Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

中小企保安事故應變指南

免責聲明

香港生產力促進局屬下的香港電腦保安事故協調中心（HKCERT）保留不時修改文件的權利而無須另行通知。

HKCERT 已盡力確保本文件所含資料均來自可靠來源，對任何錯誤或遺漏或使用相關資料所招致的結果概不負責。本文件上的所有資料均以當時情況提供，不擔保其完整性、準確性、及時性、或使用相關資料所招致的結果，亦不作任何明示或隱含的保證，包括但不限於其性能保證、適售性和特定用途的適用性。

本文件包含的資料僅供參考。 信賴或使用相關資料由讀者自行承擔風險。本文件的任何內容均不得在任何程度上替代讀者的獨立調查和合理的技術和商業判斷。在任何情況下，香港電腦保安事故協調中心、香港生產力促進局、或其合作夥伴、員工或代理商，均不對你或任何人信賴本文件相關資料做出的任何決定或行動，或任何後果性，特殊或類似的損害承擔責任。

版權

目錄

1. 簡介

1.1 目的和範圍

黑客發動網絡攻擊的成本和人手因應自動化和運算能力提升而降低，使網絡攻擊迅速發展，增加針對不同機構（包括公共或私人、跨國或本地的機構）的各種網絡攻擊。由於大多數中小型企業（中小企）缺乏資源來建立更廣泛的網絡防禦以防止或阻止網絡攻擊，以致它們更容易成為攻擊目標。

本中小企保安事故應變指南旨在幫助機構：

- 了解保安事故應變處理的崗位和責任
- 以有限的資源來維持和增強系統防禦
- 減低受網絡事故影響的業務和經濟損失
- 防止和減少類似的網絡攻擊再次發生

1.2 保安事故和事故應變的定義

英國國家網絡安全中心（NCSC）將網絡事故界定為對機構的資訊科技（Information Technology – IT）系統作出未授權的接達（或嘗試接達）。這些可能是指入侵或惡意攻擊（例如阻斷服務（DoS）攻擊、惡意軟件感染、勒索軟件或網絡釣魚攻擊）。

美國國家標準技術研究所（NIST）將「事故處理」（應變）定義為一個包含偵測和分析事故，並限制其影響的程序。保安漏洞應該在事故處理的過程得以被偵測，事故處理人員其後分析數據並判斷其攻擊的嚴重程度。那些事故會被訂下優先次序作出處理，事故處理人員將採取行動停止事故，並確保受影響的系統盡快恢復正常運作。

1.3 報告保安事故並尋求相關建議

本地企業和互聯網用戶可以致電香港電腦保安事故協調中心（HKCERT）的 24 小時熱線： **8105 6060**，就保安事故應變和復原查詢保安建議。

HKCERT 接受與電腦保安相關的事故報告，例如：惡意軟件、網絡釣魚、網頁塗改、阻斷服務攻擊等；亦會協助調查所報告的事故，提供資訊或技術建議，並與適當的本地或海外機構協調相關事故處理。

更多詳情及報告渠道可瀏覽以下 HKCERT 連結：
https://www.hkcert.org/zh/incident-reporting

1.4 指南架構

本中小企保安事故應變指南陳述了保安事故應變的處理周期的定義和解釋，並概述在保安事故發生之前、期間和之後要採取的行動，另外亦包括在機構內建立保安框架、定義崗位和責任等。本指南亦敘述了在一般保安事故情景時要作出的關鍵步驟，以指導機構加快了解和識別不同類型的保安事故。

2. 保安事故應變程序

2.1 保安事故應變的處理周期

為有效管理事故應變，不同的組織提出各種保安事故應變的處理周期模型。其中 NIST 的「Computer Security Incident Handling Guide」（2012）中的簡化版模型將事故應變的處理周期分為四個階段，如下圖所示。

從 NIST 引用的保安事故應變的處理周期圖解

籌備

第一階段是籌備。這階段讓機構建立保安事故應變能力，以準備好應變保安事故，並透過確保系統、網絡和應用程式有足夠的安全保護來防止保安事故發生。

偵測和分析

在偵測和分析階段，其目標是確保偵測保安漏洞的效率和準確性，利用分析策略來拆解保安事故的細節。機構可以了解正發生什麼保安事故，並準備移至下一個處理階段——遏制、根除和復原。

遏制、根除和復原

機構可以根據保安事故的嚴重性，對保安事故作出遏制行動以至最終從中復原，以減輕保安事故的影響。在此階段，處理周期通常會返回至偵測和分析階段，例如在根除惡意軟件事故時，亦要查看是否有其他主機感染了惡意軟件。

事故後的處理

當完成處理保安事故後，機構應發布一份詳細報告說明事故起因以及其造成的影響，以改善防禦措施並防止事故再次發生。上述行動都包含在事故後的處理階段。最重要是應將保安事故的紀錄（包括遏制、補救和解決方法）集中儲存、加密和備份。

2.2 制定總保安事故應變程序

機構應制定一個「總保安事故應變程序」（Master Incident Response Procedure），為保安事故應變提供普遍的應變指南。下列的情景問題幫助引導保安事故應變策劃人員考慮在應變程序裡每個階段的程序需要哪些元素和資訊，以記錄到總保安事故應變程序。**附錄一**包含保安事故應變程序範本以供參考。

籌備：

1. 哪些是機構營運的重要的系統、數據和資產？
2. 機構的保安事故應變團隊裡有什麼崗位和責任？機構是否擁有持份者最新的聯絡名單？
3. 機構會將此問題歸類為保安事故嗎？如會，該行為違反了哪些機構政策？
4. 哪些措施可以防止此類事故的發生或限制其影響？

偵測和分析：

1. 若有事故先兆，機構能偵測到嗎？機構會否在事故發生之前因應這些先兆採取行動？
2. 機構可以偵測到哪些保安事故的跡象？哪些跡象表明事故發生的可能性？
3. 偵測保安事故需要什麼工具？
4. 保安事故應變團隊將如何分析和驗證事故？哪些人士會參與分析和驗證？
5. 應該向機構內的哪些人士和團隊通報事故？
6. 團隊如何優先處理此事故？

遏制、根除和復原：

1. 機構應該採取哪種策略來遏制事故？為何這種策略比其他的更可取？
2. 如果事故沒有得到遏制，會發生什麼事情？
3. 哪些額外的工具需要用來應對此特定事故？
4. 哪些人員將參與遏制、根除及/或復原過程？
5. 機構需收集或保存哪些證據（例如審計和帳戶日誌）？如何收集證據？在哪裡儲存？要保留多久？

事故後的處理：

1. 誰需要參加事故的檢討會議？
2. 如何防止類似事故再次發生？
3. 如何加強偵測類似事故？

2.3 一般保安事故情景的標準操作程序

當處理不同的保安事故情景時，一些具體的處理步驟亦需要考慮。機構除需要備有一套「總保安事故應變程序」外，亦建議把這些步驟記錄到不同的「保安事故應變標準操作程序」（Security Incident Response Standard Operating Procedures – SIR SOPs）。以下列表會羅列當遇到一般網絡保安事故情景時在每個階段的關鍵步驟。

備註：**第 3 節** 將介紹和解釋「總保安事故應變程序」和「保安事故應變標準操作程序」。

情景 1 – 分散式阻斷服務（DDoS）

主要階段	關鍵步驟
籌備	1. 為 DDoS 事故準備溝通渠道 2. 界定事故的上報路徑 3. 評估和保護關鍵系統接達權限，並限制不必要的權限 4. 採用入侵檢測和防禦系統（IDPS）、抗 DDoS 服務等安全解決方案。 5. 設定防火牆限制，並盡量將其預設為拒絕所有流量

偵測和分析	1. 對比當前使用和基線加載來識別異常加載 2. 找出任何受到影響的系統，並從網絡流量日誌中偵測來源 3. 識別攻擊形式，例如攻擊是數量攻擊、漏洞的利用、直接攻擊、反射攻擊、通過網絡層還是應用層等。 4. 記錄攻擊的時間和流量 5. 聯絡受影響人士並保持聯繫
遏制、根除和復原	1. 阻止來自 IDPS 或防火牆的相關流量 / 請求互聯網服務供應商阻止離源最近的相關流量 2. 禁用可能用於對受影響系統進行 DDoS 攻擊的憑證 3. 按地區暫停流量，實際情況取決於主要用戶的位置 4. 停止非必要的服務和回應，以盡量減少系統的工作量 5. 清除伺服器和路由器上不需要的連接或程序 6. 必要時尋求第三方協助（例如，某些系統可能得到第三方如供應商的支持，使用流量清理服務等） 7. 更新受影響的系統（如適用）以修復 DoS 漏洞 8. 重啟暫停的服務 9. 確保流量復原正常，持續監察異常流量
事故後的處理	1. 檢討系統保安：檢查防火牆配置、應用系統保安、系統設計等 2. 建立事故報告並列出已採取的措施 3. 討論改進方法（汲取經驗） 4. 若需要採取進一步行動，與執法部門聯絡（例如通報因服務受到影響而造成的經濟損失等）

情景 2 – 惡意軟件（包括勒索軟件）

主要階段	關鍵步驟
籌備	1. 為惡意軟件事故準備溝通渠道 2. 界定事故的上報路徑 3. 評估及備份關鍵系統，建立系統復原點，並確保至少一個離線備份 4. 安裝保護軟件（例如防毒軟件），並將辨識檔保持更新

	5. 設定防火牆限制，並盡量將其預設為拒絕所有流量 6. 保持重要數據的離線備份
偵測和分析	1. 盡快隔離受感染系統，使受感染系統保持通電狀態 2. 確定惡意軟件及其特徵，驗證惡意軟件是否仍在運行或通訊中 3. 分析受影響範圍（即從軟件/系統、檔案系統、數據庫等角度來看，受影響的範圍有多大） 4. 檢查網絡及系統日誌以找出惡意活動和感染媒介（例如電郵附件、遠程協議、可移除硬碟、點擊的連結等） 5. 聯絡受影響人士並保持聯繫
遏制、根除和復原	1. 隔離惡意軟件，並確保在恢復系統正常運作之前將其徹底清除 2. 當遇上勒索軟件攻擊，要查看是否有來自可靠來源的解密工具 3. 若沒有可用的解密工具，找出可行的離線備份並將數據復原到不受影響的系統/電腦中 4. 阻斷疑似惡意軟件的網絡通訊 5. 如有需要，尋求第三方協助 6. 一旦惡意軟件被遏制，進行數據復原
事故後的處理	1. 檢討系統保安：檢查防火牆配置、檢查是否已安裝最新的惡意軟件辨識檔等 2. 建立事故報告並列出已採取的措施 3. 討論改進方法（汲取經驗） 4. 進行用戶保安意識培訓 5. 若需要採取進一步行動，與執法部門聯絡（例如洩露個人資料等）

情景 3 – 釣魚電郵（包括詐騙電郵）

主要階段	關鍵步驟
籌備	1. 為釣魚事故準備溝通渠道 2. 界定事故的上報路徑 3. 採用保安解決方案，例如電郵通訊閘等

	4. 進行保安意識培訓，例如釣魚演習、趨勢分享等
偵測和分析	1. 使用防惡意軟件工具對受影響的電腦進行全面掃描，以檢查其是否植入了任何惡意軟件 2. 收集網絡釣魚的信件（例如釣魚電郵），查看其標頭，找出來源 3. 與員工一起調查，要求其提供描述並驗證是否在電郵裡的釣魚網站中輸入了任何資訊 4. 確定是否有任何文件從電郵裡的連結或附件中下載 5. 檢查電腦是否有異常活動 6. 聯絡受影響人士並保持聯繫
遏制、根除和復原	1. 從電腦中刪除相關釣魚郵件 2. 確定其他同事有否也收到相同電郵，並要求他們從郵箱中刪除該電郵 3. 盡可能通過相關電郵通訊閘攔截相關釣魚來源 4. 盡快更改受影響用戶的帳戶認證（例如密碼）
事故後的處理	1. 檢討電郵閘道的規則：評估提高網絡釣魚檢測級別的可能性等 2. 建立事故報告並列出已採取的措施 3. 進行網絡釣魚演習 4. 討論改進方法（汲取經驗） 5. 如果需要採取進一步行動，與執法部門聯絡（例如，員工曾與網絡釣魚發動者聯繫、如有金錢交易則通知相關銀行等）

情景 4 – 網頁塗改 / 入侵

主要階段	關鍵步驟
籌備	1. 為網頁篡改或入侵事故準備溝通渠道 2. 界定事故的上報路徑 3. 評估和備份關鍵系統，建立可行的復原點 4. 安裝保護軟件(例如防惡意軟件工具等)，並保持辨識檔更新 5. 設定防火牆限制，並盡量將其預設為拒絕所有流量

偵測和分析	1. 檢查有否任何非必要或未經授權的存取曾連線至受影響系統，若該存取仍處於連接狀態，則要加以封阻 2. 分析受影響的區域（即從軟件/系統、文件系統、數據庫等角度來看，受影響的範圍有多大） 3. 檢查網絡及系統日誌是否有惡意活動，分析受影響系統有否被用於攻擊漏洞 4. 聯絡受影響人士並保持聯繫
遏制、根除和復原	1. 盡量把受影響的網站伺服器與網絡隔離，並將用戶轉載到替代網頁 2. 阻截來自 IDPS 或防火牆的相關網絡流量 3. 禁用可能在受影響系統用於攻擊的憑證 4. 盡可能更新受影響的系統以修復漏洞 5. 必要時尋求第三方協助
事故後的處理	1. 使用更新的軟件、保安更新、保安設置和可靠的備份重建系統 2. 建立事故報告並提及已採取的措施 3. 系統上線前進行保安風險評估 4. 討論改進方法（汲取經驗） 5. 如果需要採取進一步行動（例如洩露個人資料等），與執法部門溝通

2.4 保安事故處理清單

為了簡化應用保安事故應變的處理周期，以下清單列出了一系列保安事故處理中常見的保安最佳實踐。該清單還可用於作自我檢查在已制定的事故應變程序及事故的實際處理過程中是否涵蓋了必要的行動步驟。這些按階段分類的步驟可以確保大多數 IT 系統在應對保安事故時有足夠準備。

行動		已完成
籌備		
1	確保系統和應用程式的良好行為	○
1.1	了解網絡、系統及應用程式的正常行為（網絡及系統的配置）	○
1.2	由幾種保安軟件構建的警報來識別先兆和跡象	○
1.3	制定日誌保留政策，在所有系統上建立日誌記錄及審計的基線級別，並在所有關鍵系統上建立更高的基線級別	○
1.4	使用及維持系統及應用程式正常運作及事故處理步驟的知識庫	○
1.5	保持所有主機時鐘同步	○
2	加強資料數據保護	○
2.1	識別和驗證敏感資料數據，並加強其保護	○
2.2	保護事故中的資料數據	○
2.3	除檔案系統備份外，還通過完整的取證映像獲取系統快照	○
3	準備事故處理和運作復原計劃	○
3.1	徵集在事故處理過程中或有用處的工具及資源	○
3.2	在機構的事故應變政策中包含有關事故報告的規定	○
3.3	遵循既定的證據收集和處理程序	○
3.4	建立事故通報機制並保持更新聯絡名單	○
3.5	能夠從系統中找出非永久數據作為證據	○
3.6	根據計劃進行事故應變演習	○
3.7	定期檢討和更新計劃	○

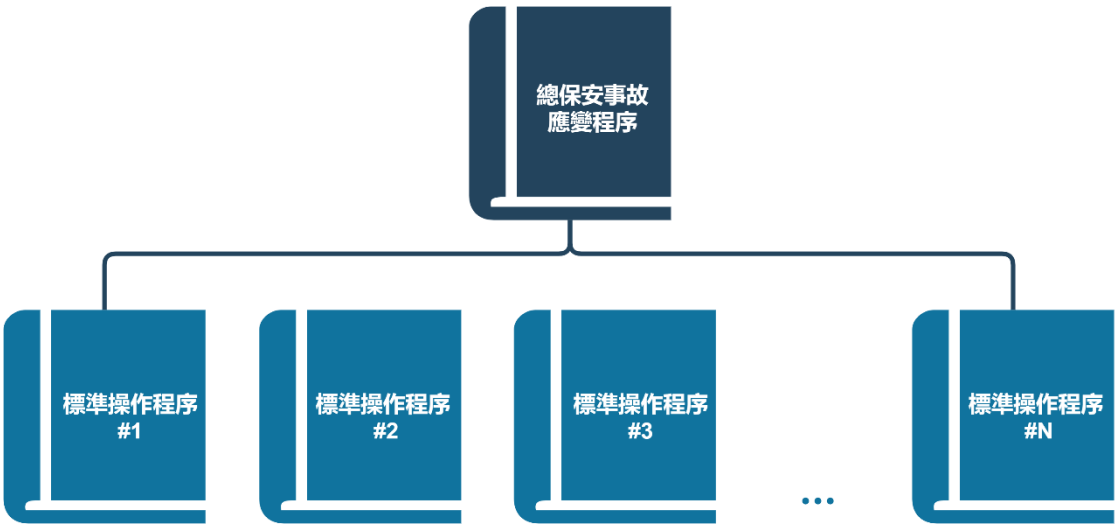
偵測和分析		
4	查證事故是否發生	○
4.1	分析事故先兆和跡象	○
4.2	進行事故關聯分析，尋找相關的資訊	○
4.3	進行研究（例如搜索引擎、知識庫）	○
4.4	當處理人員認為發生事故，就開始記錄調查並收集證據，特別是來自系統裡的非永久數據	○
5	根據相關因素（功能影響、資訊影響、復原所需人手等）斷定事故處理的優先次序	○
6	向適當的內部人員和外部機構通報事故	○
遏制、根除和復原		
7	獲取、保存、保護及記錄證據	○
8	遏制事故	○
9	根除事故	○
9.1	識別並緩解所有被利用的漏洞	○
9.2	刪除惡意軟件、不當材料和其他組件	○
9.3	如果發現更多受影響的系統（例如新的惡意軟件感染），重複檢測和分析步驟（4.1、4.2）以識別所有其他受影響的系統，然後遏制 (8) 並根除 (9) 事故	○
10	從事故中復原	○
10.1	將受影響的系統復原到運作就緒狀態	○
10.2	確認受影響的系統正常運行	○
10.3	如有必要，實行額外的監測措施以偵測將來的相關活動	○
事故後的處理		
11	建立跟進報告	○
12	召開汲取經驗會議（若屬重大事故須強制執行，否則選擇性）	○

3. 保安事故應變的管理

一間機構的保安政策應概述有關保安事故應變的程序，當中需涵蓋保安事故中所有相關單位的崗位和其責任、與外界機構的溝通、保安事故應變處理周期等。

3.1 保安事故應變程序

縱使應對不同類別的保安事故方法會因應其性質而有所差異，但始終建議機構應制定「總保安事故應變程序」，為機構的保安事故應變提供統一應對準則的指南。對於一些嚴重和頻繁發生的保安事故如勒索軟件、資料外洩、CEO 詐騙和網絡釣魚等，最好制定專屬的「保安事故應變標準操作程序」。機構可以不時就新的攻擊開發新的標準操作程序，而總程序能夠維持不變。「總保安事故應變程序」和「保安事故應變標準操作程序」的結構如下圖所示。



保安事故應變的標準操作程序連結至一個總程序

附錄一附有建立保安事故應變程序的範本，以便機構制定應變保安事故的程序。

機構有責任確保用以處理保安事故的程序既現實又有效。除了程序之外，以下是一些建議用於保護網絡、系統和應用程式的實踐，以確保其有充分的保安管理，並促進對保安事件的整體應變。

- 在進行任何更改時作出風險評估
- 根據風險評估結果而增強安全性
- 持續維護和監察主機的安全
- 持續維護和監察網絡的安全
- 設定並制定網絡攻擊的防護措施
- 對保安事故應變程序進行演習測試並驗證復原計劃
- 展開用戶意識培訓

3.2 保安事故應變中的崗位和責任

穩健的商業實踐需包括機構風險的討論。管理層會議應定期討論任何針對機構的風險及其更新。然而保安事故應變並不僅是 IT 部門的責任，以下列表陳述了在保安事故應變中的主要崗位及責任。資源有限的中小企應預先分配員工擔當一定的崗位和責任，以確保在發生保安事故時可以適當地應對。

崗位	責任
IT 管理部門	• 與營運管理部門分析事故，以評估事故在技術上的影響和嚴重程度（高、低或其他） • 收集和保存有關事故的資訊 • 協調和確保有足夠的資源進行事故應變 • 遏制、補救和解決事故，並以時間標示記錄操作 • 根據營運管理層的意見，確定是否應在事故解決之前將生產服務離線 • 上報嚴重性較高的事故 • 管理事故後的流程並與營運部門草擬評估報告，記錄事故汲取的經驗和跟進 • 定期作出系統監察 • 讓機構做好應對保安事故的準備，例如為第一應變者（系統管理員）提供指導和培訓，以及建立與營運部門的溝通渠道 • 提供事故通報熱線並作出回應
營運管理部門	• 評估事故對營運的影響 • 成為營運數據和系統的擁有者

	• 在 IT 管理層的要求下收集事故相關的資訊 • 鑒定事故是否與濫用有關 • 鑒定是否需要啟動應急計劃以應對長期的服務暫停 • 與 IT 管理人員一起草擬事故評估報告和跟進事故 • 按規定實施安全控制並監察系統是否存在攻擊跡象或未經授權/不當接達 • 為資訊資源提供實體和程序上的保障 • 向 IT 管理層報告可能導致事故發生的可疑事件
其他團隊	保安事故應變中可能還有其他團隊參與，例如持續業務運作與災難復原（BCDR）管理、危機管理。 他們應該在機構裡的保安管理團隊管理之下。
外判商	機構可能有一些硬件或軟件外判給其他 IT 公司以維持運作。機構應經常與外判商溝通，互相對事故應變處理程序保持更新，並找出「發生某些問題時誰負責」和「如何復原至正常運作」。上述兩種情況應包含在服務水平協議（Service Level Agreement, SLA）中，並由雙方互相進行詳細討論。

在處理保安事故時，一份附有所有持份者的最新聯絡資料的通報渠道名單是必不可少，聯絡名單應簡易清晰並需定期審視更新。**附錄二**列出了幾種通報保安事故的方法，在處理所有嚴重性較高的事故亦需通知 IT 管理層。 在不同保安事故的情況下，亦可能須要通報予本地和海外相關機構。

附錄一 —— 保安事故應變程序範本

資料	細節
簡短序述	
保安事故類別	☐ 分散式阻斷服務（DDoS） ☐ 網絡入侵 ☐ 惡意軟件 ☐ 網絡釣魚 ☐ 勒索軟件 ☐ 網頁塗改 ☐ 其他：
受影響的 IT 系統	硬體： 軟體：
嚴重性	低 0 | 1 | 2 | 3 | 4 | 5 高
資訊保安 CIA	機密性 ☐ 完整性 ☐ 可用性 ☐
影響規模	營運影響：
發生的日期 / 時間	
發現的日期 / 時間	
初步調查結果	怎樣發生: 為何發生: 已發現的保安漏洞:
牽涉的個人資料	☐ 是 / ☐ 否 如是，牽涉甚麼個人資料？ 已向香港個人資料私隱專員公署 (PCPD) 匯報？ ☐ 是 / ☐ 否
最長可承受時間	

處理周期階段	已採取行動
籌備	
偵測和分析	
遏制、根除和復原	
事故後的處理	

附錄二 —— 保安事故通報渠道

機構應訂立一套標準，指明每個保安事故須要收集的相關數據，並建立一個保安事故通報渠道，以令保安事故應變更有效和一致。

內部聯絡和 IT 服務供應商的通報渠道

以下所提及資源均可用作通報渠道報告保安事故以進行調查和補救。

名稱： XXX 公司 / XXX 團隊

位置： 辦公室 , x 樓 , 辦公大樓

電話號碼： +852 XXXXXXXX (24 小時 熱線)

電郵地址： [服務台的電郵地址]

服務級別： 8 x 5 x 下一個工作日 / 7 x 24 x 4

相關的保安事故 / 系統： [保安事故 / 系統]

保安事故中的溝通必須以「有需要知道」的原則進行。任何人不得向未直接參與保安事故應變的人士提供相關資訊，包括有關事故發生的事宜或用於控制或補救事故的方法，尤其是一些非內部人員，例如 IT 服務供應商。

外界機構

在處理保安事故應變時可能涉及聯繫 IT 服務供應商以外的外界機構。每個外界機構都應有專屬的聯絡方法，並應獲得高級管理層的同意方可向其報告保安事故，例如：

- 執法機構 – 報告潛在的網絡犯罪
- 監管機構 – 在法例規定的期限內報告保安事故
- 新聞中心 – 公布公司對保安事故的應對

以下列表列出當處理保安事故應變時遇到不同的情景，亦可以向不同官方通報渠道尋求協助。

事故類別	通報渠道
犯罪行為 (例如，網上詐騙和牽涉經濟損失的案件)	香港警務處 網絡安全及科技罪案調查科 (CSTCB)：https://www.erc.police.gov.hk/index_tc.html
涉及個人資料的投訴	香港個人資料私隱專員公署 (PCPD)：https://www.pcpd.org.hk/tc_chi/enforcement/data_breach_notification/dbn.html
非應邀電子訊息（垃圾郵件）	香港通訊事務管理局 (OFCA)：https://eform.one.gov.hk/form/oca014/tc/

附錄三 —— 供參考的刊物

出版者	刊物名稱
HKCERT	中小型企業資訊保安指南 (2007) https://www.hkcert.org/f/guideline/180877/1edf5b6d-7ee4-407a-b9f1-e42011a2449b-DLFE-811.pdf
HKCERT	保安事故處理自助指引 https://www.hkcert.org/tc/resources/faq/self-help-guide-for-security-incidents
HKCERT	中小企網絡安全七大攻略 (2018) https://www.hkcert.org/tc/security-guideline/seven-habits-of-cyber-security-for-smes
GovCERT.HK / OGCIO	資訊保安事故處理實務指引 (2021) https://www.govcert.gov.hk/doc/ispg-sm02-v1.2_tc.pdf
InfoSec / OGCIO	處理公司的資訊保安事故 https://www.infosec.gov.hk/tc/best-practices/business/security-incident-handling-for-companies
NIST US	Computer Security Incident Handling Guide (2012) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
NCSC UK	Small Business Guide Collection: Cyber Security Response and Recovery (2020) https://www.ncsc.gov.uk/files/NCSC_A5%20Response%20and%20Recovery%20Guide_v3_OCT20.pdf
SANS	Incident Handler's Handbook (2011) https://www.sans.org/white-papers/33901
SANS	Incident Handling for SMEs (Small to Medium Enterprises) (2008) https://www.sans.org/white-papers/32764

Hong Kong Computer
Emergency Response Team
Coordination Centre
香港電腦保安事故協調中心

HKCERT