第三章
保安事故處理

3.1 何謂資訊保安事故？

3.1.1 資訊保安事故是指在資訊系統及／或網絡上的負面事件，而且對電腦或網絡安全的機密性、完整性和可用性等方面構成威脅。

3.1.2 保安事故的例子包括：拒絕服務攻擊、受保護的資訊系統或數據資產被侵入、保密的電子資料泄漏、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，以及聯網系統被惡意腳本程式影響。

3.2 保安事故處理的目的

3.2.1 明確清晰的保安事故處理計劃對高效益及有效處理保安事故至為重要。它能於保安事故發生時減少影響和破壞，並有助迅速復原系統的運作。保安事故處理的主要目的如下：

(a) 將學校損失和隨之而來的責任減至最低。

(b) 將可能發生的衝擊，例如資料外泄、資料受損和系統受襲等機會減至最低。

(c) 確保事故應變有條不紊並具效益，而且能夠迅速復原受影響的系統。

(d) 確保具備處理事故所需的資源，包括人力資源、技術等。

(e) 確保負責的人士清楚知道他們的職責，並遵從事先訂制的步驟處理事故。

(f) 確保事故應變工作已獲確認和協調。

(g) 防止進一步的襲擊和破壞再次發生。

(h) 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。

(i) 若涉及個人資料，應向個人資料私隱專員公署報告。

(j) 在切實可行範圍內盡量保存資料作調查之用。

3.3 保安事故處理程序

3.3.1 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。

3.3.2 提早作出恰當的計劃可以確保應變程序為人所知、互相協調和有系統地進行。這亦有助管理層在追查保安事故作出恰當而有效的決策，以降低破壞程度。這計劃包括加強保安防護、適當地對事故作出回應、復原系統和其他跟進行動。保安事故處理有五個主要步驟。這些步驟概述如下：

(a) **規劃和準備**：學校應規劃和準備資源，並制定適當的程序，以備日後遵照執行，以下是給學校的建議：

- 決定學校政策。
- 確保事故應變策略和學校的保安政策相容及事故應變小組有足夠的權力進行保安行動，例如在關鍵時刻將學校的伺服器關閉。
- 界定參與保安事故處理工作各方的職務和職責。
- 建立一個列表，顯示資訊資產／服務的優先次序和可以接受的停頓時間。
- 建立匯報機制、升級處理程序和保安事故應變程序。這些程序都應該通知全體員工，包括管理層人員，以作為參考和遵守的依據。
- 建立和維護良好的備份策略。
- 建立和維護緊急事故聯絡電話表。
- 提供足夠的培訓，確保職員和管理層懂得處理保安事故。
- 教育用戶緊急應變步驟和報告事故的方法。
- 建立一個電腦系統監控和警報機制，例如安裝入侵偵測、抗惡意軟件和內容過濾工具、開啟系統及網絡審計記錄功能，以及定期利用保安掃描工具進行保安檢查。

(b) **偵測及報告**：學校應根據既定的檢測和監控機制偵測保安事件。學校也應遵循報告程序，使保安事件得到高層管理人員的關注。主要活動步驟如下：

- 偵測措施

  - ✧ 監控不正常事件，例如錯誤訊息、日誌記錄中的可疑事件、不正常的效能表現和容量不尋常地增加。
  - ✧ 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。
  - ✧ 來自校外人士（例如電訊服務供應商、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。

- 報告

  - ✧ 所有人員應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。
  - ✧ 相關資料如偵測日期／時間、受影響系統、觀察、報告該保安事件人士的聯絡資料應是報告資訊保安事件的基本內容。

(c) **評估及決定**：事件被偵測後，學校應確定事故是否實際發生。如果某事件被識別為資訊保安事故，學校應確定事故的類型，並評估其範圍，損害和影響以有效處理事故。學校應遵循事先規劃的升級處理程序通知相關方面，並將事件提升到適當的級別。這步驟中的主要活動包括：

- 事件評估

  - ✧ 資訊科技負責人及技術支援人員應判斷是否確實發生事故。然而，要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，資訊科技負責人及技術支援人員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澄清。

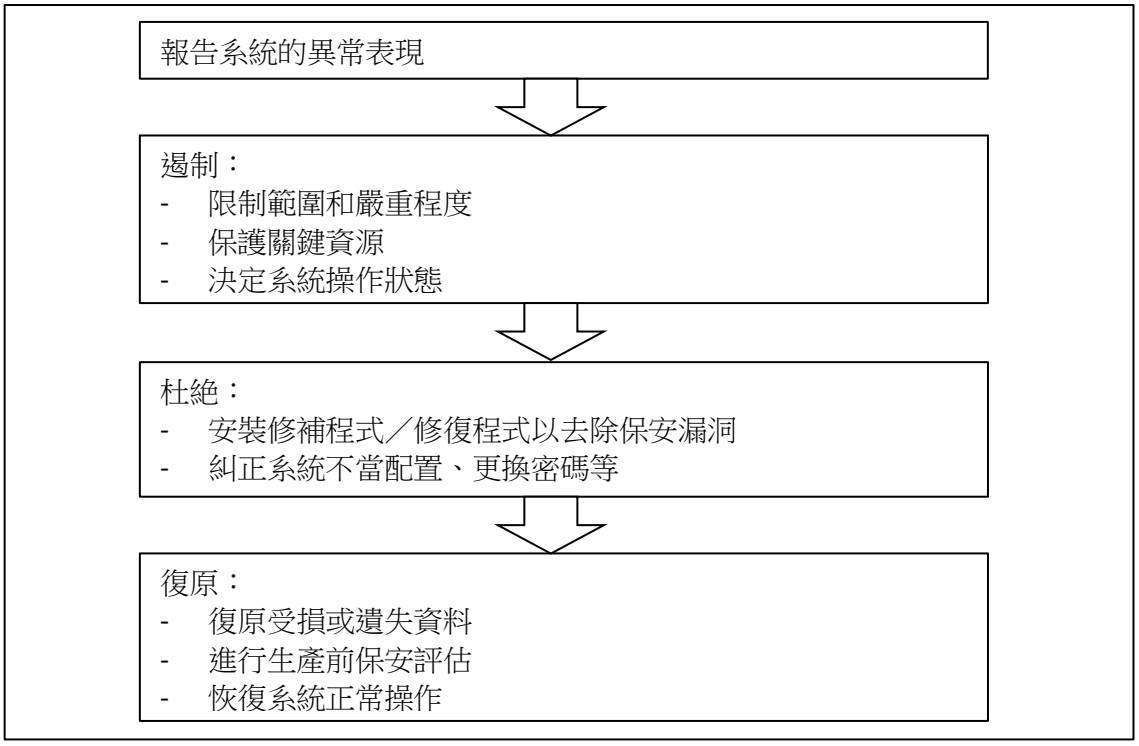
- 升級處理

  - ✧ 資訊科技負責人應判斷事故的類別、評估事故的範圍、破壞和影響，以便作出有效的應變及向學校管理層匯報。
  - ✧ 根據所造成的破壞和影響，可立即採取一些預防或防禦措施。
  - ✧ 如發現或懷疑資訊系統或服務出現任何保安事故或保安問題，必須即時

向負責人士匯報，並根據事故處理程序處理。

- ✧ 如果事故是針對學校的多點攻擊，建議學校通知 HKCERT 以獲取相關資訊及建議。
- ✧ 如學校懷疑發生電腦罪案，學校應聯絡香港警務處網絡安全及科技罪案調查科。
- ✧ 應記錄所有保安事故、已採取的行動和相關的行動結果。
- ✧ 在偵測到可疑活動後應儘早，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。

(d) **保安事故應變**：當識別到保安事故後，學校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、杜絕及復原。要注意的是，應變程序無須依足三個階段的次序進行，學校可因應其實際需要自行制訂次序。



(e) **事故後行動**：事故結束後，應採取跟進行動對事故進行評估，加強保安，防止事故再次發生。在事故發生之後應該儘快作出跟進，校長、資訊科技負責人及用戶都應該參與。

- 進行事後檢討，並找出需要改善的地方，例如：
    - ✧ 檢討現行的設定和程序是否足夠
    - ✧ 檢討是否需要給予用戶更多培訓
    - ✧ 決定是否需要由外來專家進行保安審計
    - ✧ 決定是否就事故進行法律行動
- 應向校長提交一個包括改善建議的報告。
- 校長應評估這報告，並選擇改善建議以執行。
- 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，而作出的系統改善。
- 必須定期按需要檢視及更新保安相關的政策、標準、指引及程序，以確保整體保安措施對資訊系統的效能。

3.4 培訓與教育

3.4.1 學校應確保全體人員均遵守相應的資訊系統保安事故處理／報告程序。各人員應熟習相關程序，由事故報告、確認，以至採取適當行動恢復系統正常操作。建議學校定期舉行事故處理演習，讓人員熟習有關程序。

3.4.2 此外，為了加強系統或功能範圍的保安保護措施，並減低發生事故的機會，向系統操作和支援人員提供足夠培訓亦十分重要，以加強他們有關保安預防的知識。