Office of the Commissioner of Critical Infrastructure (Computer-system Security)
Security Bureau
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

Code of Practice

Pursuant to the Protection of Critical Infrastructures (Computer Systems) Ordinance

1 January 2026

Version 1.0

Office of the Commissioner of Critical Infrastructure (Computer-system Security)
Security Bureau
The Government of the Hong Kong Special Administrative Region of
the People's Republic of China

Amendment History

Change Number	Revision Description	Revision Number	Date
1	First release	1.0	1 January 2026

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose and Scope

1.1.1 This Code of Practice ("this Code") is published by the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") in consultation with designated authorities pursuant to section 8 of the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance").

1.1.2 This Code provides practical guidance on how a Critical Infrastructure ("CI") operator complies with category 1 obligations, category 2 obligations and category 3 obligations.

1.1.3 This Code could also be adopted by designated authorities in respect of category 1 obligations and category 2 obligations of CI operators under their respective purviews. If a designated authority issues any sectoral Code of Practice ("Sectoral Code") in respect of category 1 obligations and category 2 obligations, the concerned CI operators should refer to that Sectoral Code.

1.1.4 This Code is not subsidiary legislation, nor would failure to comply with the provisions of this Code in itself constitute an offence. However, the Commissioner may issue written directions to require a CI operator to take appropriate actions in relation to the compliance with category 1 obligations, category 2 obligations and category 3 obligations if there has been non-compliance or defective compliance with such obligations, which may be considered with reference to this Code. Failure to comply with such directions would be an offence.

1.1.5 A CI operator should provide information, which is accessible in or from Hong Kong, to regulating authorities upon request in relation to the compliance with category 1 obligations, category 2 obligations and category 3 obligations.

1.1.6 The documents to be submitted by a CI operator under this Ordinance should be submitted through secured channels as advised by regulating authorities. Annex A to F of this Code provide samples of the specified forms.

1.1.7 This Code sets the baseline requirements for protecting critical computer systems ("CCSs") of CI operators, and does not target personal data nor trade secrets of CI operators. A CI operator should apply enhanced security measures, appropriate to its circumstances and commensurate with the computer-system security risk of its CCSs.

1.1.8 The Commissioner may, in consultation with designated authorities and industry stakeholders, from time to time review and amend the requirements stipulated in this Code according to the latest technological development and industry best practices.

1.1.9 For the sake of clarity, any reference to the Commissioner in relation to the designation of a CI operator and its CCSs, category 1 obligations and category 2 obligations in the following sections of this Code should be construed as a reference to the designated authorities as relevant to the context and to the extent as far as applicable, unless otherwise specified.

2. DEFINITIONS AND CONVENTIONS

2.1 Definitions

2.1.1 The terms defined in the Ordinance are applicable to this Code.

2.1.2 The terms used in this Code are defined as follows –

accessible from Hong Kong	means a computer system which can be accessed from an entry point in Hong Kong regardless of the physical location of that system;
accessible in Hong Kong	means a computer system which is physically reachable within Hong Kong;
availability	means a computer system is accessible and usable upon demand by authorized persons;
business continuity management plan	means a documented procedure on sustaining the essential services provided by an organization during disruption;
Code	means this Code of Practice for the Protection of Critical Infrastructures (Computer Systems) Ordinance;
Commissioner	means the Commissioner of Critical Infrastructure (Computer-system Security) appointed under section 3(1) of the Ordinance;
computer-system security risk	means the risk that a vulnerability in a computer system may be exploited by a malicious actor thus resulting in a computer-system security incident. It refers to the likelihood of the risk event occurring and the resulting impact;
confidentiality	means only authorized persons are allowed to know or gain access to the information stored or processed by computer systems in any aspects;
designated authority	means an authority specified in column 2 of Part 2 of Schedule 2 of the Ordinance;
disaster recovery plan	means a documented procedure to facilitate recovery of computer systems when a disaster occurs to those systems and / or the primary site, whereby there is a severe disruption to any of those systems or major loss of data;
integrity	means only authorized persons with authorized reasons are allowed to make changes to the computer systems and the information stored or processed by such computer systems in any aspects;

malware	means software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to computer systems;
regulating authority	means the Commissioner or a designated authority;
removable storage media	means portable electronic storage media such as magnetic, optical, or flash memory devices, which can be inserted into and removed from a computing device. Examples include external hard disks or solid-state drives, floppy disks, zip drives, optical disks, tapes, memory cards, flash drives, and USB storage devices;
sensitive digital data	means any electronically stored, processed, or transmitted information which unauthorized access, disclosure, alteration, or loss could cause significant harm to individuals, organizations or society;
supplier	means an individual or an organization that enters into an agreement with the acquirer for the supply of a product or service. A supplier can be a vendor, contractor, seller, producer (collectively known as "external service provider"), or a party that is in the same organization;
vulnerability	means a weakness in the design, implementation, or operation of an asset or the internal controls of a process, which may expose the computer system to computer-system security risks.

3. DESIGNATION OF CRITICAL COMPUTER SYSTEMS

3.1 Designating critical computer systems

3.1.1 This chapter serves as a reference for CI operators and advisory agencies to assist CI operators to identify their CCSs for fulfilment of the Ordinance. The regulating authority will from time to time review the list of CCSs in consultation with CI operators.

3.1.2 This chapter should be read in conjunction with section 13 of the Ordinance when determining whether a computer system should be designated as a CCS.

3.1.3 A computer system will more likely be designated as a CCS if it meets any of the following criteria:

(a) The system plays a material role in respect of the core function of the CI concerned. Whether a system is isolated from the Internet is irrelevant.

(b) The disruption or destruction of the system would cause severe impact to the core function of the CI. Whether the core function of the CI could be switched to manual processing as a failover solution is irrelevant.

(c) The system stores or processes sensitive digital data that are used directly in the provision of essential services, e.g. full set of personal data (such as name, identity document number, phone number and residential address) used in banking services or medical services. Whether there is a sophisticated mechanism on data protection or recovery is irrelevant.

(d) The system is highly related to other CI operator(s). Regulating authorities will provide guidance as and when necessary. Examples of these computer systems include centralised processing or data exchange systems within the same sector or multiple-sectors.

(e) The system is highly related to other CCSs of the CI operator concerned in the provision of essential services. Examples of these systems include, but are not limited to:

(i) Systems directly protecting the security of the CCSs described in paragraph 3.1.3(a)-(d) above (e.g. security gateway or firewalls isolating the internal network from untrusted environment); and

(ii) Systems directly strengthening the resilience of the CCSs described in paragraph 3.1.3(a)-(d) above (e.g. backup facilities in high-availability systems).

3.1.4 Industrial control systems, such as supervisory control and data acquisition ("SCADA") systems, distributed control systems ("DCS"), or Programmable Logic Controllers ("PLC"), which are collectively known as Operational Technology ("OT"), are also considered as computer systems for the meaning provided in the Ordinance.

3.1.5 The underlying IT infrastructures of a CI operator's computer system, including network components, operating platforms, middleware, Internet-of-Things devices and uninterruptible power supply systems may also be regarded as components of the computer system.

4. INFORMATION REQUIRED FOR DESIGNATION

4.1 Requiring information for designating critical computer systems

4.1.1 Examples of information required by the regulating authority for ascertaining whether to designate a computer system as a CCS include, but are not limited to:

(a) Facts and functions about the computer system, including upstream and downstream dependencies;

(b) Architecture of the computer system;

(c) Nature and volume of sensitive digital data processed by the computer system;

(d) Network diagram of the computer system providing or supporting the core functions of the CI;

(e) Manufacturers and models of computer hardware and software providing or supporting the core functions of the CI;

(f) External information technology or telecommunication services subscribed for providing or supporting the core functions of the CI;

(g) Resilient setup of the primary computer systems providing or supporting the core functions of the CI; and

(h) Documentation illustrating the design and operations of the computer system, such as diagrams or system function descriptions.

5. OBLIGATIONS OF CI OPERATORS – DIVISION 1

5.1 Obligation to maintain office in Hong Kong

5.1.1 For the purpose of section 19(1) and (3) of the Ordinance, an office in Hong Kong should serve not only as the location to which notices and other documents may be given or sent, but also as the location where a CI operator's employees or representatives conduct business activities, such as managing daily operations, making business decisions, interacting with stakeholders, or maintaining business records. A template form is set out in Annex A for notifying the office address and the relevant change of office address.

5.2 Obligation to notify operator changes

5.2.1 For the purpose of section 20(1) of the Ordinance, examples of operator changes include:

(a) The daily operation, management or maintenance of a CI is changed from the existing CI operator to another;

(b) The existing CI operator ceases to provide daily operation, management or maintenance of a CI; or

(c) Merger, acquisition, and other scenarios that result in the existing CI operator ceasing to exist.

A template form is set out in Annex B for notifying CI operator changes.

5.3 Obligation to set up and maintain computer-system security management unit

5.3.1 For the purpose of section 21(1) of the Ordinance, a computer-system security management unit need not be based in Hong Kong.

5.3.2 For the purpose of section 21(4) of the Ordinance, the employee supervising the computer-system security management unit need not be based in Hong Kong. Besides, having adequate professional knowledge in relation to computer-system security generally means possessing appropriate professional qualifications (e.g. Certified Information Security Professional ("CISP"), Certified Information Systems Auditor ("CISA"), Certified Information Security Manager ("CISM"), Certified Information Systems Security Professional ("CISSP"), etc.) and professional experience in computer-system security commensurate with the risk of their CCSs to discharge the duties effectively. A template form is set out in Annex C for notifying the appointment of the employee supervising the computer-system security management unit.

5.3.3 For the purpose of section 21(6) of the Ordinance, while the date of the change pertains to the date of assumption of duty, a CI operator is encouraged to proactively inform the regulating authority as soon as the contract of employment is signed using the template form set out in Annex C.

6. OBLIGATIONS OF CI OPERATORS – DIVISION 2

6.1 Obligation to notify material changes to certain computer systems

6.1.1 For the purpose of section 22(1) of the Ordinance, the date on which the event occurs generally refers to the moment when a change is deployed to production environments. If the deployment is conducted in phases, the date on which the event occurs should be applicable to each individual phase of the change deployment. A CI operator may opt to notify the regulating authority of all subsequent changes collectively at the initial phase of the change deployment.

6.1.2 For the purpose of section 22(3) of the Ordinance, the CI operator should report any material change, which generally refers to a change that would reasonably be expected to have **a significant effect on the computer-system security risk of a CCS or risk to the CI's core function**. Material changes in a CCS (non-exhaustive) may occur in the events below:

(a) Platform migration;

(b) Server virtualisation;

(c) Major version upgrade of a core component (e.g. database);

(d) Changes to the computing platform or hardware;

(e) Application re-design;

(f) Significant code changes;

(g) Changes to the underlying infrastructure that supports the CCS;

(h) Integration with or change in interdependency on external systems or networks;

(i) Changes of mission or major functions that alters the system's operational scope, intended purpose or requirements in security, resources or functions;

(j) Any system modification that fundamentally alters the characteristics or nature of the CCS; or

(k) Substantial changes in CCS components maintained by cloud service suppliers that the CI operator becomes aware of.

A template form is set out in Annex D for notifying material changes.

6.2 Obligation to submit and implement computer-system security management plan

6.2.1 A computer-system security management plan should cover all of the matters necessary to fulfil the statutory obligation to protect the computer-system security of the CCSs in accordance with Schedule 3 of the Ordinance. In relation to matters specified in Schedule 3 Part 1 of the Ordinance, a CI operator should fulfil the requirements stipulated in sections 6.2.5 – 6.2.27, 6.3, 6.4 and 6.5 of this Code, which provide relevant practical guidance.

6.2.2 The CI operator should ensure that the computer-system security management plan and any subsequent changes (other than contact point or editorial update) submitted to the regulating authority are endorsed by the Board of Directors ("the Board"), or a functional sub-committee delegated by the Board, or the senior management overseeing the operation of the concerned CI (e.g. Chief Executive Officer, Chief Operating Officer, or their equivalent). The plan should be reviewed upon any material changes to CCSs, and in any event at least once every two years, to ensure its effectiveness and validity.

6.2.3 In the event that the computer-system security management plan consists of a collection of policies, standards and guidelines, the CI operator should provide a clear cross-reference that maps each applicable requirement between relevant sections of the plan and sections 6.2.5 – 6.2.27, 6.3, 6.4 and 6.5 of this Code.

6.2.4 If the CI operator cannot fulfil any of the requirements stipulated in sections 6.2.5 – 6.2.27, 6.3, 6.4 and 6.5, the CI operator should implement alternative security controls that achieve comparable results. The alternative controls should be documented in the computer-system security management plan, with a detailed description showing how they effectively mitigate the relevant risks.

6.2.5 Computer-System Security Management Unit

(a) The CI operator should establish a management structure for the implementation, operation and management of computer-system security of CCSs.

(b) The organizational structure, line of authority, roles and responsibilities of each relevant personnel should be clearly set out and documented.

6.2.6 Policies, Standards and Guidelines

(a) The CI operator should define and enforce computer-system security policies, standards and guidelines that provide management direction and support for protecting CCSs in accordance with business needs and security requirements.

(b) When drafting its policies, standards and guidelines, the CI operator should consider its own requirements on security, this Code, the relevant requirements set out by statutory bodies for individual sectors, and applicable national and international computer-system security standards.

(c) The CI operators should establish a mechanism to deliver the policies, standards and guidelines, ensuring they are easily accessible to all personnel involved in CCS operation.

6.2.7 Computer-System Security Risk Management Approach

(a) The CI operator should formulate a risk management approach that outlines how computer-system security risks related to the CI operator and its CCSs are identified, assessed, mitigated, and monitored. The approach should provide a systematic and structured way to manage these risks.

(b) The CI operator should refer to nationally or internationally recognised methodologies and standards for computer-system security risk management, such as GB/T 31722, ISO/IEC 27005, or IEC 62443-3-2, in formulating the computer-system security risk management approach. The CI operator may also refer to Practice Guide for IT Security Risk Management compiled by the Digital Policy Office ("DPO") in this process.

6.2.8 Security by Design

(a) The CI operator should adopt the "security by design" principle as far as practicable to ensure that security is an integral part of CCSs throughout their entire life cycle, from initiation to design, implementation, deployment, operation and eventual disposal. Where a CCS is constrained by legacy architecture or off-the-shelf nature that makes full adoption of the "security by design" principle infeasible, the CI operator should apply such principle upon major upgrade or enhancement of the CCS. The CI operator may refer to Practice Guide for Security by Design compiled by the DPO in this process.

6.2.9 Asset Management

(a) The CI operator should define and document the identification approach, selection criteria, and the regular review mechanism for CCSs.

(b) The CI operator should ensure that up-to-date inventories (including their descriptions, major functions, physical / logical locations, and owner or key personnel) of CCSs and the associated assets, including hardware assets (name, manufacturer, model, firmware version, etc.), software assets (name, publisher, version, etc.), applications, valid warranties, service agreements and legal / contractual documents, are properly owned, kept, maintained, and restricted to access on a need-to-know basis.

(c) The CI operator should ensure the accuracy of the inventories of CCSs and the associated assets by conducting regular reviews against the inventories or implementing automatic inventory update mechanisms.

6.2.10 Access Control and Account Management

(a) The CI operator should prevent unauthorized access and ensure that only authorized personnel can access CCSs.

(b) The CI operator should enforce the least privilege principle when assigning resources and privileges of CCSs to users.

(c) The CI operator should define and document procedures for approving, granting and managing user access to CCSs (including suppliers, if any). The procedures should include, but not be limited to, user registration, user de-registration, password delivery and password reset.

(d) User privileges and data access rights should be clearly defined and reviewed at least once per year. Records for access rights approval and review should be maintained.

(e) All user privileges and data access rights should be revoked when no longer required.

(f) Each user identity (user-ID) should uniquely identify only one user. Shared or group user-IDs should not be permitted unless strictly necessary.

(g) Authorization and authentication measures commensurate with the computer-system security risk of the CCS should be set up for each access. Multi-factor authentication should be adopted where appropriate.

(h) A system use notification message (in the form of a system notification or physical notice) that provides appropriate security notices (e.g. system usage may be recorded and monitored, unauthorized use is prohibited) should be displayed to the users of CCSs before they are authenticated to use the CCSs.

6.2.11 Privileged Access Management

(a) The CI operator should ensure the privileged access rights of CCSs are provided only with authorization.

(b) The CI operator should grant privileged access rights to a user-ID that is separate from the one used for regular business activities. Alternatively, the CI operator may provide just-in-time privileged access for temporary privilege elevation, subject to a formal approval and control procedure.

(c) The CI operator should ensure that personnel have access only to the specific administrative capabilities required, thereby enforcing the principle of least privilege for administrative accounts and reducing the impact if privileged accounts are compromised.

(d) The CI operator should allow only authorized devices equipped with security controls to access privileged accounts to ensure that privileged operations are properly managed and restricted to authorized personnel.

6.2.12 Cryptography

(a) The CI operator should ensure proper and effective use of cryptography to protect the computer-system security of CCSs. The CI operator may also refer to section 6.5.4 for the alternative security controls for an OT system.

(b) The CI operator should ensure the cryptographic keys are properly managed throughout their life cycle, including generation, storage, archive, retrieval, distribution, retirement and destruction.

(c) Keys used to process sensitive digital data should be stored and distributed separately from the corresponding encrypted information.

(d) The CI operator should refer to the latest national or international computer-system security standards on the use of cryptographic algorithms and methods.

6.2.13 Password Management

(a) The CI operator should define and implement password policies for all CCS accounts (including any supplier accounts). The password policies should specify a minimum password length, complexity requirements that include alphanumeric and special characters, a maximum password lifetime, a maximum number of consecutive failed log-on attempts, and restriction on re-using previous passwords. The CI operator may also refer to section 6.5.5 for the alternative security controls for an OT system.

(b) All default passwords provided by suppliers should be changed before any computer system is put into operation.

(c) All passwords should be promptly changed if they have been or are suspected of being compromised, or after the passwords have been used by suppliers for maintenance and support.

6.2.14 Physical Security

(a) The CI operator should prevent unauthorized physical access and interference to facilities housing CCSs.

(b) Data centres, computer rooms, and premises housing CCSs should implement physical security measures to protect against unauthorized physical access.

(c) The CI operator should protect the power and communication cables of CCSs against damage and interception.

(d) The CI operator should label the power and communication cables of CCSs to facilitate physical identification and inspection.

(e) The CI operator should deploy multiple surveillance systems, such as closed-circuit televisions, detectors, intruder alarms, or security guards, to continuously detect and alert unauthorized access to or suspicious behaviours in premises housing CCSs. The CI operator should also protect the deployed surveillance systems from unauthorized access or interruption.

(f) A list of personnel authorized to access data centres, computer rooms, and premises supporting CCS operations, where computer equipment and data are located or stored, should be kept up-to-date and reviewed periodically. All access keys, cards, passwords, etc., for entry to these areas should be physically secured and subject to well-defined and strictly enforced security procedures.

(g) All visitors to data centres, computer rooms, and premises housing CCSs should be monitored at all times by authorized personnel. A visitor access record should be kept and properly maintained for audit purpose and investigating computer-system security incidents.

6.2.15 Configuration Management and System Hardening

(a) The CI operator should prevent any unauthorized configurations of CCSs and ensure that the CCSs conform to the required security configurations.

(b) The CI operator should develop, maintain and review the baseline configuration of the CCSs regularly and also whenever material changes to the CCSs occur.

(c) Both the least functionality principle and least privilege principle should be adopted when performing system hardening.

6.2.16 Change Management

(a) Changes to CCSs should be subject to strict change management controls, which include but are not limited to change planning, impact assessment, change authorization, communication of changes to relevant parties, change testing, change implementation, fall-back procedures, and maintenance of change records.

(b) The CI operator should have a non-production environment for development and testing (e.g. testing system changes and acceptance testing). The CI operator may also refer to section 6.5.6 for the alternative security controls for an OT system.

6.2.17 Patch Management

(a) The CI operator should protect their CCSs from known vulnerabilities by timely applying the latest security patches recommended by the product vendors or implementing other compensating security measures. The CI operator should adopt a risk-based approach to determine a suitable patch management strategy for their CCSs. Risks associated with the vulnerability exposure should be duly considered when deciding the patching schedule and priority.

(b) The CI operator should establish a robust patch management process for CCSs. The patch management lifecycle should include patch acquisition, testing, risk assessment, deployment and compliance.

(c) Before security patches are applied, proper risk evaluation and testing should be conducted to minimise undesirable effects on the CCSs. If patch testing for an OT system is not feasible, the CI operator may refer to section 6.5.6 for the alternative security controls. The result of risk evaluation and testing (if any) should be properly documented.

6.2.18 Remote Connection

(a) The CI operator should define appropriate usage policies and procedures that specify the security requirements for remotely accessing the CCSs from outside the CI operator's premises.

(b) The CI operator should implement suitable security measures to prevent unauthorized remote access to CCSs and their data, including encrypting remote access sessions (e.g. using virtual private networks), implementing multi-factor authentication, enforcing access restrictions for remote access, logging and monitoring remote access activities, and revoking authority and access rights when they are no longer needed.

(c) The CI operator should provide dedicated equipment for remote access. Where the CI operator permits the use of privately-owned equipment for remote access, it should, in addition to (a) and (b) specified above, establish relevant policies and procedures, require user acknowledgement of security responsibilities before use, support the separation and protection of sensitive digital data on the equipment, and consider enabling location tracking of equipment and remote data wiping.

6.2.19 Storage Media

(a) The CI operator should ensure the authorization of disclosure, modification, removal and destruction of sensitive digital data directly involved in the provision of essential services on storage media.

(b) The CI operator should disable USB-port support on CCSs that have no operational needs.

(c) The CI operator should perform malware scan for portable computing devices and removable storage media before connecting them to CCSs.

(d) The CI operator should encrypt the sensitive digital data directly involved in the provision of essential services that are stored or processed on storage media. The CI operator may also refer to section 6.5.4 for the alternative security controls for an OT system.

(e) The CI operator should protect the portable computing devices and removable storage media that store or process sensitive digital data directly involved in the provision of essential services from unauthorized access or misuse.

(f) The CI operator should completely erase and destroy the sensitive digital data directly involved in the provision of essential services from storage media before disposal or re-use. A suitable deletion method, such as degaussing, electronic overwriting or cryptographic erasure, should be employed to avoid data leakage.

6.2.20 Backup and Recovery

(a) The CI operator should perform backups at regular intervals to enable the recovery from loss of data in CCSs. The CI operator should formulate backup and recovery policies for its CCSs. Backup restoration tests should be conducted regularly without affecting the production environment. The frequency of backup reviews and restoration tests should be defined and documented.

(b) Local and off-site backups should be maintained. Off-site data backups should be stored at a secure and remote location at a sufficient distance to escape from the disasters at the main site.

(c) Proper procedures should be established for storing and handling of backup media. An immutable copy or a copy that is physically disconnected from a CCS should be stored to avoid corruption of backup data if the CCS is compromised.

(d) Access to the backup media should be limited to authorized personnel in accordance with the established mechanism. Unauthorized access to the media library or off-site storage room should not be permitted.

(e) The CI operator should ensure adequate resilience to meet the availability requirements of CCSs.

6.2.21 Network Security

(a) The CI operator should plan and implement adequate network security controls on the CCSs to prevent malicious traffic from accessing the CCS (e.g. limiting communication loads that could constitute a Denial-of-service ("DoS") attack). The CI operator may also refer to section 6.5.7 for the alternative security controls for an OT system.

(b) The CI operator should install a network intrusion detection system or a network intrusion prevention system at critical nodes of the CCS.

(c) The CI operator should divide their networks into separate network domains based on trust levels.

(d) The Internet access services used by CCSs should be equipped with the following security functions:

(i) Network traffic access control to block and allow IP addresses or domains;

(ii) Routing traffic and filtering packet; and

(iii) Intrusion detection and prevention to log, monitor, detect and stop attacks.

(e) Access to CCSs via wireless communications should be carefully planned to mitigate security risks. Where the use is justified by operational necessity, the CI operator should assess the relevant security risks and implement compensatory security measures, including proper authentication, encryption, user level network access control and adequate logging.

6.2.22 Application Security

(a) The CI operator should ensure the computer-system security of CCSs throughout the development life cycle.

(b) A CCS should be loaded only with authorized application software.

(c) The CI operator should establish and apply secure coding principles (e.g. input validation, output encoding, authentication and password management, session management, error handling and logging) to the software development of CCSs to prevent, detect and remove any potential computer-system security vulnerabilities in the code.

(d) The CI operator should conduct testing on CCSs in a structured and organized manner before they are released to production, to ensure the application could meet its design objectives and eliminate potential vulnerabilities. The scope of testing should include security functions (user authentication, access restriction, etc.), secure coding (coding practices on input validation, session management, etc.) and security configurations.

(e) The CI operator should protect the source code from unauthorized access (e.g. using configuration management tools).

(f) Test data should be carefully selected, protected and controlled. In particular, using production data in the testing environment should be authorized. Sensitive digital data should be removed or masked if it is used in the testing environment.

6.2.23 Log Management

(a) The CI operator should record and identify the events involving CCSs that may lead to a computer-system security incident.

(b) The CI operator should define policies for logging activities and retaining logs of CCSs to facilitate computer-system security incident investigations. The policies should include but not be limited to the requirement to log:

(i) Log-on attempts;

(ii) Password change attempts;

(iii) Access attempts to critical files (e.g. software configuration files, password and key files);

(iv) Use of privileged rights, such as addition and deletion of user accounts;

(v) Changes to user access rights;

(vi) Modifications to audit policies; and

(vii) Activation and de-activation of protection systems, such as anti-malware systems and intrusion detection systems.

(c) The logs should be retained for a minimum period of 6 months. Such logs should be secured so that they cannot be deleted or altered, and can be read only by authorized persons.

(d) If the requirements stipulated in sections 6.2.23(b) or 6.2.23 (c) cannot be fulfilled in certain OT CCSs owing to technical limitations, the CI operator should document such matters with justifications.

(e) Any retained log should provide sufficient information to enable comprehensive audits of the effectiveness and compliance of security measures.

(f) The CI operator should establish processes to identify exceptions through pre-determined rules, and should utilise suitable programs or tools to facilitate log analysis. All events suspected of being triggered by a computer-system security incident should be logged and monitored.

(g) The CI operator should synchronise the internal clocks of all CCSs components with a primary time source to enable accurate log-event correlation across the systems.

6.2.24 Cloud Computing Security

(a) The CI operator should ensure the computer-system security of CCSs that employ cloud technologies, regardless of the location of the cloud system.

(b) The CI operator should define and document policies of CCSs for identifying, assessing, evaluating and responding to computer-system security risks associated with the adoption of cloud computing. Any mitigation or response to the identified risks should also be properly documented.

(c) The CI operator should clearly define and implement the shared responsibilities for computer-system security of CCSs between the cloud service suppliers and the CI operator.

(d) The CI operator should regard the external cloud services for CCSs as part of the supply chain and observe the security requirements stipulated in section 6.2.25 Supply Chain Management of this Code.

(e) The CI operator should ensure that the cloud service suppliers provide proper protection for the CI's data throughout design, development, deployment and configuration of infrastructure of CCSs, and that the CI's data is properly isolated from other customer environment.

6.2.25 Supply Chain Management

(a) The CI operator should maintain an agreed level of CCS security within supplier relationships to ensure that all suppliers adhere to a defined set of computer-system security requirements.

(b) The CI operator should define and establish processes and procedures to manage the computer-system security risks in the products and services supply chain. The processes should include identifying and documenting essential supply chain components that are critical to the operations of CCSs.

(c) Depending on the level of assessed supply chain risk and geopolitical risk, the CI operator should adopt, where appropriate, components of the CCS from diverse sources and open source products. This helps avoid over-dependence on a single or a few suppliers and better manages risks arising from potential export controls imposed on certain IT and OT products and services.

(d) Security measures, service-level expectations and management requirements for supplier services or facilities commensurate with the data sensitivity and business requirements should be documented and implemented. The security responsibilities of suppliers should be defined and agreed. For example, the contracts with external service providers should require regular security reports while specify responsibilities such as data encryption, robust access controls, or log keeping. These requirements support the CI operator in performing due diligence by evaluating capable suppliers and demonstrating best efforts through ongoing oversight. Some sample contract clauses regarding the liability of external service providers are set out in Annex H for reference.

(e) The CI operator should reserve audit and compliance monitoring rights to verify that external service providers have implemented sufficient controls over its CCSs. Alternatively, the CI operator should reserve rights to obtain periodic security audit reports (e.g. a Hong Kong Standard on Assurance Engagements ("HKSAE") 3000 assurance report, a System and Organization Controls ("SOC") 2 Type 2 Report) to confirm that the measures implemented by the external service providers are satisfactory.

(f) The CI operator should ensure all sensitive digital data in external service provider services or facilities is deleted at the expiry or termination of the service or upon request of the CI operator.

(g) The CI operator should enter into confidentiality and non-disclosure agreements with external service providers to protect the sensitive digital data they can access. These agreements should be properly managed, and reviewed whenever changes occur that affect security requirement.

6.2.26 Monitoring and Detection

(a) The CI operator should establish a mechanism to monitor the continuous operation of CCSs for detecting anomalies and potential computer-system security incidents. The mechanism should define a baseline of normal behaviours and monitor deviations from that baseline.

(b) The CI operator should adopt endpoint security solutions (including but not limited to personal firewall, anti-malware software, endpoint detection and response solutions) to improve visibility and detection of computer-system security vulnerabilities and threats, and to respond quickly to potential advanced attacks. The CI operator may also refer to section 6.5.8 for the alternative security controls for an OT system.

(c) The CI operator should implement procedures to authorize, control and monitor the use of mobile codes (e.g. JavaScript, VBScript, ActiveX controls, Microsoft Office macros) and scripts within the CCS.

(d) Procedures and processes should be in place to ensure 24 x 7 monitoring and a timely response to any security events (including but not limited to credential leakage, application vulnerabilities, system misconfigurations) detected by the monitoring system.

(e) The CI operator should establish mechanisms and processes to collect and analyse information related to computer-system security threats in order to produce threat intelligence. Threat intelligence may include high-level information about the evolving threat landscape, details about attacker methodologies, tools and technologies, and specifics of each attack. Threat intelligence should be monitored 24 x 7 and used to assess threat levels and potential impacts to CCSs and appropriate mitigation actions.

(f) The CI operator should conduct regular reviews of the monitoring mechanism to ensure that it remains effective with respect to the nature of CCSs and ongoing technology advancement.

6.2.27 Computer-System Security Training

(a) The CI operator should formulate a training programme that delivers targeted and structured training periodically to all personnel involved in CCS operation, fostering their awareness and enabling them to fulfil their computer-system security responsibilities. A computer-system security training programme should include but not be limited to the following:

(i) Programme objectives: The CI operator should establish objectives for the training programme, which are aligned with the operator's overall computer-system security strategy.

(ii) Target audience: The CI operator should identify the specific groups or roles required to participate in the training activities. The CI operator should consider different levels of technical expertise, job functions, and needs to tailor the training content accordingly.

(iii) Training approach: The design of training materials and content should be aligned with the objectives and target audience. Appropriate delivery methods should also be adopted having regard to the CI operator's risks, resources, and the target audience's needs. The training approach may include presentations, videos, interactive modules, practical exercises, and case studies. The CI operator could deliver the training by internal training staff or by engaging suppliers to provide training services.

(iv) Evaluation of effectiveness of training activities: The CI operator should review the effectiveness of the training activities. An assessment may be conducted to ensure users' awareness of computer-system security requirements and responsibilities. This can be done through methods such as post-training quizzes, feedback surveys, simulation exercises, or observing changes in behaviour or the number of security incidents to evaluate knowledge gain, behavioural changes, and participant satisfaction.

(v) Regular review and update: The CI operator should regularly review and update the training programme to reflect the evolving threat landscape, emerging technologies, and changes in regulations and compliance requirements. In addition, the CI operator should use feedback to identify improvement areas and adjust or fine-tune the training programme accordingly.

(b) The CI operator may require an external service provider involved in CCS operation through contractual agreements to provide training to its personnel.

6.3 Obligation to conduct computer-system security risk assessments

6.3.1 For the purpose of section 24(1) of the Ordinance, a CI operator should refer to nationally or internationally recognised methodologies and standards for computer-system security risk assessment such as GB/T 22080, GB/T 31722, ISO/IEC 27001, ISO/IEC 27005, IEC 62443-3-2, NIST 800-30, or ISO/IEC 42001 in conducting computer-system security risk assessment. The CI operator may also refer to Practice Guide for IT Security Risk Management and Practice Guide for Security Risk Assessment & Audit ("ISPG-SM01") compiled by DPO in this process.

6.3.2 The computer-system security risk assessment should include but not be limited to all applications, hosts, and network devices of the CCSs.

6.3.3 After conducting the computer-system security risk assessment, the CI operator should document the identified risks to the CCSs, including the likelihood and severity, the level of risks that the CCSs can tolerate, and the required risk mitigation measures and monitoring.

6.3.4 The computer-system security risk assessment should include a vulnerability assessment and a penetration test which, among other steps, identify security and control weaknesses. The CI operator may also refer to section 6.5.9 for the alternative security controls for an OT system.

6.3.5 The vulnerability assessment in the computer-system security risk assessment should involve various vulnerability identification activities, including but not limited to vulnerability scanning, source code reviews, and configuration reviews, to identify potential security loopholes and vulnerabilities. The vulnerability assessment should be conducted under the supervision of a qualified security professional having suitable knowledge, relevant experience and appropriate professional qualifications (e.g. CISP, CISA, CISM, CISSP, etc.).

6.3.6 The penetration test in the computer-system security risk assessment should be carried out from the position of a potential attacker or based on threat intelligence, and can involve active exploitation of possible vulnerabilities of the CCSs. The test should include, but not be limited to, the areas of network security, system software security, client-side application security and server-side application security. The penetration test should be conducted by a tester having suitable knowledge, relevant experience and appropriate professional qualification. Examples of the professional qualification include but are not limited to:

Certification Body	Certification
China Information Technology Security Evaluation Center	Certified Information Security Professional – Penetration Test Engineer
	Certified Information Security Professional – Penetration Testing Specialist
Cyber Security Services, Accreditations & Training (CREST)	CREST Certified Simulated Attack Manager
	CREST Certified Simulated Attack Specialist
	CREST Certified Infrastructure Tester
	CREST Certified Web Applications Tester
eLearnSecurity	eLearnSecurity Certified Penetration Tester eXtreme
	eLearnSecurity Web Application Penetration Tester eXtreme
	eLearnSecurity Certified Professional Penetration Tester
	eLearnSecurity Web Application Penetration Tester
Global Information Assurance Certification (GIAC)	GIAC Penetration Tester
	GIAC Exploit Research and Advanced Penetration Tester
	GIAC Web Application Penetration Tester
ISACA	Cybersecurity Nexus – Penetration Testing Overview
Offensive Security	Offensive Security Certified Expert
	Offensive Security Exploitation Expert
	Offensive Security Certified Professional
	Offensive Security Web Expert
PentesterAcademy	Certified Red Teaming Expert
	Certified Red Teaming Professional
The Hong Kong Institute of Bankers (HKIB)	Certified Cyber Attack Simulation Professional – Certified Simulated Attack Manager
	Certified Cyber Attack Simulation Professional – Certified Simulated Attack Specialist
	Certified Cyber Attack Simulation Professional – Certified Infrastructure Tester
	Certified Cyber Attack Simulation Professional – Certified Web Applications Tester

6.3.7 The computer-system security risk assessment report should include the below sections, where applicable:

(a) Introduction / background information;

(b) Executive summary;

(c) Assessment scope, objectives, methodology, time frame and assumptions about what is and is not covered;

(d) Description of current environment or system, including network diagrams;

(e) Security requirements;

(f) Personnel involved in the computer-system security risk assessment;

(g) Summary of findings and recommendations;

(h) Risk analysis results, including identified assets, threats, vulnerabilities and their impact, likelihood and risk levels with appropriate justifications;

(i) Recommended safeguards with cost-benefit analysis if more than one alternative is available;

(j) Conclusions; and

(k) Annexes, including completed vulnerability assessment report, penetration test report, covered asset inventories[1], and asset valuation results.

[1] Details in accordance with section 6.2.9 (b) of this Code.

6.4 Obligation to arrange to carry out computer-system security audits

6.4.1 A computer-system security audit should assess whether a CI operator's computer-system security management plan is implemented and whether the security controls and measures comply with the computer-system security management plan.

6.4.2 The CI operator should arrange an independent auditor to conduct the computer-system security audit(s) for its CCSs. The auditor should possess suitable knowledge, relevant experience and appropriate professional qualifications (e.g. CISP, CISA, CISM, CISSP, etc.).

6.4.3 The selection of auditors and conduct of audits should ensure the objectivity and impartiality of the audit process. Auditors should not audit their own work. For example, the CI operator should engage auditors (internal or external) who have not been involved in designing or maintaining the computer-system security controls.

6.4.4 Nationally or internationally recognised methodologies and standards, or computer-system security best practices[2] should be referenced when conducting a computer-system security audit. An outline methodology is provided in Annex G for reference.

6.4.5 The computer-system security audit should verify the proper implementation of existing protection measures for the CCSs, including whether the computer-system security management plans are implemented and if they adhere to this Code or alternative methods. Based on this verification, the audit should also assess the overall condition of the computer-system security for the CCSs.

[2] For example, GB/T 19011, GB/T 28450, ISO 19011 and ISO/IEC 27007. DPO's Practice Guide for Security Risk Assessment & Audit (ISPG-SM01), which details the methodology and standards for security audit, may also be used as reference.

6.5 Security measures for operational technology

6.5.1 A CI operator should divide the data, applications and services of CCSs (e.g. engineer workstations, safety systems) into different partitions via physical or logical means (e.g. different computers, network addresses, operating system instances) based on criticality to facilitate zoning model implementation.

6.5.2 The CI operator should prevent the CCS from receiving general purpose person-to-person messages from parties outside the CCS (e.g. via social media or email).

6.5.3 The sections 6.5.4 – 6.5.9 aims to provide alternative measures for CCSs that are OT systems, where the corresponding security requirements stipulated in sections 6.2.5 – 6.2.27, 6.3 and 6.4 cannot be fulfilled.

6.5.4 Cryptography

(a) Alternative to section 6.2.12(a) and 6.2.19(d), the CI operator should define and implement policies and procedures on the use of cryptography to protect the computer-system security of the CCSs, taking into account:

(i) The impact on the provision of essential services;

(ii) The protection for sensitive digital data in transit (e.g. encrypting data over networks);

(iii) The effect of data visibility on system monitoring (e.g. anomaly detection tools being unable to analyse encrypted data); and

(iv) Operational difficulties (e.g. communication latency caused by encryption).

6.5.5 Password Management

(a) Alternative to section 6.2.13(a), for CCSs that use password-based authentication, the CI operator should define and implement password policies that are within the capabilities of the CCSs. The password policies should specify:

(i) Minimum password length;

(ii) Password complexity requirements;

(iii) Maximum password lifetime;

(iv) Maximum number of consecutive failed log-on attempts; and

(v) Restriction on reusing previous passwords.

If implementing password policies could adversely impact the normal functioning of an OT system, the CI operator should deploy compensating security controls (e.g. physical isolation or network isolation) and document any components that remain without password protection.

6.5.6 Change Management and Patch Management

(a) Alternative to section 6.2.16(b) and 6.2.17(c), the CI operator should define and implement policies and procedures for testing system changes (e.g. patches) when a non-production environment is not available, taking into account:

(i) The adoption of test results and issues reported by product suppliers and other parties before deploying changes and patches to the CCSs; and

(ii) The establishment of a careful deployment approach that test changes or patches in the production environment (e.g. deploying the changes to a limited subset of the system first and proceeding gradually, or deploying the changes to components that have built-in resilience for testing).

6.5.7 Network Security

(a) Alternative to section 6.2.21(a), the CI operator should plan and implement adequate network security controls on the CCSs to detect and manage malicious traffic from accessing the CCS.

6.5.8 Monitoring and Detection

(a) Alternative to section 6.2.26(b), the CI operator should define and implement policies and procedures for protecting endpoint devices against malware, taking into account:

(i) The use of anti-malware software and software whitelisting;

(ii) The impact on the normal functioning of an OT system;

(iii) The testing of anti-malware software and signatures before deployment (e.g. testing configurations on an offline system);

(iv) The timing and resources used by anti-malware software for scanning and signature updates;

(v) The identification of files to be excluded from malware scanning to avoid affecting the CCSs (e.g. not scanning certain files during production); and

(vi) The adoption of redundancy for CCS components that require ongoing signature updates without disrupting operations.

The CI operator should also document any CCS components that lack anti-malware protection, the justifications for excluding these components, and the compensating security controls applied to these components.

6.5.9 Computer-system Security Risk Assessment

(a) Alternative to section 6.3.4, the CI operator should define and implement policies and procedures for identifying vulnerabilities in the CCSs. The CI operator should evaluate vulnerability assessments and penetration tests in an offline environment before performing them in the production environment, in order to understand their impact on the CCSs. If conducting a vulnerability assessment or a penetration test could adversely impact the normal functioning of an OT system, the CI operator should use alternative vulnerability identification activities (e.g. performing targeted vulnerability scans or penetration tests on critical peripheral nodes of a CCS) to discover computer-system security weaknesses in the CCSs. The CI operator should also document any exclusions with justification.

7. OBLIGATIONS OF CI OPERATORS – DIVISION 3

7.1 Obligation to participate in computer-system security drill

7.1.1 Upon receiving a written notification from the Commissioner, a CI operator would be given reasonable time to prepare for participation in the computer-system security drill ("the drill"), which tests the CI's state of readiness in responding to computer-systems security incidents, including:

(a) Assessing the validity and effectiveness of CI operator's emergency response plan; and

(b) Assessing the participating personnel's knowledge of their roles and responsibilities in responding to computer-system security incidents.

7.1.2 The CI operator will be notified by the Commissioner to participate in a drill no more than once every two years.

7.1.3 The theme, scope and scenarios of a drill would be set by the Commissioner. The drill may be conducted in the form of tabletop exercise, functional exercise, simulated attack or any other means deemed appropriate by the Commissioner. The drill will not involve actual deployment of CCSs or their production environment, so as to avoid interrupting the CI operator's business activities.

7.1.4 A drill may involve multiple CI operators in the same or different sectors, as well as multiple government units, to test the coordination of computer-system security incidents with large societal or economic impacts and restoration of public order.

7.1.5 The following members of a CI operator should participate in a drill as appropriate under the emergency response plan:

(a) Management personnel who have a role in the emergency response plan;

(b) Computer-system security management unit;

(c) Emergency response team;

(d) Public relations or corporate communications personnel; and

(e) Other personnel deemed necessary by the drill scenarios and the CI operator, such as cybersecurity insurer.

7.1.6 Representatives of the CI operator should attend the briefing and debriefing sessions conducted by the Commissioner.

7.1.7 Regarding performance in a drill, the CI operator may receive comments from the Commissioner on areas for continuous improvement in responding to computer-system security incidents. The CI operator should take remedial actions to address those comments as recommended by the Commissioner.

7.2 Obligation to submit and implement emergency response plan

7.2.1 A CI operator should formulate an emergency response plan, and set out the protocol for responding to computer-system security incidents targeting CCSs. The scope of the plan should include the followings:

(a) Incident management; and

(b) Business continuity management and disaster recovery.

7.2.2 The CI operator should ensure that the emergency response plan and any subsequent changes (other than contact point or editorial update) submitted to the Commissioner are endorsed by the Board, or a functional sub-committee delegated by the Board, or the senior management overseeing the operation of the concerned CI (e.g. Chief Executive Officer, Chief Operating Officer, or their equivalent). The plan should be reviewed upon any material changes to CCSs, and in any event at least once every two years, to ensure its effectiveness and validity.

7.2.3 Incident Management

(a) Incident management plan ensures that the incident response activities are carried out in an orderly, efficient and effective manner, minimising the possible damages from computer-system security incidents ("incidents"). The plan should include the following:

(i) Structure of the emergency response team, including the corresponding roles, responsibilities and contact details of members for handling incidents. The role of senior management should also be specified;

(ii) Incident reporting requirements set out by the Ordinance;

(iii) Thresholds that trigger the plan and mobilise the emergency response team;

(iv) Communication plan with internal and external stakeholders, including employees, customers and the public as to what, when, how and with whom to communicate; and

(v) Playbooks covering procedures for the following matters:

(1) Containing the incident to prevent further harm;

(2) Digital evidence handling, including identification, collection, acquisition, preservation of evidence and chain of custody;

(3) Investigating the cause and impact of the incident;

(4) Recording the incident response process, including details of the incident, actions taken and decisions made; and

(5) Conducting a post-incident review.

(b) The CI operator should provide necessary resources required to implement the incident management plan.

(c) The CI operator should ensure all members of the emergency response team are familiar with both their own roles and responsibilities and those of other team members as defined in the plan. The CI operator should also provide training for all team members to ensure their capabilities to carry out their assigned duties.

(d) The CI operator should appoint at least two contact points for non-working hours emergencies in relation to computer security issues. The contact points should maintain communication with the Commissioner during an emergency, and also capable of handling security incidents or relaying security messages to responsible personnel in a timely manner. The CI operator should provide contact details of these contact points to the Commissioner.

(e) The CI operator should ensure multiple channels (e.g. phone, email) are available to effectively communicate with stakeholders in response to the incident.

(f) When balancing the need for timely system recovery and digital evidence handling, the CI operator should prioritize incidents which had impacted business operations, require swift damage containment or need immediate system recovery. Otherwise, more time should be allocated to evidence collection.

(g) The CI operator should leverage automation and orchestration to expedite incident response and forensics processes, such as automatic log collection and orchestrated recovery processes. This does not preclude the use of "human-in-the-loop" methods or other appropriate approaches to support incident response and forensics processes.

(h) The CI operator should engage capable incident response and forensic examination personnel to assist with digital evidence collection and incident investigation.

(i) The post-incident review should incorporate lessons learned to improve future response and preventive measures, encompassing:

(i) Facts and causes of the incident;

(ii) Gaps in the existing governance, risk management and compliance contributed to the incident, and the degree of consequence;

(iii) Effectiveness and efficiency in executing the emergency response plan; and

(iv) Improvement actions recommended.

7.2.4 Business Continuity Management and Disaster Recovery Planning

(a) Business continuity management focuses on sustaining the CI operator's ability to continue essential operation during disruptions arising from computer-security incidents.

(b) The business continuity management plan should include the following:

(i) Business continuity objectives to be achieved;

(ii) Business impact analysis of the CCSs to identify the maximum tolerable downtime ("MTD"), recovery time objectives ("RTO"), recovery point objectives ("RPO"), and minimum service levels ("MSL") , where applicable;

(iii) Resources needed to resume the relevant business processes;

(iv) Policies and procedures to ensure continuity of essential services;

(v) Roles and responsibilities of the management and personnel who will execute the plan;

(vi) Training and testing to ensure responsible employees are familiar with the plan and aware of the business continuity policy; and

(vii) Evaluation and review whenever there are material changes to CCSs so as to ensure the plan's effectiveness.

(c) Disaster recovery planning focuses on the effective restoration of CCSs from severe disruptions, thereby ensuring the resilience of business operations in connection with CCSs.

(d) Except item (ii) and (iii) below which may not apply to OT systems, the disaster recovery plan should include the following:

(i) Recovery strategy that aligns with the business continuity objectives;

(ii) Policies and procedures for backup, taking into account the location of the alternative site is sufficiently distant to escape from the disaster at the primary site and protection of backup data;

(iii) Recovery procedures to an alternative site, including the plan to resume data at the primary site once it is restored, where applicable;

(iv) Regular testing of backup media and telecommunication services; and

(v) Evaluation and review whenever there are material changes to CCSs so as to ensure the plan's effectiveness.

7.3 Obligation to notify computer-system security incidents

7.3.1 The purpose of a CI operator notifying the Commissioner of a computer-system security incident is to enable the Commissioner to assess the overall consequences for the continuous provision of essential services in one or multiple sectors, or for the maintenance of critical societal or economic activities in Hong Kong, and to take appropriate remedial measures to prevent the impact from spreading to other sectors.

7.3.2 A computer-system security incident must involve access or any other act performed without lawful authority and that has an actual adverse effect to the CCSs involved. An event arising from pure technical failure, natural disaster, mass power outage, a computer-system security threat that is detected and timely removed or quarantined, or personal data leakage arising from human mistake, does **not** constitute a computer-system security incident.

7.3.3 Examples of computer-system security incidents include but are not limited to:

(a) Large-scale or volumetric Distributed DoS ("DDoS") attack causing degradation of an essential service, or Ransom DDoS attack where a ransom note is received;

(b) Ransomware attack that causes suspension of an essential service or shows signs of data compromise;

(c) Unintended external connection to a CCS caused by malware infection or by an adversary exploiting a vulnerability;

(d) An employee accesses to sensitive digital data of a CCS and maliciously exfiltrates that data or maliciously misconfigures the access privilege of the CCS;

(e) Configurations or data of a CCS are modified by a malicious payload or script;

(f) An employee abuses his / her authority to interfere with the functioning of the CCS; and

(g) Any tampering with cryptographic key management devices that hampers the normal functioning of a CCS.

7.3.4 A serious computer-system security incident is an incident which has disrupted, is disrupting or is likely to disrupt the core function of the CI concerned, and must be notified within 12 hours after the CI operator becomes aware of it. An incident is considered as a serious incident if any of the below criteria are met:

(a) The downtime affecting the core function of the CI concerned has exceeded or is likely to exceed the maximum tolerable downtime defined by the CI operator in the business continuity management plan;

(b) The service performance has dropped or is likely to drop below the minimum service level defined by the CI operator in the business continuity management plan;

(c) The computer-system security incident has triggered or is likely to trigger the activation of business continuity or disaster recovery procedures;

(d) The computer-system security incident has caused or is likely to cause the leakage of material volume of customer data, where "material" is defined by the CI operator in the business continuity management plan;

(e) The computer-system security incident has leaked or is likely to leak sensitive digital data that hampers the normal functioning of the CCS;

(f) The computer-system security incident has caused or is likely to cause a material number of customer enquiries or complaints, where "material" is defined by the CI operator in the business continuity management plan; or

(g) Threat actors have threatened to launch an attack against a CCS at a specified time that would likely trigger any of the scenario described in sections 7.3.4(a) to (f).

7.3.5 When the CI operator discovers any sign of disruption or irregularity in the CCSs, the CI operator may need to spend time to ascertain whether a computer-system security incident has occurred. At the point the CI operator has a reasonable degree of certainty that a computer-system security incident has occurred, the CI operator is deemed to have become aware of the computer-system security incident.

7.3.6 Notification in Specified Form

(a) When a CI operator becomes aware that a computer-system security incident has occurred, the CI operator should notify the Commissioner by submitting a specified form (Annex E or a sector-specific form) through a designated secured channel. The CI operator should complete the form as far as practicable based on the information available.

(b) Alternatively, the CI operator may first make the notification to a designated telephone number, providing the below information, and then submit a specified form (Annex E or a sector-specific form) through a designated secured channel within 48 hours of the notification:

(i) Nature of the computer-system security incident;

(ii) CCSs involved; and

(iii) Brief incident summary.

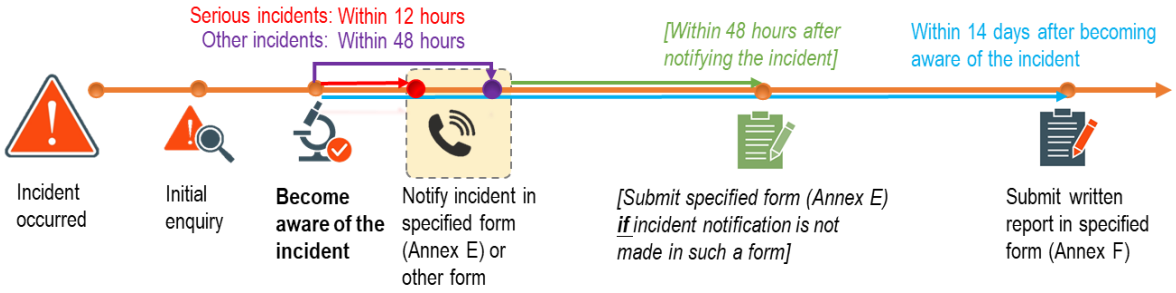
(c) For the avoidance of doubt, the CI operator is obliged to fulfil any sector specific requirements in incident notification imposed by the relevant regulatory regime or other applicable laws.

7.3.7 Written report in Specified Form

(a) The CI operator should submit a written report in a specified form (Annex F or a sector-specific form) via the designated secured channel within 14 days after becoming aware of the computer-system security incident. The report should provide updates on the incident based on the information available. If additional information become available after submitting the written report, the CI operator should also provide such information to the Commissioner as supplementary material.

(b) For the avoidance of doubt, the CI operator is obliged to fulfil any sector specific requirements in incident reporting imposed by the relevant regulatory regime or other applicable laws.

7.3.8 The following timeline illustrates the requirements on notifying and reporting a computer-system security incident:



*** ENDS ***

ANNEX A: FORM FOR NOTIFYING OFFICE ADDRESS

Pursuant to section 19 of the Protection of Critical Infrastructures (Computer Systems) Ordinance

A. Background Information	
Information of the Critical Infrastructure Operator ("CI Operator")	
Full Name:	
B. Office Address of CI Operator	
Office Address of the CI Operator	
Office Address:	
C. Reporting Entity Information	
Name:	Post Title:
Office & Mobile Contact:	Email Address:
Form Submission Date (dd/mm/yyyy):	

Personal Information Collection Statement: The personal information provided will be used for the purpose of exercising the powers and duties vested in the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") or the designated authority specified in column 2 of Part 2 of Schedule 2 of the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance"), collectively known as the regulating authority. The personnel information will be retained by the regulating authority for an appropriate period of time necessary for the fulfilment of the relevant purposes or as required by the Ordinance. The regulating authority may disclose the personal information to the parties permitted by section 57(3) of the Ordinance. The data subject or relevant persons as defined in section 2 or 17A of the Personal Data (Privacy) Ordinance ("the PDPO") have a right of access and correction with respect to personal information as provided for in sections 18 and 22 and Principle 6 of Schedule 1 of the PDPO. The right of access includes the right to obtain a copy of the personal information provided in this form. Enquiries concerning the personal information collected by means of this form, including access and corrections, should be addressed to the Commissioner (email: protection_ci@sb.gov.hk) or the designated authority concerned.

ANNEX B: FORM FOR NOTIFYING CHANGES OF CRITICAL INFRASTRUCTURE OPERATOR

Pursuant to section 20 of the Protection of Critical Infrastructures (Computer Systems) Ordinance

A. Background Information	
Information of the Current Critical Infrastructure Operator ("CI Operator")	
Full Name:	
B. Information of the New CI Operator:	
1) Organization	
Full Name:	Business Registration Number:
Office Address:	
2) Organization Contact Person	
Full Name:	Post Title:
Office Number:	Email Address:
3) Critical Computer System ("CCS") **under the New CI Operator**	
4) Reasons of Change ☐ Sale of facilities ☐ The current CI Operator ceases to provide daily operation, management or maintenance of the Critical Infrastructure	☐ Merger ☐ Acquisition ☐ Others (please specify):
5) Changes in Operational Scope (if any)	
6) Effective Date (dd/mm/yyyy)	
C. Reporting Entity Information	
Name:	Post Title:
Office & Mobile Contact:	Email Address:
Form Submission Date (dd/mm/yyyy):	

Personal Information Collection Statement: The personal information provided will be used for the purpose of exercising the powers and duties vested in the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") or the designated authority specified in column 2 of Part 2 of Schedule 2 of the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance"), collectively known as the regulating authority. The personnel information will be retained by the regulating authority for an appropriate period of time necessary for the fulfilment of the relevant purposes or as required by the Ordinance. The regulating authority may disclose the personal information to the parties permitted by section 57(3) of the Ordinance. The data subject or relevant persons as defined in section 2 or 17A of the Personal Data (Privacy) Ordinance ("the PDPO") have a right of access and correction with respect to personal information as provided for in sections 18 and 22 and Principle 6 of Schedule 1 of the PDPO. The right of access includes the right to obtain a copy of the personal information provided in this form. Enquiries concerning the personal information collected by means of this form, including access and corrections, should be addressed to the Commissioner (email: protection_ci@sb.gov.hk) or the designated authority concerned.

ANNEX C: FORM FOR NOTIFYING APPOINTMENT OF EMPLOYEE SUPERVISING COMPUTER-SYSTEM SECURITY MANAGEMENT UNIT

Pursuant to section 21 of the Protection of Critical Infrastructures (Computer Systems) Ordinance

A. Background Information	
Information of Critical Infrastructure Operator ("CI Operator")	
Full Name:	
B. Employee Details	
Information of the Employee Supervising the Computer-system Security Management Unit	
Full Name:	Post Title:
Office & Mobile Contact:	Email Address:
Relevant Professional Qualification(s): *Please attach the relevant documentary proof.	
Relevant Experience: *Please attach the relevant documentary proof.	
Effective Date (dd/mm/yyyy) *Please attach the relevant documentary proof.	
C. Reporting Entity Information	
Name:	Post Title:
Office & Mobile Contact:	Email Address:
Form Submission Date (dd/mm/yyyy):	

Personal Information Collection Statement: The personal information provided will be used for the purpose of exercising the powers and duties vested in the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") or the designated authority specified in column 2 of Part 2 of Schedule 2 of the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance"), collectively known as the regulating authority. The personnel information will be retained by the regulating authority for an appropriate period of time necessary for the fulfilment of the relevant purposes or as required by the Ordinance. The regulating authority may disclose the personal information to the parties permitted by section 57(3) of the Ordinance. The data subject or relevant persons as defined in section 2 or 17A of the Personal Data (Privacy) Ordinance ("the PDPO") have a right of access and correction with respect to personal information as provided for in sections 18 and 22 and Principle 6 of Schedule 1 of the PDPO. The right of access includes the right to obtain a copy of the personal information provided in this form. Enquiries concerning the personal information collected by means of this form, including access and corrections, should be addressed to the Commissioner (email: protection_ci@sb.gov.hk) or the designated authority concerned.

ANNEX D: FORM FOR NOTIFYING MATERIAL CHANGES TO CERTAIN COMPUTER SYSTEMS

Pursuant to section 22 of the Protection of Critical Infrastructures (Computer Systems) Ordinance

A. Background Information

Information of Critical Infrastructure Operator ("CI Operator")

Full Name:

B. Change Details

1) Type of Material Changes (Please tick the appropriate box(es))

☐ Platform migration
☐ Changes to the computing platform or hardware
☐ Major version upgrade of a core component (e.g. database)
☐ Server virtualisation
☐ Application re-design
☐ Significant code changes
☐ Integration with or change in interdependency on external systems or networks
☐ Changes to the underlying infrastructure that supports the critical computer systems ("CCS")
☐ Any system modification that fundamentally alters the characteristics or nature of the CCS
☐ Substantial changes in CCS components maintained by cloud service suppliers that the CI Operator becomes aware of
☐ Changes of mission or major functions that alters the system's operational scope, intended purpose or requirements in security, resources or functions
☐ Others (please specify):

*Please refer to section 22 of the Protection of Critical Infrastructures (Computer Systems) Ordinance for meaning of "material changes".

2) Change Details with Timeframe

3) Deployment Date (dd/mm/yyyy)

*Please refer to section 6.1 of the Code of Practice for details.

*All the changes should be endorsed and processed in accordance with the change management process defined in the computer-system security management plan.

4) Description of the Effect *(on the computer-system security risk of the CCS(s) or risk to carrying out the core function of the CI after the deployment of the material change(s))*

*Please include the relevant computer-system security risk assessment documentation in the submission of this form.

5) Updated System Documentation

*Please list the documentations attached with this form.

C. Reporting Entity Information

Name:	Post Title:
Office & Mobile Contact:	Email Address:
Form Submission Date (dd/mm/yyyy):	

Personal Information Collection Statement: The personal information provided will be used for the purpose of exercising the powers and duties vested in the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") or the designated authority specified in column 2 of Part 2 of Schedule 2 of the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance"), collectively known as the regulating authority. The personnel information will be retained by the regulating authority for an appropriate period of time necessary for the fulfilment of the relevant purposes or as required by the Ordinance. The regulating authority may disclose the personal information to the parties permitted by section 57(3) of the Ordinance. The data subject or relevant persons as defined in section 2 or 17A of the Personal Data (Privacy) Ordinance ("the PDPO") have a right of access and correction with respect to personal information as provided for in sections 18 and 22 and Principle 6 of Schedule 1 of the PDPO. The right of access includes the right to obtain a copy of the personal information provided in this form. Enquiries concerning the personal information collected by means of this form, including access and corrections, should be addressed to the Commissioner (email: protection_ci@sb.gov.hk) or the designated authority concerned.

ANNEX E: FORM FOR NOTIFYING COMPUTER-SYSTEM SECURITY INCIDENT

Pursuant to section 28(2)(b)(i) of the Protection of Critical Infrastructures (Computer Systems) Ordinance

*All fields should be completed as far as practicable based on the information available.

A. Background Information

1) Information of Critical Infrastructure Operator ("CI Operator")

Full Name:

2) Critical Computer System(s) Affected

B. Incident Details

1) Seriousness of Incident

☐ Has disrupted / is disrupting / likely to disrupt the core function of CI[a]
☐ Has actual adverse effect other than above[b]

*Subject to section 28(3) of the Ordinance, notification shall be made within *[a]* 12 hours or *[b]* 48 hours after becoming aware of the incident depending on the seriousness of the Incident

2) Nature (Please tick the appropriate box(es))

☐ Phishing / social engineering
☐ Ransomware / malware attack
☐ Data breach (leakage / tampering)
☐ Denial-of-service **(**DoS / DDoS) attack
☐ Others (please specify):

☐ Trojan horse
☐ Supply chain attack
☐ Website defacement
☐ Unauthorized system access / intrusion

☐ Spoofing
☐ Insider threat
☐ Man-in-the-Middle attack

3) Earliest Identifiable Time of the Incident	***Date*** (dd/mm/yyyy):	***Time*** (hh:mm):
4) Time Becoming Aware of the Incident	***Date*** (dd/mm/yyyy):	***Time*** (hh:mm):

5) Brief Incident Summary

C. Reporting Entity Information

Name:	Post Title:
Office & Mobile Contact:	Email Address:
Form Submission Date (dd/mm/yyyy):	

Personal Information Collection Statement: The personal information provided will be used for the purpose of exercising the powers and duties vested in the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") under the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance") and be retained by the Commissioner for an appropriate period of time necessary for the fulfilment of the relevant purposes or as required by the Ordinance. The Commissioner may disclose the personal information to the parties permitted by section 57(3) of the Ordinance. The data subject or relevant persons as defined in section 2 or 17A of the Personal Data (Privacy) Ordinance ("the PDPO") have a right of access and correction with respect to personal information as provided for in sections 18 and 22 and Principle 6 of Schedule 1 of the PDPO. The right of access includes the right to obtain a copy of the personal information provided in this form. Enquiries concerning the personal information collected by means of this form, including access and corrections, should be addressed to the Commissioner via email at protection_ci@sb.gov.hk.

ANNEX F: WRITTEN REPORT FOR COMPUTER-SYSTEM SECURITY INCIDENT

Pursuant to section 28(4) of the Protection of Critical Infrastructures (Computer Systems) Ordinance

*All fields should be completed as far as practicable based on the information available.

A. Background Information

1) Information of Critical Infrastructure Operator ("CI Operator")

Full Name:

2) Critical Computer System(s) Affected

Name	**Physical Location** *(address in Hong Kong, or specify the country name if located outside Hong Kong)*

(if insufficient space, please attach a separate signed sheet with details)

B. Incident Overview

1) Nature (Please tick the appropriate box(es))

- ☐ Phishing / social engineering
- ☐ Ransomware / malware attack
- ☐ Data breach (leakage / tampering)
- ☐ Denial-of-service (DoS / DDoS) attack
- ☐ Others (please specify):
- ☐ Trojan horse
- ☐ Supply chain attack
- ☐ Website defacement
- ☐ Unauthorized system access / intrusion
- ☐ Spoofing
- ☐ Insider threat
- ☐ Man-in-the-Middle attack

2) Brief Incident Description

3) Initial Attack Vector / Point of Intrusion

4) Root Cause Analysis Summary

Root cause(s) of the incident and contributing factor(s):

Whether the root cause was identified in previous security assessment or audit:

(if yes, why the incident could not have been prevented; if not, why it was not identified)

5) Earliest Identifiable Time of the Incident	***Date*** (dd/mm/yyyy):	***Time*** (hh:mm):
6) Time Becoming Aware of the Incident	***Date*** (dd/mm/yyyy):	***Time*** (hh:mm):

7) How was the incident first detected? (Please tick the appropriate box(es))

By External Means

☐ Threat Actor Disclosure ☐ Customer / Client ☐ External Audit

☐ Third Party Vendor ☐ Peer / Competitors ☐ Anonymous Source

By Internal Means

☐ Computer-system Security Management Unit

☐ Internal Audit Personnel ☐ Other Employee

By Other Means

☐ Please specify:

8) Hardware or software where vulnerabilities are found

(for hardware, please specify name, manufacturer, model and firmware version; for software, please specify name, publisher and version)

Item	Hardware / Software	Descriptions
1		
2		
3		

(if insufficient space, please attach a separate signed sheet with details)

C. Impact Assessment

1) Scope of Impact *(which parts of the CCS were affected):*

2) Operational / Service Impact *(how operations or services of CI were disrupted):*

3) Data Impact *(if any sensitive information was compromised, altered or lost)**:***

4) Customer / Third-party Impact *(any effect on customers or third parties):*

5) Financial Impact *(any direct financial loss as a result of the incident):*

Estimated HK$

6) Other Impact(s) *(if any):*

7) Duration of Disruption *(how long the incident impacted operations or services):*

D. Response Actions

1) Follow-up action(s) taken (Please tick the appropriate box(es))

Damage Containment:

☐ Affected systems or network segments have been isolated
☐ Compromised accounts have been removed or isolated
☐ Malicious IPs / domains have been blocked
☐ Others (please specify):

Remediation and Recovery:

☐ Malware have been removed
☐ Affected systems have been restored
☐ Security patches have been applied / Vulnerabilities have been fixed
☐ Others (please specify):

2) What is the current status of operation of the CCS(s)? (Please tick the appropriate box(es))

☐ Operation is still not available
☐ Operation is being provided by resilience site
☐ Operation in primary site has resumed normal

3) Measures planned to strengthen security and prevent re-occurrence (Please tick the appropriate box(es))

☐ Policy / Procedure updates
☐ Training / awareness building
☐ Review security assessment or audit procedures
☐ Security monitoring
☐ Configuration changes
☐ Security patches / updates
☐ Others (please specify):

Description of planned measures:

4) Timeline for implementing the remedial measures?

5) Any external team or services engaged? (Please tick the appropriate box(es))

☐ External consultant:
☐ Vendor:
☐ Internet service provider:
☐ Others (please specify):

E. Stakeholder and Media Communication

1) Has the incident been communicated with relevant stakeholders? (Please tick the appropriate box(es))

☐ The Board of Directors / Senior management
☐ Designated authority (via. HKMA / OFCA)
☐ Police (case reference number:)
☐ Office of the Privacy Commissioner for Personal Data
☐ Affected customers / clients
☐ Third parties (vendors / business partners)
☐ Others (please specify):

2) Has the incident been communicated to the media? (Please tick the appropriate box(es))

☐ Yes — Please specify the date (dd/mm/yyyy):
- ☐ Press conference _____
- ☐ Press release _____
- ☐ Reply to press enquiry was made/issued _____

☐ No

F. Reporting Entity Information

Name:	Post Title:
Office & Mobile Contact:	Email Address:
Report Submission Date (dd/mm/yyyy):	

Personal Information Collection Statement: The personal information provided will be used for the purpose of exercising the powers and duties vested in the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") under the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance") and be retained by the Commissioner for an appropriate period of time necessary for the fulfilment of the relevant purposes or as required by the Ordinance. The Commissioner may disclose the personal information to the parties permitted by section 57(3) of the Ordinance. The data subject or relevant persons as defined in section 2 or 17A of the Personal Data (Privacy) Ordinance ("the PDPO") have a right of access and correction with respect to personal information as provided for in sections 18 and 22 and Principle 6 of Schedule 1 of the PDPO. The right of access includes the right to obtain a copy of the personal information provided in this form. Enquiries concerning the personal information collected by means of this form, including access and corrections, should be addressed to the Commissioner via email at protection_ci@sb.gov.hk.

ANNEX G: OUTLINE METHODOLOGY FOR THE COMPUTER-SYSTEM SECURITY AUDIT

PURPOSE

This Annex provides an overview of the computer-system security audit ("the Audit") as required by the Ordinance.

AUDITING STEPS

The Audit is divided into the following stages:

(a) Stage 1: Planning

The CI operator and the Auditor should agree on the audit schedule during the planning stage. The CI operator should also provide basic information on its computer-system security policy and other information about its security implementation work to the Auditor at this stage to facilitate subsequent auditing work.

(b) Stage 2: Fieldwork

The Auditor reviews the documents / records / system configuration and any other information that would be useful to ascertain whether the current practices and security measures of the CI operator would fulfil the requirements. The Auditor also conducts interviews with stakeholders to clarify the information collected from the CI operator to facilitate formulation of audit findings and making of recommendations.

(c) Stage 3: Findings Compilation

After the fieldwork, the Auditor prepares the findings and recommendations. The draft audit findings will be submitted to the CI operator for discussion and verification of factual correctness. Two classifications on the status of findings would be assigned to individual findings identified in the audit work.

Status of Finding	Description
Non conformity	Absence of objective evidence to demonstrate the *fulfilment of* the relevant requirements.
Areas of Improvement	Opportunities for improvement not necessarily required by the relevant requirements, but good practices seen elsewhere that could be implemented to achieve the relevant requirements more effectively.

The CI operator will then review and provide comments on the draft findings. The CI operator may also provide supplementary supporting information for consideration by the Auditor if necessary.

After the CI operator provide comments on the draft audit findings, the Auditor compiles the audit report.

(d) Stage 4: Reporting

Generally, the audit report should contain the information given below:

(i) Executive Summary

A summary of the compliance status and the overall comments and conclusion by the Auditor on effectiveness of the computer-system security management of the CI operator to protect its CCSs should be included.

(ii) Background and objectives

Background and the objectives for conducting the Audit should be included.

(iii) Assumptions and limitations

All the assumptions and limitations in conducting the Audit should be included.

(iv) Methodology

The methodology adopted by the Auditor to conduct the Audit should be included.

(v) Scope

The CCS and the audit period covered by the Audit should be included.

(vi) Findings

Details of the findings, including observations, recommendations and the respective CI operator's responses should be included.

(vii) List of Stakeholder

A list of stakeholders participated in the Audit should be included.

The Auditor should include additional information in the report which is deemed appropriate and useful for assessing the computer-system security posture and resilience of the CI operator.

ASSUMPTIONS AND LIMITATIONS

The following assumptions are made for the Audit:

(a) The CI operator should keep records to evidence compliance with the requirements and support the Audit for effective implementation of corresponding security measures. All information provided by the CI operator is assumed to be current and correct; and

(b) The assessment is made with reference to the interviews, documents and records review and samples checking. No technical assessment such as host scanning, network scanning, application scanning, code review, penetration testing, ethical hacking, etc., have been conducted during the Audit.

ANNEX H: SAMPLE CONTRACT CLAUSES REGARDING THE LIABILITY OF EXTERNAL SERVICE PROVIDERS

PURPOSE

This Annex provides sample contract clauses to assist CI operators in preparing their contract documents regarding the liability of external service providers to comply with the Ordinance.

DISCLAIMER

The sample contract clauses are provided for reference only. The CI operators should consult their legal advisers before adaptation. The Commissioner takes no responsibility for the sample contract clauses, makes no representation, warranty or guarantee of any kind, express or implied, as to their accuracy, completeness or suitability for use in any particular circumstances, and expressly disclaims any liability whatsoever for any loss howsoever arising from or in reliance upon the whole or any part of the sample contract clauses.

SAMPLE CONTRACT CLAUSES

1. In this Contract, unless the context otherwise requires, the following expressions have the following meanings:

"Contract"	means the contract made between <CI operator> and <external service provider>.
"Contractor"	means the <external service provider>.
"Contractor Personnel"	means all persons deployed for performing this Contract (or any part thereof) including the <persons nominated in this contract> (as from time to time replaced), the employees of the Contractor, the sub-contractors, and the employees of the sub-contractors.
"Contract Period"	means the period commencing from <contract start date> and ending on the <contract end date>, unless earlier terminated or extended in accordance with any applicable provision of the Contract.
"Deliverables"	means all tangible and intangible subject matters, including without limitation the <programs, documentation, source codes, configuration, designs, etc., to be delivered by the external service provider> and other materials created, compiled, designed, developed, prepared, supplied, modified, maintained, and/or updated by the Contractor to <CI operator> pursuant to or for the purpose of this Contract or in relation to the Services (including all drafts and uncompleted versions (whether published or unpublished) of any of the aforementioned items).

"Good Industry Practice"	means the standards, practices, methods and procedures conforming to law and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in a similar type of services as the Services under the same or similar circumstances.
"Government"	means the Government of the Hong Kong Special Administrative Region of the People's Republic of China.
"Overall Specifications"	means the <specifications of the project, systems, etc.> and those specifications published by the Contractor, manufacturers and developers in respect of the hardware and/or the software supplied by the Contractor and <CI operator>.
"Services"	means the <services of implementation, system support and maintenance, etc., to be provided by the external service provider> and all other services, obligations and duties to be provided and performed by the Contractor under the Contract (including for the avoidance of doubt the sale or supply of all and any items as specified in the Contract).
"System"	means <all sub-systems, infrastructure, network, programs, applications, etc.> which have to be implemented and integrated as one whole in the production as well as non-production environments as more particularly described in <specifications of the project>.

2. The Contractor acknowledges and agrees that when entering into the Contract, it has already been supplied with sufficient information to enable it to supply to <CI operator> the System and perform the Services which shall comply fully with the requirements set out in the Overall Specifications and other provisions of the Contract. The Contractor shall not be entitled to any additional payment or extension of time and shall not be excused from any obligation or liability under the Contract as a consequence of any alleged lack of knowledge or information or any misinterpretation by the Contractor of any matter or fact relating to the System or Overall Specifications or any other provisions of the Contract.

3. The Contractor shall perform its obligations under the Contract:

   (a) with appropriately experienced, qualified and trained personnel and with all due care, skill and diligence;

   (b) in accordance with Good Industry Practice; and

   (c) in compliance with all applicable laws.

4. The appointment or replacement of any Contractor Personnel to undertake any part of the Services shall not relieve the Contractor from any liability or obligation under this Contract and the Contractor shall be responsible for the acts, omissions, defaults and neglects of anyone of the Contractor Personnel, its agents, employees and contractors as fully as if they were the acts, omissions, defaults or neglects of the Contractor.

5. Any postponement or consequential extension of time or change or suspension pursuant to any applicable provisions of this Contract shall not release the Contractor from any of its obligations or liabilities or give rise to any waiver or estoppel in relation to any of its obligations or liabilities.

6. The Contractor hereby warrants and represents to <CI operator> that:

6.1 the entry into the Contract and the performance by the Contractor of its obligations under it and the performance of the Services and the provision of the Services will not conflict or result in breach of:

(a) any provision of the Memorandum and Articles of Association, or other equivalent constitutional documents governing the Contractor;

(b) any contract or arrangement to which the Contractor is a party or by which the Contractor is bound;

(c) any order, judgment or decree of any court or government agency to which the Contractor is a party or by which the Contractor is bound; or

(d) any applicable laws or regulations.

6.2 the Services shall be performed, and the System and all Deliverables and the provision of any location and network for the System (if required) shall be in compliance with all applicable laws and regulations; all Services shall be performed, the System and all Deliverables, any location and network shall be in accordance with all professional methodologies, standards, guidelines and code of practices as published by relevant government bureau and department from time to time during the Contract Period, unless and to the extent any provisions therein are inconsistent with any express requirements of the Contract or unless otherwise agreed by <CI operator> on a case by case basis.

7. The Contractor shall and its Contractor Personnel comply with the Protection of Critical Infrastructures (Computer Systems) Ordinance (Chapter 653 of the Laws of Hong Kong) and all guidelines (including codes of practice) issued by <the regulating authority>.

8. The Contractor shall (and shall ensure that its Contractor Personnel) comply with:

(a) any applicable privacy or data protection laws (including the Personal Data (Privacy) Ordinance, Chapter 486 of the Laws of Hong Kong) and all guidelines issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong; and

(b) any privacy procedures or policies stipulated by the Government from time to time.

9. The Contractor shall not be relieved from any of its obligations hereunder by entering into any sub-contract for the performance of any part of this Contract. The Contractor shall be responsible for all acts, omissions, defaults and neglects of each sub-contractor, and the agents and employees of such sub-contractor as fully as if they were the acts, omissions, defaults or neglects of the Contractor.

10. This Contract is governed by and construed in accordance with the laws of Hong Kong. The Contractor hereby submits to the exclusive jurisdiction of the courts of the Hong Kong.