數字政策辦公室

資訊保安

資訊保安事故處理

實務指引

[ISPG-SM02]

第 1.8 版

2025 年 2 月

版權公告

修改記錄

修改次數	修改詳情	經修改頁數	版本編號	日期
1	G54 資訊保安事故處理指引第 5.0 版已轉換成資訊保安事故處理實務指引。修改報告可於政府內聯網「資訊科技情報網」查閱：(http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	整份文件	1.0	2016 年 12 月
2	增加關於資訊科技保安管理的新章節及與其他實務指引保持參考上的一致。	整份文件	1.1	2017 年 11 月
3	詳細解釋政府資訊系統的範圍，以及舉例說明對事故的評估和決定。報告機制的表格亦作出輕微修改。	第 6 頁、26 頁、附件 C	1.2	2021 年 6 月
4	如發現有跡象顯示可能發生資訊保安事故，政府部門可諮詢政府資訊保安事故應變辦事處常設辦公室的建議。	第 20 頁、26 頁、附件 F	1.3	2022 年 9 月
5	更新個人資料私隱專員公署的資料外泄事故通報表格的超連結，以及修改報告機制的表格。	第 23 頁、附件 C	1.4	2023 年 6 月
6	基於最新的《資訊科技保安指引》(G3) v10.0 而作出的修改	整份文件	1.5	2024 年 4 月
7	將「政府資訊科技總監辦公室」修改為「數字政策辦公室」 將「香港電腦保安事故協調中心」修改為「香港網絡安全事故協調中心」		1.6	2024 年 7 月
8	增加資訊保安事故報告的新要求。修改報告機制表格。	第 22 頁、附件 C 、 D 和 E	1.7	2024 年 8 月
9	修改部門資訊科技保安聯絡人資料更新表和報告機制表格。	附件 A 和 C	1.8	2025 年 2 月

目錄

1. 簡介

有效的資訊保安管理包括識別、防範、偵測、應變和復原的互相配合。除部署強而有力的保安保護措施外，決策局／部門還應具備事故應變能力，以備在發生資訊保安事故（以下簡稱為保安事故或事故）時啟動適當程序。適當及預早的計劃能確保人員知悉、協調及有系統地進行事故應變和復原活動。決策局／部門須建立、記錄、測試及維護一套本身資訊系統的保安事故應變／報告程序。

1.1 目的

本文件就資訊保安事故處理的制訂，以及資訊保安事故的防範、偵測及應變，為管理、行政及其他技術和操作人員提供指導說明。由於不同資訊系統的資訊保安事故可能構成不同的影響和導致不同的後果，決策局／部門應根據其實際的操作需要，為本身的資訊系統制訂合適的資訊保安事故應變計劃。

本文件旨在提供政府內部資訊保安事故處理的實際指引和參考，但並不包括對個別具體電腦硬件或操作系統平台的詳細技術描述。決策局／部門應就有關技術細節諮詢相關的系統管理員、技術支援人員和產品供應商。

1.2 參考標準

以下的參考文件為本文件在應用上的參考：

- 香港特別行政區政府《基準資訊科技保安政策》[S17]
- 香港特別行政區政府《資訊科技保安指引》[G3]
- Information technology - Security techniques - Information security management systems –Overview and vocabulary (fifth edition), ISO/IEC 27000:2018
- Information technology - Security techniques - Information security management systems - Requirements (third edition), ISO/IEC 27001:2022
- Information technology - Security techniques - Code of practice for information security controls (third edition), ISO/IEC 27002:2022
- Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management (second edition), ISO/IEC 27035-1:2023
- Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response (second edition), ISO/IEC 27035-2:2016

- NIST SP 800-61 – Computer Security Incident Handling Guide

1.3 定義及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用的及以下的定義及慣用詞。

縮寫及術語	
中央處理單元	中央處理單元是電腦的主要組件，可作為電腦的「控制中心」。 中央處理單元也稱為「中央」或「主」處理器，是一組複雜的電子電路，用於運行機器的作業系統和應用程式。
主機入侵偵測系統	主機入侵偵測系統是一種監察網絡流量是否有可疑活動並在發現此類活動時發出警報的系統。
資訊保安事件	發生可能違反資訊保安或控制失效的情況。
資訊保安事故	會對政府資訊系統及／或數據資產造成傷害，或會損害其運作的一個或多個相關的及已證實資訊保安事件。
入侵指標	入侵指標充當主機系統或網絡潛在入侵的鑑證證據。
隨機存取記憶體	隨機存取記憶體是一種電腦記憶體，可依任何順序搜尋並根據需要進行變更。
復原點目標	復原點目標定義為從災難、故障或類似事件中復原後，在資料遺失超出組織可接受範圍之前可能遺失的最大資料量（按時間衡量）。
復原時間目標	復原時間目標是應用系統、電腦、網絡或系統在發生意外災難、故障或類似事件後可以停機的最長可接受時間。
SYN 泛濫	SYN 泛濫（半開放性攻擊）是一種分佈式拒絕服務攻擊，其目的是透過消耗所有可用的伺服器資源來使伺服器無法用於合法流量。

1.4 聯絡方法

1.4.1 一般聯絡

本文件由數字政策辦公室編製及備存。如有任何意見或建議，請寄往：

電郵： it_security@digitalpolicy.gov.hk

Lotus Notes 電郵： IT Security Team/DPO/HKSARG@DPO

CMMP 電郵： IT Security Team/DPO

2. 資訊保安管理

資訊保安是關於保安控制和措施的規劃、實施和持續提升，以保護資訊資產的機密性、完整性和可用性，適用於資訊的存儲、處理或傳輸過程及其相關資訊系統中。資訊保安管理是一套有關規劃、組織、指導、控制的原則和應用這些原則的法則，來迅速有效地管理實體、財務、人力資源和資訊資源，以及確保資訊資產和資訊系統的安全。

資訊保安管理涉及一系列需要持續監測和控制的活動。這些活動包括但不限於以下的範疇：

- 保安管理框架與組織；
- 管治、風險管理和遵行要求；
- 保安操作；
- 保安事件和事故管理；
- 保安意識培訓和能力建立；和
- 態勢感知和資訊共享。

保安管理框架與組織

決策局／部門須根據業務需要和政府保安要求，制定和實施部門資訊保安政策、標準、指引和程序。

決策局／部門亦須制定資訊保安的組織架構，並為有關各方就保安責任提供清晰的定義和適當的分配。

管治、風險管理和遵行要求

決策局／部門須採用風險為本的方法，以一致及有效的方式識別資訊系統的保安風險、訂定應對風險的緩急次序和應對有關風險。

決策局／部門須定期和在必要時對資訊系統和生產應用系統進行保安風險評估，以識別與保安漏洞相關的風險和後果，並為建立具成本效益的保安計劃和實施適當的保安保護和保障措施提供依據。

決策局／部門亦須定期對資訊系統進行保安審計，以確保當前的保安措施符合部門資訊保安政策、標準和其他合約或法律上的要求。

保安操作

為保護資訊資產和資訊系統，決策局／部門應根據業務需要實施全面的保安措施，涵蓋業務上不同的技術領域，並在日常操作中採取「預防、偵測、應變和復原」原則。

- 預防措施避免或阻止不良事件的發生；
- 偵測措施識別不良事件的發生；
- 應變措施是指在發生不良事件或事故時，採取相應行動來遏制損害；和
- 復原措施是將資訊系統的機密性、完整性和可用性恢復到預期狀態。

保安事件和事故管理

在現實環境中，由於存在不可預見並致服務中斷的事件，故此保安事故仍可能會發生。若保安事件危及業務的連續性或引起數據保安風險，決策局／部門須啟動其常規保安事故管理計劃，以實時識別、管理、記錄和分析保安威脅、攻擊或事故。決策局／部門亦應準備與有關各方適當地溝通，透過分享對有關保安風險的應變以消除不信任或不必要的猜測。當制定保安事故管理計劃時，決策局／部門應規劃和準備適當的資源，並製定相關程序，以配合必要的跟進調查。

保安意識培訓和能力建立

因為資訊保安是每個人的責任，所以決策局／部門應不斷提升機構內的資訊保安意識，透過培訓及教育，確保有關各方了解保安風險，遵守保安規定和要求，並採取資訊保安的良好作業模式。

態勢感知和資訊共享

因應網絡威脅形勢不斷變化，決策局／部門亦應不斷關注由保安行業和政府電腦保安事故協調中心發布的現時保安漏洞訊息、威脅警報和重要通知。應將即將或已經發生具威脅的保安警報傳達及分享給決策局／部門內的負責同事，以便採取及時的應對措施來緩解風險。

決策局／部門可以利用威脅情報網絡平台接收和分享保安事務、保安漏洞和網絡威脅情報的訊息。

人員亦可以通過參與保安演習和參加研討會、展示會或瀏覽載有保安情報資訊和一般保安資訊（例如網絡安全資訊站、資訊安全網）的專題網頁來提高保安意識。

3. 保安事故處理簡介

在資訊保安管理中，「保安操作」職能範疇包括適當地部署保安保護和保安措施以降低成功攻擊的風險。但是，儘管採取了這些措施，保安事故仍會發生。故此，資訊保安事故應變計劃應預先準備，這是保安事件與事故管理下的一個主要範疇。一旦服務下降或暫停，這些計劃能幫助決策局／部門對事故做好應對和恢復服務的準備。應當委派適當的人員和各按其職、預留資源和規劃好處理程序，以應付保安事故。預先的準備將有助於回應保安事故，並能讓資訊系統以更有組織、有效率和有效地恢復。

3.1 資訊保安事故

保安威脅是指可能會為資訊資產、系統及網絡帶來負面影響（例如利用資訊系統或網絡的漏洞）的潛在事件或任何情況。資訊保安事件是指可能違反資訊保安或控制失效的事件。資訊保安事件的發生並不一定代表攻擊成功。不是所有資訊保安事件都會被分類為資訊保安事故。「資訊保安事故」一詞在本文件中指會對政府資訊系統（包括由政府提供和負責維護的資訊系統，不論該資訊系統是在政府內部或以外推行）及數據資產造成傷害，或會損害其運作的一個或多個相關的已證實資訊保安事件。例如，資訊保安事故可以是指不合乎政府利益的資料泄漏，或資訊系統及／或網絡內的負面事件，而且對電腦或網絡保安的機密性、完整性和可用性構成影響。本實務指引的重點是資訊保安相關的事故，自然災害、硬件／軟件故障、數據線故障、停電等負面事件並不包括在本實務指引範圍內。這些負面事件應通過相關系統維修和運作復原計劃處理。

常見的保安事故包括：拒絕服務攻擊、入侵資訊系統或數據資產、保密資料在電子形態下、惡意破壞或竄改數據、濫用資訊系統、大規模感染惡意軟件、網站遭塗改，以及影響聯網系統的惡意腳本程式。

下圖解釋威脅、保安事件及保安事故之間的關係：

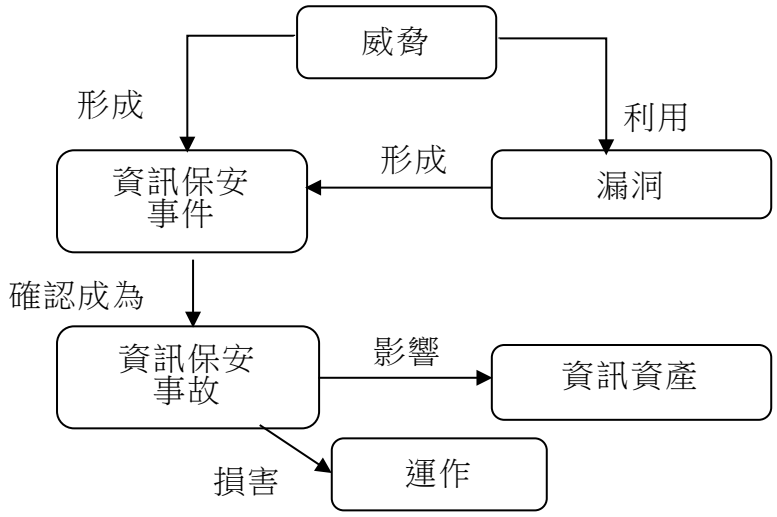


圖 3.1 保安事件及保安事故的關係

3.1.1 保安事故處理

保安事故處理是一系列持續進行的程序，規管保安事故發生前、發生時和發生後所採取的措施。

保安事故處理始於規劃和準備資源，以及制訂適當程序（例如升級處理和保安事故應變程序），以備日後遵照執行。

一旦保安事故被識別，負責保安事故應變的各方須按照預定程序實施應變。保安事故應變是指為處理保安事故並恢復系統的正常操作狀態，而進行的工作或採取的措施。

保安事故過後，應採取跟進行動對事故進行評估，並加強保安保護措施，以防止再度發生事故。應覆檢規劃和準備的工作，並作出相應的修訂，以確保有足夠的資源（包括人力資源、設備和技術知識）和有妥善制訂的程序處理日後的同類事故。

3.2 保安事故處理的目的

事故處理的主要目的如下：

- 確保具備處理事故所需的資源（包括人力資源、技術等）。
- 確保負責保安事故處理的各方明確了解，在發生保安事故時應按預定程序進行的工作。
- 確保事故應變有條不紊並具效益，而且能夠迅速復原受襲系統。
- 確保事故應變工作已獲確認和互相配合。
- 盡量減少泄漏資料、破壞資料和系統中斷等事故可能造成的影響。
- 在適當情況下，分享事故應變經驗。
- 防止受到進一步的攻擊和破壞。
- 處理相關的法律問題及在認為有需要時轉介警方作刑事調查。
- 若涉及個人資料，應向個人資料私隱專員公署報告。
- 在切實可行範圍內盡量保存資料作調查之用。

鑒於資訊科技在政府內部迅速發展，所有決策局／部門都必須制訂一套保安事故處理應變計劃，尤其是設有下列資訊系統的決策局和部門：

- 與外部（例如互聯網）連接的系統。
- 處理敏感數據和資料的系統。
- 關鍵任務系統。
- 任何可因保安事故的發生而受重大不良影響的系統。

3.3 披露事故資訊

除向負責處理保安事故及系統保安工作，或獲授權參與調查電腦罪行或濫用電腦事故的人士外，所有人員不得向任何人士披露有關電腦罪行及濫用電腦事故中的受害人、決策局／部門、受影響系統或造成該次事故的系統保安漏洞和入侵方法的資料。

披露任何事故資訊，包括被攻擊的方法、系統背景資料如實體位置或操作系統等，可能會鼓勵黑客入侵具有相同漏洞的其他系統，亦可能會影響警方偵查時的鑑證及檢控工作。但是，在事故事後分析之後，可能會得出防止類似保安事故的行動建議。如果建議內不包含個人、決策局／部門和系統發生事故的具體資訊，便可以在政府內分享，讓其他決策局／部門也可以防止類似的事故，並改善其保安處理程序。

4. 組織架構

下圖所示為政府內部保安事故應變組織架構的通用參考模型。

根據基準資訊科技保安政策，每個決策局／部門須成立一個資訊保安事故應變小組以協調處理與決策局／部門有關的資訊保安事故。政府資訊保安事故應變辦事處則集中統籌並支援各決策局／部門內部的資訊保安事故應變小組。各決策局／部門的資訊保安事故應變小組負責監督決策局／部門內部特定資訊科技系統、電腦服務或職能範圍的事故處理程序。

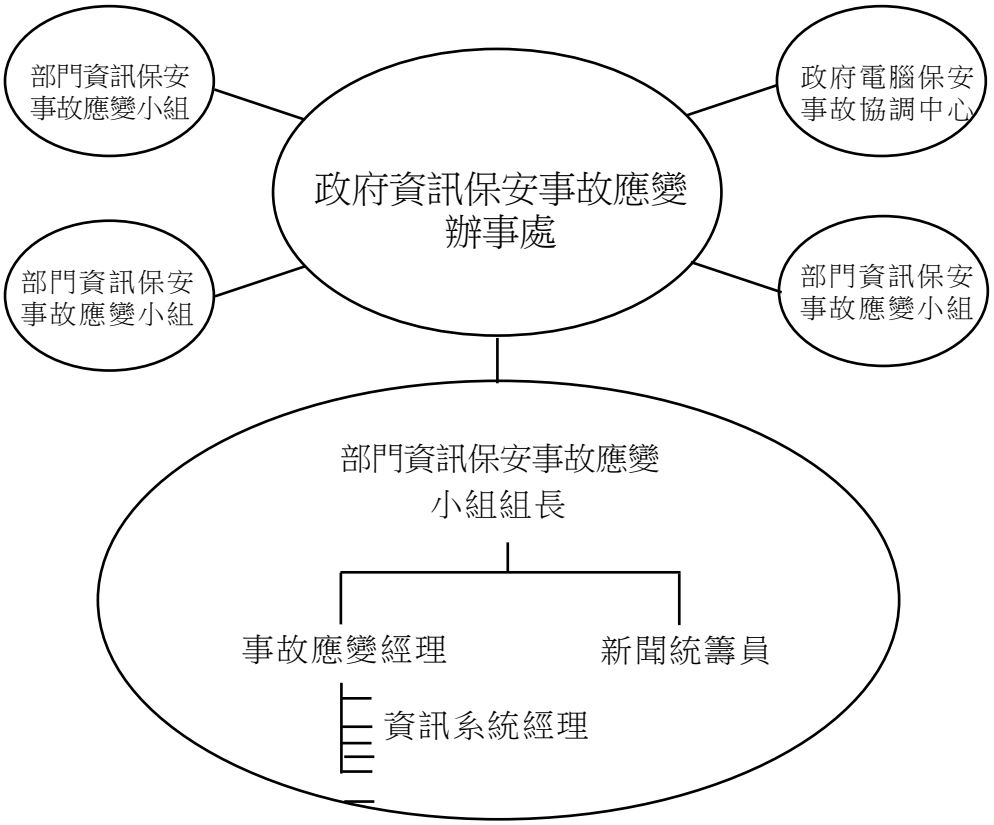


圖 4.1 參與保安事故處理的各方

本章闡述資訊保安事故處理的高層次組織架構和參與資訊保安事故處理工作各方的職務和職責。資訊保安事故應變小組及負責部門資訊系統的人員，應根據決策局／部門或相關系統的特殊業務需要和操作要求，制訂詳細的資訊保安事故處理程序。

4.1 政府資訊保安事故應變辦事處

政府資訊保安事故應變辦事處（GIRO）是為整個政府提供服務的組織，負責中央統籌及支援各個決策局／部門內的資訊保安事故應變小組，以處理資訊保安事故。

政府資訊保安事故應變辦事處常設辦公室扮演政府資訊保安事故應變辦事處的執行機構。政府資訊保安事故應變辦事處常設辦公室主要功能包括：

- 在資訊保安事故報告中扮演資訊保安事故應變小組組長的中心聯絡點，以及為可能涉及整個政府的資訊保安事故作應變協調。
- 就事故跟進進度，以及提醒相關的部門資訊保安事故應變小組提交事後報告及中期報告。
- 與政府電腦保安事故協調中心緊密合作，並在有需要時尋求對方建議。
- 若涉及刑事行為，與香港警務處網絡安全及科技罪案調查科緊密合作。

4.1.1 政府資訊保安事故應變辦事處的職能

政府資訊保安事故應變辦事處主要有以下職能：

- 設立中央數據庫，並監督政府內部對所有資訊保安事故的處理。
- 定期編製政府資訊保安事故統計報告。
- 充當中央協調辦事處，以應付多點保安攻擊（即不同的政府資訊系統同時遭受攻擊）。
- 促使決策局／部門的資訊保安事故應變小組互相分享和交流資訊保安事故處理的經驗和資料。

4.1.2 政府資訊保安事故應變辦事處的結構

政府資訊保安事故應變辦事處的核心成員包括來自下列決策局／部門的代表：

- 數字政策辦公室
- 保安局
- 香港警務處

視乎不同保安事故的性質，必要時可能會邀請個別決策局／部門的資訊保安事故應變小組成員和其他專家，為政府資訊保安事故應變辦事處的運作提供協助。

政府資訊保安事故應變辦事處常設辦公室負責為政府資訊保安事故應變辦事處提供秘書處和職能方面的支援，並於應付可能影響整個政府的資訊保安事故時，擔任各部門資訊保安事故應變小組組長間的中心聯絡點，以收集資訊保安事故報告和統籌應變行動。

各決策局和部門須向政府資訊保安事故應變辦事處常設辦公室提供資訊保安事故應變小組組長的聯絡資料，如資料有任何更改，應向常設辦公室提供最新的資料，以確保資訊有效傳遞。部門資訊科技保安聯絡資料更新表載於**附件 A**。

政府資訊保安事故應變辦事處在必要時可成立特殊專責小組（例如在發生多點攻擊時），就影響遍及多個決策局／部門及／或政府整體運作和穩定的保安事故，協調應變工作。

4.2 政府電腦保安事故協調中心

政府電腦保安事故協調中心於 2015 年 4 月成立，與政府資訊保安事故應變辦事處常設辦公室合作，負責協調政府內部的資訊和網絡保安事故。該中心還與其他電腦應變小組合作共享事故資訊和威脅情報，並互相交流良好實踐及做法，以加強該地區的資訊和網絡保安能力。政府電腦保安事故協調中心具有以下主要功能：

- 就即將發生和實際威脅，向決策局／部門發出保安警報。
- 作為電腦保安事故協調中心與其他電腦應變小組合作在處理網絡保安事件時的橋樑。

4.3 部門資訊保安事故應變小組

根據基準資訊科技保安政策，各決策局／部門須成立資訊保安事故應變小組。該小組是決策局／部門內部負責協調、傳訊和採取保安事故處理行動的協調中心。資訊保安事故應變小組的規模應按不同決策局／部門資訊系統的規模和範圍、系統的敏感程度以及保安事故對決策局／部門的潛在影響，作出相應調整。

雖然政府資訊保安事故應變辦事處負責集中統籌資訊保安事故的報告，並為個別資訊保安事故應變小組提供協調和諮詢支援，但各決策局／部門的資訊保安事故應變小組，仍須在處理決策局／部門內發生的保安事故時，負責整體指揮和控制。

4.3.1 資訊保安事故應變小組的職能

資訊保安事故應變小組的主要職能應包括：

- 整體監督和協調決策局／部門內部所有資訊科技系統的保安事故處理。
- 在報告保安事故方面，與政府資訊保安事故應變辦事處合作，以便中央記錄和採取必要的跟進行動，例如報告警方作進一步罪案調查。
- 轉發政府資訊保安事故應變辦事處就即將發生及已經發生的事故所發放的警報，給決策局／部門內部負責有關工作的各方人士。
- 促進決策局／部門內部就保安事故處理，以及其他相關事務分享經驗和交流資訊。

4.3.2 資訊保安事故應變小組的結構

資訊保安事故應變小組是決策局／部門內協調所有資訊科技保安事故的中央聯絡點。決策局／部門首長應從高層管理人員中挑選一名人員，擔任資訊保安事故應變小組組長。組長應有權任命資訊保安事故應變小組的核心成員。

在籌組資訊保安事故應變小組時，部門資訊科技保安主任應給予建議和支持，以協助資訊保安事故應變小組組長為部門資訊系統制訂個別系統的特定保安政策和事故應變計劃，並制訂相關的後勤安排。部門資訊科技保安主任還須確保所在決策局／部門的所有資訊系統，已遵守和履行部門整體資訊科技保安政策的規定。

雖然資訊保安事故應變小組可根據決策局／部門的不同電腦設備情況，決定小組成員的實際組合，但資訊保安事故應變小組內也有一些必要的關鍵職務，包括資訊保安事故應變小組組長、事故應變經理、新聞統籌員和資訊系統經理等。這些職務可由多人或一人負責。決策局／部門應定期評估團隊的工作量並相應地分配資源，以避免瓶頸和延誤。

下文將詳述資訊保安事故應變小組內各角色的職責。

4.3.3 資訊保安事故應變小組成員的職責

(a) 組長

組長的職責包括：

- 全面監督及協調處理決策局／部門內所有資訊系統的資訊保安事故。
- 根據事故應變經理提供的事故報告及分析，就控制損毀、系統復原、外部機構委聘及其所參與工作的程度，以及復原後恢復正常服務的後勤工作等關鍵事項作出決策。
- 因應事故對決策局／部門業務運作的影響，在適當情況下啟動部門的運作復原程序。
- 代表管理層批核為事故處理程序投放的資源。
- 代表管理層批核就事故的立場所作的公眾發布。
- 在報告資訊保安事故（特別是報告具有下列特點的資訊保安事故）方面，與政府資訊保安事故應變辦事處常設辦公室協調及合作，以便作中央記錄及採取必要的跟進行動：
  - (i) 直接提供公共服務的系統，而且系統故障可能導致服務中斷（例如向政府互聯網網站的拒絕服務攻擊）
  - (ii) 處理保密資料的系統
  - (iii) 支援關鍵任務操作的系統
  - (iv) 一旦發生保安事故，可能造成重大不良影響的系統，例如因網站遭塗改而使政府形象受損
- 促進決策局／部門內部互相交流和分享資訊保安事故處理及相關事宜的經驗和資料。
- 與調查機關協調及配合調查保安事故。

(b) 事故應變經理

事故應變經理負責監察決策局／部門內部的所有保安事故處理程序，並為處理事故程序尋求管理層提供資源和支持。事故應變經理的職責包括：

- 整體管理及監督決策局／部門內部與保安事故處理相關的所有事務。
- 在接獲影響部門資訊系統的保安事故報告後，通知資訊保安事故應變小組組長。
- 與資訊系統經理和有關方面跟進保安事故，彙編事故報告和進行分析。
- 向資訊保安事故應變小組組長匯報保安事故處理程序的進展情況。

- 在處理資訊事故時與警方、個人資料私隱專員公署、服務承辦商、服務支援供應商及保安顧問等外部機構和人士協調。
- 為事故處理工作，向資訊保安事故應變小組組長尋求提供所需的資源和支持。

(c) 新聞統籌員

新聞統籌員負責回覆公眾有關決策局／部門保安事故的查詢。新聞統籌員還負責整體控制和監督向公眾（包括傳媒）發布資訊的工作。

(d) 資訊系統經理

應撥出特定的資源來應付個別資訊系統、電腦服務或職能範圍可能發生的保安事故。

當處理資訊保安事故時，個別部門支援小組的規模和結構將視乎部門系統的範圍和性質而有所區別。舉例來說，就小型、非關鍵的內部系統而言，一人便已足以履行事故應變的職責。

對於個別部門的資訊系統，相關的部門資訊系統經理將監督整個系統保安事故處理流程或其職責範圍。經理應代表個別部門資訊系統下的支援小組，提供以下主要功能：

- 監督所負責職能範圍的保安事故處理程序。
- 事先制訂相關的事故處理程序和聯絡名單，以加快及推動處理程序。
- 提供直接接收可疑事故報告的途徑。
- 直接並即時回應可疑活動。
- 協助將破壞減至最少，並回復系統正常操作。
- 向服務承辦商、電腦產品供應商、警方或個人資料私隱專員公署等外部機構和人士尋求有關保安問題的意見。
- 與其他外部機構和人士協調相關資訊系統的保安事故處理工作。
- 就所負責職能範圍，對來自資訊保安事故應變小組和政府電腦保安事故協調中心的保安警報，進行影響分析。

如果資訊系統的部分操作或全部操作均已外判予外部服務供應商及／或已包括在其他政府部門提供的服務範圍內，則外判服務供應商及／或提供服務的部門亦應委任資訊系統經理及成立類似的支援小組以應對該特定的資訊系統，並提供與其職責相應的服務。

除提供以上主要功能，資訊系統經理應負責以下職務:

- 制訂及推行個別系統的保安事故應變程序。
- 遵守並遵從保安事故應變程序，向決策局／部門的資訊保安事故應變小組報告事故。
- 與服務供應商、承辦商和產品支援供應商等相關各方安排及協調，針對事故採取修正和復原行動。
- 向資訊保安事故應變小組報告保安事故，在資訊保安事故應變小組的管理支持下，於調查和收集證據的過程中對外尋求協調，例如尋求警方、個人資料私隱專員公署或香港網絡安全事故協調中心的協助。
- 掌握最新的資訊保安科技和技術，並了解與系統或所負責職能範圍相關的最新保安警報和保安漏洞。
- 利用保安工具／軟件及／或系統記錄並檢查審計追蹤記錄，找出可疑的攻擊或未獲授權的接達。
- 在診斷問題和復原系統過程中，提供有助於證據收集、系統備份和復原、系統配置和管理等技術支援。
- 為資訊系統安排定期保安評估、影響分析和覆檢。

5. 保安事故處理步驟概覽

保安事故處理共有 5 個主要步驟，有關概述見下文。各步驟所涉及的過程在相應章節會有更詳細描述。

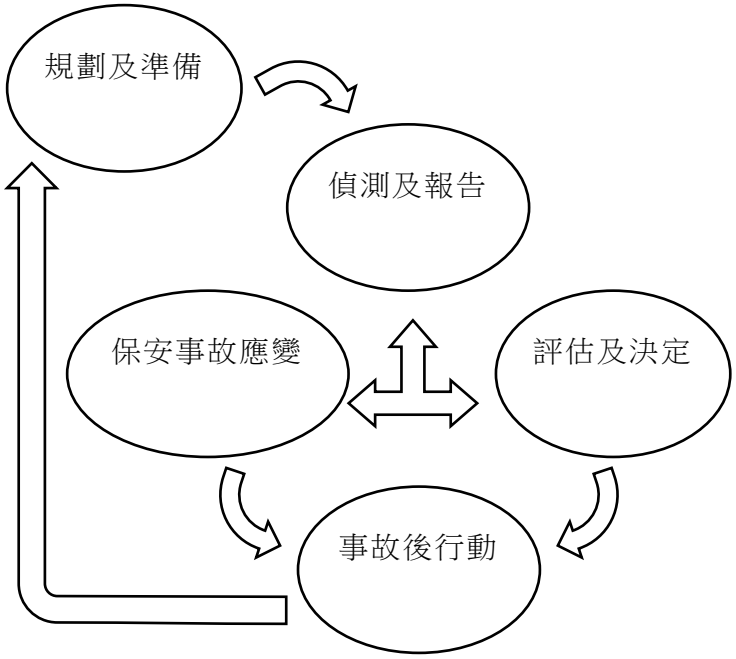


圖 5.1 保安事故處理的循環過程

A. 規劃和準備（第 6 章）

在這步驟中，決策局／部門應規劃和準備資源，並制訂適當程序，以備日後遵照執行。本步驟中規劃和準備所涉及的主要活動如下。

- 規劃事故監察和偵測
- 規劃保安事故應變
- 規劃培訓與教育

B. 偵測及報告（第 7 章）

在這步驟中，決策局／部門應根據建立的檢測和監控機制檢測保安事件。決策局／部門也應遵循報告程序，使保安事件得到部門資訊保安事故應變小組的關注。這一步有兩個主要的活動：

- 偵測措施
- 報告

C. 評估及決定（第 8 章）

偵測到事件後，決策局／部門應確定是否真有事故發生。如果事件被識別為資訊保安事故，決策局／部門應確定事故的類型，並評估其範圍、損害和影響，以有效處理事故。決策局／部門還應遵循事先規劃的升級處理程序通知相關方面，並將事件升級到適當的級別。這步驟涉及的主要活動有：

- 事故評估
- 升級處理

D. 保安事故應變（第 9 章）

當識別到保安事故時，決策局／部門應遵循保安事故應變程序，採取行動處理保安事故，恢復系統正常運作。應變程序大致分為三個階段：

- 遏制
- 杜絕
- 復原

E. 事後跟進（第 10 章）

事故結束後，應採取後續行動對事故進行評估，加強保安防範，防止再次發生。主要後續行動如下：

- 事故事後分析
- 保安事故報告
- 保安評估
- 覆檢現行的保護措施
- 調查及檢控

6. 規劃和準備

適當的事先規劃可確保人員對應採取的事故應變及復原行動有所了解，使其能在互相配合及有條不紊的情況下執行。決策局／部門須備存最新資訊系統清單，當中附有保安事故處理的緊急聯絡點。及早計劃還有助決策局／部門在處理保安事故時作出適當和有效的決定，從而將保安事故可能造成的破壞減到最少。保安事故應變計劃包括加強保安保護措施、採取適當的事故應變、系統復原和其他跟進工作。

規劃和準備所涉及的主要工作如下：

- 規劃事故監察和偵測
- 規劃保安事故應變
- 規劃培訓與教育

保安事故應變準備工作清單列於**附件 B**，以供參考。

6.1 規劃事故監察和偵測

須推行足夠程度的事故監察保安措施，以便在系統正常操作期間保護系統，同時監察潛在的保安事故。所採取措施的程度和範圍取決於系統、系統數據及系統功能的重要性和敏感度。

下列是一些常用的保安事故監察措施：

- 安裝防火牆設備，並採取認證和接達控制措施，以保護重要系統和數據資源。
- 安裝入侵偵測工具，主動監察、偵測並就系統入侵或黑客活動作出應變。
- 安裝抗惡意程式工具和惡意軟件偵測及修復工具，以偵測及清除惡意軟件，並防止惡意軟件影響系統操作。
- 利用保安掃描工具定期進行保安檢查，以找出現有的保安漏洞，並進行既定保安政策與實際保安安排之間的差距分析。
- 安裝內容過濾工具，以偵測電子郵件或網絡通訊的惡意內容或程式碼。
- 開啓系統及網絡審計記錄功能，以便偵測和追蹤未獲授權的活動。
- 開發程式和指令碼協助偵測可疑活動、監察系統和數據的完整性，以及分析審計記錄資料。

- 訂閱保安新聞、警報、漏洞資訊、報告和其他資訊保安出版物，對新興的保安威脅和相關風險保持警覺。
- 備存並記錄漏洞管理機制，以識別、評估和減低保安風險。
- 將威脅情報來源和資料應用到監察流程中。威脅情報整合與應用請參考《資訊科技保安威脅管理實務指引》。

6.2 規劃保安事故應變

決策局／部門須委任兩位指定人士作為事故處理的 7x24 聯絡點，以確保持續可用及可即時回應保安事故。這些人員必須全天候（包括週末和假日）隨時可聯繫，並準備好參與事故處理活動。

對聯絡點的期望包括：

- 指定的聯絡點必須隨時待命，以接聽和回應有關資訊科技保安問題的緊急電話，即使是在非工作時間。這對於促進即時溝通和快速事故處理、有效減少保安事故造成的潛在損害和損失至關重要。
- 指定聯絡人應迅速確認收到的任何通訊並採取行動，確保事故應變過程不會出現延誤。
- 指定聯絡人必須能夠直接處理保安事故，或有權限和能力將緊急保安資訊及時轉發給負責人員。
- 決策局／部門應定期核實指定人士的聯絡方式，以確保他們的聯絡方式是最新的，並且在有需要時可以無障礙地立即聯繫他們。

須制訂及記錄保安事故應變計劃。保安事故應變計劃須至少包括以下內容：

- 事故應變小組的結構以及相應的角色和職責；
- 報告程序；
- 緩解事故影響、保留證據、調查事件原因和影響的程序；
- 復原計劃；
- 與利益相關者和公眾的溝通計劃；和
  事故後的覆檢程序。

保安事故應變計畫須至少每兩年定期檢討一次，或當決策局／部門的運作環境有任何重大改變時進行。決策局／部門須確保所有相關人員熟悉該計劃，並且全體人員（包括管理層人員）均應知悉該計劃，以作為參考和遵行有關要求。這套計劃應清晰直接而且容易理解，讓全體人員清楚了解他們需採取的行動。決策局／部門應在事故應變計畫中納入不同的場景及相應的應變程序。事故應變計劃須定期進行測試和更新，以確保可迅速及有效地就資訊保安事故作出應變。此外，決策局／部門須至少每兩年進行一次演習，最好每

年進行一次，以評估計劃的有效性。事故應變小組成員須參加演練，以熟習自己在保安事故應變計畫中的角色，確保快速和有效地應變保安事件。

有關事故應變演習流程及不同情景的行動卡詳情，請參閱政府內聯網「資訊科技情報網」的「資訊科技保安專題」網頁 (https://itginfo.ccgo.hksarg/content/itsecure/sih/actioncard/index.html)。

6.2.1 事故應變小組的結構以及相應的角色和職責

事故應變小組的結構和參與保安事故應變工作各方的角色和職責應明確制定。上述第 4 章為制定保安事故應變小組主要成員的職務和職責提供了參考的模型。

6.2.2 報告程序

(a) 報告

須建立及記錄一套報告程序，清楚制定任何可疑活動的報告步驟和程序，以便及時向有關各方作出報告。報告程序應列明詳盡的聯絡資料，例如電話號碼（包括辦公時間及非辦公時間內的聯絡電話號碼和流動電話號碼）、電郵地址和傳真號碼等，以確保負責人員之間能夠有效溝通。一些建議的報告機制載於**附件 C** 第 1 節，以供參考。

事先應制訂適當的報告程序，以便一旦發生保安事故，參與事故應變的全體人員知悉應向何人和以何種方式報告，以及應注意和報告的事項。

為有效執行報告程序，應注意以下幾點：

- 報告程序應載列明確的聯絡點，並制訂簡單但明確的步驟以便遵從。
- 向所有相關人員發布報告程序，以供參閱和參考。
- 確保所有相關人員熟習報告程序，並能夠立即報告保安事故。
- 編製保安事故報告表，以規範所收集的資料。
- 考慮是否需要在非辦公時間啟動報告程序，如確有需要，應制訂一份獨立的非辦公時間報告程序，並指定相關人員擔任非辦公時間聯絡人。
- 有關事故的資料應根據「有需要知道」原則披露，除資訊保安事故應變小組組長外，任何其他人士均無權閱覽，也不得授權他人將有關保安事故的資料與他人分享。

為改善資訊科技保安事故處理的效率和效益，當政府部門發現有跡象顯示可能發生資訊保安事故，可諮詢政府資訊保安事故應變辦事處常設辦公室的建

議。**附件 F** 第 1 節載列了此類事故的常見跡象。

透過向政府資訊保安事故應變辦事處尋求意見，決策局／部門可以主動識別和解決系統異常情況，確保及早發現整個政府的資訊科技保安威脅和事件。這種協作方法可以維護整體安全並創造一個具復原能力和安全的環境，從而使政府受益。

當知悉資訊保安事故時，部門資訊保安事故應變小組須：

- 於 **60 分鐘**內向政府資訊保安事故應變辦事處常設辦公室作電話滙報，並於 **48 小時**內提交完整的資訊保安事故初步報告表（見**附件 C** 第 2 節）；
- 如保安事故牽涉關鍵電子政府服務、對保安有重大影響，或會引起傳媒注意，盡快向政府資訊保安事故應變辦事處常設辦公室分享以下資料：
  - (i) 事故類別及對事故範圍、破壞及影響的評估；
  - (ii) 為遏止破壞及修正問題而正在或將會採取的行動；
  - (iii) 若引起傳媒注意時的回應口徑；以及
  - (iv) 傳媒的查詢及回應建議（如有）。
- 每日向政府資訊保安事故應變辦事處常設辦公室更新受影響的關鍵電子政府服務的修復狀況，直至服務恢復為止。
- 就任何已向香港警務處、個人資料私隱專員公署報告或向傳媒機構發布的保安事故，通知政府資訊保安事故應變辦事處常設辦公室。

根據總務通告第 6/2024 號「加強資訊科技系統的管治和保安」，若決策局／部門的政府資訊科技系統發生資訊科技保安事故，而有關局長認為事故已令政府尷尬或損害其監督角色的形象，有關的項目負責人員(就「指定資訊科技系統」)或部門資訊科技保安主任(就決策局／部門的所有其他資訊科技系統)須在事故發生後兩個曆日內向其局長提交資訊科技保安事故初步報告，然後在七個曆日內提交資訊科技保安事故全面報告。載有建議跟進工作並經相關局長批核的事故全面報告須提交予數字辦，以作記錄、監察和視乎情況給予技術意見。決策局／部門應參閱總務通告第 6/2024 號及其專題網站(https://sgsits.host.ccgo.hksarg)以了解更多有關提交和匯報政府資訊科技保安事故報告的詳情。

決策局／部門被視為「知悉」事故的成立基準是，當合理程度上確定資訊保安事件已對政府資訊系統或數據資產的機密性、完整性或可用性造成損害，或已對決策局／部門的運作造成損害。這種認知通常在對情況進行初步評估後建立，這可能需要一些時間才能徹底進行。

對事故的知悉可能在多種情況下產生。例如：

- 如果檢測到不尋常的系統行為，例如非預期的資料匯出或不尋常的登錄模式，並且經調查發現這些行為與未獲授權的接達或資料洩露有關，決策局／部門將被視為對事故「知悉」。
- 如果決策局／部門從外部實體收到可靠資訊表明未獲授權的披露，則該確認將構成對事故的「知悉」。
- 如果發生勒索軟件攻擊，決策局／部門發現攻擊者的加密文件和勒索字條，一旦該攻擊得到內部驗證，決策局／部門將被視為對事故「知悉」。

對事故的知悉不一定是最初發現異常時，而是在初步調查確認保安事故確實發生後。事故的具體細節將影響確認事件的時間線。

決策局／部門在發現或收到潛在事故通知後立即作出應變，啟動初步調查以確定事故是否確實發生，這一點至關重要。這初始階段是關鍵的，不應被誤認為是對事故的「知悉」階段。只有當調查以合理的確定性證實該事故時，決策局／部門才正式「知悉」。

然而，重點仍應是迅速採取行動調查保安事件，如果得到證實，則採取修正措施並進行相應報告。及早報告可疑保安事故可以為保護整體安全和營造一個完善和安全的環境作出貢獻，使政府受益匪淺。值得注意的是，在初步報告後，如後續調查顯示懷疑的保安事故並未發生，決策局／部門須向數字政策辦公室通報情況。

應在解決事故後的 1 星期內，向政府資訊保安事故應變辦事處常設辦公室提交事故事後報告。對於需要較長時間完成調查的個案，有關的部門資訊保安事故應變小組須根據以下規定，就最新的修復情況及調查進度向政府資訊保安事故應變辦事處常設辦公室提交中期報告：

- 於首次報告事故後 14 日內向政府資訊保安事故應變辦事處常設辦公室提交第一份中期報告；以及
- 為令管理層獲悉狀況，每 3 個月向政府資訊保安事故應變辦事處常設辦公室提交事故調查進度，直到結案爲止。

附件 C 第 3.1 節載有報告樣本以供參考。

(b) 升級處理

升級處理程序是指將事故上報管理層和有關方面，以確保立即作出重要決策的程序。

在發生事故時，往往需要處理大量緊急事項，所以很難找到適當人選處理林林總總的事項。為順利執行保安事故處理的各階段工作，應事先編備處理法律、技術和管理事項所需的重要聯絡名單。因此，制訂升級處理程序是準備和規劃階段的主要工作之一。

升級處理程序按事故的類別和影響的嚴重程度，載列內部和外部各級別人員的聯絡點及各聯絡點的聯絡資料。

就不同類別的事故，升級處理程序的聯絡點和跟進行動也可能有所區別。不同類別的事故涉及不同的專業知識或管理決策，所以應編備特定的聯絡名單以處理這些事故。

有關升級處理程序的建議和升級處理程序示例載於**附件 D**，以供參考。報告及升級處理政府資訊保安事故的工作流程示例載於**附件 E**，以供參考。

6.2.3 保安事故應變程序

視乎不同系統和管理需要，事故處理程序宜包括：

- 評估事故的影響和破壞
- 盡快使系統恢復正常操作
- 盡量減輕事故對其他系統的影響
- 避免進一步發生事故
- 找出事故的根本成因
- 收集證據為日後的個案調查提供證明
- 有必要時更新政策和程序

部分事故的性質過於複雜或規模過大，以致難以在同一時間解決所有問題。為處理的事項訂定緩急次序便是一個關鍵步驟，讓事故應變人員可以聚焦先處理最關鍵事項。建議優先處理以下的事項：

- 保障生命和人身安全
- 保護關鍵資源
- 保護遺失或損毀後會造成較大損失的敏感或重要資料
- 防止停頓後會造成較大損失及復原成本較高的系統受到損壞
- 對服務中斷的影響減到最少
- 維護決策局／部門或政府整體的公眾形象

6.2.4 復原計畫

有效的復原計畫對於保安事故後將系統恢復正常操作至關重要。復原計畫應該全面、有據可查，並包括確保恢復後系統安全性和完整性的步驟。

復原計畫應包括：

- 評估損害和識別受影響服務的程序。
- 復原系統和恢復服務的緩急次序。
- 安全地重新安裝損壞或受入侵組件的步驟。
- 確保系統恢復到正常狀態的驗證過程。
- 用於通知相關方復原狀態的通訊規約。

復原過程應包括以下步驟：

- 進行徹底的損害評估，以確定事故的範圍和影響。
- 確定功能和服務的恢復順序，優先考慮必需服務和影響大多數使用者的服務。
- 從可信賴來源重新安裝損壞或刪除的文件，確保軟件的完整性和安全性。
- 從最關鍵的服務開始，以受控方式恢復功能／服務。
- 確認系統已恢復至正常操作且沒有留下保安事故的痕跡。
- 通報所有相關方系統恢復操作的情況，確保操作員、管理員和高級管理人員了解當前狀態。
- 關閉所有不必要的服務，以最大程度地減少系統的攻擊面。
- 記錄復原過程中採取的所有操作。

第 9 章提供處理保安事故的參考模型，特別在遏制、杜絕和復原程序等方面。

6.2.5 溝通計畫

應建立與利益相關者和公眾的溝通程序。溝通對於控制圍繞事故的訊息至關重要，包括傳遞訊息的地點、時間、內容和方式。有效應變和恢復需要內部溝通，維護政府形象也離不開外部溝通。有關事故的不受控制的溝通可能會產生嚴重後果。只有經過適當授權和準備的人員才可以在最佳時機以適當的形式代表決策局／部門進行溝通，告知必要的資訊。

有效的溝通計畫應先確定事件期間需要通知的關鍵受眾。這些通常包括內部利益相關者（例如使用者、管理層和事故應變團隊）和外部利益相關者（例如民眾、合作夥伴、監管機構和媒體）。對於每個受眾，計畫應指定具體的訊息、溝通渠道以及提供更新的頻率。

該計畫應詳細說明通訊基礎設施，包括主要和備用通訊方法，以確保資訊流不間斷。這可能涉及電子郵件、內部公告、新聞稿、社交媒體和新聞發布會。基礎設施必須足夠完善以應對危機期間增加的通訊量。

溝通計畫中必須明確定義角色和職責。這包括任命接受過危機溝通訓練的一名發言人或一隊發言人團隊，向公眾和媒體傳遞訊息。還應該有訊息的批准和傳播的規約，以確保一致性和準確性。

該計畫還應包括針對各種場景而預先起草的範本，以加快溝通速度。這些範本可以快速調整以符合事故的具體細節，確保快速應變。

溝通計畫必須靈活並就不斷變化的事故性質而調整。它應包括一個回饋循環來評估溝通的有效性並作出必要的調整。事故解決後，覆檢溝通流程對於確定甚麼內容有效以及甚麼內容可以為未來事故進行改進至關重要。此覆檢過程確保溝通計畫是一個根據過去的經驗不斷發展的動態文件。

6.2.6 事故後的覆檢程序

事故後覆檢是保安事故應變計畫的重要組成部分。它徹底分析了事故、其應變和復原步驟。事故後覆檢程序應有條理並記錄在案，納入吸取的經驗教訓，以改善未來的應變和預防措施。覆檢應評估保安事故的處理，識別成功和失敗之處，並詳細說明提高未來事故應變能力的行動。覆檢應包括：

- 事故的初步發現和報告。
- 應變和遏制策略的有效性。
- 執行溝通計畫的準確性和效率。
- 復原計畫的充分性及其執行情況。
- 恢復正常操作和服務。
- 證據保存過程及其在分析中的作用。

覆檢程序的結構應如下：

- 覆檢應在恢復階段後和恢復正常操作後啟動。
- 應收集和覆檢與事故相關的所有文件和日誌，以重建時間表和採取的行動。
- 根據既定指標評估應變績效，並識別與應變計畫的任何偏差。
- 與事故應變團隊、管理層和其他相關利益者召開會議，討論事故並收集回饋。
- 準備一份綜合報告，其中包括：
    - 事故及其影響的摘要。
    - 應對措施的優點和缺點。
    - 未來改進的建議。
    - 解決已發現的弱點的可行步驟。

- 應召開會議討論報告結果，確保所有利益相關者了解結果和必要的改進。

事故應變小組須負責以下事項：

- 追蹤覆檢期間所識別改進的實施情況。
- 根據需要更新政策、程序和應變計畫。
- 進行培訓和提高意識課程，以解決已發現的差距。
- 重新評估並調整指標，以更好地衡量未來的事故應變。

應保留所有事故後覆檢的記錄，以便為未來的事故應變和合規要求提供資訊。這些記錄應是安全並只有獲授權人員才能接達。事故後覆檢過程應是迭代的，每個事故都為保安事故應變計畫的持續改進提供見解。

6.3 規劃培訓與教育

決策局／部門須確保全體員工均遵守及遵從相應的資訊系統保安事故應變計畫。各人員應熟習由事故報告、確認、採取適當行動到恢復系統正常操作的處理事故程序。決策局／部門應定期舉行事故處理演習，使人員熟習有關程序。決策局／部門亦須參加數字政策辦公室指定的保安演習。進行演習後，應對結果進行覆檢，並提出建議，以在適當情況下改善事故處理程序。

此外，為了加強系統或職能範圍的保安保護措施，並減低發生事故的機會，應向系統操作和支援人員提供足夠的培訓，使他們掌握有關保安預防的知識。由於終端用戶往往最先察覺問題發生，因此應鼓勵他們報告異常情況或涉嫌違反保安的情況。

7. 偵測及報告

7.1 偵測措施

決策局／部門應確保推行偵測及監察機制以偵測保安事件。決策局／部門應偵測資訊保安事件的發生，並輔以以下資料，就事件作出報告：

- 網絡監察裝置（例如防火牆、網絡流量分析工具或網頁過濾工具）的警示。
- 保安監察裝置（例如入侵偵測系統、入侵防禦系統、抗惡意軟件方案、記錄監察系統或保安資訊管理系統）的警示。
- 來自裝置、服務、主機及不同系統的記錄資料分析。
- 來自用戶或服務台的報告。
- 來自外來人士（例如威脅情報平台、其他資訊保安事故應變小組、電訊服務供應商、互聯網服務供應商、一般大眾、媒體或外聘服務供應商）的外部通知。

資訊保安事故應變小組應維護決策局／部門裡所有資訊保安事件的清單。

7.2 報告

人員應跟從報告程序，讓資訊保安事故應變小組注意有關保安事件。所有人員都須清楚知道及可以取得報告程序，以便報告不同種類的潛在資訊保安事件。下列資料應是報告資訊保安事件的依據：

- 偵測日期／時間
- 受影響系統
- 觀察
- 報告該保安事件人士的聯絡資料

8. 評估及決定

在發現可疑活動後，資訊系統的用戶、操作員或管理員應遵照既定的報告程序，向有關資訊系統經理報告事故。收集資料時可使用標準保安事故報告表，該報告表還可用作進一步調查和分析之用。另一方面，入侵偵測工具和系統審計記錄等監察工具亦可用來協助偵測未獲授權或異常活動。

在偵測到異常情況後，資訊系統經理應確認事故，此階段的工作包括以下步驟：

- 判斷是否已發生事故，並進行初步評估
- 記錄事故
- 如有需要，記錄系統當前狀況

要決定是否已發生事故，決策局／部門應考慮包括但不限於以下情況：

- 有關系統是否在政府內部推行；
- 如有關系統並非在政府內部推行，

(i) 該系統是否由政府提供和維護；以及

(ii) 事故是否由系統的保安漏洞或不受政府控制的因素造成；例如推行該系統的一方犯錯或違反政府的建議遺漏部分程序。

舉例來說，決策局／部門發現由其提供和維護的系統存在保安漏洞，而該系統並非在政府內部推行。其後，決策局／部門為保安漏洞提供修補程式，並通知推行該系統的用戶安裝。如果用戶沒有安裝，然後所推行的系統被黑客入侵，這通常不應視為政府保安事故。在類似情況下，如智能手機所安裝的流動應用程式已獲提供保安修補程式，但用戶沒有安裝該修補程式，該手機所發生的違反保安事件也不算保安事故。

8.1 事故評估

首先，資訊系統經理應判斷是否確實發生事故。然而，判斷所發現的異常情況是否就是發生事故的跡象往往十分困難。有些異常情況可能是由另外一些原因造成的（例如硬件故障或用戶操作錯誤）。

為判斷某種異常情況是系統問題還是真正事故所造成，資訊保安事故應變小組應收集有關資訊保安事件的資訊，並要求報告保安事件的人士作任何澄清。當政府部門發現有跡象顯示可能發生資訊保安事故，如有需要，可諮詢政府資訊保安事故應變辦事處常設辦公室的建議。**附件 F** 載列了一些值得特別注意的典型事故跡象、典型保安事故，以及決定事故範圍及影響時需考慮的因素，以供參考。

8.2 升級處理

在某事件被識別為資訊保安事故後，系統經理應判斷事故的類別、評估事故的範圍、破壞和影響，以便作出有效的應變。此初步分析流程對於了解事故和制定適當的相應措施起著至關重要的作用。通過實施結構化的初步分析流程，我們可以確保對事故進行徹底評估，並及時採取必要的預防措施和防禦措施。應利用標準化的檢查表作為收集事故詳細資訊和評估關鍵因素的指南，以輔助此流程。

在通知適當的有關各方並將事件升級到適當的級別時，檢查表應與升級處理流程無縫整合。在描述升級處理過程中的事故時，建議包含以下資訊：

A. ***事故詳細資訊：***記錄事故的日期和時間，以及簡短的摘要描述。此資訊將提供事故時間線和性質的快照。

1. ***日期和時間：***記錄事故發生或首次檢測到的確切日期和時間。該時間戳記將作為追蹤事故進展和回應時間線的參考點。
2. ***事故摘要：***提供事故的簡明描述。包括相關詳細資訊，例如事故的性質（例如保安性漏洞、系統中斷、資料丟失）、受影響的系統以及任何初步觀察結果或症狀。該摘要將幫助利益相關者快速掌握事故的背景並採取適當的應對行動。
3. ***事故分類：***根據預先定義的類別或嚴重級別對事故進行分類。常見的分類可能包括保安事故、技術故障、人為錯誤或自然災害。對事故進行分類有助於確定回應工作的緩急次序並有效地分配資源。
4. ***事故來源：***確定事故的來源或起因（如果已知）。這可能是觸發事故的特定事件、操作或外部因素。了解事故來源可以提供對潛在原因的寶貴見解，並有助於確定預防措施。

5. ***報告方：***注明報告該事故的個人或團隊。如有必要，附上他們的聯繫資訊，以便進一步溝通或澄清。此資訊有助於與報告方建立直接溝通渠道，以獲取更多事故詳細資訊或更新。
6. ***通知和升級：***記錄有關事故的任何初始通知或升級。包括通知的個人或團隊、使用的溝通渠道以及通知時間。此資訊可以幫助確保正確啟動事故應變流程並將其傳達給利益相關者。

   (i) 知情方：記錄向哪些相關方通報了該事故，包括香港警務處、個人資料私隱專員公署和媒體（如果相關）。

   (ii) 採取的行動：記錄事故發生後立即採取的行動。這可能包括隔離受影響的系統、啟動鑑證或啟動危機管理團隊。

B. ***系統資訊：***包括有關受影響系統及其擁有者的詳細資訊。如果多個部門共同擁有一個系統，請注明所涉及的相關部門。了解擁有權對於有效的溝通和協作至關重要。

1. ***系統擁有者聯繫資訊：***提供一個子欄位來記錄系統擁有者或受影響系統負責人的詳細聯繫資訊（姓名、電子郵件、電話）。這些資訊將有助事故應變期間的溝通和協調。

2. ***系統關鍵性：***系統關鍵性有助於確定與事件相關的影響程度和緊急程度。評估系統關鍵性時考慮以下因素：

   2.1. ***系統等級：***每個受影響系統的指定系統等級。
   2.2. ***業務影響：***評估受影響系統的丟失或降級對關鍵業務運營的影響。考慮創收、使用者服務、規管遵行性和聲譽等因素。
   2.3. ***可用性要求：***根據業務和操作需求確定系統可用性的預期級別。考慮服務級別協定、正常執行時間要求以及系統在支援時間敏感流程中的角色等因素。
   2.4. ***數據敏感性：***評估受影響系統處理、存儲或傳輸的資料的敏感性和機密性。
   2.5. ***復原時間目標：***復原時間目標表示事故發生後將系統恢復到全部功能的最大可容忍持續時間。它有助於優先考慮應變工作並有效分配資源。
   2.6. ***復原點目標：***復原點目標表示復原過程中可容忍丟失的最大資料量。它有助於建立備份和資料恢復策略，以最大限度地減少潛在的資料丟失。

3. ***系統描述：***提供受事故影響的系統的概述。包括系統／應用系統的用途、其主要功能以及其在支援業務流程中所扮演的角色等詳細資訊。此描述將有助利益相關者了解該應用系統的重要性及其與決策局／部門運作的相關性。

3.1. ***工作流程概述：***描述系統內的典型工作流程或流程。確定使用應用系統實現特定結果所涉及的關鍵步驟、操作或交互。此概述將提供對應用系統的使用方式及其關鍵路徑的宏觀理解。

3.2. ***受影響的功能：***確定受事故影響的系統的特定功能或特性。描述這些功能受到影響的程度以及它們不可用或降級的潛在後果。了解受影響的功能將有助於評估事故的嚴重性並確定應變行動的緩急次序。

3.3. ***系統依賴性：***識別並記錄受影響的系統對其他系統／應用系統或服務的任何依賴性。這可以包括資料庫、應用系統介面、網絡連接或第三方集成。了解這些依賴性對於評估事故對互連系統的潛在影響至關重要。

3.4. ***與用戶的交互：***描述使用者如何與系統交互。這可以包括使用者介面、輸入機制或通信管道。了解用戶交互將有助於評估事故對用戶體驗、生產力和用戶滿意度的影響。

4. ***系統文檔：***包含一個子欄位來記錄系統文檔的可用性，例如用戶手冊或架構圖。這些資訊將協助事故應變團隊全面了解系統的結構和功能。

4.1. ***用戶手冊：***記錄與受影響系統相關的用戶手冊或指南的可用性。這些手冊提供了有關系統設置、配置和操作的詳細說明。請注意手冊是否易於接達，以及它們是否涵蓋了受事故影響的系統的相關方面。用戶手冊在手有助於事故應變團隊了解系統的預期用途、其功能以及任何特定的配置要求。

4.2. ***架構圖：***記錄架構圖的可用性以描述受影響系統的整體設計以及與其他系統或組件的整合。架構圖提供了對系統模組、介面和依賴關係的深入了解。指出架構圖是否可接達以及它們是否準確地表示了系統的當前狀態。了解系統的架構有助於識別潛在的弱點，評估事故對系統功能的影響，並規劃有效的應變。

4.3. ***備份和復原過程：***附加受影響系統的備份和復原過程。包括備份頻率、存儲位置以及最近備份的可用性等詳細資訊。此資訊對於評估復原選項和規劃恢復過程非常有價值。

4.4. ***其他相關文檔：***考慮可能與受影響的系統相關的任何其他文檔。這可能包括系統規格、配置指南、保安政策或任何其他提供系統結構、配置或保安控制見解的文檔。請注意此類文檔的可用性和可接達性。額外的文檔可以增強事故應變團隊對系統的理解，並有助於在整個調查和緩解過程中做出明智的決策。

5. ***系統配置：***包含一個子欄位來記錄受影響系統的配置詳細資訊，例如硬件規格、軟件版本和已安裝的修補程式。此資訊將有助於了解系統的漏洞和潛在的受入侵領域。

5.1. ***硬件規格：***記錄受影響系統的硬件規格。這包括處理器類型和速度、隨機存取記憶體數量、存儲容量以及任何其他相關硬件組件等詳細資訊。了解硬件規格有助於評估系統的功能、性能以及對事故應變活動的潛在影響。

5.2. ***軟件版本：***識別並記錄受影響系統上安裝的軟件版本。這包括操作系統、應用系統、框架、庫和任何其他軟件組件。指定確切的版本號以提供準確的資訊。了解軟件版本有助於識別已知漏洞、保安修補程式和潛在的危害區域。

5.3. ***已安裝的修補程式：***記錄受影響系統上已安裝的修補程式和更新。這包括操作系統修補程式、應用系統更新、固件更新以及任何其他相關已應用的修補程式。指定修補程式名稱、版本號和安裝日期。了解修補程式狀態有助於評估系統對已知漏洞的恢復能力，並確定是否有任何缺失的修補程式可能導致該事故。

5.4. ***配置更改：***記錄最近對受影響系統所做的任何配置更改。這包括對防火牆規則、使用者許可權、網絡設置的更改或任何其他相關配置修改。指定更改的性質、更改時間以及負責人。追蹤配置更改有助於識別可能導致事故的潛在錯誤配置、未獲授權的修改或政策違規。

6. ***網絡圖：***記錄與事故相關的內部互聯網規約位址，並提供與事故相關的網絡拓撲。這將有助於識別潛在的攻擊媒介並了解事故的範圍。

6.1. ***網絡拓撲概述：***提供與事故相關的網絡拓撲的概述。這包括網絡基礎設施的佈局和結構，包括路由器、交換機、防火牆和其他網絡設備。描述不同組件如何互連以及網絡的整體架構。

6.2. ***內部互聯網規約位址***：記錄與事故關聯的內部互聯網規約位址。這包括受影響的系統、伺服器和網絡設備的互聯網規約位址。通過記下這些互聯網規約位址，您可以識別事故中涉及的特定組件並追蹤它們在網絡內的連接。

6.3. ***子網信息：***識別與事故相關的子網或網段。這包括與每個子網關聯的互聯網規約地址範圍以及任何相關的子網遮罩。了解子網結構將有助於分析網絡流量模式和潛在的漏洞區域。

6.4. ***網絡設備配置：***記錄事故涉及的網絡設備的配置詳細資訊，例如路由器、交換機、防火牆和入侵偵測系統。包括相關資訊，例如設備型號、固件版本以及可能影響事故的任何特定配置或規則。

6.5. ***攻擊媒介：***分析網絡圖以識別攻擊者可能利用的潛在攻擊媒介或路徑。這包括檢查系統之間的連接、存取控制機制以及網絡基礎設施中潛在的保安弱點。通過識別可能的攻擊媒介，您可以評估事故的範圍以及對網絡的潛在影響。

6.6. ***事故範圍：***根據網絡圖，評估事故影響的網段、系統和服務的範

圍。確定事故在網絡內傳播的程度，並識別可能面臨風險的任何關鍵資產或敏感區域。該評估將有助於確定應變行動和遏制工作的緩急次序。

C. ***入侵指標：***列出與事故相關的所有受影響的互聯網規約地址、主機名稱和用戶名稱。識別可疑文件或流程以及未獲授權的接達或活動的任何證據。

1. ***受影響的互聯網規約位址：***識別並列出已受影響或與事故相關的互聯網規約位址。這包括與調查相關的內部和外部互聯網規約位址。記錄受影響的互聯網規約位址有助於追蹤網絡流量的來源和目的地、識別潛在的攻擊媒介以及了解事故的範圍。
2. ***受影響的主機名稱：***記錄受事故影響的任何主機名稱或功能變數名稱。這可能包括受入侵的網站、未獲授權的子域或異常的域名系統解析模式。列出受影響的主機名稱可以深入了解潛在的威脅區域，並表明哪些系統或服務可能成為攻擊目標。
3. ***受影響的用戶名稱：***識別在事故期間受到影響或洩露的任何用戶名稱或帳戶。這包括與受影響的系統、應用系統或服務關聯的使用者帳戶。記錄受影響的用戶名稱有助於追蹤未獲授權的接達、識別潛在的內部威脅以及評估損害的程度。
4. ***可疑文件或流程：***記錄調查期間發現的任何可疑文件或流程。這包括惡意軟體、惡意腳本、未獲授權的可執行文件或任何其他引起懷疑的文件或流程。提供詳細資訊，例如檔案名稱、文件位置和關聯的流程名稱（如適用）。識別可疑文件或流程有助於了解事故的性質、檢測潛在的惡意軟件感染並啟動適當的應變操作。
5. ***未獲授權的訪問或活動的證據：***記錄表明未獲授權的接達或惡意活動的任何證據或指標。這可能包括日誌條目、時間戳、異常網絡流量模式或調查期間觀察到的任何其他異常情況。擷取未獲授權的接達或活動的證據有助於了解攻擊者的技術、識別潛在的資料洩露並減輕進一步的風險。

D. ***備註：***在本節中，提供每個入侵指標的詳細支援資訊。解釋爲何將這些指標視為入侵並表明信賴度。此外，請注明與事故相關的任何其他觀察結果或資訊。

1. ***入侵指標詳細資訊：***對於每個已識別的入侵指標（互聯網規約位址、主機名稱、用戶名稱、可疑文件或進程、未獲授權的接達或活動的證據），提供支援詳細資訊，解釋爲何它們被視為入侵。包括導致其被納入指標的具體觀察、行為或特性。這可以包括日誌條目、網絡流量分析、系統日誌或調查期間收集的任何其他證據。
2. ***入侵理據：***解釋將每個指標視為入侵的例句。描述與該指標相關的潛在影響或風險，以及它如何與已知的攻擊模式、漏洞或惡意活動保持

一致。該理據將為將每個指標列為入侵指標提供背景和理由。

3. ***信賴度：***指示與每個入侵指標相關的信賴度。該範圍可以從低到高，反映評估的確定性水準。考慮證據的品質、來源的可靠性以及調查人員的專業知識等因素。指定信賴度有助於確定應變行動的緩急次序並適當地分配資源。
4. ***其他觀察結果：***記下任何其他與事故相關但可能不適合特定入侵指標的觀察結果或資訊。這可能包括異常的系統行為、漏洞評估的結果或任何其他可能有助於了解事故或其潛在影響的見解。這些額外的觀察結果提供了寶貴的背景資訊，有助於全面了解該事故。

在升級處理過程中提供的資料應明確簡潔、準確而真實。決策局／部門必須保持系統資訊／文件的持續可用性，以支援溝通的準確性和完整性。提供不準確、誤導或不完整的資料可能會妨礙應變程序，甚至令情況惡化。決策局／部門還應考慮可否對外提供某些敏感資料。

相關的資訊系統經理與負責整體協調的資訊保安事故應變小組的事故應變經理應通知適當人士，及跟從之前訂立的升級程序，將事故提升至適當級別。

如果決策局／部門確認有事故發生，有關資訊保安事故應變小組組長應在確認事故後的 60 分鐘內，向政府資訊保安事故應變辦事處常設辦公室報告事故。報告事故並不標誌著資訊保安事故應變小組職責的結束。資訊保安事故應變小組預期將隨時待命並積極參與。報告事故後立即遺下工作可能會導致事故應變流程出現延誤或間隙，從而損害資訊保安事故應變小組保護決策局／部門的能力。

為便於記錄和協調事故處理工作，資訊保安事故應變小組組長還應完成初步分析並提供一份資訊保安事故初步報告（請參閱**附件 C** 第 2 節），向政府資訊保安事故應變辦事處常設辦公室報告，包括但不限於下列各類資訊保安事故（有關詳情，請參閱**附件 F**）。

- 濫用資訊系統
- 入侵資訊系統或數據資產
- 拒絕服務攻擊（包括中央或部門互聯網通訊閘、電郵系統、政府網站及／或向公眾提供電子服務的系統）
- 洩漏電子保密資料
- 遺失存有保密資料的流動裝置或抽取式媒體
- 偽冒
- 大規模惡意軟件感染
- 勒索軟件
- 網站遭塗改

與保安無關的事故（如下所列）無須向政府資訊保安事故應變辦事處常設辦公室報告，而應該按照現行系統管理及操作的準則和程序處理。

- 系統受颱風、水浸、火災等自然災害影響
- 硬件或軟件問題
- 數據／通訊線故障
- 停電
- 例行系統關閉或維修時間
- 因管理／操作錯誤導致的系統故障
- 因系統或人為錯誤遺失或損毀保密資料
- 不影響政府系統和數據的欺詐電郵或網站

如發生對政府服務及／或形象構成重大影響的嚴重事故，政府資訊保安事故應變辦事處常設辦公室與資訊保安事故應變小組組長會密切監察事態發展。如果事故是針對整個香港特別行政區政府的多點攻擊，常設辦公室會立即通知政府資訊保安事故應變辦事處並採取必要的行動。

在處理資料外泄事故時，決策局／部門宜考慮採取補救措施如下：

- 立即收集有關外泄事故的重要資料。
- 採取適當措施，制止資料外泄。
- 評估造成傷害的風險。
- 考慮發出有關資料外泄的通報。

如果保安事故涉及個人資料，決策局／部門應盡快向個人資料私隱專員公署報告，《資料外洩事故通報表格》可於個人資料私隱專員公署網站下載 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/forms/files/DBN_c.pdf)。通報表格亦可以透過網上方式遞交 (https://www.pcpd.org.hk/tc_chi/enforcement/data_breach_notification/dbn_form.html) 。

此外，決策局／部門可參考個人資料私隱專員公署發出的《資料外洩事故的處理及通報指引》。

(https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/guidance_note_dbn_c.pdf)

決策局／部門應盡可能通知受影響人士。如基於合理原因而不作出通報，必須得到決策局局長／部門主管的批准方可。

如果決策局／部門懷疑發生電腦罪案，應聯絡香港警務處網絡安全及科技罪案調查科。在向警方報告案件前，應在完成初步分析的同時事先徵求資訊保安事故應變小組高級管理層的意見和批准。此外，如果需要向警方或個人資料私隱專員公署報告保安事故，決策局／部門應通知政府資訊保安事故應變辦事處常設辦公室，以便作中央記錄和協調。

有關升級處理程序示例和有關保安事故升級處理程序的其他相關資料，請參閱**附件 D**。政府保安事故報告及升級處理工作流程闡述於**附件 E**，以供參考。

8.3 記錄事故

須記錄所有保安事故、已採取的行動和相關的行動結果。這些記錄應以加密、上鎖或接達控制方法妥善儲存。這些記錄有助確認和評估事故，為檢控提供證據，並為及後的事故處理階段提供有用的資料。整個保安事故應變過程都應保留記錄。為事故設定編號有助在整個事故處理過程中作跟進和追蹤。

事故記錄最低限度必須包括以下資料：

- 系統事件和其他相關資料，例如審計記錄
- 已採取的所有行動，包括日期、時間和參與行動人員
- 所有對外通訊，包括日期、時間、內容及有關各方

8.4 記錄系統狀況

在偵測到可疑活動後應以最快速度，並在技術和操作上可行的情況下記錄受襲系統的狀況。這些資料可防止攻擊者銷毀證據，並為日後的個案調查（例如收集法證證據）提供了證據。所記錄的系統資料可包括下列項目：

- 伺服器記錄、網絡記錄、防火牆／路由器記錄、接達記錄等系統記錄檔案
- 仍在進行活動的系統登入或網絡連接，以及有關程序狀態的資料
- 受襲系統影像，以供調查，並作為日後採取跟進行動的證據

9. 保安事故應變

保安事故應變涉及制訂程序評估事故並作出應變，盡快將受影響的系統元件和服務恢復正常。有關程序大致可分為 3 個階段：即下圖 9.1 所示的*遏制*、*杜絕和復原*。認識各階段具體工作有利於制訂有效的保安事故應變程序。

應變程序無須依足 3 個階段的次序進行，決策局／部門可因應本身的實際需要自行制訂應變程序各階段的次序。

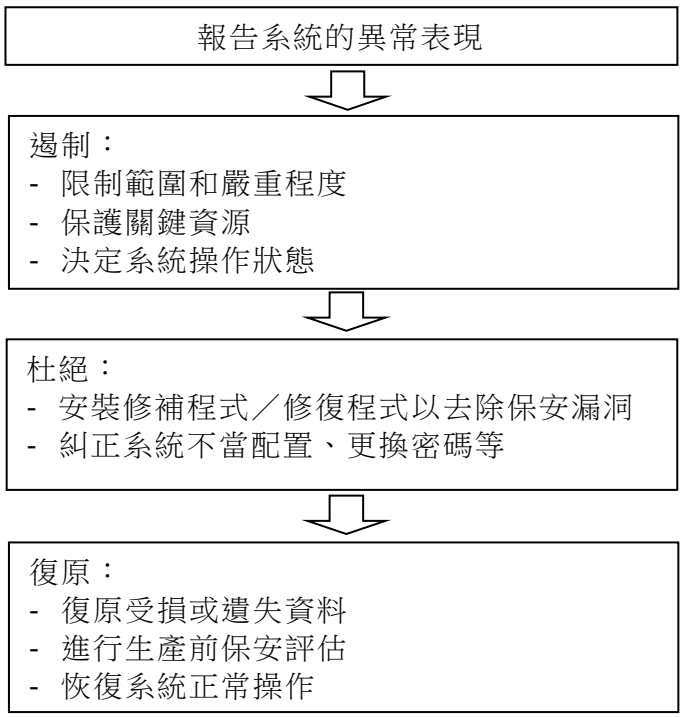


圖 9.1 保安事故應變的主要階段

9.1 遏制

事故應變的第一階段是遏制。遏制的目的是限制事故的範圍、嚴重程度和影響。有些事故，例如惡意軟件感染可迅速傳播，並造成大規模破壞。因此，在事故造成進一步破壞前，應限制事故的影響程度。

事先應清晰釐定並在保安事故應變程序中列明，針對不同的事故應採取哪種應變策略和程序，以及投入哪種資源。如果需要採取關鍵行動，便可能須要徵求資訊保安事故應變小組管理層的意見和批准（如有需要，資訊保安事故應變小組也可能須要諮詢政府資訊保安事故應變辦事處的意見）。

這一階段的工作宜包括：

- 評估事故對數據和資訊系統的影響，以確定有關的數據或資料是否已受事故破壞或感染。
- 保護敏感或關鍵資料和系統，例如將關鍵資料轉移至與受襲系統或網絡隔開的其他媒體（或其他系統）。
- 決定受襲系統的當前操作狀態。
- 複製受襲系統的當前映像映射，以供調查，並作為日後採取跟進行動的證據；
- 記錄這一階段採取的所有行動。
- 檢查共用網絡服務，或任何因可信賴關係而與受襲系統連接的系統。

9.1.1 決定受襲系統的當前操作狀態

有待作出的其中一項重要決定，是繼續還是終止受襲系統的操作和服務。這項決定在很大程度上取決於事故的類別和嚴重程度、系統要求、對公共服務和決策局／部門以至整個政府形象的影響，以及事故處理應變計劃內預定的目標和優先事項。

可採取的行動宜包括：

- 暫時關閉或隔離受襲的電腦或系統，以防止事故對互相連接的其他系統造成進一步破壞。這尤其是當事故會快速傳播時，當儲存敏感資料的電腦受到威脅時，又或是為了防止受襲系統被利用而向相連的系統發起攻擊。
- 終止受襲資訊系統的操作。
- 關閉系統的部分功能。
- 禁止用戶接達或登入系統。
- 繼續操作以收集有關事故的證據。該行動只適用於可承受某程度風險如服務中斷或數據受損的第 1 級資訊系統，而且在處理時須格外小心，並加以嚴密監控。

9.2 杜絕

遏制後的下一個階段是杜絕。杜絕是指從系統清除導致事故的肇因，例如從受感染的系統和媒體清除惡意軟件。

在移除任何檔案或終止／刪掉任何程式前，宜收集所有必需的資料，包括所有記錄檔案、仍在進行活動的網絡連接及程序狀態資料。這將有助於為日後的調查收集證據，因為這些資料可能會在清理系統時被刪除或重新設定。

9.2.1 可杜絕事故的行動

在杜絕階段，決策局／部門宜根據事故的類別和性質及系統要求，採取以下行動：

- 終止或刪掉黑客在系統中產生或啟動的所有程序，以停止破壞及逼使黑客離開。
- 刪除黑客建立的所有偽冒檔案。系統操作員在刪除檔案前應將偽冒檔案作備分，以便日後調查。
- 清除黑客安裝的所有後門程式和惡意程式。
- 採用修補和修復程式修補在所有操作系統、伺服器和網絡設備等發現的保安漏洞。在系統恢復正常操作前，應徹底測試所採用的修補或修復程式。
- 糾正系統和網絡的不當設定，例如防火牆和路由器配置不當。
- 如發生惡意軟件事故，應遵照抗惡意軟件供應商的指引，在適當情況下，從所有受感染的系統和媒體清除惡意軟件。
- 確保備份未受感染，以免系統在下一階段利用備份復原系統時再度受到感染。
- 利用其他的保安工具，協助進行杜絕工作，例如利用保安掃描工具偵測入侵，並採用建議的解決方案。應確保使用具有最新檢測模式的保安工具。
- 更換所有可能被黑客接達的登入帳戶的密碼。
- 在某些情況下，支援人員可能須要將所有受感染的媒體重新格式化，並利用備份重新安裝系統和數據，尤其是在不確定事故對第 2 級或以上的資訊系統造成破壞的嚴重程度，或難以完全清理系統之時。
- 記錄已採取的所有行動。

以上所列只是在處理保安事故時常見的措施示例。杜絕行動視乎事故的性質及事故對受襲系統的影響而定。在某些情況下，決策局／部門可能須尋求外部機構（例如警方、個人資料私隱專員公署及／或外部服務供應商）的意見，並參考其他決策局／部門處理類似事故的經驗。此外，應尋求資訊保安事故應變小組和政府資訊保安事故應變辦事處的意見和協調。

9.3 復原

事故應變的最後階段是復原。本階段的目的在於恢復系統的正常操作。復原工作包括：

- 評估事故的破壞。
- 必要時從可信賴的來源取得檔案和資料，以重新安裝被刪除／遭破壞的檔案或整個系統。
- 在受控制的情況下，按照需求的緩急次序逐階段恢復功能／服務，例如可優先恢復最重要的服務或以大多數人為對象的服務。
- 檢驗復原操作是否成功，系統是否已恢復正常操作。
- 在恢復系統操作前，事先通知所有相關人士，如操作員、管理員、高級管理層和升級處理程序所涉及的其他人士等。
- 關閉不需要的服務。
- 記錄已採取的所有行動。

在系統恢復正常操作前，其中的一項重要工作是進行生產前保安評估，以確保受襲系統及其相關元件已安全。這項工作可能會運用到保安掃描工具，以確定事故的問題根源已清除，同時找出系統內任何可能存在的其他保安漏洞。視乎事故的嚴重程度和系統的服務水準要求，評估可集中處理某個領域，也可以涵蓋整個系統。

在進行一切復原工作前，須得到資訊保安事故應變小組高級管理層批准。如有需要，可尋求政府資訊保安事故應變辦事處的支持和意見。

10. 事故後行動

系統恢復正常操作並不代表保安事故處理程序的結束。採取必要的跟進行動是十分重要的。跟進行動包括評估事故所造成的破壞、改良系統以防止再度發生事故、更新保安政策和程序及為日後的檢控進行個案調查。

跟進行動可收以下效果：

- 改善事故應變程序。
- 改善保安措施，以保護系統日後免受攻擊。
- 向違法者提出檢控。
- 有助他人認識保安事故應變程序。
- 有助參與事故應變的各方人士汲取教訓。

跟進行動包括：

- 事故事後分析。
- 事故事後報告。
- 保安評估。
- 覆檢現行的保護措施。
- 調查及檢控。

10.1 事故事後分析

事故事後分析是對事故及事故應變措施的分析，以作為日後的參考。這項分析有助更深入地了解系統受到的威脅及可能存在的保安漏洞，以便採取更有效的保障措施。

分析的範圍包括：

- 防止再度受攻擊的建議行動。
- 迅速取得所需的資料及獲取有關資料的方法。
- 供偵測及杜絕程式所用或所需的額外工具。
- 準備和應變措施的足夠程度。
- 溝通的足夠程度。
- 實際困難。

- 事故的破壞，當中包括：
  (i) 處理事故所需的人力消耗
  (ii) 金錢成本
  (iii) 中斷操作的損失
  (iv) 遺失或遭破壞數據、軟件和硬件的價值，包括被泄露的敏感資料
  (v) 受託機密資料的法律責任
  (vi) 難堪或令信譽喪失
- 汲取的其他教訓。

分析結果應納入資訊科技保安風險管理及持續改進程序，以加強決策局／部門的保安保護，減少事故發生的機會。

10.2 事故事後報告

根據事故分析所編製的事故事後報告，應概述事故、應變、復原行動、破壞和汲取的教訓。相關資訊系統的經理負責編製報告，並提交資訊保安事故應變小組作參考，以便日後及時採取預防措施，避免其他系統和服務再度發生同類保安事故。

事故事後報告應包括下列項目：

- 事故的類別、範圍和程度。
- 事故的詳情：攻擊的來源、時間和可能方法，以及發現攻擊的方法等。
- 概述受攻擊的系統，包括系統範圍及功能、技術資料（例如系統硬件、軟件和操作系統，以及版本、網絡體系結構及程式編製語言等）。
- 事故應變及杜絕的方法。
- 復原程序。
- 汲取的其他教訓。

事故事後報告應在解決保安事故後的 1 週內提交予政府資訊保安事故應變辦事處。事故事後報告樣本載於**附件 C** 第 3.2 節，以供參考。

10.3 保安評估

可能受到保安風險威脅的系統宜定期進行保安風險評估和審計，尤其是曾經受保安事故影響的系統。保安覆檢及系統審計應持續進行，以便及時發現可能存在的保安漏洞及／或因應保安保護措施及攻擊／入侵科技的發展，而須作出的系統改善。

在發生保安事故時收集的資料亦有助於事後的保安評估，這對找出系統的保安漏洞和保安威脅尤其有用。

10.4 覆檢現行保護措施

根據事故事後分析與定期保安評估所得出的結果，可確認系統的保安政策、程序和保護機制中可改善的範圍。科技發展一日千里，所以必須定期更新保安相關政策、程序和保護機制，以確保整體保安保護措施對資訊系統的效用。在進行事故事後分析時，如有需要應覆檢和修訂政策、標準、指引和程序，以配合預防措施。

10.5 調查及檢控

在適當的情況下，還應對引起事故的個人採取個案調查、紀律處分或法律檢控等行動。

如經評估後，事故已構成刑事罪行，則應向香港警務處網絡安全及科技罪案調查科報告，以便展開個案調查和收集證據。在向警方報告案件前，應事先徵求資訊保安事故應變小組高級管理層的意見和批准。決策局／部門可能需要跟進法律程序及提供所需證據。

如果保安事故涉及個人資料，則決策局／部門應盡快向個人資料私隱專員公署報告。決策局／部門也應盡可能通知受影響的人。如基於合理原因而不作出通報，應得到決策局／部門主管的批准方可。

另外，對於向警方或個人資料私隱專員公署報告的任何保安事故，亦應通知政府資訊保安事故應變辦事處常設辦公室以進行中央記錄和協調支援。

完

附件 A：部門資訊科技保安聯絡人資料更新表

決策局／部門名稱	
提交更新表的單位資料	
姓名：	職位：
聯絡號碼：	電郵地址：
提交至 IT Security Team/DPO	
請將填妥的表格透過電子郵件提交至 IT Security Team， 並副本抄送更新表內的所有相關聯繫人： 電郵地址：*it_security@digitalpolicy.gov.hk*	

新增 / 更換 / 刪除的更新請求*	
人員職務	
☐ 部門資訊科技保安主任 ☐ 部門資訊科技保安副主任 ☐ 參與支援部門資訊科技保安主任 / 副主任工作的人員 ☐ 部門資訊保安事故應變小組組長 ☐ 部門事故應變經理 ☐ 部門資訊保安事故應變小組組員	
擬更換的現任人員（如有）：_____	
更新請求聯絡資料	
姓名：	職位：
辦公室聯絡號碼：	流動電話號碼： *（作 7x24 緊急聯絡之用）*
電郵地址：	有效日期：

*(*刪除不適用部分)*

附件 B：保安事故應變準備工作清單

B.1 保安事故應變準備工作清單樣本

	項目	詳情	進展情況
1	事故監察和偵測	安裝防火牆設備，並採取接達控制措施，以保護重要系統和數據資源	
		安裝抗惡意軟件和修復工具，定期執行掃描和更新識別碼	
		安裝監察工具，例如入侵偵測系統	
		開啟系統和網絡設備的審計記錄功能	
2	保安事故應變	準備保安事故應變計畫	
		設計及準備報告機制	
		向全體人員頒布報告機制	
		收集需要聯絡／參與工作的全體人員（內部和外部）的聯絡資料	
		準備升級處理程序	
		向參與工作的全體人員頒布升級處理程序	
		向參與工作的全體人員頒布保安事故應變計畫	
3	培訓與教育	向操作及支援人員提供有關保安事故處理的培訓	
		確保各人員熟習事故應變程序	

附件 C：報告機制

C.1 報告機制建議

電話熱線

這是最便利和快捷的報告事故途徑。部分系統可能已設有專門處理查詢及／或保安事故報告的電話熱線。

如果系統需要日夜不停運作，便可能需要提供 24 小時電話熱線服務。

電子郵件

通過電郵報告事故也是個有效的途徑。然而，如果發生屬於網絡攻擊或針對電郵系統的事故，以電郵報告的途徑便會受到影響。要解決這個問題，應採用其他的報告途徑，例如電話或傳真。

傳真號碼

通過傳真報告是一個補充機制，特別是當要提交可能無法通過電話清楚及準確地報告的詳細資訊。但是，透過傳真機報告事故應特別注意，最好由專人負責接收傳真。此外，還應特別注意處理傳真報告，以防止向未經授權的人員披露事故。鑑於通過傳真報告的須留意這些額外的保安措施，為了更有效率和更具成本效益，通常會使用電子郵件來提交報告。

親身報告

這個辦法被認為沒有效率，而且還會構成不便。這只應用於，必須親身由報告事故的人員提供詳細資料或與報告事故的人員討論事故的情況，又或者事故地點與事故報告聯絡人的所在地十分接近，否則應避免採取親身報告的方式。

C.2 資訊保安事故初步報告

限 閱

事故參考編號： _____
（只供政府資訊保安事故應變辦事處常設辦公室填寫）

資訊保安事故初步報告

背景資料	
決策局／部門名稱：	
概述受影響的系統（例如功能、網址等）：	
系統等級： ☐第 1 級　☐第 2 級　☐第 3 級	
受影響系統的實體位置： ☐決策局／部門內部　☐ 外聘服務供應商設施 ☐中央服務：_____ **系統管理員／操作員：** ☐ 內部人員　☐ 終端用戶　☐ 外判服務供應商	
報告人資料	
姓名：	***職位：***
辦公室聯絡號碼：	***24 小時聯絡號碼：***
電郵地址：	***資訊保安事故初步報告提交日期：***
事故詳情	
發生事故的日期／時間：	
發現事故的日期／時間：	**向政府資訊保安事故應變辦事處常設辦公室報告的日期／時間：**

事故說明：

發生事情：

_____

初步調查結果（如有）：

發生經過：

_____

發生原因：

_____

已識別漏洞：

_____

類別：

- ☐ 濫用資訊系統
- ☐ 入侵資訊系統或數據資產
- ☐ 拒絕服務攻擊
- ☐ 洩漏電子保密資料
- ☐ 偽冒
- ☐ 遺失存有保密資料的流動裝置或抽取式媒體
- ☐ 大規模惡意軟件感染
- ☐ 勒索軟件
- ☐ 網站遭塗改
- ☐ 其他：_____

受影響組件／資產：

- ☐ 電郵系統
- ☐ 硬件
- ☐ 資料／數據
- ☐ 網絡
- ☐ 軟件
- ☐ 網站
- ☐ 其他：_____

受影響組件／資產詳情：

_____

影響：

- ☐ 機密性
- ☐ 完整性
- ☐ 可用性
- ☐ 政府形象
- ☐ 其他：_____

請提供有關影響和中斷服務時間（如有）的詳情：

_____

事故有否涉及保密資料？

☐ 有，涉及　☐限閱類別　☐機密類別

☐ 沒有

請提供所涉及保密資料的詳情（例如數據是否加密、數據類型等）：

_____

事故有否涉及個人資料？

☐ 有，所涉及個人資料為：_____

☐ 沒有

已通知人士／單位：

☐ 資訊系統經理　☐ 新聞統籌員

☐ 事故應變經理　☐ 資訊保安事故應變小組組長

☐ 政府資訊保安事故應變辦事處常設辦公室　☐ 其他：_____

已通知外部人士／單位（日期／時間）：

☐ 香港警務處網絡安全及科技罪案調查科：_____
檔案參考編號：_____

☐ 個人資料私隱專員公署：_____

☐ 保安局：_____

☐ 其他：_____

為解決事故所採取的行動：

為解決事故所計劃的行動：

未進行的行動：

目前系統的狀況：

其他資料：

媒體／公眾查詢（如適用）	
媒體查詢數目：	**公眾查詢數目：**

C.3.1事故中期報告

限 閱

事故參考編號：_____

（只供政府資訊保安事故應變辦事處常設辦公室填寫）

事故中期報告

背景資料	
決策局／部門名稱：	
概述受影響的系統（例如功能、網址等）：	
系統等級: ☐第 1 級　☐第 2 級　☐第 3 級	
受影響系統的實體位置： ☐ 決策局／部門內部　☐ 外聘服務供應商設施 ☐ 中央服務：_____ 系統管理員／操作員： ☐ 內部人員　☐ 終端用戶　☐ 外判服務供應商	
報告人資料	
姓名：	*職位：*
辦公室聯絡號碼：	*24 小時聯絡號碼：*
電郵地址：	*事故中期報告提交日期：*
事故詳情	
發生事故的日期／時間：	
發現事故的日期／時間：	向政府資訊保安事故應變辦事處常設辦公室報告的日期／時間：

事故說明：

發生事情：

_____

調查結果：

發生經過：

_____

發生原因：

_____

已識別漏洞：

_____

最新狀況：

C.3.2 事故事後報告

限 閱

事故參考編號：_____

（只供政府資訊保安事故應變辦事處常設辦公室填寫）

事故事後報告

背景資料	
決策局／部門名稱：	
概述受影響的系統（例如功能、網址等）：	
系統等級： ☐第 1 級　☐第 2 級　☐第 3 級	
受影響系統的位置： ☐ 決策局／部門內部　☐ 外聘服務供應商設施 ☐ 中央服務：_____ **系統管理員／操作員：** ☐ 內部人員　☐ 終端用戶　☐ 外判服務供應商	
報告人資料	
姓名：	***職位：***
辦公室聯絡號碼：	***24 小時聯絡號碼：***
電郵地址：	***事故事後報告提交日期：***
事故詳情	
發生事故的日期／時間：	
發現事故的日期／時間：	**向政府資訊保安事故應變辦事處常設辦公室報告的日期／時間：**

事故說明：

發生事情：

_____

調查結果：

發生經過：

_____

發生原因：

_____

已識別漏洞：

_____

類別：

- ☐ 濫用資訊系統
- ☐ 入侵資訊系統或數據資產
- ☐ 拒絕服務攻擊
- ☐ 洩漏電子保密資料
- ☐ 偽冒
- ☐ 遺失存有保密資料的流動裝置或抽取式媒體
- ☐ 大規模惡意軟件感染
- ☐ 勒索軟件
- ☐ 網站遭塗改
- ☐ 其他：_____

受影響組件／資產：

- ☐ 電郵系統
- ☐ 硬件
- ☐ 資料／數據
- ☐ 網絡
- ☐ 軟件
- ☐ 網站
- ☐ 其他：_____

受影響組件／資產詳情：

_____

其他受影響場地／系統（如有）：

_____

影響：

☐ 機密性　　☐ 完整性

☐ 可用性　　☐ 政府形像

☐ 其他：_____

請提供有關影響和中斷服務時間（如有）的詳情：

_____

已通知人士／單位：

☐ 資訊系統經理　　☐ 新聞統籌員

☐ 事故應變經理　　☐ 資訊保安事故應變小組組長

☐ 政府資訊保安事故應變辦事處常設辦公室　　☐ 其他：_____

已通知外部人士／單位（日期／時間）：

☐ 香港警務處網絡安全及科技罪案調查科：_____
檔案參考編號：_____

☐ 個人資料私隱專員公署：_____

☐ 保安局：_____

☐ 其他：_____

香港警務處調查結果（如有）：

_____

事件發生的次序：

日期／時間	*事件*

已採取的行動及結果：

目前系統的狀況：

參與人員：

姓名	*職位*	*電話號碼*	*電郵地址*	*職務*

肇事者（如有）詳情：

_____

涉及的肇事者：

☐ 人　　☐ 組織

☐ 沒有肇事者　　☐ 不明

☐ 其他：_____

事故的懷疑動機：

☐ 經濟利益　　☐ 黑客攻擊

☐ 政治　　☐ 報復

☐ 不明　　☐ 其他：_____

惡意軟件（如有）詳情：

如事故涉及保密資料，請提供詳情（例如數據是否加密、數據類型等）：

保密資料：　☐限閱類別　☐機密類別

備註：

_____

如事故涉及個人資料，請提供詳情（例如受影響人數、個人資料類別（如香港身份證號碼）、是否已通知受影響人士等）：

受影響人數：_____

（*內部人員和市民人數分項數字*）

個人資料類別（如香港身分證號碼）：

_____

是否已通知受影響人士：是／否。如否，原因： _____ 備註： _____
成本因素（包括因事故招致的損失和復原成本／人力資源）：
防止再度發生事故的建議行動：
汲取的教訓：

媒體／公眾查詢 （如適用）	
媒體查詢數目：	公眾查詢數目：

C.4.1 資訊科技保安事故初步報告

限 閱

資訊科技保安事故初步報告參考編號： _____

資訊科技保安事故初步報告

（應在事故發生後兩日內向局長提交報告）

背景資料	
決策局／部門名稱：	
概述受影響的系統： *（例如系統名稱、面向公眾的資訊科技服務、網址等）*	
系統等級： ☐第 1 級　☐第 2 級　☐第 3 級	
事故詳情	
發生事故的日期／時間： 按一下或點選以輸入日期。	**發現事故的日期／時間：** 按一下或點選以輸入日期。
事故說明： ***事情發生和影響：*** _____	
調查結果（如有）： ***發生經過：*** _____ ***發生原因：*** _____	
涉及數據： **事故有否涉及保密資料？** ● ☐ 有，涉及 ☐限閱類別／ ☐機密類別數據 - 已通知保安局　☐ 有及於：_____ ☐ 沒有，將完成於：_____ - 請提供所涉及保密資料的詳情： （例如數據是否加密、數據類型等） _____ ● ☐ 沒有	

事故有否涉及個人資料？ ● ☐ 有，所涉及個人資料為：_____ - 已通知保安局 ☐ 有及於：_____ ☐ 沒有，將完成於：_____ ● ☐ 沒有
事故有否涉及涉嫌犯罪行為？ ● ☐ 有 - 已報告香港警務處網絡安全及科技罪案調查科 ☐ 有及於：_____ ☐ 沒有，將完成於：_____ ● ☐ 沒有
為短期遏制或完全解決事故所採取的行動：
為解決事故所計劃的行動：
目前系統的狀況（完全恢復／有限服務）：

媒體／公眾查詢 （如適用）	
媒體查詢數目：	**公眾查詢數目：**
項目負責人員／部門資訊科技保安主任資料	
姓名：	***職位：***
辦公室聯絡號碼：	***24 小時聯絡號碼：***
電郵地址：	***向局長提交報告的日期：*** 按一下或點選以輸入日期。
備註*（如有）**：***	

決策局局長資料	
姓名：	*職位：*
辦公室聯絡號碼：	*24 小時聯絡號碼：*
電郵地址：	
備註（如有）： 批核 ☐ 不批核 ☐	

C.4.2 資訊科技保安事故全面報告

限 閱

資訊科技保安事故全面報告參考編號： _____

資訊科技保安事故全面報告

（應在事故發生後七日內向部門首長提交報告）

背景資料	
決策局／部門名稱：	
概述受影響的系統： *（例如系統名稱、面向公眾的資訊科技服務、網址等）*	
系統等級： ☐第 1 級　☐第 2 級　☐第 3 級	
事故詳情	
附上資訊科技保安事故初步報告副本 *(與資訊科技保安事故初步報告參考編號）*	
發生事故的日期／時間： 按一下或點選以輸入日期。	**發現事故的日期／時間：** 按一下或點選以輸入日期。
事故說明： ***事情發生和影響：*** _____	
有佐證的調查結果： ***事件發生的順序：*** _____	

日期／時間	*事件*
按一下或點選以輸入日期。	
按一下或點選以輸入日期。	
按一下或點選以輸入日期。	
按一下或點選以輸入日期。	
按一下或點選以輸入日期。	

有佐證的事故發生原因：

_____

涉及數據：

事故有否涉及保密資料？

- ☐ 有，涉及 ☐ 限閱類別／ ☐機密類別數據
  - 已通知保安局於：_____
  - 請提供所涉及保密資料的詳情：
    （例如數據是否加密、數據類型等）

_____

- ☐ 沒有

事故有否涉及個人資料？

- ☐ 有，所涉及個人資料為：_____
  - 受影響人數：_____
    （內部人員和市民人數分項數字）
  - 個人資料類別（如香港身份證號碼）：

    _____
  - 是否已通知受影響人士：是／否。如否，原因：

    _____
  - 已通知個人資料私隱專員公署於：_____
    (附有向個人資料私隱專員公署提交的資料外洩事故通報表格)
- ☐ 沒有

事故有否涉及涉嫌犯罪行為？

- ☐ 有
  - 已報告香港警務處網絡安全及科技罪案調查科於

    _____
- ☐ 沒有

已採取的行動及結果：

目前系統的狀況（完全恢復／有限服務）：

如果恢復了有限服務，請提供完全恢復服務的時間表：

於責任方的問責和建議採取的後續行動並提供佐證：

（根據相關事故報告的調查結果、既定機制或適用規則和條例，以及相關管治框架，責任方可能包括承建商、人員和／或相關公共機構）

媒體／公眾查詢（如適用）	
媒體查詢數目：	公眾查詢數目：
項目負責人員／部門資訊科技保安主任資料	
姓名：	*職位：*
辦公室聯絡號碼：	*24 小時聯絡號碼：*
電郵地址：	*向局長提交報告的日期：* 按一下或點選以輸入日期。
備註（如有）：	
決策局局長資料	
姓名：	*職位：*
辦公室聯絡號碼：	*24 小時聯絡號碼：*
電郵地址：	
備註（如有）： 批核☐ 不批核☐	

附件 D：升級處理程序

D.1 需要通知的各方

升級處理程序內需要包括哪些人員，取決於事故的性質和嚴重程度，及系統要求。舉例來說，發生事故的初期可能只需要內部支援人員處理問題。其後可能需要通知高級管理層。如果問題仍無法解決，便可能需要視乎情況，尋求服務承辦商、產品供應商、警方及個人資料私隱專員公署等外部支援服務機構的意見。

應為各系統設定個別的升級處理程序和聯絡人，以滿足系統的特殊操作需要。

視乎系統受到的破壞或系統的敏感程度，在不同的階段可通知不同的人員。聯絡人包括，但不限於：

內部：

- 操作及技術支援人員
- 相關資訊系統的經理、資訊保安事故應變小組／部門資訊科技保安主任／項目負責人員及政府資訊保安事故應變辦事處常設辦公室
- 決策局局長
- 其他受影響／有關聯的系統或功能操作人員
- 香港警務處網絡安全及科技罪案調查科
- 新聞統籌員，為準備對事故的立場和向傳媒發布的新聞稿

外部：

- 支援服務供應商，包括系統的硬件或軟件供應商、應用程式開發商和保安顧問等
- 服務供應商（例如電訊供應商、互聯網服務供應商）
- 個人資料私隱專員公署
- 受影響人士

D.2 聯絡名單

參與工作人員的聯絡名單應包括下列資料：

- 專責人員的姓名
- 職銜
- 電郵地址
- 聯絡電話號碼（按需要加入 24 小時聯絡號碼）
- 傳真號碼

D.3 升級處理程序示例

以下所列是資訊保安事故的升級處理程序示例。

報告時限	**聯絡名單**	**聯絡方法**
事故發生後 15 分鐘內	有關的資訊系統經理、技術支援人員、提供支援的相關供應商和服務承辦商	*流動電話及供應商 24 小時電話熱線*
事故發生後 30 分鐘內	上述各人員及資訊保安事故應變小組的事故應變經理和新聞統籌員	*流動電話*
事故發生後 60 分鐘內	通知資訊保安事故應變小組組長	*流動電話*
事故發生後 60 分鐘內	資訊保安事故應變小組通知政府資訊保安事故應變辦事處 (及於事故發生後 48 小時內向政府資訊保安事故應變辦事處常設辦公室提供資訊保安事故初步報告)	*預設的電話熱線或電子郵件*
其後每 30 分鐘	向上述各人員匯報最新情況	*流動電話或電子郵件*
2 日內（就事故已令政府尷尬或損害其監督角色的形象）	項目負責人員或部門資訊科技保安主任向決策局局長遞交資訊科技保安事故初步報告	*電子郵件*
定期	資訊保安事故應變小組向政府資訊保安事故應變辦事處匯報事故的最新情況	*電子郵件*
7 日內（就事故已令政府尷尬或損害其監督角色的形象）	項目負責人員或部門資訊科技保安主任向決策局局長遞交資訊科技保安事故全面報告，並將已批核的資訊科技保安事故全面報告的副本遞交予數字辦	*電子郵件*

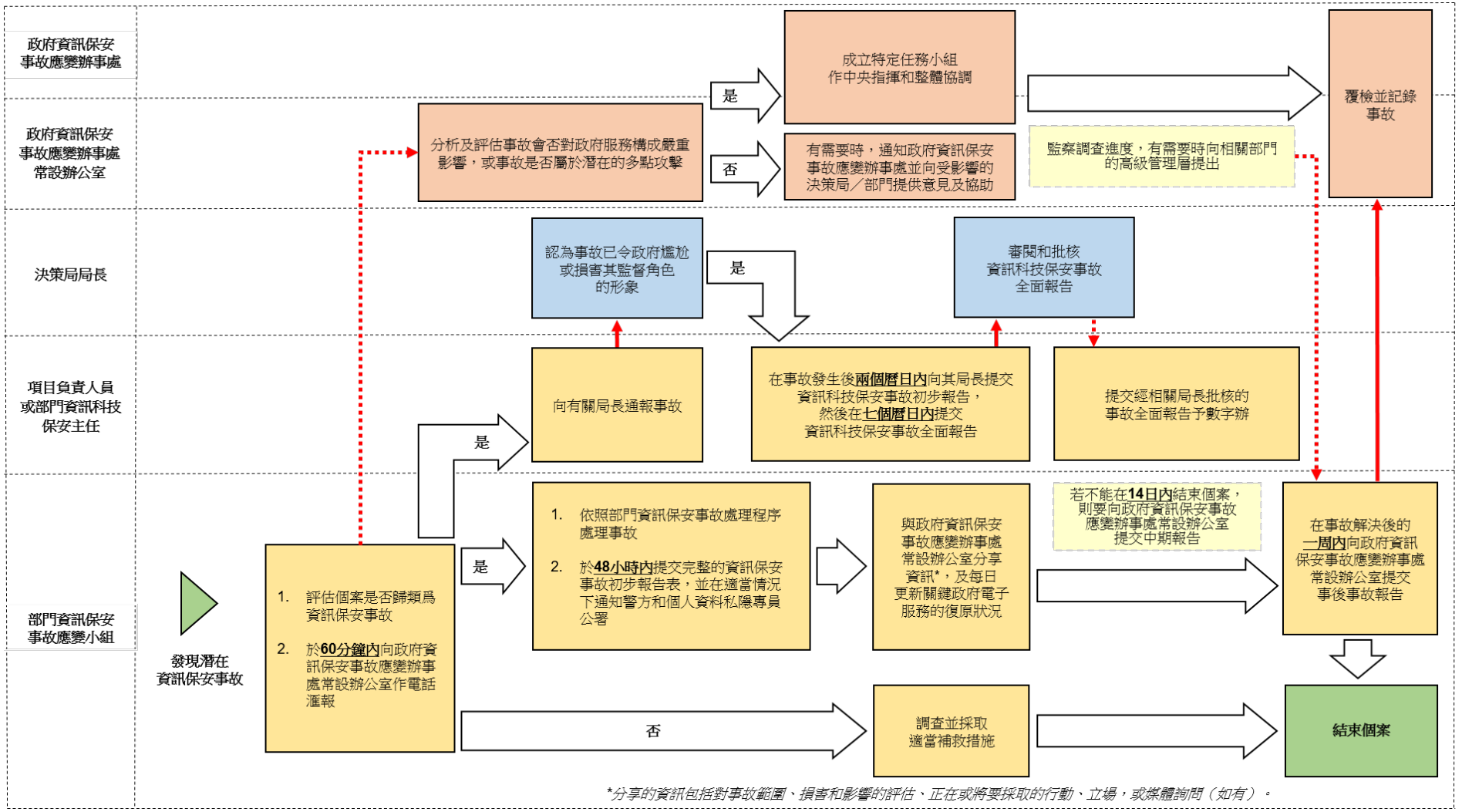
系統復原後（1 星期內）	資訊保安事故應變小組向政府資訊保安事故應變辦事處遞交一份事故事後報告作記錄	*電子郵件*
如懷疑構成刑事犯罪，則由資訊保安事故應變小組決定	向警方舉報以調查案件	*預設的電話熱線*
如涉及個人資料	向個人資料私隱專員報告 （並盡可能通知受影響人士）	*預設的電話熱線或任何其他途徑*

報告應包括下列資料：

- 概括描述問題：發生何事、何時發生、如何發生及持續時間
- 表明系統是否受到攻擊
- 表明攻擊者（如有）是否仍在系統進行活動
- 表明攻擊是否來自本地
- 系統復原的最新進展情況

附件 E：資訊保安事故應變機制的流程

下圖所示為政府保安事故報告及升級處理工作流程圖：



附件 F：確認事故

F.1 保安事故的典型類型和跡象

為判斷異常情況是由系統問題還是確實事故所造成，可留意保安事故一些特定跡象。保安事故的常見類型和跡象包括以下任意一種。此列表僅供參考，並非詳盡無遺。

資訊保安事故	描述	跡象	初步分析／處理	識別／分析所需的資訊
濫用資訊系統	當有人利用資訊系統作非獲准用途，例如為資訊資產帶來負面影響，即已構成濫用。	• 資訊系統上的異常或未獲授權的活動。 • 故意濫用或未獲授權接達的證據。 • 對資訊資產造成不利影響的行為。	1. 收集有關舉報活動或濫用事故的資訊。 2. 確定所涉及的個人或帳戶。 3. 分析系統日誌和審計追蹤以確定濫用的程度。 4. 採訪相關人員或使用者以收集更多資訊。 5. 評估濫用行為對資訊資產的影響，並確定需要立即採取的行動，例如撤銷接達或阻止未獲授權的活動。 6. 如有必要，記錄事故並將其報告給適當的利益相關者或當局。	• 系統接達和使用者活動日誌。 • 未獲授權的系統操作或違反政策的記錄。 • 與濫用事件相關的通訊日誌（電子郵件、聊天記錄等）。 • 任何擷取的證據，例如螢幕截圖或錄音。

資訊保安事故	描述	跡象	初步分析／處理	識別／分析所需的資訊
入侵資訊系統或數據資產	在未得到系統擁有者批准的情況下，實體或邏輯接達整個或部分資訊系統及／或其數據。入侵可以經由不可信源頭的手動交互或透過自動化技術造成。	• 異常帳戶活動，例如未獲授權的接達嘗試或權限升級。 • 異常系統或網絡日誌條目。 • 未獲授權更改系統配置或數據。 • 存在未知或未獲授權的使用者帳戶。 • 非預期的系統行為或性能下降。 • 未獲授權接達或洩露資料的證據。 • 安全工具檢測到的惡意軟件或入侵跡象。 • 系統未獲授權的遠端存取或控制。 • 異常的網絡流量模式或連接。	1. 識別並隔離受影響的系統或帳戶，以防止進一步受到入侵。 2. 收集並保存相關日誌和系統工件以供分析。 3. 分析系統日誌、網絡流量和其他可用資料，以確定攻擊的切入點和程度。 4. 進行徹底調查以確定危害的性質，包括識別任何惡意軟件、後門或未獲授權的修改。 5. 評估入侵的影響，例如資料洩露或未獲授權的接達，並採取適當的補救措施以減輕進一步的損害。 6. 將事件通知利益相關者，例如系統擁有者、使用者和管理層。	• 顯示未獲授權的接達或可疑活動的日誌。 • 顯示入侵跡象的系統或應用系統日誌。 • 惡意軟件樣本（如有）。 • 顯示與懷有惡意的人士通訊的網絡流量日誌。 • 用於入侵的使用者帳戶憑證或帳戶。 • 任何擷取的證據，例如系統快照或鑑證圖像。
拒絕服務攻擊	蓄意或無意地妨礙使用資訊資源，以影響資訊資源的可用性。拒絕服務攻擊的	• 網絡流量異常增加或網絡擁塞。 • 系統性能下降或中斷。	1. 確定遇到拒絕服務情況的受影響系統或服務。 2. 確定攻擊的類型和性質，例如基於網絡或基於應用系統。	• 流量日誌，包括源互聯網規約位地址和攻擊模式。 • 攻擊的持續時間和強度。

資訊保安事故	描述	跡象	初步分析／處理	識別／分析所需的資訊
	例子包括 SYN 泛濫、死亡之 Ping 和 Ping 泛濫，這些攻擊嘗試使資訊系統或網絡連接超出負荷，而無法向其用戶提供正常的服務。	• 無法接達或使用特定資源或服務。 • 傳入異常模式的請求或連接。 • 網絡流量或日誌中存在已知的拒絕服務攻擊識別碼。 • 非預期的系統或應用系統崩潰。	3. 分析網絡流量日誌、系統日誌或入侵偵測系統警報，以識別攻擊的模式或識別碼。 4. 通過實施流量過濾、速率限制或其他應對措施來減輕攻擊的影響。 5. 與局部區域網絡/系統管理員或服務供應商合作，識別攻擊的來源或起源。 6. 記錄事故，包括觀察到的攻擊模式以及對系統或服務的影響，以供進一步分析和報告。	• 任何擷取的攻擊證據，例如流量擷取或日誌。 • 表明與攻擊相關的任何贖金要求或威脅的通訊日誌。 • 來自防火牆、路由器或其他保安設備的日誌。
洩漏電子保密資料	保密資料外泄，或被未獲授權人士接達。	• 對保密資料進行異常或未獲授權的接達。 • 異常的資料傳輸或複製活動。 • 存在未獲授權的使用者接達保密資料的情況。 • 不尋常的接達模式，例如在正常工作時間之外或從未獲授權的位置接達保密資料。	1. 確定保密資料洩露或暴露的來源和性質。 2. 確定洩露資料的範圍和敏感性，包括保密級別和潛在影響。 3. 收集並分析系統日誌、接達記錄和其他相關證據，以識別未獲授權的接達或活動。 4. 保留任何可用的鑑證證據以供進一步分析或採取法律行動。 5. 將事件通知適當的利益相關者，例如資料擁有人、資訊	• 顯示未獲授權的接達或資料洩露的日誌。 • 顯示資料洩露跡象的系統或應用系統日誌。 • 與事件相關的通訊日誌（電子郵件、聊天記錄等）。 • 有關洩露資料的資訊，包括其性質和敏感性。

資訊保安事故	描述	跡象	初步分析／處理	識別／分析所需的資訊
		• 資料洩露或未獲授權共用保密資訊的證據。 • 未獲授權披露或發佈保密資料。	科技保安管理部門或管理層。 6. 評估資料洩露的影響並立即採取行動以控制進一步的洩露或未獲授權的接達。 7. 進行徹底調查以確定事件的根本原因，包括保安控制措施中的潛在漏洞或弱點。	• 任何擷取的證據，例如螢幕截圖或錄音。
遺失存有保密資料的流動裝置或抽取式媒體	流動裝置／抽取式媒體因意外或失竊而遺失。	• 流動裝置或抽取式媒體錯放或丟失。 • 對丟失或被盜的裝置進行未獲授權的接達嘗試。 • 異常的使用者行為或模式，例如在未獲授權的設備上接達保密資料。 • 未獲授權接達與丟失或被盜設備相關的資料或帳戶的證據。	1. 收集有關丟失或被盜的移動設備或可移動媒體的資訊，包括設備識別碼、內容和存儲資料的分類。 2. 確定丟失或被盜的日期、時間和地點。 3. 採訪相關人員或證人以收集更多詳細資訊。 4. 分析系統日誌、接達記錄或保安監控視像（如有），以識別與丟失或被盜設備相關的任何未獲授權的接達嘗試或可疑活動。 5. 評估丟失或被盜的潛在影響，例如資料的敏感性和未獲授權接達的可能性。	• 有關丟失設備或媒體的資訊，包括其品牌、型號和序號。 • 丟失的設備或媒體上存儲的資料的詳細資訊。 • 應用於設備或媒體的任何加密或保安措施。 • 表明丟失時間和地點的報告或日誌。 • 任何擷取的證據，例如照片或證人陳述。

資訊保安事故	描述	跡象	初步分析／處理	識別／分析所需的資訊
			6. 將事件通知適當的利益相關者，例如資料擁有者、保安人員或管理層。 7. 採取措施降低資料洩露風險，例如遠程刪除、密碼重置或帳戶暫停。	
偽冒	使用他人身份，以取得超出本身原有的資訊系統接達權限。	• 使用其他用戶的憑據進行異常或未獲授權的登錄嘗試。 • 使用者帳戶使用的異常模式，例如無正當理由接達敏感性資料或系統。 • 未獲授權接達或濫用使用者帳戶的證據。 • 用戶對未獲授權的接達或可疑行為的投訴或報告。 • 試圖繞過身份驗證機制或冒充合法用戶的證據。 • 使用者帳戶設置或許可權的異常更改。	1. 識別已觀察到偽冒嘗試的受影響使用者帳戶或系統。 2. 收集相關日誌、審計記錄或系統工件，以分析與偽冒事件相關的活動。 3. 分析登錄嘗試、帳戶使用模式或系統接達記錄，以識別未獲授權的接達或可疑行為。 4. 核實所報告的與偽冒相關的投訴或事件的真實性。 5. 評估偽冒事件的影響和潛在風險，例如未獲授權接達敏感性資料或系統。 6. 立即採取措施防止進一步未獲授權的接達，例如禁用遭入侵的帳戶或增強身份驗證機制。	• 指示未獲授權的接達或偽冒嘗試的日誌。 • 顯示偽裝活動跡象的系統或應用程式日誌。 • 用於偽冒的使用者帳戶憑證或帳戶。 • 與事件相關的通訊日誌（電子郵件、聊天記錄等）。 • 任何擷取的證據，例如螢幕截圖或錄音。

資訊保安事故	描述	跡象	初步分析／處理	識別／分析所需的資訊
大規模惡意軟件感染	惡意軟件感染可以損毀檔案、刪改數據、加密檔案、秘密偷取數據、關閉硬件或軟件運作，或拒絕合法用戶接達等。決策局／部門須識別及評估是否對業務運作有嚴重影響。	• 異常的系統行為，例如頻繁崩潰或凍結。 • 非預期的彈出窗口或錯誤訊息。 • 系統性能緩慢或無回應。 • 異常的網絡流量模式，例如頻繁連接到可疑或惡意域。 • 通過保安軟件檢測已知的惡意軟件識別碼或指示碼。 • 磁碟活動異常或中央處理單元使用率高。 • 未獲授權接達或更改文件或系統配置。 • 用戶關於可疑文件或活動的報告或投訴。 • 非預期的加密或與加密相關的活動。	1. 識別出現惡意軟件感染跡象的受影響系統或網段。 2. 將受感染的系統與網絡隔離，以防止進一步傳播和破壞。 3. 收集惡意軟件樣本以進行進一步分析和識別。 4. 分析系統日誌、網絡流量和保安軟件報告，以識別惡意軟件活動的模式或指標。 5. 確定惡意軟件的類型和行為，例如其傳播方法、持續機制和負載。 6. 評估惡意軟件感染對決策局／部門的系統、資料和運作的影響。 7. 進行初步調查，了解感染載體和潛在的切入點。 8. 部署適當的工具和技術來消除或減輕惡意軟件感染。 9. 識別並關閉任何允許惡意軟件滲透系統的保安性漏洞或弱點。 10. 從未被感染的備份中恢復受影響的系統或在必要時重建它們。	• 惡意軟件樣本（如有）。 • 入侵指標或已知的惡意軟件識別碼。 • 顯示可疑活動或連接的系統日誌。 • 顯示與惡意域或互聯網規約地址的通訊的網絡流量日誌。 • 受惡意軟件影響的文件或目錄。 • 有關惡意軟件行為或負載的資訊。

資訊保安事故	描述	跡象	初步分析／處理	識別／分析所需的資訊
		• 資料洩露或與指令和控制伺服器通訊的證據。		
勒索軟件	勒索軟件是一種通過加密以阻止和限制用戶接達其系統或檔案並要求付款解密的惡意軟件。	• 無法接達或打開檔案並顯示勒索消息或警告。 • 異常的文件擴展名稱或檔案名稱更改。 • 無用戶干涉而被加密或修改的文件。 • 異常網絡流量模式，例如與已知勒索軟件指令和控制伺服器的通訊。 • 系統上存在與勒索軟件相關的文件或可執行文件。 • 勒索軟件感染後出現異常系統行為，例如性能緩慢或崩潰。 • 攻擊者要求支付贖金或進行通訊。	1. 識別受影響的系統或網段。 2. 將受感染的系統與網絡隔離，防止進一步傳播。 3. 收集勒索軟件樣本以供進一步分析（如有）。 4. 分析系統日誌、網絡流量和保安軟件報告，以識別勒索軟件活動的指標。 5. 確定勒索軟件的類型和變種。 6. 評估勒索軟件感染對系統和資料的影響。 7. 識別切入點或感染載體。 8. 解密來自攻擊者的任何可用的贖金票據或通訊。 9. 確定贖金金額和加密貨幣錢包地址（如提供）。 10. 收集有關受影響文件及其加密狀態的資訊。 11. 研究任何潛在的備份系統或資料恢復選項。	• 勒索軟件樣本（如有）。 • 來自攻擊者的勒索字條或通訊。 • 入侵指標或已知勒索軟件識別碼。 • 顯示可疑活動或連接的系統日誌。 • 顯示與惡意域或互聯網規約地址的通訊的網絡流量日誌。 • 勒索軟件附加的加密文件或文件擴展名稱。 • 有關贖金金額和加密貨幣錢包位址的資訊。 • 備份系統和資料恢復資訊。 • 任何相關的系統或網絡配置。

資訊保安事故	描述	跡象	初步分析／處理	識別／分析所需的資訊
網站遭塗改	未獲授權竄改互聯網網頁的內容。	• 網頁外觀或內容發生顯著變化。 • 未獲授權添加、刪除或修改內容。 • 含有未獲授權的消息或內容的網頁被污損或破壞。 • 非預期的重新定向到未知或惡意網站。 • 異常的網絡服務器日誌，例如多次失敗的登錄嘗試或對敏感目錄的接達。 • 使用者對可疑或更改的網絡內容的報告或投訴。 • 未獲授權接達或修改網站配置或檔案的證據。 • 搜尋引擎排名或網站可見度發生非預期的變化。	1. 識別被破壞的網站。 2. 擷取被篡改內容的螢幕截圖或記錄。 3. 分析網絡服務器日誌以確定損壞的程度和持續時間。 4. 識別日誌中任何未獲授權的接達或修改。 5. 評估污損對網站功能和聲譽的影響。 6. 確定用於破壞的方法（例如，利用漏洞、未獲授權的接達）。 7. 調查任何潛在的保安配置錯誤或弱點。 8. 從未被感染的備份中將網站恢復到原始狀態（如有）。	• 被破壞網站的劃一資源定位址或網址。 • 被篡改內容的螢幕截圖或記錄。 • 顯示未獲授權的接達或修改的網絡服務器日誌。 • 有關對網站功能和聲譽的影響的資訊。 • 任何保安配置錯誤或漏洞的詳細資訊。 • 原始網站內容的備份副本（如有）。 • 任何相關的系統或網絡配置。

然而，單憑一種跡象未必可確定是否有事故發生。擁有豐富保安和技術知識的技術人員應參與判斷，以根據上述的一種或多種跡象確認事故。此外，在確認事故時，多人集思廣益作出的判斷往往優勝於一人作出的判斷。

儘早偵測和識別潛在的保安事故至關重要。因此，決策局／部門必須保持警惕，留意其裝置／環境內任何異常或可疑的活動。以上僅列出了常見的跡象，該列表並非詳盡無遺。決策局／部門應主動監察其系統，並及時調查任何異常行為或與保安相關異常的跡象。以上提供的初步分析步驟和識別／分析所需的資訊僅供參考。由於各決策局／部門的情況和事故應變程序可能有所不同，決策局／部門應相應調整其應變措施。決策局／部門應優先考慮持續監察，並對任何異常或可疑活動保持警惕，以提高及時偵測和識別潛在保安事故的能力，以便及時作出應變和緩解措施。

F.2 影響事故範圍和後果的因素

影響事故範圍和後果的因素包括：

- 事故的影響程度：影響單一系統還是多個系統
- 對公共服務及／或政府形象可能造成的影響
- 新聞媒體的介入
- 涉及犯罪活動
- 事故的潛在影響
- 是否涉及保密資料
- 事故的進入點，例如網絡、互聯網、電話線、局部終端機等
- 攻擊來自本地的可能性
- 預計事故後復原所需的時間
- 處理事故所需的資源，包括人員、時間和設備
- 造成進一步破壞的可能性