external computers and computer systems which it interfaces with.

4.1.3 The CIIO shall update the inventory as and when there are any changes to any CII asset.

4.1.4 Pursuant to section 15(1)(b) of the Act, at least once a year, starting from the date of the notice issued under section 7 the Act, CIIO must conduct a cybersecurity risk assessment of the CII, that includes all the items listed in the CII inventory in clause 4.1.1.

5. PROTECTION REQUIREMENTS

5.1 Access Control

5.1.1 The CIIO shall ensure that access to the CII is restricted to

(a) Authorised personnel and activities; and

(b) Authorised process interfaces and devices.

5.1.2 With respect to the CIIO's obligation under clause 5.1.1, the CIIO shall for each authorised personnel, activity and process put in place authentication techniques commensurate with the cybersecurity risk profile for each mode of access into the CII.

5.1.3 The CIIO shall maintain logs of all access into a CII and of all attempts to access the CII, and review these logs for anomalous activities on a regular basis. The regularity with which these logs are to be reviewed should commensurate with the frequency or regularity of such access activities.

5.1.4 The CIIO shall ensure that all vendors' access to a CII's interfaces (e.g. USB, Serial port) and vendor service applications are:

(a) Made only under the supervision of the CIIO; and

(b) Performed on-site where possible.

5.2 System Hardening

5.2.1 The CIIO shall establish security baseline configuration standards for all operating systems, applications and network devices of a CII that commensurate with the cybersecurity risk profile of the CII.

5.2.2 The security baseline configuration standards shall address the following security principles:

(a) Least access privilege and separation of duties;

(b) Enforcement of password complexities and policies;

(c) Removal of unused accounts;

(d) Removal of unnecessary services and applications, e.g. removal of compilers and vendor support applications;

(e) Closure of unused network port;

(f) Protection against malwares; and

(g) Timely update of software and security patches that are approved by system vendors.

5.2.3 The CIIO shall ensure that the respective security baseline configuration standards are applied before using the CII where there are any new CII assets connected to the CII, or where there are any changes or enhancements made to the CII.

5.2.4 The CIIO shall review each security baseline configuration standard of its CII once every 12 months starting from the time of the establishment of the standard, or, where an existing standard was already established prior to the designation of the CII, then once every 12 months from the time of designation of the CII, to ensure that these standards remain effective against cybersecurity threats.

5.2.5 The CIIO shall establish a change management process to authorise and validate all system changes to a CII.

5.3 Remote Connection

5.3.1 The CIIO shall ensure that all remote connections to the CII have effective cybersecurity measures to prevent and detect unauthorised access.

5.3.2 For remote connection to CII, the CIIO shall adopt the following practices:

(a) Where functionally possible, enable the connection to or from a remote site only when required;

(b) Implement strong authentication techniques, transmission security, and message integrity, where available;

(c) Implement encryption for all network connections;

(d) Disallow remote connection from issuing system commands that would impact the CII operation, unless explicitly authorised due to business need; and

(e) Limit the data flow to only the minimum function required of the connection.

5.4 Removable Storage Media

5.4.1 The CIIO shall ensure that strict control is exercised over the connection of removable storage media and portable computing devices (e.g. laptop) to a CII by adopting the following measures with respect to the CII:

(a) Where the function is available, disable all external connection ports (e.g. USB ports) supporting removable storage media and portable computing devices, and enable only when required;

(b) Use only storage media authorised under clause 5.1.1(b); and

(c) Check that all removable storage media and portable computing devices are free of malware prior to connecting to the CII.

5.4.2 All CII's sensitive information[2] on removable storage media shall be encrypted.

5.5 Vulnerability Assessment and Penetration Testing

5.5.1 The CIIO shall conduct a vulnerability assessment of its CII to identify security and control weaknesses:

(a) for a CII which is an IT system - within 12 months from the time the CII is designated under the Act and, subsequently, at least once every 12 months from the time of the previous vulnerability assessment, or

(b) for a CII which is an OT system - within 12 months from the time the CII is designated under the Act and, subsequently, at least once every 24 months from the time of the previous vulnerability assessment.

5.5.2 The CIIO shall ensure that the scope of each vulnerability assessment includes:

(a) A Host Security Assessment;

(b) A Network Security Assessment; and

(c) An Architecture Security Review.

[2] Examples of sensitive information include production data and system configuration information.

5.5.3 The CIIO shall also conduct a vulnerability assessment on its CII to identify security and control weaknesses prior to commissioning any new systems connected to the CII or implementing any major system changes to the CII. Major system changes include adding on application modules, system upgrades and technology refresh.

5.5.4 The CIIO shall conduct a penetration test on a CII which is an IT system within 12 months upon CII designation under the Act and, subsequently, at least once every 12 months from the time of the previous penetration test.

5.5.5 The CIIO shall ensure that the scope of a penetration test includes penetrating tests of the CII's hosts, networks and applications.

5.5.6 The CIIO shall also conduct one or more penetration tests where necessary to validate the cybersecurity posture of the CII prior to commissioning of new system or major system changes, for example add-on modules, system upgrade and technology refresh.

5.5.7 Where the CII is an OT system, while the requirement to conduct penetration tests is not mandatory, CIIOs should consider conducting such tests where they are able to do so.

5.5.8 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-recognised accreditations and certifications respectively, for example CREST[3] or equivalent accreditations and certifications:

(a) Penetration testers performing the penetration tests must have industry-recognised penetration testing certification to demonstrate assurance of their knowledge and practical skills.

(b) Service providers must have industry-recognised 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.

5.5.9 The CIIO shall ensure that all penetration tests by third-party penetration testing service providers are conducted under the supervision of the CIIO.

5.5.10 The CIIO shall establish a process to track and address vulnerabilities identified in a vulnerability assessment and in a penetration test, and validate that all identified vulnerabilities have been adequately addressed.

5.5.11 The CIIO shall, if requested by the Commissioner, submit a copy of the report of any completed vulnerability assessments or penetration tests to the Commissioner within 30 working days of receiving the request.

[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/

6. MONITORING AND DETECTION REQUIREMENTS

6.1 Detection

6.1.1 The CIIO shall establish mechanisms and processes for the purpose of:

(a) detecting all cybersecurity events in respect of its CII;

(b) collating and analysing the cybersecurity events detected; and

(c) identifying whether there are any cybersecurity threats or cybersecurity incidents in respect of the CII.

6.1.2 The CIIO shall conduct a review of the mechanisms and processes at least once every 24 months from the time it establishes the mechanisms and processes, or, where there are already existing mechanisms and processes established prior to the designation of the CII, at least once every 24 months from the time of the designation of the CII, to ensure that the mechanisms and processes are still effective for their purposes under clause 6.1.1.

7. CYBERSECURITY INCIDENT RESPONSE REQUIREMENTS

7.1 Cybersecurity Incident Response Plan

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 Cyber 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 Act and any subsidiary legislation made thereunder, as well as with its reporting obligations under legislation and regulatory requirements applicable to the CII;

(c) Thresholds and procedures to activate the incident response and the CIRT.

(d) Procedures for the containment of the impact of cybersecurity incidents, the activation of the recovery process;

(e) Procedures to investigate into the cause and impact of the incident;

(f) Procedures for the preservation of evidence prior to the initiation of recovery process, including but not limited to log acquisition, seizure of evidence, acquisition computers or other equipment, placement of additional passive monitoring equipment to support investigation;

(g) Engagement protocols with external parties, including their contact details, for example vendors for forensic/recovery services and law enforcement for prosecution; and

(h) After-action review process to identify and recommend mitigating actions to prevent a recurrence.

7.1.2 The CIIO shall ensure that the cybersecurity incident response plan is effectively communicated to all relevant personnel supporting the CII.

7.1.3 The CIIO shall review their cybersecurity incident response plan at least once every 24 months starting from the establishment of the plan, or, where there is already an existing plan established prior to the designation of the CII, at least once every 24 months from the time of the designation of the CII.

7.1.4 The CIIO shall also review their cybersecurity incident response plan when there are material changes in the CII cyber operating environment or incident response requirements.

7.2 Crisis Communication Plan

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 plans of action;

(c) Identifies target audiences and stakeholders for each type of cybersecurity incident scenario;

(d) Identifies primary spokesperson(s) and technical experts who will represent the organisation when addressing the media; and

(e) Identifies appropriate outreach platforms/channels (e.g. traditional media and social media) for dissemination of information;

7.2.3 The CIIO shall ensure that the Crisis Communication Plan includes coordination between all affected parties to ensure coordinated and consistent responses during a crisis.

7.2.4 The CIIO shall conduct an exercise[4] of the Crisis Communication Plan once every 12 months starting from the establishment of this plan, or, where there is already an existing plan established prior to the designation of the CII, once every 12 months from the time of the designation of the CII, to ensure that the CIIO is able to communicate and disseminate information timely and effectively during a crisis due to cybersecurity incident.

8. CYBERSECURITY AWARENESS & INFORMATION SHARING REQUIREMENTS

8.1 Cybersecurity Awareness

8.1.1 The CIIO shall establish a cybersecurity awareness programme to educate and build cybersecurity awareness for its employees, contractors and third-party vendors who have access to the CII.

8.1.2 The cybersecurity awareness programme shall minimally include the following:

(a) Awareness activities for all categories of personnel, including:

i. New employees;

ii. Users and management;

iii. CII support staff, e.g. IT and OT operators; and

iv. Vendors, contractors and service providers;

(b) Dissemination of respective groups' and individuals' responsibilities for cybersecurity of CII;

(c) Awareness of cybersecurity laws, regulations, codes of practices policies, standards and procedures pertaining to the usage, deployment and access to CII; and

(d) Regular and timely communication covering general cybersecurity awareness messages and prevailing cybersecurity threats, impacts and mitigations.

8.1.3 The CIIO shall review the cybersecurity awareness programme once every 12 months starting from the establishment of the programme, or, where there is already an existing programme established prior to the designation of the CII, once every 12 months from the time of the designation of the CII, to ensure that the contents of the programme remain current and relevant.

[4] Crisis Communication Plan may be exercised as part of a cybersecurity exercise.

8.2 Information Sharing

8.2.1 The CIIO shall establish procedures to share, to the extent it is able to, information on any cybersecurity incidents and cybersecurity threats in respect of its CII and any mitigation measures taken in response to such incidents or threats, with persons affected or potentially affected by the cybersecurity incident or cybersecurity threat (such as users of the CII, contractors providing services to the CII and owners of computers or computer systems which are required to be connected to the CII) so that they can take the necessary protection measures.

9. CYBERSECURITY EXERCISE REQUIREMENTS

9.1 Pursuant to section 16(2) of the Act, a CIIO must participate in a cybersecurity exercise if directed in writing to do so by the Commissioner. Such cybersecurity exercises may be conducted either at the national level or the sectoral level. The CIIO shall ensure the relevant personnel identified in the Cybersecurity Incident Response Plan established under clause 7 participate in all such cybersecurity exercises.

9.2 A CIIO shall comply with any request by the Commissioner to provide information relating to its CII for the purpose of planning and conducting of a cybersecurity exercise. Information which may be requested by the Commissioner under this Clause includes cybersecurity incident response plan and crisis communication plan established under Clause 7 and standard operating procedures related to the operations of the CII.

10. RESILIENCY REQUIREMENTS

10.1 The CIIO shall establish a Business Continuity Plan ("BCP") and a Disaster Recovery Plan ("DRP") to ensure that its CII can continue to deliver essential services in the event of disruptions due to a cybersecurity incident.

10.2 The CIIO shall ensure that BCP and DRP exercises[5] are conducted at least once yearly to assess the effectiveness of the BCP and DRP of its CII against cybersecurity threats and cybersecurity incidents.

11. VENDOR MANAGEMENT REQUIREMENTS

11.1 Vendor Management

11.1.1 The CIIO shall put in place cybersecurity requirements for mitigating the risks associated with vendor's access, process, storage, communication, and operation of CII in the service level agreement or terms of contract with the vendor. The requirements should take into consideration the following:

[5] Can be conducted as part of the organisation's BCP or DRP exercises

(a) Type of vendor access to CII assets based on the organisation's business needs and cybersecurity risk profile;

(b) Obligations of vendor to protect the CII against cybersecurity threats;

(c) Risks associated with service and product supply chains; and

(d) Rights of the CIIOs to commission audit of vendor's cybersecurity.

11.1.2 The CIIO shall establish processes for validating vendor's compliance with cybersecurity requirements in the terms of contract, for example third party review, and product validation.

11.2 Outsourcing

11.2.1 The CIIO shall be responsible and accountable for the maintenance of the/ cybersecurity of its CII, even if it outsources any of its operations in respect of its CII.

11.2.2 The CIIO shall ensure that it is able to renegotiate the terms of its outsourcing contracts in the event of new legal or regulatory requirements.

12. REFERENCES

1. Cybersecurity Agency of Singapore, "Security By Design Framework", 2017

2. Cybersecurity Agency of Singapore, "Industrial Control Systems Cybersecurity Guidelines", 2018

3. ISO/IEC 27001, "Information technology – Security techniques – Information security management systems – Requirements", 2013

4. ISO/IEC 27002, "Information technology – Security techniques – Code of practice for information security controls", 2013

5. ISO/IEC 27005, "Information technology – Security techniques – Information security risk management", 2011

6. ISO/IEC 27031, "Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity", 2011

7. IEC 62443-3, "Industrial communication networks – Network and system security – Part3-3: System security requirements and security levels", 2013

8. “Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2”, NIST, 2015

9. “Security and Privacy Controls for Federal Information Systems and Organisations, NIST Special Publication 800-53 Revision 4”, NIST, 2013

ANNEX A: OT SYSTEMS REQUIREMENTS

OT SYSTEMS REQUIREMENTS

The section, OT Systems Requirements, shall apply to a CII, which is an OT system.

A.1 Network Segmentation

A.1.1 The CIIO shall segment the CII network architecture into network zones.

A.1.2 For each CII network, the CIIO shall:

(a) Limit network communications between the different network zones to only data required for operating the CII; and

(b) Monitor the network communication between the different network zones for anomalous network traffic.

A.2 Access Control

A.2.1 The CIIO shall establish role-based access control over the CII.

A.2.2 The CIIO shall monitor and review such role-based access control at least once every 12 months from the time of the designation of the CII or when there are changes to the access required by the roles, to ensure the correctness of the role-based access control.

A.2.3 Where shared user accounts are required for operating the CII, the CIIO shall establish procedures to monitor and review the usage of such shared user accounts on a regular basis to ensure the prevention of unauthorised access to the shared user accounts. The regularity with which these shared user accounts are to be reviewed should commensurate with the frequency or regularity of such access activities.

A.2.4 The CIIO shall maintain user activities logs within the CII, and review these activities logs for anomalous activities on a regular basis. The regularity with which these activities are to be reviewed should commensurate with the frequency or regularity of such access activities.

A.2.5 The CIIO shall implement multi-factor authentication for privilege accounts on CII assets that support this function.

A.3 Network Security

A.3.1 The CIIO shall establish a process to identify and implement approved network protocols on the CII network. Changes to existing baseline and introduction of new network protocols shall be managed through the CIIO's change management process.

A.3.2 The CIIO shall implement the appropriate host-based security on supported workstations and servers operating within the CII.

A.4 Application Security

A.4.1 The CIIO shall establish a list of approved applications for use in the CII. Such list shall only contain applications required for the operation and the cybersecurity of the CII. The list of approved applications shall be reviewed once every 12 months from the designation of the CII or when there are any changes to the list of approved applications, to ensure that only applications required for the operation and the cybersecurity of the CII are allowed to be installed.

A.4.2 The CIIO shall use these approved applications only for the purpose of the operation and the cybersecurity of the CII.

A.4.3 The CIIO shall establish processes to verify that applications and its patches are obtained through legitimate sources.

A.4.4 Where compilers and debuggers are required within the CII, the CIIO shall further restrict the use of these tools to authorised workstations on a need-to-basis.

A.5 Wireless Communications

A.5.1 The CIIO shall implement multi-factor authentication for user access through wireless LAN within the CII.

A.6 Patch Management

A.6.1 The CIIO shall establish a patch management process for the CII. The CIIO shall adopt the following patch management strategy:

(a) Aligning patch management with other processes including operations, vulnerability management, change management, configuration management, backup, testing, incident response, and disaster recovery;

(b) Prioritising the patching of CII assets that have higher vulnerability exposure, impact or ease of exploitation;

(c) Applying patches in a systematic and timely approach to reduce system vulnerability exposure while ensuring ongoing operations to the CII; and

(d) If the measures set out at (a) to (c) above are not technically possible, putting in place any equivalent measures.

A.6.2 The CIIO shall test all patches offline in a test environment that contains a similar environment to the CII to determine whether such patches do not have unintended consequences of interfering with the functions or cybersecurity of the CII.

A.7 Removable Storage Media

A.7.1 The CIIO shall use only authorised workstations connected to the CII to transfer data between removable storage media and the CII.

A.8 Monitoring and Detection

A.8.1 The CIIO shall use a consistent time source for all event logs within the CII.

A.8.2 The CIIO shall establish a baseline of expected network traffic and process functionality for normal operations of the CII so that anomalous traffic or user actions that may indicate cybersecurity events can be isolated.

A.8.3 The CIIO shall establish continuous monitoring of the CII cyber operating environment to control visibility to cybersecurity threats and ensure that the security controls implemented are working as intended.