

政府資訊科技總監辦公室

資訊保安事故處理指引

[G54]

第 3.1 版

二零零八年十一月
香港特別行政區政府

版權公告

© 2008 香港特別行政區政府

除非另有註明，本出版物所載資料的版權屬香港特別行政區政府所有。在符合下列條件的情況下，這些資料一般可以任何格式或媒介複製及分發：

- (a) 有關資料沒有特別註明屬不可複製及分發之列，因此沒有被禁止複製及分發；
- (b) 複製並非為製造備份作售賣用途；
- (c) 必須準確地複製資料，而且不得在可能誤導他人的情況下使用資料；以及
- (d) 複製版本必須附上“經香港特別行政區政府批准複製／分發。香港特別行政區政府保留一切權利”的字眼。

如須複製資料作上述核准用途以外的用途，請聯絡政府資訊科技總監辦公室尋求准許。

目錄

1	目的	1-1
2	範圍	2-1
2.1	資訊科技保安文件概覽.....	2-2
3	參考資料	3-1
4	定義及慣用詞	4-1
4.1	定義.....	4-1
4.2	慣用詞.....	4-1
5	保安事故處理簡介	5-1
5.1	資訊保安管理中的保安事故處理.....	5-1
5.2	保安事故處理是什麼.....	5-1
5.2.1	資訊保安事故.....	5-1
5.2.2	保安事故處理.....	5-2
5.3	保安事故處理的重要性.....	5-2
6	政府內部資訊保安事故處理的組織架構	6-1
6.1	香港電腦保安事故協調中心.....	6-1
6.2	政府資訊保安事故應變辦事處.....	6-2
6.2.1	政府資訊保安事故應變辦事處的職能.....	6-2
6.2.2	政府資訊保安事故應變辦事處的結構.....	6-2
6.3	資訊保安事故應變小組.....	6-3
6.3.1	資訊保安事故應變小組的職能.....	6-4
6.3.2	資訊保安事故應變小組的結構.....	6-4
6.3.3	資訊保安事故應變小組成員的職責.....	6-4
6.3.3.1	組長.....	6-4
6.3.3.2	事故應變經理.....	6-5
6.3.3.3	新聞主任.....	6-5
6.4	部門資訊系統.....	6-5
6.4.1	部門資訊科技系統經理.....	6-6
7	保安事故處理步驟概覽	7-1
8	規劃和準備	8-1
8.1	保安事故處理計劃.....	8-1
8.1.1	範圍.....	8-1
8.1.2	目標和優先處理事項.....	8-1
8.1.3	職務和職責.....	8-2
8.1.4	限制.....	8-2
8.2	報告程序.....	8-2
8.3	升級處理程序.....	8-3
8.4	保安事故應變程序.....	8-3
8.5	培訓與教育.....	8-4
8.6	事故監察措施.....	8-4
9	保安事故應變	9-1

9.1	確認事故	9-2
9.1.1	判斷是否發生事故.....	9-2
9.1.2	進行初步評估	9-3
9.1.3	記錄事故	9-3
9.1.4	記錄系統狀況	9-3
9.2	升級處理	9-4
9.3	遏制	9-4
9.3.1	決定是否須要暫停受襲系統的操作.....	9-5
9.4	杜絕	9-5
9.4.1	可杜絕事故的行動.....	9-5
9.5	復原	9-6
10	事後跟進	10-1
10.1	事故事後分析	10-1
10.2	事故事後報告	10-2
10.3	保安評估	10-2
10.4	覆檢現行保護措施.....	10-2
10.5	調查及檢控	10-2

附錄

A	保安事故處理準備工作清單
A.1	保安事故處理準備工作清單樣本
B	報告程序
B.1	報告機制建議
B.2	資訊保安事故初步報告表
B.3	事故事後報告
C	升級處理程序
C.1	需要通知的各方
C.2	聯絡名單
C.3	升級處理程序示例
D	確認事故
D.1	保安事故的典型跡象
D.2	為確認事故收集的資料
D.3	事故類別
D.4	影響事故範圍和後果的因素
E	保安事故升級處理工作流程
F	部門資訊科技保安聯絡資料更新表

1 目的

有效的資訊保安管理包括防範、偵測和應變的互相配合。除部署強而有力的保安保護措施外，系統還應具備事故應變能力，以備在發生資訊保安事故時啟動適當程序。保安事故處理是資訊保安管理中重要的一環。

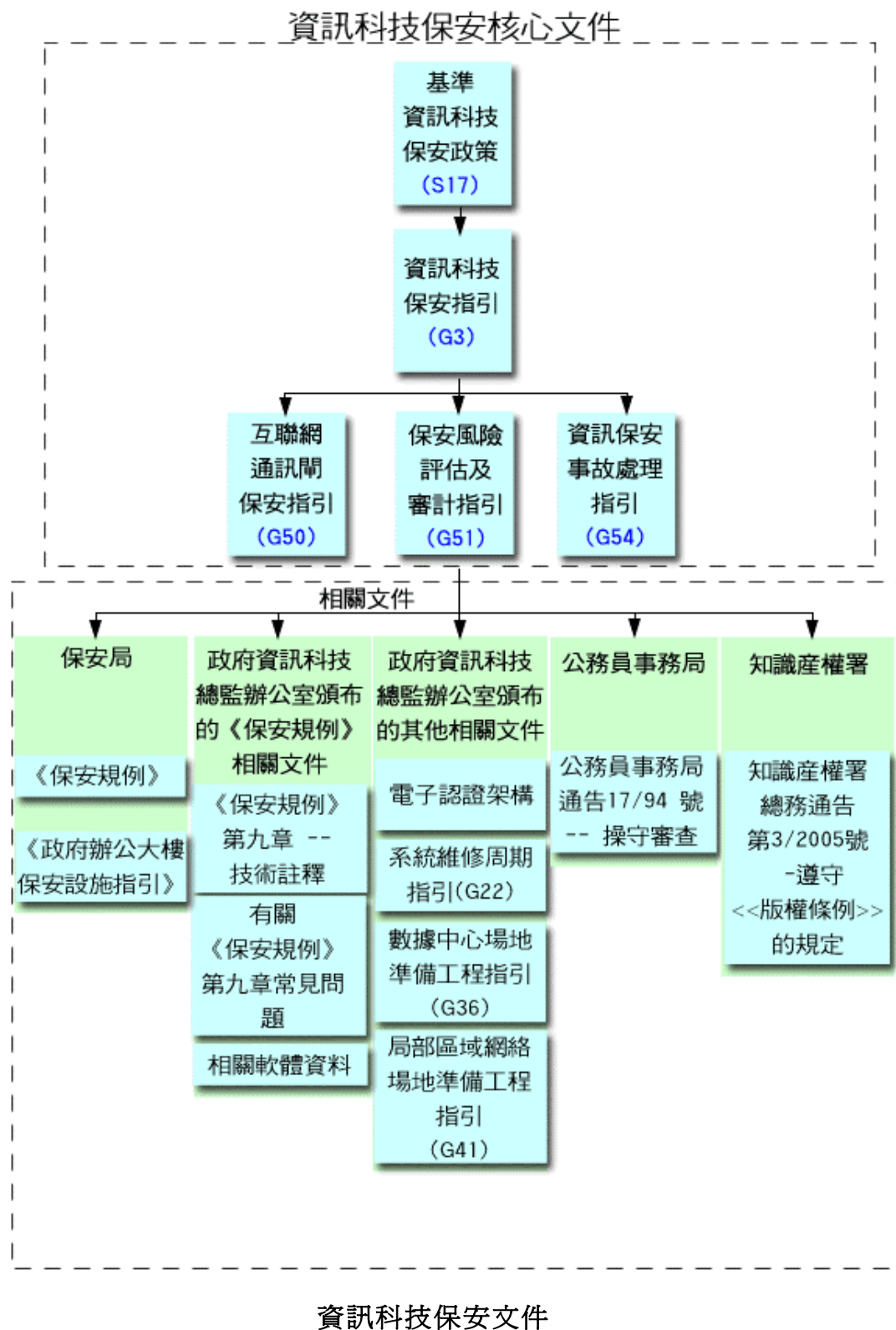
本指引旨在就保安事故處理計劃的制訂，以及資訊保安事故的防範、偵測及應變，為管理、行政及其他技術和操作人員提供參考。由於不同電腦系統的保安事故可能構成不同的影響和導致不同的後果，政策局／部門應根據其實際的操作需要，制訂合適的保安事故處理計劃。

2 範圍

本文件旨在提供資訊保安事故處理的實際指引和參考，但並不包括對具體電腦硬件或操作系統平台的詳細技術描述。政策局／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。

2.1 資訊科技保安文件概覽

下圖所示為政府內部各資訊科技保安文件之間的關係：



五份核心資訊科技保安文件的目的及概要簡述如下：

- 《基準資訊科技保安政策》：**
(S17)
- 最高層次的指令文件，為全體政策局／部門制訂保安規格必須達到的最低標準。這份文件列明了對政策局／部門至關重要的保安工作領域。《基準資訊科技保安政策》可視為必須遵守的強制性基準規例，此外，各政策局／部門亦可採取其他適當的措施加強保安。
- 《資訊科技保安指引》：**
(G3)
- 介紹資訊科技保安的一般概念，並對《基準資訊科技保安政策》作出詳細詮釋。這份文件為制訂保安要求提供了指引和應予考慮的事項。
- 《互聯網通訊閘保安指引》：**
(G50)
- 《資訊科技保安指引》的補充文件，為互聯網通訊閘保安提供一般指引。這些指引是針對互聯網公開平台，將保安風險控制在可接受水平的最佳作業實務。這份文件專為參與互聯網通訊閘操作及技術工作的人員而制訂。
- 《保安風險評估及審計指引》：**
(G51)
- 《資訊科技保安指引》的補充文件，介紹資訊科技保安風險評估及保安審計的通用模型。這份文件的重點並非介紹如何進行保安風險評估或審計的詳情，而是提供一個參考模型，以確保由獨立保安顧問或審計師提供的服務，在範圍、方法及成品方面有所參照。
- 《資訊保安事故處理指引》：**
(G54)
- 《資訊科技保安指引》的補充文件，為管理、行政及其他技術和操作人員提供參考，以便制訂保安事故處理計劃。此外，亦可用作資訊保安事故防範、偵測及應變的參考資料。

3 參考資料

- a) 《資訊科技保安指引》(G3)
(<http://www.ogcio.gov.hk/chi/prodev/csecpol.htm>)
- b) Establishing a Computer Security Incident Response Capability, NIST (National Institute of Standards and Technology) Special Publication 800-3, Nov 1991.
(<http://csrc.nist.gov/topics/inchand.html>)
- c) Sample Incident Handling Procedures, from SANS (System Administration, Networking, and Security Institute), April 1998.
(<http://www.sans.org/newlook/resources/policies/item7.pdf>)
- d) IETF (The Internet Engineering Task Force) RFC 2196 Site Security Handbook.
(<http://www.ietf.org/rfc/rfc2196.txt>)
- e) IETF RFC 2350 Expectations for Computer Security Incident Response.
(<http://www.ietf.org/rfc/rfc2350.txt>)
- f) Responding to Computer Security Incidents: Guidelines for Incident Handling, University of California Lawrence Livermore National Laboratory, July 1990.
(<ftp://ciac.llnl.gov/pub/ciac/ciacdocs/ihg.txt>)

4 定義及慣用詞

4.1 定義

無

4.2 慣用詞

無

5 保安事故處理簡介

5.1 資訊保安管理中的保安事故處理

資訊保安管理可視為一個須反覆持續進行的循環過程。下圖 5.1 所示為過程中涉及的部分工作程序：

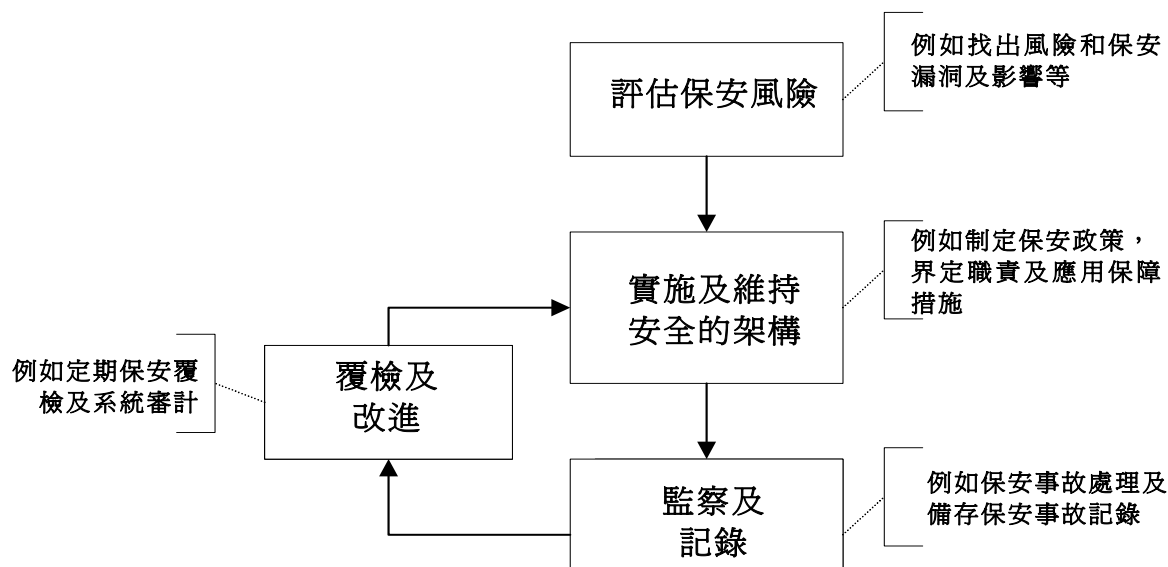


圖 5.1 資訊科技保安管理反覆進行的程序

部署適當的保安措施和保障措施可減低在受到攻擊時被入侵的機會。加強保護的保安措施包括進行風險評估以找出風險和保安漏洞、制定保安政策和指引、採取技術保護措施等。

然而，即使已採取上述各種措施，仍難免有機會發生保安事故，所以必須為保安事故應變作好準備。應指定適當人員負責不同的工作、預留資源並規劃事故處理程序等工作，為發生保安事故作好準備。一旦發生保安事故，這些準備工作將有利於事故應變，使電腦系統能夠以較具條理和更有效率和效益的方式復原。

5.2 保安事故處理是什麼

5.2.1 資訊保安事故

“**保安事故**”一詞在本指引泛指任何與資訊科技保安有關的事故。保安事故是指不合乎政府利益的資料洩漏或資訊系統及／或網絡內的負面事件，對電腦或網絡保安的可用性、完整性和機密性構成威脅。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指引範圍內，這些負面事件應通過系統維修和運作復原計劃處理。

常見的保安事故包括：未獲授權接達、未獲授權擅用服務、資訊系統資源受攻擊致無法使用、服務中斷、破解已採取保護措施的數據／程式／網絡系統權限、機密資料在電子形態下洩漏、惡意破壞或竄改數據／資料、滲透及入侵、濫用系統資源、電腦病毒及惡作劇電子郵件、以及影響聯網系統的惡性程式碼或腳本程式。

5.2.2 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料及制定適當程序（例如升級處理和保安事故應變程序），以備日後遵照執行。

一旦偵測到保安事故，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。一般可成立特定的事故應變小組，負責進行保安事故應變工作。

保安事故過後，應採取跟進行動評估事故，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）和妥善制定的程序處理日後的同類事故。

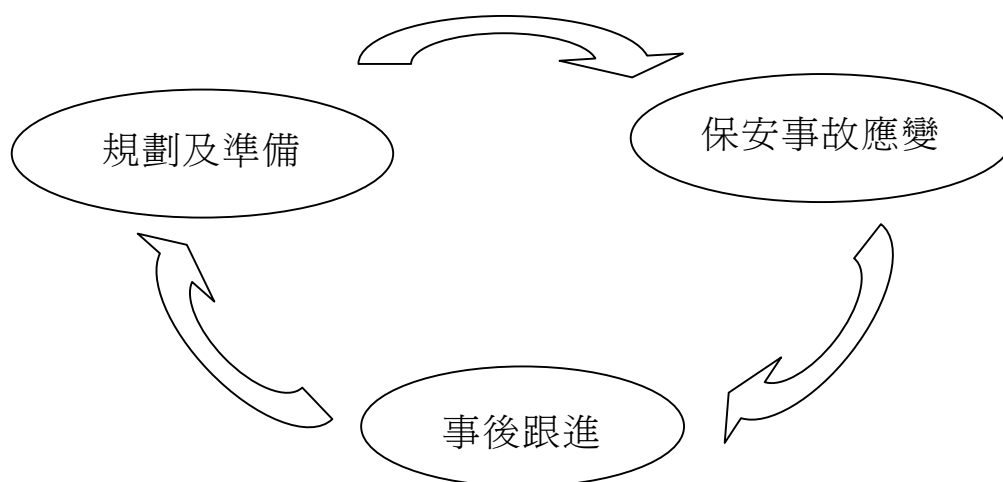


圖 5.2 保安事故處理的循環過程

下文將詳細闡述保安事故處理循環過程的三個程序。

5.3 保安事故處理的重要性

明確清晰的保安事故處理計劃不僅對電腦系統的有效操作至關重要，而且還能影響政策局／部門的整體運作。保安事故處理的主要目的如下：

- a. 確保具備處理事故所需的資源（包括人力資源、技術等）；
- b. 確保負責保安事故處理的各方明確了解，在發生保安事故時須按預定程序進行的工作；
- c. 確保事故應變有條不紊並具效益，而且能夠迅速復原受損系統；
- d. 確保事故應變工作已獲確認和互相配合；
- e. 將洩漏資料、破壞資料和系統中斷等事故可能造成的影響儘量減少；
- f. 在政府內部及與外界分享事故應變經驗；
- g. 防止受到進一步的攻擊和破壞；以及
- h. 處理相關的法律問題。

鑒於資訊科技在政府內部迅速發展，所有政策局和部門都有必要制定一套保安事故處理計劃，尤其是目前正使用下列電腦系統的政策局和部門：

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

6 政府內部資訊保安事故處理的組織架構

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。

每個政策局／部門宜成立一個**資訊保安事故應變小組**，而**政府資訊保安事故應變辦事處**則集中統籌並支援各政策局／部門內部的資訊保安事故應變小組。各政策局／部門的資訊保安事故應變小組負責監督政策局／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。

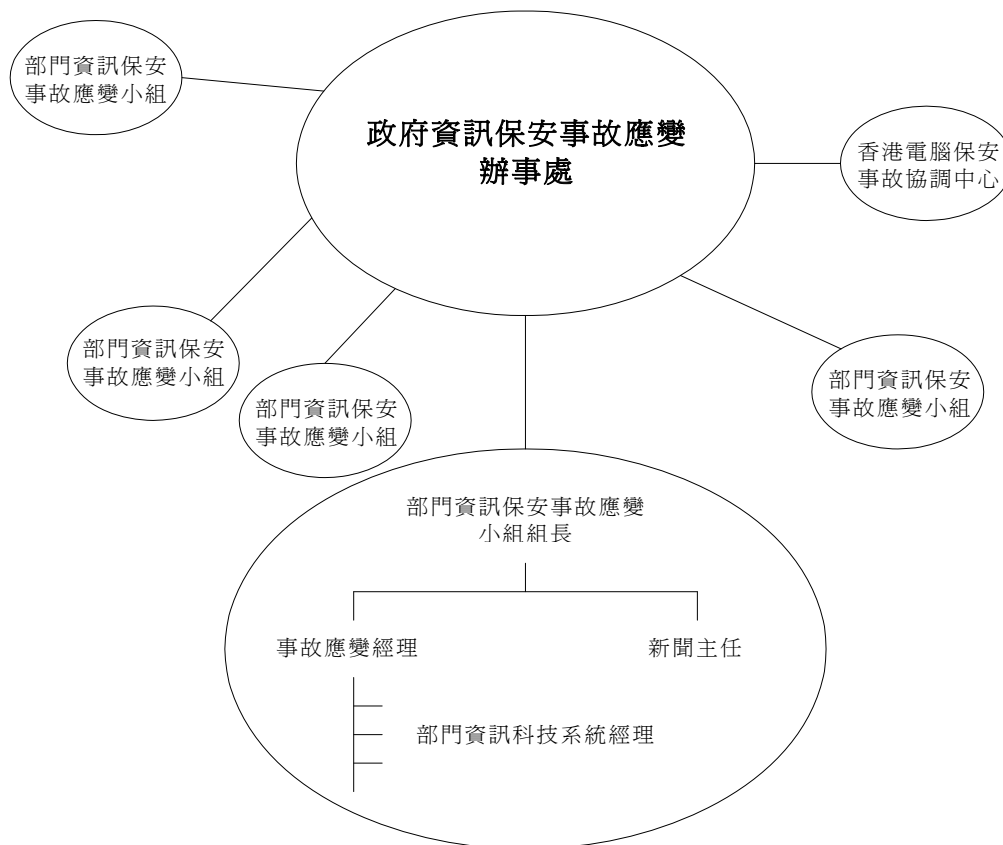


圖 6.1 參與保安事故處理的各方

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，應根據政策局／部門或相關系統的特殊業務需要和操作要求，制定詳細的資訊保安事故處理程序。政府資訊保安事故應變辦事處亦會制定其內部配合程序。

6.1 香港電腦保安事故協調中心

資訊科技、互聯網接達及電子商務的使用量近年來大幅飆升，從而令網絡入侵、電腦病毒攻擊及電腦入侵有機可乘。事實上，近年來記錄的資訊保安事故數目成倍攀升。為了應付這些保安威脅，香港特區政府創新及科技基金撥款予香港生產力促進局以成立香港電腦保安事故協調中心。

香港生產力促進局為香港電腦保安事故協調中心所訂的目標是：

- a. 成為香港電腦保安事故報告和應變的中心點；
- b. 提高電腦保安意識，並推廣國際標準和作業實務；
- c. 協助改善電腦系統的保安，並防範與電腦保安相關的事故；
- d. 為電腦保安事故的復原行動提供協助和協調；以及
- e. 與海外電腦緊急事故應變中心保持聯繫，以便互相合作和協調。

作為電腦保安事故應變的一站式中心，香港電腦保安事故協調中心的主要職能如下：

- a. 通過專門的網站和其他適當的渠道，發出電腦保安警報和報告；
- b. 處理電腦保安事故報告，並為復原行動提供協助；
- c. 通過中心的網站、資訊保安簡訊和報告發布與電腦保安相關的技術訊息和資料，並就保安事故的防範和入侵偵測工具作出建議；
- d. 舉行講座和工作坊等活動以提高電腦保安意識；
- e. 收集事故報告統計數據和報告摘要；以及
- f. 與大專院校、電腦供應商、互聯網服務供應商和其他電腦緊急事故應變中心合作，共同找出解決電腦保安事故的方法。

6.2 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，負責集中統籌及支援各個政策局／部門內部的資訊保安事故應變小組，以處理影響政府資訊科技系統的保安事故。

6.2.1 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：

- a. 就即將及已經發生的威脅，向部門資訊科技保安主任發出保安警報；
- b. 設立中央資料庫，並監督政府內部對所有資訊保安事故的處理；
- c. 定期編製政府資訊保安事故統計報告；
- d. 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受攻擊）；
- e. 在政府資訊保安事故事宜上，充當香港電腦保安事故協調中心與政府之間的聯絡橋梁；以及
- f. 促使政策局／部門的資訊保安事故應變小組與香港電腦保安事故協調中心，互相分享和交流資訊保安事故處理的經驗和資料。

6.2.2 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政策局／部門的代表：

- 政府資訊科技總監辦公室
- 保安局
- 香港警務處

政府資訊保安事故應變辦事處由政府資訊科技總監辦公室、保安局和香港警方代表組成。視乎不同保安事故的性質，必要時可能會邀請個別政策局／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。

政府資訊科技總監辦公室內成立了一個常設辦公室，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。政府資訊保安事故應變辦事處常設辦公室向各政策局／部門提供的服務如下：

- 就即將及已經發生的事故，向政策局／部門發出保安警報；
- 設立中央資料庫，並監督政府內部對所有資訊保安事故的處理；
- 定期編製政府保安事故統計報告，作為各政策局及部門的參考資料；
- 協調政策局／部門報告的保安事故，並向香港電腦保安事故協調中心傳達技術支援的要求；
- 促使政策局／部門及香港電腦保安事故協調中心，互相分享和交流保安事故處理的經驗和資料；以及
- 收集已報告的所有政府保安事故資料，定期為政府資訊保安事故應變辦事處編製統計資料和報告以供參考。

各政策局和部門應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錄 F。

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

6.3 資訊保安事故應變小組

各政策局／部門應成立資訊保安事故應變小組。資訊保安事故應變小組是各政策局／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政策局／部門電腦系統的規模和範圍、系統的敏感程度以及保安事故對政策局／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，但有關的資訊保安事故應變小組，仍須在處理所在政策局／部門的保安事故時，負責整體指揮和控制。

6.3.1 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包括：

- a. 整體監督和協調政策局／部門內部所有資訊科技系統的保安事故處理；
- b. 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，並尋求香港電腦保安事故協調中心提供進一步協助；
- c. 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，給政策局／部門內部負責有關工作的各方；以及
- d. 促進政策局／部門內部，就保安事故處理和其他相關事務分享經驗和交流資訊。

6.3.2 資訊保安事故應變小組的結構

資訊保安事故應變小組是政策局／部門內協調所有資訊科技保安事故的中央聯絡點。政策局／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定個別系統的特定保安政策和事故處理計劃，並制定相關的後勤安排。部門資訊科技保安主任還須確保所在政策局／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政策局／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，例如資訊保安事故應變小組組長、事故應變經理和新聞主任等。視乎各政策局／部門電腦設備的規模和範圍，這些職務可由多人或一人負責。

下文將詳述資訊保安事故應變小組內各項職務及職能。

6.3.3 資訊保安事故應變小組成員的職責

6.3.3.1 組長

組長的職責包括：

- a. 根據事故應變經理提供的事務報告及分析，就系統復原、委聘外部機構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；
- b. 因應事故對政策局／部門業務運作的影響，在適當情況下啟動部門運作復原程序；
- c. 代表管理層批核為事故處理程序投放的資源；
- d. 代表管理層批核就事故的立場所作的公眾發布；
- e. 與政府資訊保安事故應變辦事處合作，協調處理事故報告及必要的跟進行動；以及
- f. 在報告電腦系統的資訊保安事故（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合作：
 - 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發出的拒絕服務攻擊）
 - 處理敏感數據和資料的系統
 - 支援關鍵任務操作的系統
 - 一旦發生保安事故，可能造成重大不良影響的系統，例如因網站遭塗改致使政府形象受損

6.3.3.2 事故應變經理

事故應變經理負責監察政策局／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：

- a. 整體管理及監督政策局／部門內部與保安事故處理相關的所有事務；
- b. 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；
- c. 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；
- d. 在處理資訊事故時與警方、服務承包商、支援服務供應商及保安顧問等外部機構和人士協調；以及
- e. 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。

6.3.3.3 新聞主任

新聞主任負責回覆公眾有關政策局／部門保安事故的查詢。新聞主任還負責整體控制和監督向公眾（包括傳媒）發布資訊的工作。

6.4 部門資訊系統

各部門資訊系統應撥出特定的資源來應付個別資訊科技系統、電腦服務或職能範圍可能發生的保安事故，以便在事故應變上達到最佳的協調及支持。

各資訊系統／服務事故應變小組的規模和結構視乎系統或服務的範圍和性質而有所區別。舉例來說，如果是小型、非關鍵的內部系統，一人便已足以履

行事故應變小組的職責。資訊系統／服務事故應變小組的主要職能包括：

- a. 監督所負責職能範圍的保安事故處理程序；
- b. 事先制定相關的事故處理程序和聯絡名單，以加快及推動處理程序；
- c. 提供直接接收可疑事故報告的途徑；
- d. 直接並即時回應可疑活動；
- e. 協助將破壞減至最少，並恢復系統正常操作；
- f. 向服務承包商、電腦產品供應商或警方等外部機構和人士尋求有關保安問題的意見；
- g. 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；以及
- h. 就所負責職能範圍，對來自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成立類似的事務應變小組，以提供與其職責相應的服務。

6.4.1 部門資訊科技系統經理

部門資訊系統經理監督由其負責的系統或職能範圍內的整個保安事故處理程序。其職責包括：

- a. 制定及推行個別系統的保安事故應變程序；
- b. 遵守並遵從保安事故應變程序，向政策局／部門的事故應變經理和資訊保安事故應變小組報告事故；
- c. 與服務供應商、承包商和產品支援服務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；
- d. 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，例如尋求警方或香港電腦保安事故協調中心的協助；
- e. 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；
- f. 利用保安工具／軟件及／或系統記錄及檢查審計追蹤記錄，找出懷疑攻擊或未獲授權的接達；
- g. 在診斷問題和系統復原過程中，提供有助於收集證據、系統備份和復原、系統配置和管理等技術支援；以及
- h. 為電腦系統或所負責職能範圍安排定期保安評估、影響分析和覆檢。

7 保安事故處理步驟概覽

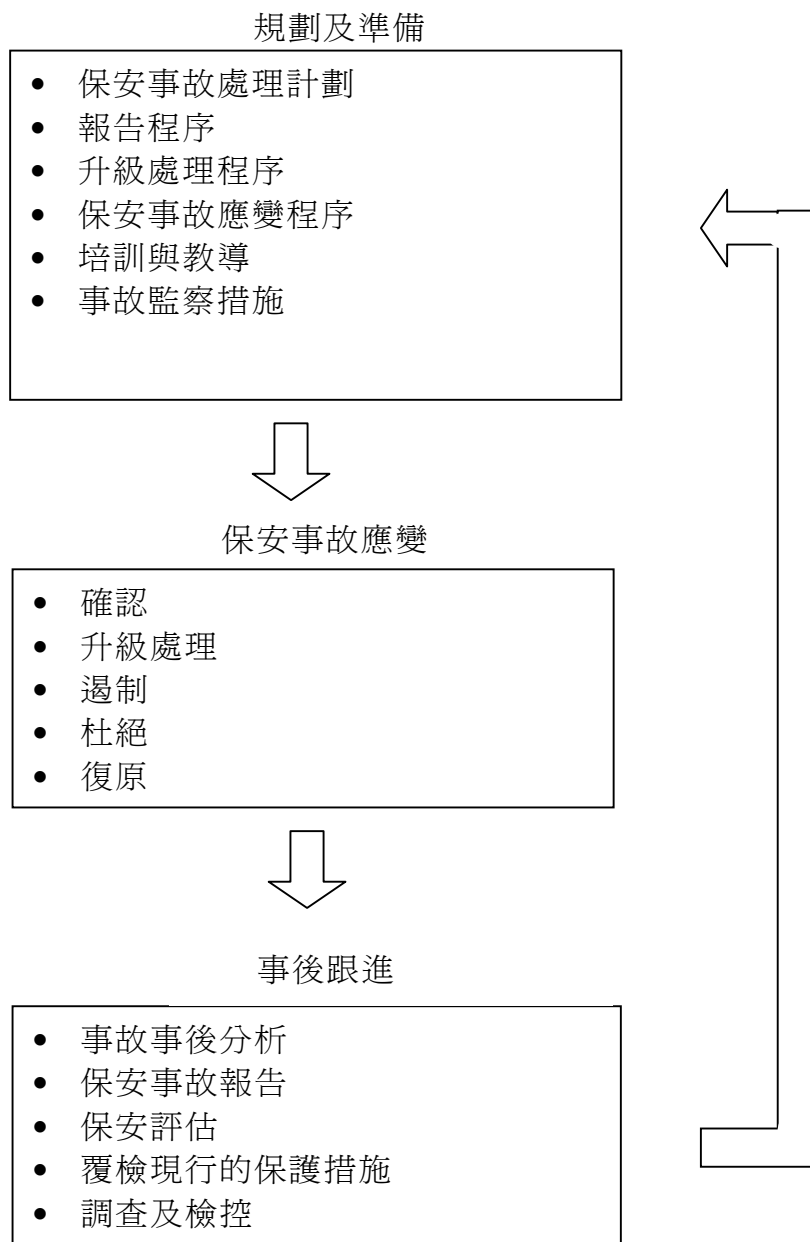


圖 7.1 保安事故處理步驟

保安事故處理的三個主要步驟如上圖 7.1 所示。下文將詳細闡述各步驟所涉及的處理程序。

8 規劃和準備

適當的事先規劃可確保人員對應採取的應變行動有所瞭解，使其能在互相配合及有條不紊的情況下執行。同時還有助政策局／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：

- a. 保安事故處理計劃
- b. 報告程序
- c. 升級處理程序
- d. 保安事故應變程序
- e. 培訓與教育
- f. 事故監察措施

保安事故處理準備工作清單列於附錄 A，以供參考。

8.1 保安事故處理計劃

保安事故處理計劃一般涵蓋以下幾個主要部分：

- a. 範圍
- b. 目標和優先處理事項
- c. 職務和職責
- d. 限制

8.1.1 範圍

這部分為界定保安事故應變小組的職能範圍。有關範圍既可包括整個政策局／部門（即資訊保安事故應變小組），亦可局限於政策局／部門內部的特定資訊系統或應用系統。

8.1.2 目標和優先處理事項

事先應明確制定保安事故處理計劃的目標，並根據系統和管理需要為目標排列緩急次序。及後制定的保安事故應變程序應配合這些預定的目標。

視乎不同系統和管理需要，事故處理的目標可包括：

- a. 儘快使系統恢復正常操作
- b. 儘量減輕事故對其他系統的影響
- c. 避免發生同類事故

- d. 找出事故的根本成因
- e. 評估事故的影響和破壞
- f. 有必要時更新政策和程序
- g. 收集證據為日後的個案調查提供證明

部分事故的性質過於複雜，或規模過大，致難以在同一時間解決所有問題。為處理的事項排列緩急次序便成為必不可少的步驟，因為可以使事故應變人員將焦點首先集中在最關鍵的事項。以下是建議優先處理的事項：

- a. 保障生命和人身安全
- b. 保護敏感或關鍵資源
- c. 保護遺失或損毀後造成較大損失的重要資料
- d. 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
- e. 對服務中斷的影響減到最少
- f. 維護政策局／部門或政府整體的公眾形象

8.1.3 職務和職責

參與保安事故處理工作各方的職務和職責應明確界定。上述第6章為界定保安事故應變小組主要成員的職務和職責提供了參考模型。

8.1.4 限制

資源、科技和時間等限制因素應予考慮。這些限制可能影響保安事故處理工作的結果。舉例來說，政策局／部門如缺乏內部技術專才，便可能須委聘外部顧問或服務承包商。這些準備工作應事先辦妥，確保在發生保安事故時能夠順利處理事故。

8.2 報告程序

報告程序應訂明報告任何可疑活動的步驟和程序，以便及時通知參與事故應變工作的全體人員。報告程序應列明詳盡的聯絡資料，確保負責人員之間能夠有效溝通。在有需要的情況下，應填報辦公時間電話熱線及非辦公時間電話熱線、電郵地址、流動電話及／或傳呼機號碼等聯絡資料。一些建議的報告機制載於附錄 B 第 1 節，以供參考。

此外，應編製事故事後報告，以確保資料貫徹一致及報告所收集的資料完整無缺。事故事後報告樣本載於附錄 B 第 3 節，以供參考。

事先應制定適當的報告程序，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：

- a. 報告程序應載列明確的聯絡點，並制定簡單但明確的步驟以便遵從；
- b. 向相關的全體人員頒布報告程序，以供參閱和參考；
- c. 確保相關的全體人員熟習報告程序，並能夠立即報告保安事故；
- d. 編製保安事故報告表，以規範所收集的資料；
- e. 考慮是否需要在非辦公時間啟動報告程序，如確有需要，應制定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；以及
- f. 有關事故的資料應根據“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。

8.3 升級處理程序

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，所以很難找到適當的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，制定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。

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。不同類別的事故可能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錄 C，以供參考。報告及升級處理政府資訊保安事故的典型工作流程載於附錄 E，以供參考。

8.4 保安事故應變程序

保安事故應變程序界定了一旦發生事故應採取的步驟，其目的在於根據預定的目標和首要工作將破壞減至最少，杜絕事故的肇因，使系統恢復正常操作等。

系統或職能範圍的經理應制定保安事故應變程序，以便在事故處理程序中為保安事故應變小組提供指引。全體員工（包括管理層人員）均應知悉該程序，以作為參考和遵守的依據。這套程序應清晰明確而且容易理解，確保全體人員清楚了解應採取的行動。

第9章將提供處理保安事故的參考模型，特別在確認事故、升級處理、遏制、杜絕和復原程序等方面。

8.5 培訓與教育

政策局／部門應提供足夠的員工培訓，以確保相關的全體員工和管理層人員均懂得如何處理保安事故。各人員應熟習由事故報告、確認和採取適當行動到恢復系統正常操作的處理事故程序。政策局／部門可組織事故處理演習，使全體人員熟習處理保安事故的程序。

此外，爲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。

8.6 事故監察措施

應採取足夠的事故監察保安措施以便在正常操作時保護系統，同時防範潛在的保安事故。所採取措施的程度和範圍則取決於系統、系統處理的資料及系統提供的功能的重要性和敏感程度。

下列是一些常見的保安事故監察措施：

- a. 安裝防火牆構件並採取認證和接達控制措施，以保護重要系統和數據資源；
- b. 安裝入侵偵測工具，主動監察、偵測並就系統入侵或黑客入侵作出應變；
- c. 安裝抗電腦病毒工具和惡性程式碼偵測及修復軟件，以偵測及清除電腦病毒及惡性程式碼，並防止電腦病毒和惡性程式碼影響系統操作；
- d. 定期利用保安掃描工具進行保安檢查，以找出目前存在的保安漏洞，並進行既定保安政策水平與實際保安工作環境之間的差距分析；
- e. 安裝內容過濾工具，以偵測電子郵件或網絡通訊的惡性內容或程式碼；
- f. 開啓系統及網絡審計記錄功能，以便偵測和追蹤未獲授權活動；以及
- g. 利用自行開發的程式和腳本程式協助偵測可疑活動、監察系統和數據的完整性，以及分析審計記錄資料。

9 保安事故應變

保安事故應變涉及制定程序評估事故並作出應變，儘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五個階段：即下圖 9.1 所示的*確認*、*升級處理*、*遏制*、*杜絕*和*復原*。認識各階段具體工作有利於制定有效的保安事故應變程序。

應變程序無須依足五個階段的次序進行，政策局／部門可因應本身的實際需要自行制定應變程序各階段的次序。舉例來說，在報告某些事故時可同時將事故升級處理。

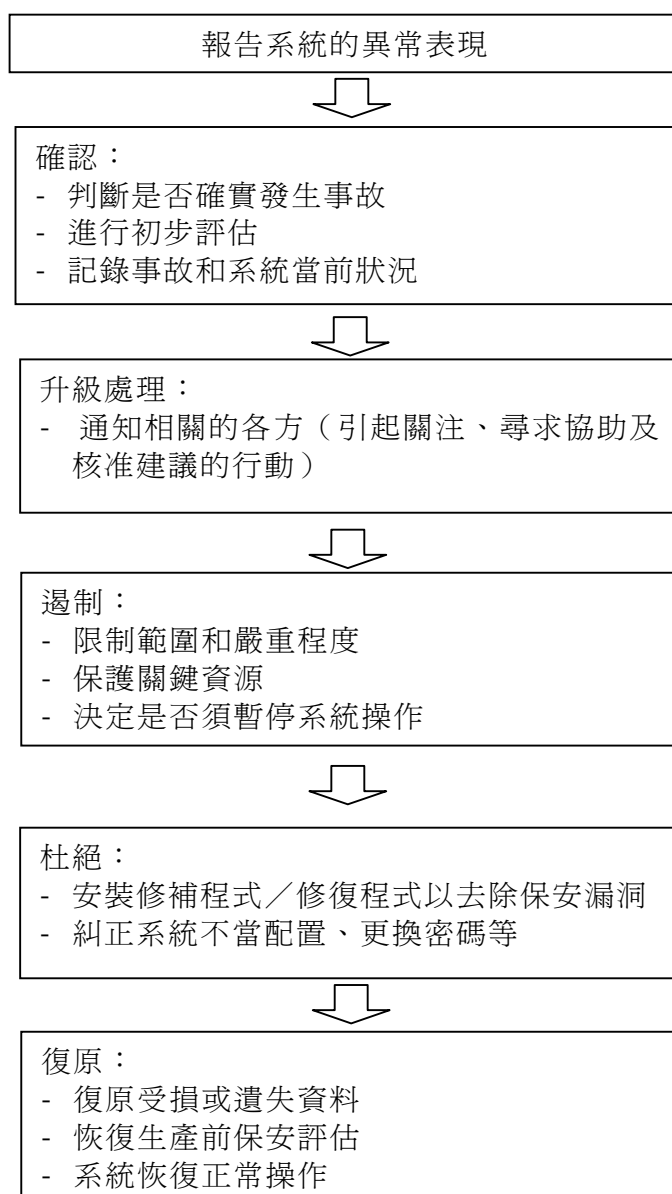


圖 9.1 保安事故應變的主要階段

9.1 確認事故

在發現可疑活動後，電腦系統的用戶、操作員或管理員應遵照既定的報告程序，向有關系統的經理報告事故。收集資料時可使用標準保安事故報告表，該報告表還可用來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，資訊科技系統經理應確認事故，此階段的工作包括以下步驟：

- a. 判斷是否發生事故
- b. 進行初步評估
- c. 記錄事故
- d. 如有需要，記錄系統當前狀況

9.1.1 判斷是否發生事故

首先，資訊科技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。有些看上去好像是保安事故的證據，事實上可能是由另外一些原因造成(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事故所造成，有關人員應從多方面作考慮。附錄 D 載列了一些值得特別注意的典型事故跡象，以供參考。

如果政策局或部門認為事故的性質嚴重，並會對公共服務及／或政府形象構成重大影響，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。

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填妥一份資訊保安事故初步報告表(請參閱附錄 B 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)下列各類嚴重資訊保安事故(有關詳情，請參閱附錄 D 第 3 節)。

- 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)
- 電子郵件轟炸
- 大規模惡性程式碼攻擊
- 網頁遭塗改(包括部門或政府資訊中心網站的首頁及／或公眾經常登入的網頁)
- 數據被竊聽
- 洩露／竄改數據、程式或網絡系統權限
- 滲透／入侵系統
- 偽冒
- 未獲授權接達系統及／或資料
- 濫用系統、資源及／或資料

- 欺詐網站或電郵

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

- 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
- 計劃關閉或維修系統工作
- 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敏感資料

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。如果事故可能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。

9.1.2 進行初步評估

在某事故確認為保安事故後，資訊科技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。了解事故的類別有助確定處理事故的適當應變措施。此外，根據所造成的破壞和影響，還可立即採取一些預防或防衛措施。

附錄 D 載錄部分常見的保安事故類別，以及判斷事故範圍和影響的準則。

9.1.3 記錄事故

資訊科技系統經理記錄所有保安事故、已採取的行動和行動結果。這些記錄有助確認和評估事故，為檢控提供證據，並為及後的事務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。

事故記錄最低限度應包括以下資料：

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

9.1.4 記錄系統狀況

在偵測到可疑活動後以最快的速度，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：

- a. 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
- b. 仍在進行活動的系統登入或網絡連接及程序狀態資料
- c. 留下受襲系統影像，以供調查，並作為日後採取跟進行動的證據。

9.2 升級處理

事故應變的第二階段是通知適當的人員，並根據既定的升級處理程序將事故提升到適當的級別。相關的資訊系統的經理負責升級處理工作，資訊保安事故應變小組的事故應變經理則負責整體協調。

在升級處理過程中，建議在描述事故時提供下列資料：

- a. 簡單描述事故：什麼事故、事故在何時發生、系統如何受到攻擊、所造成的破壞／影響；
- b. 說明攻擊者（如有）是否仍在系統中活動；
- c. 系統資料，例如系統名稱、功能和主機名稱、互聯網規約地址、操作系統及版本等其他技術資料；以及
- d. 補充資料（如有需要），例如屏幕畫面、系統訊息等。

在升級處理過程中提供的資料應明確簡潔、準確而真實。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。政策局／部門還須考慮可否對外提供某些敏感資料。

如果政策局／部門懷疑發生電腦罪案，應聯絡香港警務處商業罪案調查科科技罪案組。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。假如該保安事故涉及個人資料時，政策局／部門必須盡快向個人資料私隱專員公署報告與及在切實可行範圍內盡量通知受影響的有關人士。必須有充份理由並獲得政策局／部門首長的批准，方可不作出以上報告。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，政策局／部門應通知政府資訊保安事故應變辦事處，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，請參閱附錄 C。政府保安事故報告及升級處理工作流程載於附錄 E，以供參考。

9.3 遏制

事故應變的第三階段是遏制。遏制的目的是限制事故的範圍、嚴重程度和影響。有些事故，例如電腦病毒、蠕蟲和惡性程式碼可迅速傳播，並造成大規模破壞。因此，在事故造成進一步破壞前，必須限制事故的影響程度。

事先應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，以及投入什麼不同的資源。如果需要採取關鍵行動，便可能須

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需要諮詢政府資訊保安事故應變辦事處的意見）。

這一階段的工作包括：

- a. 評估事故對系統數據和資料的影響，以確定有關的數據或資料是否已受事故破壞或感染；
- b. 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）；
- c. 決定是否須要暫停受襲系統的操作；
- d. 留下受襲系統的當前記錄，以供調查，並作為日後採取跟進行動的證據；
- e. 記錄這一階段採取的所有行動；以及
- f. 檢查通過共用網絡服務或任何可信賴關係與受襲系統連接的系統。

9.3.1 決定是否須要暫停受襲系統的操作

有待作出的重要決定之一，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、對公共服務和政策局／部門以至整個政府形象的影響，以及系統事故處理計劃預定的目標和優先事項。

可採取的行動包括：

- a. 暫時關閉或隔離受襲的主機或系統，以防止事故對互相連接的其他系統造成進一步破壞。如事故是可快速傳播的、儲存敏感資料的電腦受到威脅，或為了防止受襲系統被利用向相連的系統發起攻擊，就尤其應考慮暫時關閉系統；
- b. 終止受襲伺服器的操作；
- c. 關閉系統的部分功能；
- d. 禁止用戶接達或登入系統；以及
- e. 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服務中斷或資料受損風險的非關鍵任務系統，而且在處理時須格外小心，並加以嚴密監控。

9.4 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電腦病毒。

在移除任何檔案或終止／滅除任何程序前，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。

9.4.1 可杜絕事故的行動

在杜絕階段，政策局／部門可根據事故的類別和性質及系統要求，採取以下行動：

- a. 終止黑客在系統中啟動而仍在運行中的所有程序，以逼使黑客離開；
- b. 刪除黑客建立的所有偽冒檔案。系統操作員在刪除檔案前可能需要將偽冒檔案作備分，以便日後調查；
- c. 清除黑客安裝的所有後門程式（backdoors）和惡性程式；
- d. 採用修補和修復程式修補在所有操作系統、伺服器及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；
- e. 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；
- f. 如發生電腦病毒事故，應遵照抗電腦病毒軟件供應商的指引，在適當情況下從所有受感染的系統和媒體清除惡性程式碼或電腦病毒；
- g. 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；
- h. 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。確保使用具有最新入侵模式的保安工具；
- i. 更換可能被黑客接達的所有登入賬戶的接達密碼；
- j. 在某些情況下，支援人員可能須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關鍵系統造成破壞的嚴重程度，或難以完全清理系統之時；以及
- k. 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，政策局／部門可能須尋求外部機構（例如警方及／或香港電腦保安事故協調中心）的意見，並參考曾經處理類似事故的其他企業或政策局／部門的經驗。此外還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。

9.5 復原

事故應變的第五階段是復原。本階段的目的是在於恢復系統的正常操作。復原工作包括：

- a. 如果是簡單事故（例如入侵失敗），應確保系統或資料沒有受到事故的影響或破壞；
- b. 評估事故的破壞；
- c. 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；
- d. 在受控制的情況下，按照需求的緩急次序逐步恢復功能／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；
- e. 檢驗復原操作是否成功，系統是否已恢復正常操作；
- f. 在恢復系統操作前，事先通知操作員、管理員、高級管理層和升級處理程序所涉及的其他人士等所有相關人士；
- g. 關閉非必要服務；以及

h. 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。這項工作需要利用保安掃描工具，確定事故的問題根源已清除，同時找出系統內可能存在的任何其他保安漏洞。視乎事故的嚴重程度和系統的服務水平要求，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，必須獲得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 事後跟進

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十分重要。跟進行動包括評估事故所造成的破壞、系統改良以防止再度發生事故、保安政策和程序更新及為日後的檢控進行個案調查。

跟進行動可收以下效果：

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

跟進行動包括：

- a. 事故事後分析；
- b. 事故事後報告；
- c. 保安評估；
- d. 覆檢現行的保護措施；以及
- e. 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：

- a. 防止再度受攻擊的建議行動；
- b. 在事故應變時，須迅速取得的資料及獲取有關資料的方法；
- c. 供偵測及杜絕程序所用或所需的額外工具；
- d. 準備和應變措施的足夠程度；
- e. 溝通的足夠程度；
- f. 實際困難；
- g. 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. 遺失或遭破壞的資料、軟件和硬件，包括被洩露的敏感資料
 - v. 受託保密資料的法律責任
 - vi. 難堪或喪失信譽
- h. 汲取的其他教訓。

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，避免其他政府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：

- a. 事故的類別、範圍和程度；
- b. 事故的詳情：攻擊的來源、時間和可能方法及發現攻擊的方法等；
- c. 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）；
- d. 事故應變及杜絕方法；
- e. 復原程序；以及
- f. 汲取的其他教訓。

事故事後報告應在成功復原系統後的一週內提交予政府資訊保安事故應變辦事處。保安事故報告樣本載於附錄 B 第 3 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保安評估，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，可確定應對系統的保安政策、程序和保護機制作出哪些改善。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電腦系統的效用。在進行事故事後分析時，如有需要應覆檢和修訂政策、程序和指引，以配合預防措施。

10.5 調查及檢控

在適當的情況下，還必須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。

如懷疑事故已構成刑事罪行，則應向香港警務處商業罪案調查科科技罪案組報告，以便展開調查和收集證據。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。此外，如果需要向警方報告保安事故，政策局／部門應通知政府資訊保安事故應變辦事處，以便作中央記錄和協調。

附錄 A — 保安事故處理準備工作清單

A.1 保安事故處理準備工作清單樣本

	項目	詳情	進展情況
1	保安事故處理計劃	為保安事故處理制定計劃	
2	報告程序	設計及準備報告機制	
		向全體人員頒布報告機制	
3	升級處理程序	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	
4	保安事故應變程序	準備保安事故應變程序	
		向參與工作的全體人員頒布保安事故應變程序	
5	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	
6	事故監察措施	安裝防火牆設備和接達控制措施,以保護重要的系統和數據資源	
		安裝抗電腦病毒、惡性程式碼偵測及修復軟件和內容過濾工具,定期進行掃描並更新識別碼	
		安裝監察工具,例如入侵偵測軟件	
		開啓系統及網絡設備的審計記錄功能	

附錄 B — 報告程序

B.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，便可能需要以 24 小時電話熱線服務支持。

傳真

以傳真報告事故是電話熱線報告以外的另一個有效機制，尤其適用於當有需要提交詳細資料，而這些資料又無法在電話清晰準確地提供。用來報告事故的傳真機應有人負責收發傳真，如有專人負責收發則更佳。此外，政策局／部門還應特別注意處理傳真報告，以免將事故資料洩露予未獲授權人士。

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。在某些情況下，電郵系統被黑客破解，使黑客能夠截獲電郵而有所提防。解決這個問題的對策包括為電郵加密，或採用其他的報告途徑，例如電話或傳真。

親身報告

這個辦法沒有效率，而且還會構成不便。除非必須由報告事故的人員提供詳細資料或當面與報告事故的人員討論事故，或事故地點與接受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。

限閱

B.2 資訊保安事故初步報告表

背景資料	
政策局／部門名稱：	
概述受影響的系統（例如功能、網址等）：	
受影響系統的位置： <input type="checkbox"/> 政策局／部門內部 <input type="checkbox"/> 第三方服務供應商設施	
系統管理員／操作員： <input type="checkbox"/> 內部資訊科技人員 <input type="checkbox"/> 終端用戶 <input type="checkbox"/> 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：	傳真號碼：
事故詳情	
偵測到事故的日期／時間：	向政府資訊科技總監辦公室報告的日期／時間：
事故跡象：	
影響： <input type="checkbox"/> 網站遭塗改 <input type="checkbox"/> 服務中斷（拒絕服務攻擊／電子郵件轟炸／系統故障） <input type="checkbox"/> 大規模惡性程式碼攻擊 <input type="checkbox"/> 遺失／損毀／未獲授權竄改資料 <input type="checkbox"/> 洩露／洩漏敏感資料 <input type="checkbox"/> 入侵／未獲授權的接達 <input type="checkbox"/> 其他，請說明 _____	
請提供有關影響和中斷服務時間（如有）的詳情：	
採取的行動：	

限閱

限閱

目前系統的狀況：
其他資料：

限閱

限閱

B.3 事故事後報告

事故編號：_____

事故事後報告

政策局／部門：	_____
報告人資料	
報告日期：	_____
報告人	
姓名：	_____
職位：	_____
電話號碼：	_____
電郵地址：	_____
事故詳情	
事故發生日期：	_____
事故類別：	
系統名稱及描述：	
事故概要：	
事件發生的次序：	
<u>日期／時間</u>	<u>事件</u>

限閱

限 閱

已採取的行動及結果：										
目前系統的狀況：										
參與人員： <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid black;"><u>姓名</u></th> <th style="text-align: left; border-bottom: 1px solid black;"><u>職位</u></th> <th style="text-align: left; border-bottom: 1px solid black;"><u>電話號碼</u></th> <th style="text-align: left; border-bottom: 1px solid black;"><u>電郵地址</u></th> <th style="text-align: left; border-bottom: 1px solid black;"><u>職務</u></th> </tr> </thead> <tbody> <tr> <td style="height: 50px;"> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	<u>姓名</u>	<u>職位</u>	<u>電話號碼</u>	<u>電郵地址</u>	<u>職務</u>					
<u>姓名</u>	<u>職位</u>	<u>電話號碼</u>	<u>電郵地址</u>	<u>職務</u>						
黑客（如有）詳情： 電腦病毒（如有）詳情：										
其他受影響場地／系統：										
破壞（包括中斷／暫停服務）：										
成本因素（包括因事故招致的損失和復原成本／人力資源）：										

限 閱

限閱

防止再度發生事故的建議行動：

其他意見：

汲取的教訓：

限閱

附錄 C — 升級處理程序

C.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，尋求服務承包商、產品供應商及警方等外部支援服務機構的意見。

應為各系統設定特有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：

- a. 操作及技術支援人員
- b. 相關資訊系統的經理、資訊保安事故應變小組及政府資訊保安事故應變辦事處
- c. 其他受影響／有關聯的系統或功能操作人員和資訊科技經理
- d. 警方商業罪案調查科科技罪案組
- e. 資訊保安事故應變小組的新聞主任，為向傳媒公布消息準備立場和新聞稿

外部：

- a. 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
- b. 服務供應商（例如數據通訊供應商、互聯網服務供應商）

C.2 聯絡名單

參與工作人員的聯絡名單應包括下列資料：

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

C.3 升級處理程序示例

以下所列是電腦系統 X 的升級處理程序示例。

A. 嚴重及公開事故

這類事故包括當服務中斷或遭黑客入侵時會對公眾造成影響及／或關鍵系統設備發生的事故。

報告時限	聯絡名單	聯絡方法
事故發生後 15 分鐘內	系統 X 的資訊科技經理、技術支援人員、提供支援的相關供應商和服務承包商	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主任	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	預先安排的電話熱線
其後每 30 分鐘	上述各人員	流動電話
系統復原後	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	預先安排的電話熱線

B. 其他事故

這類事故包括不對公眾造成影響的服務中斷及不嚴重的違反保安事故或黑客入侵事故。

報告時限	聯絡名單	聯絡方法
事故發生後 30 分鐘內	系統 X 的資訊科技經理、技術支援人員、提供支援的相關供應商、承包商	流動電話及供應商 24 小時電話熱線
其後每 60 分鐘	資訊科技系統經理及資訊保安事故應變小組	電子郵件
系統復原後	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	預先安排的電話熱線

所有報告都應包括下列資料：

- 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

附錄 D — 確認事故

D.1 保安事故的典型跡象

為判斷異常情況是由系統問題所造成，還是確實已發生事故，可留意保安事故一些明顯跡象。保安事故的常見跡象包括下列任何或全部跡象：

與系統操作相關的跡象：

- a. 入侵偵測工具發出系統警報或類似的訊息
- b. 可疑的系統或網絡賬戶（例如用戶沒有經過正常程序而取得“根”接達權限）
- c. 賬戶資料不符
- d. 部分或全部系統記錄遺失或遭竄改
- e. 系統崩潰
- f. 系統性能突然大幅下降
- g. 未獲授權下執行程式
- h. 可疑的試探，例如多次的登入失敗
- i. 可疑的瀏覽，例如擁有根權限的賬戶接達不同用戶賬戶的多個檔案
- j. 系統時間出現預計以外的大幅偏差
- k. 網絡通訊量出現異常偏差

與用戶賬戶相關的跡象：

- a. 突然建立或刪除用戶賬戶
- b. 頻繁使用以往使用頻率低的賬戶
- c. 因賬戶遭竄改而無法登入
- d. 突然更換用戶密碼
- e. 使用時間異常
- f. 對上一次使用用戶賬戶的情況可疑
- g. 異常使用模式（例如沒有參與程式編製的用戶賬戶在編製程式）
- h. 電腦系統顯示奇怪的訊息
- i. 在無法解釋的情況下，無法接達電腦系統
- j. 大量可疑內容的回彈電郵
- k. 用戶報告收到恐嚇電郵信息

與檔案及數據相關的跡象：

- a. 突然建立、竄改或刪除檔案或數據
- b. 陌生的檔案名稱
- c. 突然竄改檔案大小或數據，尤其是系統的可執行檔案
- d. 突然嘗試寫入系統檔案，或修改系統檔案
- e. 無法接達檔案和數據
- f. 在公開地方（例如打印機出紙口）發現無人看管的敏感資料
- g. 主機入侵偵測系統、抗電腦病毒或惡性程式碼偵測軟件發出的警報

然而，單憑一種跡象一般不能確定是否發生事故。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。

D.2 為確認事故收集的資料

在確認事故時還應查閱下列資料：

- a. 系統記錄、防火牆／路由器記錄、伺服器記錄和入侵偵測系統記錄等審計追蹤或記錄檔案
- b. 仍在進行活動的網絡連接及系統程序狀態資料
- c. 有助調查人員更好地了解系統功能、網絡基本設施及對外連接情況的任何其他資料

D.3 事故類別

凡對政府服務及／或形象造成重大影響的資訊保安事故應予報告，下表列載一些保安事故的類別及其描述：

資訊保安事故	描述
拒絕服務攻擊	蓄意或無意中妨礙使用資訊科技資源，以影響資訊科技資源的可用性。拒絕服務攻擊包括 SYN flood、Ping O death 和 Ping flooding，這些攻擊嘗試使電腦系統或網絡連接超出負荷，使系統癱瘓而無法向其用戶提供正常的服務。
電子郵件轟炸	擅自向郵件伺服器發出大量垃圾電郵，從而向郵件伺服器發起拒絕服務式的攻擊，或利用受害者的系統作基地向第三方的郵件伺服器發起類似攻擊，以誣陷受害者。
大規模惡性程式碼攻擊	惡性程式碼攻擊包括利用如電腦病毒、特洛伊木馬、蠕蟲和腳本程式等發動攻擊，電腦破壞者／黑客藉此而竊取權限、盜取密碼及／或竄改審計記錄，以刪除當中有關未獲授權活動的記錄。電腦病毒和蠕蟲等自我複製的惡性程式碼可迅速複製，因而令遏制加倍困難。
網頁遭塗改	未獲授權竄改互聯網網頁的內容。
數據被竊聽	非法擷取和竊取在網絡或其他通訊渠道的數據、小包。

洩露	違反保安政策的行爲，在未獲授權的情況下洩露或遺失敏感資料。
滲透	在未獲授權的情況下，成功接達資訊系統。
入侵	意圖令資源的完整性、機密性或可用性受損的任何行動。
偽冒	冒用他人身份，以取得超出自己原有的系統接達權限。
未獲授權的接達	未經系統擁有人事先准許，實體或邏輯接達整個或部分資訊科技系統及／或系統的數據。
濫用	如有人利用電腦應用系統作非獲准用途，即已構成濫用，例如用戶利用政府電腦和電郵賬戶向他人發起電子郵件轟炸攻擊。
欺詐性網站或電郵	使用虛假政府網站或聲稱來自政府部門的仿冒電郵，該等行爲均可能涉及詐騙成分。常見的攻擊技術包括仿冒詐騙 ¹ 及域欺騙 ² 。

¹仿冒詐騙：爲了竊取個人資料，利用欺詐性或偽冒電郵，誘騙接收者洩漏個人資料。欺詐電郵通常將接收者引導至看似合法機構的欺詐性網站。

²域欺騙：一般透過入侵領域名稱系統，誤導用戶至欺詐性網站或代理伺服器。

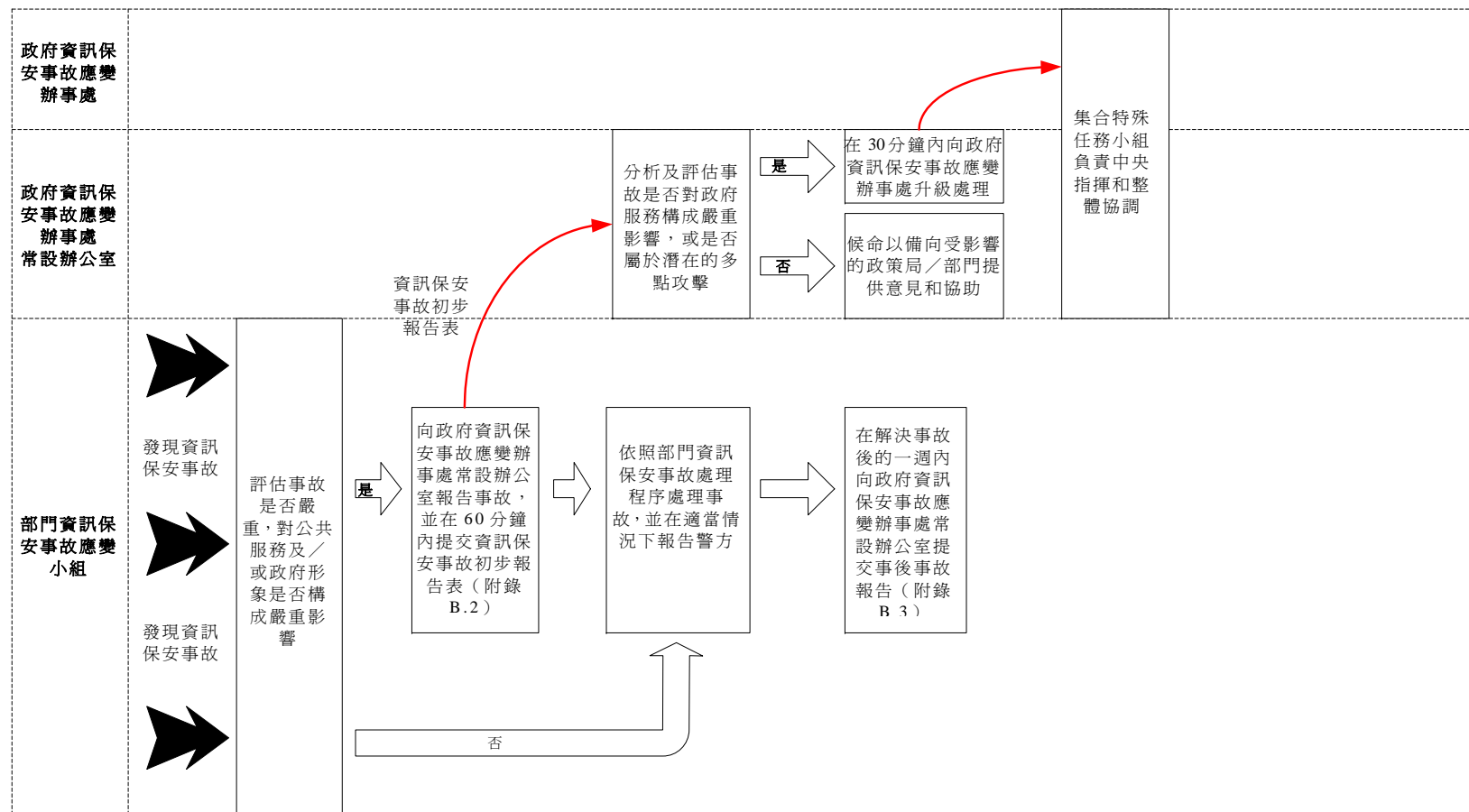
D.4 影響事故範圍和後果的因素

影響事故範圍和後果的因素包括：

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

附錄 E — 保安事故升級處理工作流程

下圖所示為政府保安事故報告及升級處理工作流程圖：



附錄 F — 部門資訊科技保安聯絡資料更新表

政策局／部門名稱	
人員職務	
<input type="checkbox"/> 部門資訊科技保安主任 <input type="checkbox"/> 部門資訊科技保安主任後備聯絡 <input type="checkbox"/> 部門資訊保安事故應變小組組長 <input type="checkbox"/> 部門資訊保安事故應變小組組長後備聯絡 <input type="checkbox"/> 部門互聯網系統管理員 (系統名稱：____) <input type="checkbox"/> 部門互聯網系統管理員後備聯絡 (系統名稱：____) <input type="checkbox"/> 資訊科技保安短訊警報服務用戶	
更換人員：_____	
聯絡資料	
姓名：	職位：
辦公室聯絡號碼：	傳真號碼：
24 小時聯絡號碼：	手機號碼： <small>(資訊科技保安短訊警報服務用戶需填寫此欄)</small>
Lotus Notes 電郵地址： <small>(所有資訊科技保安聯絡人均會收取與資訊科技保安有關的資料)</small>	
收取資訊科技保安小組有關資訊科技保安資料的其他電郵地址：	
委任人	
部門資訊科技保安主任／資訊保安事故應變小組組長姓名：	職位：
部門資訊科技保安主任／資訊保安事故應變小組組長簽署： <small>(可使用 Lotus Notes 系統的數碼簽署)</small>	委任日期：
送交政府資訊科技總監辦公室資訊科技保安小組	
請以下列任何方式，將填妥的資料更新表呈交資訊科技保安小組： xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx (傳真號碼：xxxx xxxx, 電郵：xxxxxxxxxxxxxxxxxxxxxxxx)	