



中華人民共和國香港特別行政區政府  
保安局  
關鍵基礎設施(電腦系統安全)專員辦公室

# 《保護關鍵基礎設施(電腦系統)條例》 實務守則

2026年1月1日

第 1.0 版

中華人民共和國香港特別行政區政府

保安局

關鍵基礎設施(電腦系統安全)專員辦公室

本文件的版權屬香港特別行政區政府所有。  
未經中華人民共和國香港特別行政區政府明確批准，  
不得翻印本文件的全部或部分內容。

## 修改記錄

修改次數	修改詳情	版本編號	日期
1	首次發布	1.0	2026年1月1日

## 重要告示

此中文實務守則為英文版本譯本。如中、英文兩個版本有任何抵觸或不相符之處，應以英文版本為準。

## 目錄

<b>1. 引言</b> .....	<b>4</b>
1.1 目的及範圍 .....	4
<b>2. 定義及慣用詞</b> .....	<b>5</b>
2.1 定義 .....	5
<b>3. 指定關鍵電腦系統</b> .....	<b>7</b>
3.1 指定關鍵電腦系統 .....	7
<b>4. 為指定而要求提供的資料</b> .....	<b>9</b>
4.1 為指定關鍵電腦系統而要求提供資料 .....	9
<b>5. 關鍵基礎設施營運者的責任 — 第 1 分部</b> .....	<b>10</b>
5.1 在香港持續設有辦事處的責任 .....	10
5.2 就營運者變更作出通知的責任 .....	10
5.3 設立和持續設有電腦系統安全管理單位的責任 .....	10
<b>6. 關鍵基礎設施營運者的責任 — 第 2 分部</b> .....	<b>11</b>
6.1 就某些電腦系統的重大變化作出通知的責任 .....	11
6.2 提交和實施電腦系統安全管理計劃的責任 .....	12
6.3 進行電腦系統安全風險評估的責任 .....	24
6.4 安排進行電腦系統安全審核的責任 .....	27
6.5 運營科技的保安措施 .....	28
<b>7. 關鍵基礎設施營運者的責任 — 第 3 分部</b> .....	<b>31</b>
7.1 參與電腦系統安全演習的責任 .....	31
7.2 提交和實行應急計劃的責任 .....	32
7.3 就電腦系統安全事故作出通知的責任 .....	35
<b>附錄</b>	
附件 A：辦事處地址通知表格 .....	38
附件 B：關鍵基礎設施營運者變更通知表格 .....	39
附件 C：委任僱員監管電腦系統安全管理單位通知表格 .....	40
附件 D：某些電腦系統重大變化通知表格 .....	41
附件 E：電腦系統安全事故通知表格 .....	42
附件 F：電腦系統安全事故書面報告 .....	43
附件 G：電腦系統安全審核方法概要 .....	47
附件 H：有關外聘服務供應商責任的合約條款範本 .....	49

## 1. 引言

### 1.1 目的及範圍

- 1.1.1 本實務守則(“本守則”)乃根據《保護關鍵基礎設施(電腦系統)條例》(“《條例》”)第 8 條，由關鍵基礎設施(電腦系統安全)專員(“專員”)經諮詢各指定當局後發出。
- 1.1.2 本守則就關鍵基礎設施營運者(“營運者”)如何履行第 1 類責任、第 2 類責任和第 3 類責任提供實務指引。
- 1.1.3 本守則亦可供指定當局就其轄下營運者採用，以履行第 1 類責任和第 2 類責任。如指定當局就第 1 類責任和第 2 類責任發出任何適用於其界別的實務守則(“界別守則”)，有關營運者應參照該界別守則。
- 1.1.4 本守則並非附屬法例，沒有遵守本守則的條文本身並不構成罪行。然而，若按照本守則，營運者沒有遵從上述責任或在遵從上有欠妥之處，專員可發出書面指示，要求營運者採取適當行動，以遵從第 1 類責任、第 2 類責任和第 3 類責任。若不遵從該等指示，即屬犯罪。
- 1.1.5 在遵從第 1 類責任、第 2 類責任和第 3 類責任方面，營運者應按要求向規管當局提供可在香港或從香港接達的資料。
- 1.1.6 營運者根據《條例》提交的文件應透過規管當局建議的安全渠道提交。指明格式的範本載於本守則附件 A 至附件 F。
- 1.1.7 本守則就保護營運者的關鍵電腦系統訂立基線要求，並非針對營運者的個人資料或商業秘密。營運者應視乎個別情況及其關鍵電腦系統的電腦系統安全風險，採取相應的加強保安措施。
- 1.1.8 因應最新科技發展和業界良好作業模式，專員可透過諮詢指定當局及業界持份者，不時審視和修訂本守則所訂的規定。
- 1.1.9 為清晰起見，除另有指明外，在本守則下文各章節中，凡就指定營運者及其關鍵電腦系統、第 1 類責任和第 2 類責任對專員的提述，在相關的內容和適用的範圍內，應解釋為提述指定當局。

## 2. 定義及慣用詞

### 2.1 定義

2.1.1 在《條例》中已界定的詞語適用於本守則。

2.1.2 在本守則所用的詞語界定如下：

可從香港接達	指可從香港某一進入點接達的電腦系統，不論該系統的實體位置為何；
可在香港接達	指可在香港境內實體接觸到的電腦系統；
可用性	指某電腦系統在獲授權人士提出要求時，可供該人士接達及使用；
業務持續運作管理計劃	指機構在服務中斷期間持續提供必要服務的書面程序；
守則	指本實務守則，就《保護關鍵基礎設施(電腦系統)條例》而發出；
專員	指根據《條例》第 3(1)條委任的關鍵基礎設施(電腦系統安全)專員；
電腦系統安全風險	指因電腦系統內的保安漏洞或會被惡意者利用而導致電腦系統安全事故的風險。該風險指風險事件發生的可能性及所造成的影響；
機密性	指在任何方面只有獲授權人士能夠知悉或接達電腦系統所儲存或處理的資料；
指定當局	指《條例》附表 2 第 2 部第 2 欄指明的當局；
運作復原計劃	指電腦系統及／或主電腦場地因發生災難以致任何該等系統受嚴重干擾或出現重大數據損失時，促使該等系統復原的書面程序；
完整性	指在任何方面只有獲授權人士基於獲授權理由，方能修改電腦系統及該等電腦系統所儲存或處理的資料；

惡意軟件	指以惡意意圖設計的軟件，內含可能直接或間接對電腦系統造成損害的功能或能力；
規管當局	指專員或指定當局；
抽取式儲存媒體	指可插入電腦裝置及從電腦裝置移除的便攜式電子儲存媒體，例如磁性、光學和閃存記憶裝置。例子包括外置硬磁碟或固態硬碟、軟磁碟、壓縮磁碟、光碟、磁帶、記憶卡、閃存盤和通用串列匯流排(USB)儲存裝置；
敏感數碼資料	指任何以電子方式儲存、處理或傳遞的資料，若被未獲授權接達、披露、更改或導致遺失，可對個人、機構或社會造成重大損害；
供應商	指與購買方訂立協議以供應產品或服務的個人或機構。供應商可以是產銷商、承辦商、銷售商、生產商(統稱“外聘服務供應商”)，或屬同一機構的某一方；
保安漏洞	指資產在設計、推行或操作方面，或在過程內部控制中的弱點，有關弱點或使電腦系統暴露於電腦系統安全風險之中。

### 3. 指定關鍵電腦系統

#### 3.1 指定關鍵電腦系統

3.1.1 本章旨在為營運者及諮詢機構提供參考，以協助營運者識別其關鍵電腦系統，從而履行《條例》的規定。規管當局會透過諮詢營運者，不時審視關鍵電腦系統的名單。

3.1.2 在釐定是否指定某電腦系統為關鍵電腦系統時，本章應與《條例》第 13 條一併閱讀。

3.1.3 如某電腦系統符合下列任何一項準則，將較有可能被指定為關鍵電腦系統：

- (a) 該系統在有關關鍵基礎設施的核心功能方面擔當重要角色。系統是否與互聯網隔絕並不相關。
- (b) 該系統如受到干擾或損毀，將對關鍵基礎設施的核心功能造成嚴重影響。該關鍵基礎設施的核心功能能否切換至手動方式作為故障處理方案並不相關。
- (c) 該系統儲存或處理的敏感數碼資料會直接用於提供必要服務，例如用於銀行服務或醫療服務的完整個人資料(例如姓名、身份證號碼、電話號碼及住址)。該系統是否具備精密的數據保護或復原機制並不相關。
- (d) 該系統與其他營運者甚為相關。規管當局會在有需要時提供指引。這些電腦系統的例子包括同一界別或跨界別的中央處理或數據交換系統。
- (e) 該系統在提供必要服務方面與有關營運者的其他關鍵電腦系統甚為相關。這些系統的例子包括但不限於：
  - (i) 直接保護上文第 3.1.3(a)至(d)節所述關鍵電腦系統安全的系統(例如將內部網絡與不可信環境分隔的保安通訊閘或防火牆)；以及
  - (ii) 直接提升上文第 3.1.3(a)至(d)節所述關鍵電腦系統復原能力的系統(例如高可用性系統的備份設施)。

- 3.1.4 統稱為運營科技(OT)的工業控制系統，例如監控及資料收集系統(SCADA)、分配監控系統(DCS)及可編程邏輯控制器(PLC)，亦視為《條例》涵義訂明的電腦系統。
- 3.1.5 營運者電腦系統下的資訊科技基礎設施，包括網絡組件、操作平台、中間件系統、物聯網裝置及不間斷電源供應系統，亦可視為該電腦系統的組件。

## 4. 為指定而要求提供的資料

### 4.1 為指定關鍵電腦系統而要求提供資料

4.1.1 規管當局為確定是否指定某電腦系統為關鍵電腦系統而要求的資料，例子包括但不限於：

- (a) 該電腦系統的實際情況和功能，包括與上下游系統的相依性；
- (b) 該電腦系統的體系結構；
- (c) 該電腦系統處理的敏感數碼資料的性質和數量；
- (d) 提供或支援該關鍵基礎設施核心功能的電腦系統網絡圖；
- (e) 提供或支援該關鍵基礎設施核心功能的電腦硬件及軟件的製造商和型號；
- (f) 為提供或支援該關鍵基礎設施核心功能而使用的外聘資訊科技或電訊服務；
- (g) 提供或支援該關鍵基礎設施核心功能的主要電腦系統的復原配置；以及
- (h) 闡述該電腦系統的設計和運作的文件記錄，例如圖表和系統功能描述。

## **5. 關鍵基礎設施營運者的責任 — 第 1 分部**

### **5.1 在香港持續設有辦事處的責任**

5.1.1 就《條例》第 19(1)及(3)條而言，在香港的辦事處除了應用作可給予通知或送予其他文件的地點，亦應用作營運者的僱員或代表進行業務活動的地點，該等活動的例子包括管理日常運作、作出業務決定、與持份者互動或保存業務記錄。就辦事處地址及辦事處地址相關變更作出通知的表格範本載於附件 A。

### **5.2 就營運者變更作出通知的責任**

5.2.1 就《條例》第 20(1)條而言，營運者變更的例子包括：

- (a) 關鍵基礎設施的日常運作、管理或維護由現有營運者改為另一個營運者負責；
- (b) 現有營運者停止提供關鍵基礎設施的日常運作、管理或維護；  
或
- (c) 現有營運者因被合併、收購及其他情況而不再存在。

就營運者變更作出通知的表格範本載於附件 B。

### **5.3 設立和持續設有電腦系統安全管理單位的責任**

5.3.1 就《條例》第 21(1)條而言，電腦系統安全管理單位無須常駐在香港。

5.3.2 就《條例》第 21(4)條而言，監管電腦系統安全管理單位的僱員無須常駐在香港。此外，就電腦系統安全擁有足夠專業知識一般指因應其關鍵電腦系統風險，具備合適專業資格(例如註冊信息安全專業人員(CISP)、註冊信息系統審計師(CISA)、註冊信息安全經理(CISM)、註冊資訊系統安全師(CISSP)等)和專業經驗以有效履行職責。就委任監管電腦系統安全管理單位的僱員作出通知的表格範本載於附件 C。

5.3.3 就《條例》第 21(6)條而言，雖然變更日期與履職日期有關，但營運者在簽署僱傭合約後，應盡快使用附件 C 所載的表格範本，主動向規管當局作出通知。

## 6. 關鍵基礎設施營運者的責任 — 第 2 分部

### 6.1 就某些電腦系統的重大變化作出通知的責任

6.1.1 就《條例》第 22(1)條而言，“該事件發生當日”一般指在生產環境部署某一項變化的時候。如有關變化分階段部署，“該事件發生當日”應適用於部署變化的每個階段。營運者可選擇在部署變化的首階段，就所有其後的變化向規管當局一併作出通知。

6.1.2 就《條例》第 22(3)條而言，營運者應通報任何重大變化。重大變化一般指可合理預期對某關鍵電腦系統的電腦系統安全風險或有關關鍵基礎設施核心功能的風險構成重大影響的變化。關鍵電腦系統發生重大變化的情況例子如下：

- (a) 平台遷移；
- (b) 伺服器虛擬化；
- (c) 核心組件(如資料庫)的主要版本升級；
- (d) 運算平台或硬件變化；
- (e) 應用系統重新設計；
- (f) 重大程式碼變化；
- (g) 支援關鍵電腦系統的基礎設施變化；
- (h) 與外部系統或網絡的整合或相互依賴的轉變；
- (i) 任務或主要功能改變，令系統的操作範圍、原來用途或保安、資源或功能要求有所變更；
- (j) 任何系統修改，以致從根本上改變關鍵電腦系統特徵或性質；  
或
- (k) 營運者知悉的由雲端服務供應商維護的關鍵電腦系統組件的重大變化。

就重大變化作出通知的表格範本載於附件 D。

## 6.2 提交和實施電腦系統安全管理計劃的責任

- 6.2.1 電腦系統安全管理計劃應涵蓋根據《條例》附表 3 所列明為保障關鍵電腦系統的電腦系統安全而履行法定責任所需的一切事宜。有關附表 3 第 1 部列明的事宜，本守則第 6.2.5 至 6.2.27、6.3、6.4 及 6.5 節提供相關實務指示，營運者應遵從這些規定。
- 6.2.2 營運者應確保向規管當局提交的電腦系統安全管理計劃及其後任何變更(聯絡點或編輯更新除外)已獲董事會、董事會授權的專項小組委員會或負責監察有關關鍵基礎設施運作的高層管理人員(例如行政總裁、營運總監或同級人員)通過。有關計劃應在關鍵電腦系統發生重大變化時審視，並且至少每兩年審視一次，以確保其有效和合宜。
- 6.2.3 若電腦系統安全管理計劃包含一系列政策、標準和指引，營運者應就每項適用的規定，將計劃的相關章節的每項適用規定與本守則第 6.2.5 至 6.2.27、6.3、6.4 及 6.5 節的規定作出清晰的相互參照。
- 6.2.4 營運者如未能履行第 6.2.5 至 6.2.27、6.3、6.4 及 6.5 節訂明的任何規定，應實施效果相若的替代保安控制措施。這些措施應記錄在電腦系統安全管理計劃內，當中應詳述措施如何有效減低相關風險。
- 6.2.5 電腦系統安全管理單位
- (a) 營運者應就關鍵電腦系統的電腦系統安全制定管理架構，闡明有關的實施、運作及管理事宜。
  - (b) 單位的組織架構和決策架構，以及每名相關人員的角色及責任，均應清楚闡述和記錄。
- 6.2.6 政策、標準及指引
- (a) 營運者應根據業務需要和安全要求，制定和執行電腦系統安全政策、標準及指引，以提供保護關鍵電腦系統的管理指示和支援。
  - (b) 營運者擬備其政策、標準及指引時，應考慮其自身的安全要求、本守則、法定機構為個別界別訂立的相關要求，以及適用的國家及國際電腦系統安全標準。

- (c) 營運者應建立政策、標準及指引的發布機制，確保參與關鍵電腦系統運作的所有人員均可方便閱覽。

#### 6.2.7 電腦系統安全風險管理方法

- (a) 營運者應制定安全風險管理方法，簡述如何識別、評估、減低和監控與營運者及其關鍵電腦系統相關的電腦系統安全風險。該套方法應提供系統化和結構化的風險管理方式。
- (b) 營運者制定電腦系統安全風險管理方法時，應參照國家或國際認可的電腦系統安全風險管理方法和標準，例如 GB/T 31722、ISO/IEC 27005 和 IEC 62443-3-2。就此過程，營運者亦可參考由數字政策辦公室（“數字辦”）編製的《資訊科技保安風險管理實務指引》。

#### 6.2.8 設計層面保安

- (a) 營運者應在可行情況下盡量採納“設計層面保安”原則，以確保在關鍵電腦系統由開展至設計、推行、部署、運作到最終棄用的整個生命週期中，保安是重要的一環。若因受制於舊有架構或現成設計而未能在關鍵電腦系統全面採納“設計層面保安”原則，營運者應在關鍵電腦系統進行主要升級或改良時，引入這項原則。就此過程，營運者可參考由數字辦編製的《設計層面保安實務指引》。

#### 6.2.9 資產管理

- (a) 營運者應制定和記錄關鍵電腦系統的識別方式、篩選條件和定期審視機制。
- (b) 營運者應確保能妥善持有、保管和備存關鍵電腦系統及其相關資產(包括硬件資產[名稱、製造商、型號、固件版本等]、軟件資產[名稱、發行商、版本等]、應用系統、有效保用證、服務協議和法律／合約文件)的最新清單(包括系統和資產的描述、主要功能、實體／邏輯位置，以及持有人或主要人員)，並按“有需要知道”原則限制存取。
- (c) 營運者應定期審視關鍵電腦系統及其相關資產的清單，或實施自動更新清單機制，確保清單準確。

#### 6.2.10 接達控制及帳戶管理

- (a) 營運者應防止關鍵電腦系統被未獲授權接達，並確保只有獲授權人員可接達關鍵電腦系統。

- (b) 營運者向用戶分配關鍵電腦系統的資源和權限時，應貫徹最小權限原則。
- (c) 營運者應制定和記錄審批、授予和管理用戶(包括供應商[如有者])接達關鍵電腦系統的程序。有關程序應包括但不限於用戶註冊、註銷用戶註冊、傳送密碼和重設密碼。
- (d) 用戶權限及數據接達權限應予以明確界定，並每年審視至少一次，批准和審視接達權限的記錄亦應予以備存。
- (e) 所有不再需要的用戶權限及數據接達權限應予以註銷。
- (f) 每個用戶名稱應只限識別一個用戶，除非有絕對需要，否則不得批准使用共用或群組用戶名稱。
- (g) 應根據關鍵電腦系統的電腦系統安全風險，為每次接達建立相應的授權和認證措施。在合適情況下，應採用多重認證。
- (h) 關鍵電腦系統用戶獲認證使用關鍵電腦系統前，系統應向用戶展示有關使用系統的通知訊息(以系統通知或實體告示的形式)，提供適當的安全通知(例如系統使用情況可能會被記錄和監控、禁止未獲授權使用系統等)。

#### 6.2.11 特權接達管理

- (a) 營運者應確保關鍵電腦系統的特權接達權限必須在獲授權的情況下才予以提供。
- (b) 營運者應將特別接達權限授予有別於常規業務活動所使用的用戶名稱。營運者亦可就臨時提升特權給予即時特權接達，但仍須遵照正式審批及控制程序。
- (c) 營運者應確保人員只能接達所需的特定管理功能，藉此貫徹管理帳戶最小權限原則，並減低在特權帳戶遭入侵時所造成的影響。
- (d) 營運者應只允許配備保安控制措施的獲授權裝置接達特權帳戶，以確保特權操作得以妥善管理，並只限獲授權人員執行。

#### 6.2.12 加密方法

- (a) 營運者應確保適當和有效地使用加密方法，以保障關鍵電腦系統的電腦系統安全。營運者亦可參閱第 6.5.4 節，了解運營科技系統的替代保安控制措施。

- (b) 營運者應確保密碼匙的整個生命周期得到妥善管理，包括密碼匙的產生、儲存、存檔、獲取、分發、退役及銷毀。
- (c) 用作處理敏感數碼資料的密碼匙應與相應的經加密資料分開儲存和分發。
- (d) 有關加密算法及方法的使用，營運者應參照最新的國家或國際電腦系統安全標準。

#### 6.2.13 密碼管理

- (a) 營運者應為所有關鍵電腦系統帳戶(包括任何供應商帳戶)制定和實施密碼政策。政策應訂明最短密碼長度、包含字母數字字符及特殊字符的複雜程度規定、密碼的最長有效期、連續嘗試登入失敗的次數上限，以及重用先前密碼的限制。營運者亦可參閱第 6.5.5 節，了解運營科技系統的替代保安控制措施。
- (b) 任何電腦系統啓用前，所有由供應商提供的預設密碼均應予以更改。
- (c) 如密碼已外泄或懷疑已外泄，或曾被供應商用作維修及支援用途，應立即予以更改。

#### 6.2.14 實體保安

- (a) 營運者應防止放置關鍵電腦系統的設施在未獲授權的情況下被實體接達及干擾。
- (b) 放置關鍵電腦系統的數據中心、電腦室及場地應實施實體保安措施，以防範未經授權的實體進入。
- (c) 營運者應保護關鍵電腦系統的電力及通訊電纜免受損毀或被截取。
- (d) 營運者應為關鍵電腦系統的電力及通訊電纜加上標籤，以作實體識別和檢查。
- (e) 營運者應部署多重監控系統，例如閉路電視、偵測器、入侵警報器或保安人員，以持續偵測及警報放置關鍵電腦系統的場地有否出現未獲授權的進入或可疑行為。營運者亦應保護已部署的監控系統，免受未獲授權的接達或阻礙。
- (f) 獲授權進入放置或儲存電腦設備和數據的數據中心、電腦室及支援關鍵電腦系統操作的場地的人員清單，應持續更新和定期審視。凡用作進入這些地點的鑰匙、匙卡、密碼等的實體安全應得到保障，並受到清晰明確及嚴格執行的保安程序所規管。

- (g) 所有進入放置關鍵電腦系統的數據中心、電腦室及場地的訪客，應時刻受獲授權人員監視。訪客出入記錄亦應妥善備存，以作審核及調查電腦系統安全事故用途。

#### 6.2.15 配置管理及系統強化

- (a) 營運者應防止任何未獲授權的關鍵電腦系統配置，並確保關鍵電腦系統符合所要求的保安配置。
- (b) 營運者應建立和維持關鍵電腦系統的基本配置，並定期和在關鍵電腦系統發生重大變化時進行審視。
- (c) 進行系統強化時，應採取最少功能和最小權限兩項原則。

#### 6.2.16 變更管理

- (a) 關鍵電腦系統的變更應受到嚴格的變更管理控制措施，包括但不限於變更策劃、影響評估、變更授權、向有關各方傳達變更、變更測試、變更實施、復原程序，以及備存變更記錄。
- (b) 營運者應設有非生產環境，以進行開發及測試(例如系統變更測試及驗收測試)。營運者亦可參閱第 6.5.6 節，了解運營科技系統的替代保安控制措施。

#### 6.2.17 修補程式管理

- (a) 營運者應及時安裝產品供應商建議的最新保安修補程式，或實施其他補償性保安措施，以保護其關鍵電腦系統免受已知保安漏洞的影響。營運者應採取風險為本的方法，為其關鍵電腦系統制定適當的修補程式管理策略。在決定修補計劃及優次時，應充分考量當保安漏洞暴露時所涉及的風險。
- (b) 營運者應為關鍵電腦系統建立完善的修補程式管理程序。修補程式管理流程應包括取得修補程式、測試、風險評估、部署及遵從要求。
- (c) 安裝保安修補程式之前，應進行妥善的風險評估及測試，以減低對關鍵電腦系統的不利影響。如運營科技系統測試修補程式並不可行，營運者亦可參閱第 6.5.6 節，了解替代保安控制措施。風險評估及測試(如有)的結果應妥善記錄。

### 6.2.18 遠程連接

- (a) 營運者應制定合適的使用政策及程序，訂明從營運者處所以外地點遠程接達關鍵電腦系統的安全要求。
- (b) 營運者應實施適當的保安措施，包括加密遠程接達通訊(例如使用虛擬私有網絡)、實施多重認證、對遠程接達施加存取限制、記錄和監察遠程接達活動，以及在不再需要授權和接達權限時予以註銷，藉此防止關鍵電腦系統及當中的數據受到未獲授權的遠程接達。
- (c) 營運者應提供專用設備以供遠程接達。若准許使用私人擁有的設備進行遠程接達，除上述(a)及(b)項所訂明外，營運者應訂立相關政策及程序、要求用戶於使用前確認知悉保安責任、支援對設備上的敏感數碼資料進行隔離與保護，並考慮啓用設備位置追蹤及遠程數據刪除。

### 6.2.19 儲存媒體

- (a) 營運者應確保儲存媒體上與提供必要服務直接相關的敏感數碼資料，須獲授權後方可披露、修改、移除及銷毀。
- (b) 營運者應關閉關鍵電腦系統中沒有操作需要的通用串列匯流排埠(USB)的支援功能。
- (c) 營運者將便攜式電腦裝置及抽取式儲存媒體連接至關鍵電腦系統之前，應進行惡意軟件掃描。
- (d) 營運者應加密在儲存媒體上儲存或處理與提供必要服務直接相關的敏感數碼資料。營運者亦可參閱第 6.5.4 節，了解運營科技系統的替代保安控制措施。
- (e) 營運者應保護用作儲存或處理與提供必要服務直接相關的敏感數碼資料的便攜式電腦裝置及抽取式儲存媒體，以免被未獲授權接達或誤用。
- (f) 營運者應在棄置或重用儲存媒體前，徹底刪除並銷毀當中與提供必要服務直接相關的敏感數碼資料，並採用適當的刪除方法(例如消磁、電子蓋寫或加密刪除)，以防止數據外泄。

#### 6.2.20 備份及復原

- (a) 營運者應定期進行備份工作，以確保關鍵電腦系統能復原遺失的資料。營運者應為其關鍵電腦系統制定備份及復原政策。備份復原測試應在不影響生產環境的情況下定期進行。營運者亦應訂立和記錄備份審查及復原測試的頻率。
- (b) 應備存本地及場外備份。場外數據備份應存放於安全且遠離主場地的地點，距離足以避免因主場地發生災難而受到影響。
- (c) 應制定適當程序儲存及處理備份媒體。該複本應為無法變更的複本，或實體上與關鍵電腦系統中斷連接，以避免備份數據在關鍵電腦系統被入侵時遭到破壞。
- (d) 備份媒體的接達應只限由獲授權人員按既定機制進行。未獲授權人士不得進入媒體儲存庫或場外儲存室。
- (e) 營運者應確保具備足夠的恢復能力，以符合關鍵電腦系統的可用性規定。

#### 6.2.21 網絡保安

- (a) 營運者應為關鍵電腦系統規劃並實施足夠的網絡保安控制措施，以防止惡意通訊接達關鍵電腦系統(例如限制可能構成拒絕服務攻擊的通訊負載)。營運者亦可參閱第 6.5.7 節，了解運營科技系統的替代保安控制措施。
- (b) 營運者應在關鍵電腦系統的關鍵節點安裝網絡入侵偵測系統或網絡入侵防禦系統。
- (c) 營運者應按可信任的程度，將其網絡劃分為分隔的網域。
- (d) 關鍵電腦系統使用的互聯網接達服務應具備以下保安功能：
  - (i) 網絡通訊接達控制，以攔截及允許互聯網規約地址或網域；
  - (ii) 通訊路由及小包過濾；以及
  - (iii) 入侵偵測及防禦，以記錄、監察、偵測及阻止攻擊。

- (e) 應謹慎規劃透過無線通訊接達關鍵電腦系統，以減低安全風險。若因運作上的需要而使用，營運者應評估相關的安全風險，並實施補償性保安措施，包括適當的認證、加密、用戶層網絡接達控制及充足的備存記錄。

#### 6.2.22 應用系統保安

- (a) 營運者應確保關鍵電腦系統在整個發展周期的電腦系統安全。
- (b) 關鍵電腦系統只應載入獲授權的應用軟件。
- (c) 營運者應在關鍵電腦系統的軟件開發過程中建立並應用保安編碼作業模式(例如輸入驗證、輸出編碼、認證及密碼管理、對話管理、誤差處理及記錄)，以防範、偵測和移除程式碼中任何潛在的電腦系統安全保安漏洞。
- (d) 營運者應在關鍵電腦系統正式投入服務前，以結構化及有組織的方式進行測試，以確保應用系統能達到設計目的，並消除潛在的保安漏洞。測試範圍應包括保安功能(用戶身份驗證、接達限制等)、保安編碼(如輸入驗證、工作階段管理等編碼作業模式)及保安配置。
- (e) 營運者應保護源碼免被未獲授權接達(例如使用配置管理工具)。
- (f) 用作測試的數據應予以審慎選擇、保護及控制，尤其是生產數據應獲授權方可在測試環境中使用。如在測試環境中使用敏感數碼資料，應予以移除或遮蔽。

#### 6.2.23 記錄管理

- (a) 營運者應記錄和識別涉及關鍵電腦系統並可能導致電腦系統安全事故的事件。
- (b) 營運者應制定政策，記錄關鍵電腦系統的活動，並保存有關記錄，以便調查電腦系統安全事故。有關政策的要求應包括但不限於記錄：
  - (i) 登入的嘗試；
  - (ii) 更改密碼的嘗試；
  - (iii) 接達關鍵檔案(例如軟件配置檔案、密碼和密碼匙檔案)的嘗試；
  - (iv) 特別權限的運用(例如新增和刪除用戶帳戶)；

- (v) 用戶接達權限的變更；
  - (vi) 對審核政策的修改；以及
  - (vii) 啓用或停用保護系統，例如抗惡意程式系統和入侵偵測系統。
- (c) 記錄應保留至少六個月，亦應確保記錄安全，以免被刪除或竄改，並只可由獲授權人士閱覽。
- (d) 如第 6.2.23(b)或 6.2.23(c)條所規定的要求因某些運營科技關鍵電腦系統技術限制而無法遵從，營運者應記錄相關事宜及理據。
- (e) 任何保留的記錄應提供足夠的資料，作為對保安措施的成效及遵從情況進行全面審核的憑證。
- (f) 營運者應訂立程序，透過預定的規則識別例外情況，並應使用合適的程式或工具協助分析有關記錄。所有懷疑因電腦系統安全事故而引發的事件應予以記錄和監察。
- (g) 營運者應將所有關鍵電腦系統組件的內部時鐘與主要時間來源同步，以確保能夠在系統之間準確對應記錄事件。

#### 6.2.24 雲端運算保安

- (a) 營運者應確保採用雲端技術的關鍵電腦系統的電腦系統安全，不論雲端系統位處何地。
- (b) 營運者應制定和記錄關鍵電腦系統的政策，以識別、評估、檢討和應對與採用雲端運算有關的電腦系統安全風險，並應妥善記錄如何減低或應對已識別的風險。
- (c) 營運者應明確制定和實施雲端服務供應商與營運者對關鍵電腦系統的電腦系統安全的共同責任。
- (d) 營運者應視關鍵電腦系統的外部雲端服務為供應鏈的一部分，並遵守本守則第 6.2.25 節“供應鏈管理”下訂明的安全要求。
- (e) 營運者應確保雲端服務供應商在關鍵電腦系統基礎設施的設計、開發、部署和配置過程中，對關鍵基礎設施的數據提供適當保護，並把關鍵基礎設施的數據與其他客戶環境適當隔離。

## 6.2.25 供應鏈管理

- (a) 營運者與供應商之間應維持雙方同意的關鍵電腦系統安全水平，確保所有供應商遵從一套已制定的電腦系統安全要求。
- (b) 營運者應制定和確定流程和程序，以管理產品和服務供應鏈中的電腦系統安全風險。有關流程應包括識別和記錄對關鍵電腦系統運作不可或缺的必要供應鏈組件。
- (c) 營運者應視乎經評估的供應鏈風險及地緣政治風險水平，在合適情況下採用來自不同源頭及開放源碼產品的關鍵電腦系統組件。這有助避免過分依賴單一或數個供應商，並更有效管理因某些資訊科技及運營科技產品及服務可能受出口管制而帶來的風險。
- (d) 就供應商的服務或設施而言，應根據數據敏感度和業務要求，記錄和實施相應的保安措施、服務水平期望和管理要求，並應制定和協定供應商的安全責任。舉例而言，與外聘服務供應商簽訂的合約應要求定期提交安全報告，並訂明責任如數據加密、完善的接達控制及備存記錄等。這些要求有助營運者進行盡職審查，評估有能力的供應商，並透過持續監察，證明已盡最大的努力。有關外聘服務供應商責任的合約條款範本載於附件 H，以供參考。
- (e) 營運者應保留審核和監察合規的權利，以證實外聘服務供應商已對其關鍵電腦系統實施足夠的控制措施。另外，營運者應保留權利定期索取安全審核報告(例如《香港鑒證業務準則》第 3000 號鑒證報告、系統與組織控制措施(SOC) 2 第二類報告)，以確定外聘服務供應商實施的措施達到滿意程度。
- (f) 營運者應確保外聘服務供應商的服務期屆滿或終止時，或在營運者要求時，服務或設施內的所有敏感數碼資料會被刪除。
- (g) 營運者應與外聘服務供應商簽訂有關保密及不可向外披露資料的協議，以保護供應商可接達的敏感數碼資料。這些協議應予以妥善管理，並在出現任何影響安全要求的變更時予以審視。

## 6.2.26 監察及偵測

- (a) 營運者應建立機制，監察關鍵電腦系統的持續運作狀況，以偵測異常情況及潛在的電腦系統安全事故。該機制應界定正常行為的基準，並監察偏離該基準的情況。

- (b) 營運者應採用端點保安解決方案(包括但不限於個人防火牆、抗惡意程式軟件、端點偵測與回應解決方案)，以提升對電腦系統安全保安漏洞及威脅的了解和偵測能力，並迅速應對潛在的進階攻擊。營運者亦可參閱第 6.5.8 節，了解運營科技系統的替代保安控制措施。
- (c) 營運者應實施相關程序，以授權、控制及監察在關鍵電腦系統內使用的流動程式碼(例如 JavaScript、VBScript、ActiveX 控制項、Microsoft Office 巨集)及批次檔。
- (d) 應制定相關程序和流程，以確保 24 小時全天候監察和及時應對監察系統偵測到的任何安全事故(包括但不限於憑證外泄、應用系統保安漏洞及系統錯誤配置)。
- (e) 營運者應建立機制和流程，以收集和分析與電腦系統安全威脅有關的資訊，從而得出威脅情報。威脅情報可包括有關不斷變化的威脅形勢概括資訊、攻擊者手法、工具及技術詳情，以及每宗攻擊的具體內容。營運者應 24 小時全天候監察威脅情報，用作評估對關鍵電腦系統的威脅程度及潛在影響，並採取適當的緩解措施。
- (f) 營運者應定期審視監察機制，以確保該機制能因應關鍵電腦系統的性質及持續技術發展維持有效。

#### 6.2.27 電腦系統安全培訓

- (a) 營運者應制定培訓計劃，定期向參與關鍵電腦系統操作的所有人員提供具針對性及有系統的培訓，提升人員的安全意識，以履行電腦系統安全的相關責任。電腦系統安全培訓計劃應包括但不限於以下內容：
  - (i) 計劃目標：營運者應就培訓計劃制定目標，該等目標應與營運者整體的電腦系統安全策略一致。

- (ii) 對象：營運者應識別須參與培訓活動的特定群組或角色，並應根據不同的技術專業水平、工作職能和需求，制定相應的培訓內容。
  - (iii) 培訓方式：培訓教材及內容的設計應配合目標及對象，亦應根據營運者的風險、資源及對象的需要，採用適當的培訓方法。培訓方法可包括演示、影片、互動模組、實踐練習及案例研究。營運者可安排內部培訓人員或委聘供應商提供培訓服務。
  - (iv) 評估培訓活動成效：營運者應審視培訓活動的成效，同時可進行評估，以確保人員了解有關電腦系統安全的要求及責任，例如透過培訓後測試、意見調查、模擬練習，以及觀察行為變化或安全事故數目等方法，評估人員的知識增長、行為變化及參與者滿意度。
  - (v) 定期審視及更新：營運者應定期審視及更新培訓計劃，以反映不斷變化的威脅形勢、新興技術，以及規例和遵從要求方面的改變。此外，營運者應善用調查結果，找出須改善的地方，從而調整或微調培訓計劃。
- (b) 營運者可透過合約協議，要求參與關鍵電腦系統運作的外聘服務供應商向其人員提供培訓。

## 6.3 進行電腦系統安全風險評估的責任

- 6.3.1 就《條例》第 24(1)條而言，營運者進行電腦系統安全風險評估時，應參考國家或國際認可的電腦系統安全風險評估方法及標準，例如 GB/T 22080、GB/T 31722、ISO/IEC 27001、ISO/IEC 27005、IEC 62443-3-2、NIST 800-30 和 ISO/IEC 42001。就此過程，營運者亦可參考由數字辦編製的《資訊科技保安風險管理實務指引》及《保安風險評估及審計實務指引》(ISPG-SM01)。
- 6.3.2 電腦系統安全風險評估應包括但不限於關鍵電腦系統的所有應用系統、主機及網絡裝置。
- 6.3.3 在進行電腦系統安全風險評估後，營運者應記錄關鍵電腦系統的已識別風險，包括可能性及嚴重性、關鍵電腦系統可承受的風險程度，以及減低風險所需的措施及監測。
- 6.3.4 電腦系統安全風險評估應包含保安漏洞評估及滲透測試，其中須識別保安及控制措施的弱點。營運者亦可參閱第 6.5.9 節，了解運營科技系統的替代保安控制措施。
- 6.3.5 電腦系統安全風險評估的保安漏洞評估應包括多項保安漏洞識別活動，包括但不限於保安漏洞掃描、源碼審查及配置審查，以識別潛在的保安漏洞。保安漏洞評估應在具備適當知識、相關經驗和合適專業資格(例如 CISP、CISA、CISM、CISSP 等)的合資格安全專家監督下進行。

6.3.6 電腦系統安全風險評估的滲透測試應從潛在攻擊者的角度或基於威脅情報進行，並可涉及主動利用關鍵電腦系統可能存在的漏洞。測試應包括但不限於網絡保安、系統軟件保安、客戶端應用系統程式保安及伺服器端應用系統保安的範疇。滲透測試應由具備適當知識、相關經驗和合適專業資格的測試人員進行。專業資格的例子包括但不限於：

認證機構	認證
中國信息安全測評中心	註冊信息安全專業人員 – 滲透測試工程師
	註冊信息安全專業人員 – 滲透測試專家
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 滲透測試員
	GIAC Exploit Research and Advanced Penetration Tester
	GIAC Web Application Penetration Tester
國際信息系統審計協會	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
香港銀行學會	模擬網絡攻擊專業認證 – Certified Simulated Attack Manager
	模擬網絡攻擊專業認證 – Certified Simulated Attack Specialist
	模擬網絡攻擊專業認證 – Certified Infrastructure Tester
	模擬網絡攻擊專業認證 – Certified Web Applications Tester
	模擬網絡攻擊專業認證 – Certified Web Applications Tester

6.3.7 電腦系統安全風險評估報告應包括以下章節(如適用)：

- (a) 引言／背景資料；
- (b) 摘要；
- (c) 評估範圍、目標、方法、時間範圍，以及對報告涵蓋和不涵蓋的內容所作的假設；
- (d) 現時環境或現行系統描述(包括網絡圖)；
- (e) 保安要求；
- (f) 參與電腦系統安全風險評估的人員；
- (g) 結果和建議摘要；
- (h) 風險分析結果，包括已識別資產、威脅、保安漏洞及其影響、可能性和風險水平，並提供適當理據；
- (i) 建議保護措施和成本效益分析(如有多於一個選項)；
- (j) 結論；以及
- (k) 附件，包括已完成的保安漏洞評估報告、滲透測試結果、所涵蓋的資產清單<sup>1</sup>，以及資產估價結果。

---

<sup>1</sup> 詳情按照本守則第 6.2.9(b)節。

## 6.4 安排進行電腦系統安全審核的責任

- 6.4.1 電腦系統安全審核應評估營運者的電腦系統安全管理計劃有否實行，以及有關保安控制和措施是否遵從該電腦系統安全管理計劃。
- 6.4.2 營運者應安排獨立的審核員，為其關鍵電腦系統進行電腦系統安全審核。該審核員應具備適當知識、相關經驗和合適專業資格(例如 CISP、CISA、CISM、CISSP 等)。
- 6.4.3 在審核過程中，甄選審核員和進行審核的工作應客觀持平。審核員不得審核自己有份參與的工作。舉例來說，營運者應聘請的審核員(內部或外聘)均沒有參與設計或維護電腦系統保安控制措施。
- 6.4.4 進行電腦系統安全審核時，應參照國家或國際認可的方法和標準，或電腦系統安全的良好作業模式<sup>2</sup>。相關方法概要載於附件 G，以供參考。
- 6.4.5 電腦系統安全審核應用作核實為關鍵電腦系統採取的現行保障措施有否妥善實行，包括電腦系統安全管理計劃有否實行，以及這些計劃有否遵循本守則或其他方法。審核工作也應基於此核實結果，評估關鍵電腦系統的整體電腦系統安全狀況。

---

<sup>2</sup> 例如 GB/T 19011、GB/T 28450、ISO 19011 及 ISO/IEC 27007。數字政策辦公室的《保安風險評估及審計實務指引》(ISPG-SM01)詳述安全審核的方法和標準，也可作參考用途。

## 6.5 運營科技的保安措施

6.5.1 營運者應根據關鍵程度，以實體或邏輯方式(例如不同電腦、網址、操作系統實例)，把關鍵電腦系統的數據、應用程式和服務(例如工程工作站、安全系統)分為不同分區，以便實施分區模型。

6.5.2 營運者應防止關鍵電腦系統接收從系統以外的途徑(例如社交媒體或電郵)、並為一般目的發送的人對人訊息。

6.5.3 第 6.5.4 至 6.5.9 節旨在為作為運營科技系統而未能達到第 6.2.5 至 6.2.27、6.3 及 6.4 節訂明的相應安全要求的關鍵電腦系統，提供替代措施。

### 6.5.4 加密方法

(a) 作為第 6.2.12(a)及 6.2.19(d)節的替代措施，營運者應制定和實施政策及程序，使用加密方法保障關鍵電腦系統的電腦系統安全，當中考慮以下因素：

- (i) 對提供必要服務的影響；
- (ii) 對傳輸中的敏感數碼資料的保護(例如加密經網絡傳輸的數據)；
- (iii) 數據可見性對系統監察的影響(例如異常情況檢測工具不能分析加密數據)；以及
- (iv) 運作困難(例如加密造成的通訊延遲)。

### 6.5.5 密碼管理

(a) 作為第 6.2.13(a)條的替代措施，營運者應為採用密碼認證方法的關鍵電腦系統，制定和實施符合關鍵電腦系統能力的密碼政策。密碼政策應訂明：

- (i) 最短密碼長度；
- (ii) 密碼複雜程度規定；
- (iii) 密碼的最長有效期；
- (iv) 連續嘗試登入失敗的次數上限；以及
- (v) 重用先前密碼的限制。

如實施密碼政策不利於運營科技系統的正常運作，營運者應採取補償性保安控制措施(例如實體隔離或網絡隔離)，並記錄尚未受密碼保護的組件。

#### 6.5.6 變更管理和修補程式管理

- (a) 作為第 6.2.16(b)及 6.2.17(c)條的替代措施，營運者應制定和實政策及程序，在缺乏非生產環境的情況下進行系統變更測試(例如修補程式)，當中考慮以下因素：
  - (i) 在對關鍵電腦系統部署變更及修補程式前，採納產品供應商及其他相關各方匯報的測試結果和問題；以及
  - (ii) 訂立謹慎的部署方法，在生產環境中測試變更和修補程式(例如先在某限定的子系統部署變更，其後再逐步推進，或在內置復原能力的組件部署變更以進行測試)。

#### 6.5.7 網絡保安

- (a) 作為第 6.2.21(a)條的替代措施，營運者應為關鍵電腦系統規劃並實施足夠的網絡保安控制措施，以偵測及管理惡意通訊接達關鍵電腦系統。

#### 6.5.8 監察及偵測

- (a) 作為第 6.2.26(b)節的替代措施，營運者應制定和實政策及程序，保護端點裝置免受惡意軟件入侵，當中考慮以下因素：
  - (i) 採用抗惡意程式軟件和軟件白名單；
  - (ii) 對運營科技系統正常運作的影響；
  - (iii) 部署抗惡意程式軟件和識別碼前進行測試(例如在離線系統測試配置)；
  - (iv) 抗惡意程式軟件用以掃描和更新識別碼的時機和資源；
  - (v) 識別為避免影響關鍵電腦系統而未有進行惡意軟件掃描的檔案(例如在生產過程中不掃描個別檔案)；以及
  - (vi) 為需要持續更新識別碼的關鍵電腦系統組件採用冗餘設計，令組件運作不受影響。

營運者亦應記錄缺乏抗惡意程式軟件保護的關鍵電腦系統組件、不為這些組件提供保護的理據，以及用於這些組件的補償性保安控制措施。

#### 6.5.9 電腦系統安全風險評估

- (a) 作為第 6.3.4 節的替代措施，營運者應制定和實行政策及程序，識別關鍵電腦系統的保安漏洞。營運者在生產環境進行保安漏洞評估和滲透測試前，應先在離線環境進行評估，以了解兩者對關鍵電腦系統的影響。如進行保安漏洞評估或滲透測試不利於運營科技系統的正常運作，營運者應利用替代的保安漏洞識別活動（例如在關鍵電腦系統的關鍵周邊節點進行針對性的漏洞掃描或滲透測試），以尋找關鍵電腦系統的電腦系統安全弱點。營運者亦應記錄任何可豁免評估的情況，並提供理據。

## 7. 關鍵基礎設施營運者的責任 — 第 3 分部

### 7.1 參與電腦系統安全演習的責任

7.1.1 營運者收到專員的書面通知後，會獲給予合理時間為參與電腦系統安全演習(“演習”)作準備。演習旨在測試關鍵基礎設施在應對電腦系統安全事故上的準備狀態，內容包括：

- (a) 評估營運者的應急計劃是否合宜和有效；以及
- (b) 評估參與人員在應對電腦系統安全事故時，對其角色及責任的認識。

7.1.2 營運者會每兩年不多於一次獲專員通知參與演習。

7.1.3 演習的主題、範圍和情境會由專員訂出。演習或會以桌上演練、功能性演習、模擬攻擊，或專員認為合適的任何其他方式進行。演習不會涉及實際使用關鍵電腦系統或其生產環境，以免干擾營運者的業務活動。

7.1.4 演習可涉及多個相同或不同界別的營運者及多個政府單位，以測試在發生嚴重影響社會或經濟的電腦系統安全事故時互相協調和恢復公共秩序的情況。

7.1.5 在應急計劃中，下列營運者的成員應視乎適當情況參與演習：

- (a) 在應急計劃中獲指派角色的管理人員；
- (b) 電腦系統安全管理單位；
- (c) 應急小組；
- (d) 公共關係或企業傳訊人員；以及
- (e) 在演習情境中及營運者認為有需要參與的其他人員，例如網絡安全保險公司。

7.1.6 營運者的代表應出席由專員舉行的簡介會和匯報會。

7.1.7 在演習表現方面，營運者或會收到專員的意見，就應對電腦系統安全事故提出可持續改善的地方。營運者應針對專員提出的建議，採取補救行動。

## 7.2 提交和實行應急計劃的責任

7.2.1 營運者應制定應急計劃，並為針對關鍵電腦系統的電腦系統安全事故訂立應變程序。計劃範圍應包括以下內容：

- (a) 事故管理；以及
- (b) 業務持續運作管理和災後復原。

7.2.2 關鍵基礎設施營運者應確保向專員提交的應急計劃及其後任何變更(聯絡人或編輯更新除外)已獲董事會、董事會授權的專責小組委員會或負責監察有關關鍵基礎設施運作的高級管理人員(例如行政總裁、營運總監或同級人員)通過。有關計劃應在關鍵電腦系統發生重大變化時審視，並且至少每兩年審視一次，以確保其有效和合宜。

7.2.3 事故管理

- (a) 事故管理計劃確保事故應變行動能以有序、迅速和有效的方式實行，從而把電腦系統安全事故(“事故”)可能造成的損毀減至最少。該計劃應包括以下內容：
  - (i) 應急小組的架構，包括各成員在處理事故時的相應角色、責任及聯絡資料。高級管理人員的角色亦應予以訂明；
  - (ii) 《條例》所訂明的事務通報規定；
  - (iii) 啟動計劃及調動應急小組的基本準則；
  - (iv) 與內部及外部持份者(包括僱員、客戶及公眾)的溝通計劃，包括溝通事項、時間、方式及對象；以及
  - (v) 應對手冊涵蓋下列事項的處理程序：
    - (1) 控制事故以防止進一步的損害；
    - (2) 處理數碼證據，包括證據的識別、收集、獲取和保存證據及證據鏈；
    - (3) 調查事故成因及影響；
    - (4) 記錄事故應對過程，包括事故詳情、已採取的行動及所作出的決定；以及
    - (5) 進行事故後的檢討。

- (b) 營運者應提供實行事故管理計劃所需的資源。
- (c) 營運者應確保應急小組所有成員均熟悉其自身及其他小組成員在計劃中所訂定的角色及責任。營運者亦應為所有成員提供培訓，以確保其具備履行獲指派職務的能力。
- (d) 營運者應就非辦公時間內發生的電腦安全相關緊急事故委任至少兩名聯絡人。在發生緊急事故時，聯絡人應與專員保持聯繫，並能及時處理安全事故或向負責人員轉達安全訊息。營運者應向專員提供該等聯絡人的聯絡資料。
- (e) 營運者應確保設有多種通訊渠道(例如電話、電郵)，就事故與持份者作出有效溝通。
- (f) 營運者在平衡及時復原系統與處理數碼證據兩者的需要時，應優先處理對業務運作造成影響、須迅速控制損害或即時復原系統的事故；否則，應預留更多時間進行證據收集工作。
- (g) 營運者應善用自動化及編排技術，加快事故應變及鑑證流程，例如採用自動日誌收集及編排復原流程。此舉並不排除採用“人機協作”方法或其他適當方式支援事故應變及鑑證流程。
- (h) 營運者應聘用具備事故應變及法理鑑證能力的人員，協助收集數碼證據及調查事故。
- (i) 事故後檢討應納入所汲取的經驗，以改善日後的應變及預防措施，內容包括：
  - (i) 事故的事實及成因；
  - (ii) 現行管治、風險管理及合規方面導致事故發生的不足之處及其影響程度；
  - (iii) 實行應急計劃的成效及效率；以及
  - (iv) 建議的改善措施。

#### 7.2.4 業務持續運作管理及災後復原計劃

- (a) 業務持續運作管理着重讓營運者在發生電腦安全事故導致服務受干擾期間，持續維持必要運作的能力。
- (b) 業務持續運作管理計劃須包括以下各項：
  - (i) 擬達到的業務持續運作目標；
  - (ii) 關鍵電腦系統的業務影響分析，以找最大可容忍停止運作時間、復原時間目標、復原點目標和最低服務水平(如適用)；
  - (iii) 恢復相關業務程序所需的資源；
  - (iv) 確保必要服務得以持續運作的政策及程序；
  - (v) 實行計劃的管理層和人員的角色及責任；
  - (vi) 培訓和測試，以確保負責的僱員熟悉有關計劃，並認識業務持續運作政策；以及
  - (vii) 當關鍵電腦系統出現重大變化時進行評估和審視，以確保計劃行之有效。
- (c) 災後復原計劃着重在關鍵電腦系統服務受嚴重干擾時得以有效復原，從而確保與關鍵電腦系統有關連的業務運作具備復原能力。
- (d) 除下文(ii)及(iii)項可能不適用於運營科技系統外，災後復原計劃須包括以下各項：
  - (i) 配合業務持續運作目標的復原策略；
  - (ii) 備份政策及程序，當中須考慮替代場地的地點應與主場地保持充足距離，以免因主場地發生災難而受到影響，並確保備份資料受到保護；
  - (iii) 在替代場地的復原程序，包括在主場地復原後恢復資料的計劃(如適用)；
  - (iv) 恆常測試備份媒體和電訊服務；以及
  - (v) 當關鍵電腦系統出現重大變化時進行的評估和審視，以確保計劃行之有效。

### 7.3 就電腦系統安全事故作出通知的責任

7.3.1 營運者就電腦系統安全事故通知專員的目的，是要讓專員能夠評估事故對一個或多個界別持續提供必要服務，或對維持香港的關鍵社會或經濟活動所造成的整體影響，並採取適當的補救措施，以遏止有關影響擴散至其他界別。

7.3.2 電腦系統安全事故必須涉及在無合法權限下的接達或其他行為，並對相關關鍵電腦系統構成實際不良影響。因純技術故障、天災、大規模停電、已被偵測和及時移除或隔離的電腦系統安全威脅，或因人為錯誤而導致個人資料外泄所引致的事件，均不構成電腦系統安全事故。

7.3.3 電腦系統安全事故的例子包括但不限於：

- (a) 大規模或高流量的分布式阻斷服務攻擊，導致必要服務的質素下降，或接獲勒索訊息的勒索式拒絕服務攻擊；
- (b) 導致必要服務暫停或出現數據外泄跡象的勒索軟件攻擊；
- (c) 因感染惡意軟件或攻擊者利用保安漏洞而導致關鍵電腦系統與外部產生非預期的連接；
- (d) 僱員接達關鍵電腦系統中的敏感數碼資料，並惡意泄露該等資料，或惡意錯誤配置關鍵電腦系統的接達權限；
- (e) 關鍵電腦系統的配置或資料被惡意負載或編碼修改；
- (f) 僱員濫用其職權干擾關鍵電腦系統的運作；以及
- (g) 任何對密碼匙管理裝置的擅自改動，以致妨礙關鍵電腦系統的正常運作。

7.3.4 嚴重電腦系統安全事故指已干擾、正干擾或相當可能干擾有關關鍵基礎設施核心功能的事故，營運者得悉事故後必須於 12 小時內作出通知。任何事故如符合以下任何準則，即視作嚴重事故：

- (a) 有關關鍵基礎設施核心功能的停止運作時間，已超過或相當可能超過由營運者在業務持續運作管理計劃中界定的最大可容忍停止運作時間；
- (b) 服務表現已低於或相當可能低於由營運者在業務持續運作管理計劃中界定的最低服務水平；

- (c) 該電腦系統安全事故已啓動或相當可能啓動業務持續運作或災後復原程序；
- (d) 該電腦系統安全事故已導致或相當可能導致大量客戶資料外泄，而“大量”的定義按照營運者在業務持續運作管理計劃中界定；
- (e) 該電腦系統安全事故已泄露或相當可能泄露敏感數碼資料，以致妨礙關鍵電腦系統的正常運作；
- (f) 該電腦系統安全事故已導致或相當可能導致大量客戶查詢或投訴，而“大量”的定義按照營運者在業務持續運作管理計劃中界定；或
- (g) 威脅者曾威脅於指定時間對關鍵電腦系統發動攻擊，而該攻擊可能引發第 7.3.4(a)至(f)節所述的任何情況。

7.3.5 營運者發現關鍵電腦系統有任何受到干擾或不尋常的跡象後，或需要時間確定是否發生了電腦系統安全事故。當營運者有相當程度的把握確定電腦系統安全事故已發生，將被視為已知悉該電腦系統安全事故。

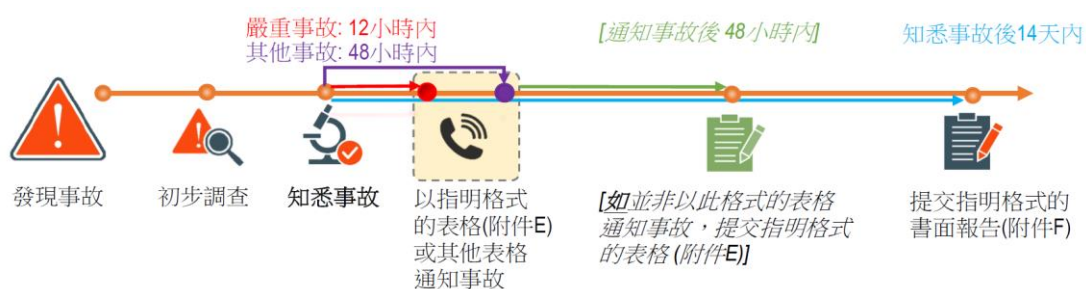
#### 7.3.6 以指明格式作出通知

- (a) 當營運者知悉已發生電腦系統安全事故，應透過指定的安全渠道，以指明格式向專員提交通知(載附件 E 或界別專用表格)。營運者應根據已有資料，盡可能填妥表格。
- (b) 營運者也可選擇先透過指定電話號碼作出通知，提供下列資料，並於作出通知後 48 小時內透過指定的安全渠道，提交指明格式的表格(附件 E 或界別專用表格)：
  - (i) 電腦系統安全事故的性質；
  - (ii) 涉及的關鍵電腦系統；以及
  - (iii) 事故撮要。
- (c) 為免生疑問，營運者必須履行由相關監管制度或其他適用法律施加於特定界別的事故通知規定。

### 7.3.7 以指明格式提交書面報告

- (a) 營運者在知悉電腦系統安全事故後 14 天內，應透過指定的安全渠道，以指明格式提交書面報告(附件 F 或界別專用表格)。該報告應根據已有資料，提供事故的最新情況。若在提交書面報告後得悉額外資料，營運者亦應向專員提供該等資料，作為補充資料。
- (b) 為免生疑問，營運者必須履行由相關監管制度或其他適用法律施加於特定界別的事故通知規定。

### 7.3.8 下列時間表闡述就電腦系統安全事故作出通知和通報的規定：



\*\*\*完\*\*\*

**ANNEX A: FORM FOR NOTIFYING OFFICE ADDRESS**  
*Pursuant to section 19 of the Protection of Critical Infrastructures (Computer Systems) Ordinance*

<b>A. Background Information</b>	
<b>Information of the Critical Infrastructure Operator</b> (“CI Operator”)	
Full Name:	
<b>B. Office Address of CI Operator</b>	
<b>Office Address of the CI Operator</b>	
Office Address:	
<b>C. Reporting Entity Information</b>	
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*

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

<b>A. Background Information</b>	
<b>Information of Critical Infrastructure Operator (“CI Operator”)</b>	
Full Name:	
<b>B. Employee Details</b>	
<b>Information of the Employee Supervising the Computer-system Security Management Unit</b>	
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.	
<b>C. Reporting Entity Information</b>	
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*

<b>A. Background Information</b>	
<b>Information of Critical Infrastructure Operator (“CI Operator”)</b>	
Full Name:	
<b>B. Change Details</b>	
<b>1) Type of Material Changes</b> (Please tick the appropriate box(es))	
<input type="checkbox"/> Platform migration <input type="checkbox"/> Changes to the computing platform or hardware <input type="checkbox"/> Major version upgrade of a core component (e.g. database) <input type="checkbox"/> Integration with or change in interdependency on external systems or networks <input type="checkbox"/> Changes to the underlying infrastructure that supports the critical computer systems (“CCS”) <input type="checkbox"/> Any system modification that fundamentally alters the characteristics or nature of the CCS <input type="checkbox"/> Substantial changes in CCS components maintained by cloud service suppliers that the CI Operator becomes aware of <input type="checkbox"/> Changes of mission or major functions that alters the system’s operational scope, intended purpose or requirements in security, resources or functions <input type="checkbox"/> Others (please specify):	<input type="checkbox"/> Server virtualisation <input type="checkbox"/> Application re-design <input type="checkbox"/> Significant code changes
*Please refer to section 22 of the Protection of Critical Infrastructures (Computer Systems) Ordinance for meaning of “material changes”.	
<b>2) Change Details with Timeframe</b>	
<b>3) Deployment Date</b> (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.	
<b>4) Description of the Effect</b> (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.	
<b>5) Updated System Documentation</b>	
*Please list the documentations attached with this form.	
<b>C. Reporting Entity Information</b>	
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.

<b>A. Background Information</b>		
<b>1) Information of Critical Infrastructure Operator</b> (“CI Operator”)		
Full Name:		
<b>2) Critical Computer System(s) Affected</b>		
<b>B. Incident Details</b>		
<b>1) Seriousness of Incident</b>		
<input type="checkbox"/> Has disrupted / is disrupting / likely to disrupt the core function of CI <sup>[a]</sup> <input type="checkbox"/> Has actual adverse effect other than above <sup>[b]</sup>		
*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		
<b>2) Nature</b> (Please tick the appropriate box(es))		
<input type="checkbox"/> Phishing / social engineering <input type="checkbox"/> Ransomware / malware attack <input type="checkbox"/> Data breach (leakage / tampering) <input type="checkbox"/> Denial-of-service (DoS / DDoS) attack <input type="checkbox"/> Others (please specify):	<input type="checkbox"/> Trojan horse <input type="checkbox"/> Supply chain attack <input type="checkbox"/> Website defacement <input type="checkbox"/> Unauthorized system access / intrusion	<input type="checkbox"/> Spoofing <input type="checkbox"/> Insider threat <input type="checkbox"/> Man-in-the-Middle attack
<b>3) Earliest Identifiable Time of the Incident</b>	Date (dd/mm/yyyy):	Time (hh:mm):
<b>4) Time Becoming Aware of the Incident</b>	Date (dd/mm/yyyy):	Time (hh:mm):
<b>5) Brief Incident Summary</b>		
<b>C. Reporting Entity Information</b>		
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.

<b>A. Background Information</b>	
<b>1) Information of Critical Infrastructure Operator</b> (“CI Operator”)	
Full Name:	
<b>2) Critical Computer System(s) Affected</b>	
<b>Name</b>	<b>Physical Location</b> <i>(address in Hong Kong, or specify the country name if located outside Hong Kong)</i>
<i>(if insufficient space, please attach a separate signed sheet with details)</i>	
<b>B. Incident Overview</b>	
<b>1) Nature</b> (Please tick the appropriate box(es))	
<input type="checkbox"/> Phishing / social engineering	<input type="checkbox"/> Trojan horse
<input type="checkbox"/> Ransomware / malware attack	<input type="checkbox"/> Supply chain attack
<input type="checkbox"/> Data breach (leakage / tampering)	<input type="checkbox"/> Website defacement
<input type="checkbox"/> Denial-of-service (DoS / DDoS) attack	<input type="checkbox"/> Unauthorized system access / intrusion
<input type="checkbox"/> Others (please specify):	<input type="checkbox"/> Spoofing
	<input type="checkbox"/> Insider threat
	<input type="checkbox"/> Man-in-the-Middle attack
<b>2) Brief Incident Description</b>	
<b>3) Initial Attack Vector / Point of Intrusion</b>	
<b>4) Root Cause Analysis Summary</b>	
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
  Security monitoring  
 Training / awareness building
  Configuration changes  
 Review security assessment or audit procedures
  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.

## 附件 G：電腦系統安全審核方法概要

### 目的

本附件旨在概述《保護關鍵基礎設施(電腦系統)條例》規定的電腦系統安全審核(“審核”)。

### 審核步驟

審核分為下述各個階段：

#### (a) 第 1 階段：規劃

關鍵基礎設施營運者(“營運者”)與審核員應在規劃階段商定審核時間表。營運者亦應在這個階段向審核員提供有關其電腦系統安全政策的基本資料和有關實施保安措施的其他資料，以便進行之後的審核工作。

#### (b) 第 2 階段：實地審核工作

審核員審視文件／記錄／系統配置及任何有助確認營運者的現行作業模式和保安措施是否符合要求的其他資料，亦會與持份者會面，釐清從營運者收集的資料，以便擬備審核結果和提出建議。

#### (c) 第 3 階段：編撰結果

完成實地審核工作後，審核員會擬備結果和建議。審核結果草擬本會提交營運者，以便討論和核實相關事實的真確性。審核工作中識別的各項結果會分為兩類狀況。

審核結果狀況	內容
不符合要求	欠缺能證明已遵從相關要求的客觀證據。
有可改善之處	相關要求沒有作出改善的必要，但可採取其他良好作業模式，以更有效達到相關要求。

營運者會審視審核結果的草擬本並提出意見。如有需要，營運者亦可提供補充資料，以供審核員考慮。

營運者就審核結果草擬本提出意見後，審核員會編撰審核報告。

#### **(d) 第 4 階段：報告**

一般而言，審核報告應載有下列資料：

##### **(i) 摘要**

應包括遵從狀況概要及審核員的整體意見和總結，說明營運者為保護其關鍵電腦系統而實行的電腦系統安全管理工作的成效。

##### **(ii) 背景和目的**

應包括進行審核的背景和目的。

##### **(iii) 假設和限制**

應包括進行審核的所有假設和限制。

##### **(iv) 方法**

應包括審核員進行審核所採用的方法。

##### **(v) 範圍**

應包括審核涵蓋的關鍵電腦系統和審核期。

##### **(vi) 結果**

應包括詳細結果，包括觀察、建議和各營運者的回應。

##### **(vii) 持份者名單**

應包括有份參與審核的持份者名單。

審核員應在報告內包括其認為合適並有助評估營運者電腦系統安全態勢和復原能力的額外資料。

#### **假設和限制**

就審核作出的假設如下：

- (a)** 營運者應保存證明已遵從要求的記錄，以及支持相應保安措施已有效實行的審核記錄。由營運者提供的所有資料均假定為最新和準確無誤；以及
- (b)** 評估工作是以會面、文件及記錄審視和樣本檢查作為參考。審核期間並無進行技術評估，例如主機掃描、網絡掃描、應用程式掃描、程式碼審查、滲透測試和道德黑客入侵。

## 附件 H：有關外聘服務供應商責任的合約條款範本

### 目的

本附件提供合約條款範本，以協助關鍵基礎設施營運者（“營運者”）擬備合約文件，訂明外聘服務供應商在遵從《保護關鍵基礎設施(電腦系統)條例》規定方面的責任。

### 免責聲明

合約條款範本只供參考。營運者對範本作適應化修改前，應諮詢其法律顧問。關鍵基礎設施(電腦系統安全)專員（“專員”）對合約條款範本概不承擔責任，對其準確性、完整性或於任何特定情況下的適用性，亦不作出任何性質的明示或隱含的申述、保證或擔保，並明確表示概不會因合約條款範本的全部或任何部分所產生的或因依賴該等內容所引致的任何損失承擔任何責任。

### 合約條款範本

1. 在本合約中，除文意另有所指外，下列各詞句具有以下涵義：

- “合約” 指<營運者>與<外聘服務供應商>訂立的合約。
- “承辦商” 指<外聘服務供應商>。
- “承辦商人員” 指為履行本合約(或其任何部分)而被調派的所有人員，包括<本合約所指明的人員>(及其不時更換的人員)、承辦商的僱員、次承辦商及次承辦商的僱員。
- “合約期” 指自<合約生效日期>起至<合約終止日期>為止的期間，惟根據合約任何適用條文而提前終止或延長者除外。
- “可交付成果” 指承辦商根據本合約或為履行本合約的目的或因與合約所指的服務有關而為<營運者>創造、編製、設計、開發、準備、提供、修改、維護及／或更新的一切有形及無形事宜，包括但不限於<由外聘服務供應商交付的程式、文件、源碼、配置、設計等>及其他資料(包括上述項目的所有草擬本及未完成版本，不論是否已發布)。

“業界良好作業模式”	指符合法律的標準、作業模式、方法及程序，並合理地 and 一般地預期一名熟練和擁有經驗的人，在同樣或類似情況下從事與合約所指的服務類似的服務時所具備的技術、謹慎、勤奮、審慎及有遠見的程度。
“政府”	指中華人民共和國香港特別行政區政府。
“整體規格”	指<項目、系統等的規格>，以及由承辦商、製造商及開發商就承辦商及<營運者>提供的硬件及／或軟件所發布的規格。
“服務”	<由外聘服務供應商提供的實施、系統支援及維護等服務>，以及承辦商根據合約提供及履行的所有其他服務、義務及職責(為免生疑問，包括銷售或供應合約訂明的所有及任何項目)。
“系統”	指在生產及非生產環境中須實施及整合為一整體的<所有子系統、基礎設施、網絡、程式、應用程式等>，<項目規格>對此有更詳盡的描述。

2. 承辦商確認並同意，承辦商在訂立合約時已獲提供足夠資料，令其能夠向<營運者>提供系統和履行服務以至完全符合整體規格及合約其他條文所載的規定。承辦商不得因承辦商聲稱對關乎系統或整體規格或合約任何其他條文的任何事宜或事實缺乏知識或資料，或有任何誤解，而有權獲得任何額外償付或延時，或因此而無須履行合約所訂定的任何義務或法律責任。
3. 承辦商在履行合約所訂的義務時須：
  - (a) 調配擁有合適經驗和資歷並受過合適訓練的人員，並以應有的謹慎、技術和勤奮行事；
  - (b) 按照業界良好作業模式；以及
  - (c) 遵從所有適用法律。
4. 聘任或更換任何承辦商人員承擔服務的任何部分，不得免除承辦商在本合約下的任何法律責任或義務。承辦商須對任何承辦商人員、其代理人、僱員和次承辦商的作為、不作為、違約及疏忽負責，猶如承辦商本身的作為、不作為、違約或疏忽一般。
5. 根據本合約任何適用條文作出的任何延遲或相應而生的延時或更改或暫停，不得解除承辦商的任何義務或法律責任，或不得視作對承辦商的任何義務或法律責任構成任何棄權或禁止反言。

6. 承辦商現向<營運者>保證並申述：
  - 6.1 承辦商訂立合約和履行合約所訂的義務，並履行服務和提供服務，不會抵觸或導致違反：
    - (a) 組織章程大綱及章程細則或規管承辦商的其他同等章程文件的任何條文；
    - (b) 任何合約或安排，而承辦商為該合約或安排的其中一方或受其約束；
    - (c) 任何法庭或政府機構的命令、判決或判令，而承辦商為該命令、判決或判令其中一方或受其約束；或
    - (d) 任何適用法律或規例。
  - 6.2 服務的履行、系統及所有可交付成果及為系統提供的任何位置或網絡(如有需要)須符合所有適用法律及規例。服務的履行、系統及所有可交付成果，以及任何位置或網絡須符合相關政府政策局及部門在合約期內不時發布的所有專業方法、標準、指引和實務守則，除非該等專業方法、標準、指引和實務守則內的任何條文與合約中的任何明文規定有所矛盾，或除非<營運者>因應個別情況另有議定，並以有所矛盾或另有議定的範圍為限。
7. 承辦商及其承辦商人員須遵從《保護關鍵基礎設施(電腦系統)條例》(香港法例第 653 章)及由<規管當局>發出的所有指引(包括實務守則)。
8. 承辦商須(並須確保其承辦商人員)遵從：
  - (a) 任何適用的私隱或保障資料法例(包括香港法例第 486 章《個人資料(私隱)條例》)和香港個人資料私隱專員公署發出的所有指引；以及
  - (b) 政府不時制定的任何私隱程序或政策。
9. 承辦商不得透過為履行本合約任何部分而訂立的任何分判合約，獲免除其於本合約下的任何義務。承辦商須對每個次承辦商及前述次承辦商的代理人及僱員的一切作為、不作為、違約及疏忽負責，猶如承辦商本身的作為、不作為、違約或疏忽一般。
10. 本合約受香港法律管轄並據其解釋。承辦商受香港法院的專有司法管轄權所管轄。