第二章
保安管理

2.1 資訊保安簡介

2.1.1 資訊保安是指保護各方面資訊和資訊系統，免於未經授權的接達、使用、透露、中斷、修改或毀壞，以確保資訊系統和其資訊的機密性、完整性和可用性。

(a) **機密性**：僅允許經授權人員知道或獲接達到資訊系統所儲存或處理的資訊。

(b) **完整性**：僅允許經授權人員修改資訊系統所儲存或處理的資訊。

(c) **可用性**：用戶可在特定時間內使用資訊系統。

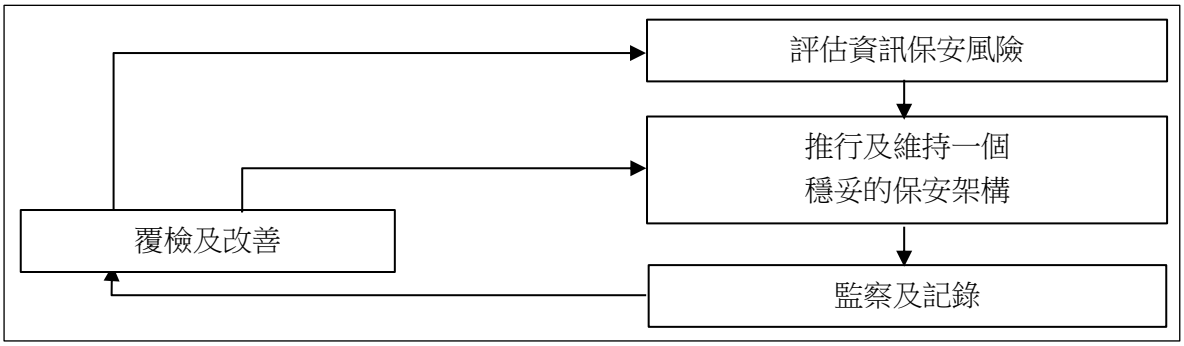
2.2 資訊保安管理周期

2.2.1 使用正確的預防及保護措施可以減少資訊受惡意攻擊的機會。

2.2.2 資訊保安管理涉及綜合性的預防、偵測及應變過程。它是一個重複活動和過程的周期，並需要不斷的監察和控制。

2.2.3 要使資訊保安管理收效，學校中所有成員的參與、理解和支持至為重要。

2.2.4 下圖點出了資訊保安周期所涉及的主要活動。



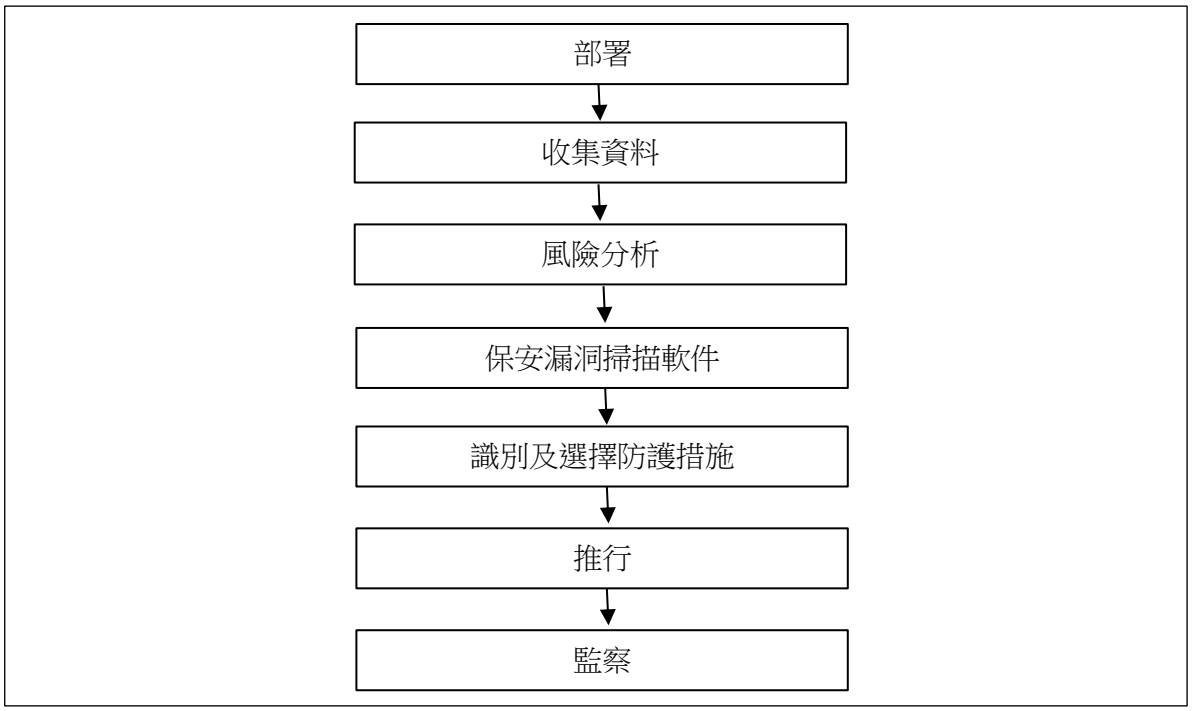
2.3 評估資訊保安風險

2.3.1 資訊保安管理周期始於資訊保安風險評估。進行資訊保安風險評估是為了確定需要採取哪些安全措施。這是評估和識別與漏洞相關的風險及後果的第一步，並為管理層確立具成本效益的保安計劃提供依據。

2.3.2 根據評估結果，便可推行適當的資訊保安防護措施，以維持一個穩妥的保安架構。這包括制訂保安政策和指引、委派保安職責，以及推行技術性的資訊保安防護工作。

2.3.3 緊隨這個步驟是周期性的遵行情況覆檢和再三評估，以確保保安措施正確地執行，以達至用戶的保安要求和應對科技及環境上的急劇轉變。這有賴持續性的回饋和監察。覆檢工作可以透過定期的保安審計來進行，以找出須加強的地方。

2.3.4 通過評估一系列關注事項，學校便能識別出需要保護的資產、它們的相對重要性，以及每個資產的防護迫切性的緩急次序和所需防護程度。以下的流程圖顯示了保安風險評估的主要步驟。



2.4 推行及維持一個穩妥的保安架構

2.4.1 根據從資訊保安風險評估中取得的結果，資訊保安管理周期便進入推行及維護的階段，以推行適當的資訊保安防護措施來建立一個穩妥的保安架構。這包括制訂保安政策和指引、委派保安職務，以及推行技術及行政上的保安防護措施。所有這些步驟對於促進學校資產的保障至關重要。

2.4.2 制訂及推行保安政策：

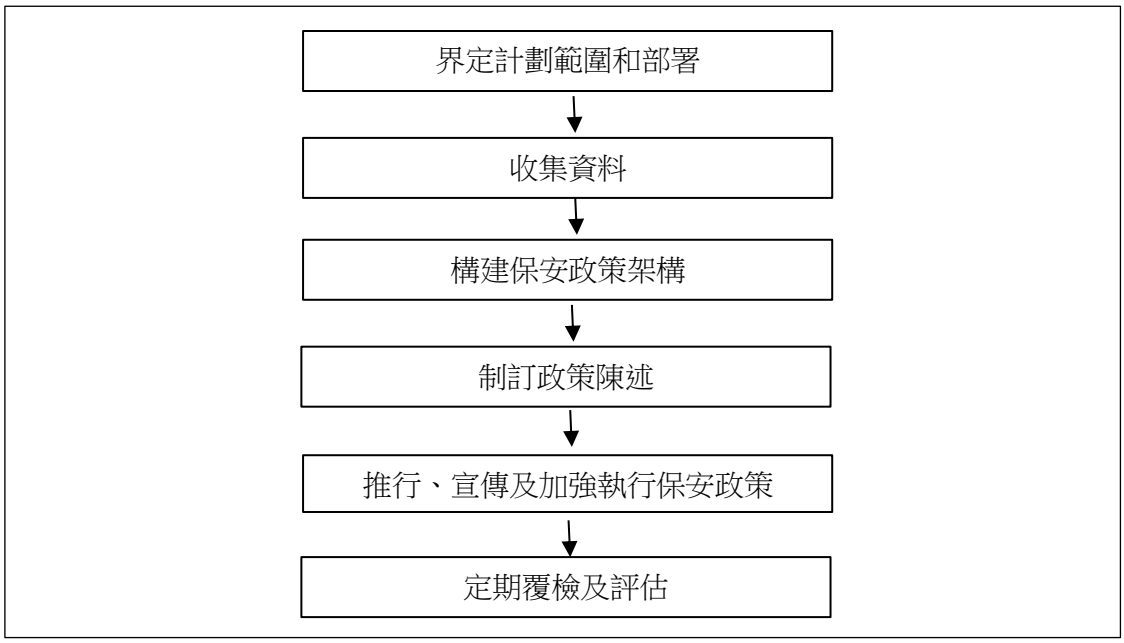
(a) 良好的保安政策就學校的資訊保安設定基本守則。這些守則是強制性的，整所學校內的人員必須遵守。由於每所學校的保安需求均有不同，故其保安政策亦會各異。因此，最重要是保安政策應符合該學校的保安需求、運作目標和政策，才可得到所有員工的支持和落實施行。

(b) 事實上，保安政策可以非常高層次而不受科技所限，又或詳盡而指向等定的科技。保安政策可以分為三個基本類別：

- 程式層面政策
- 問題特定政策
- 系統特定政策

(c) 系統特定政策著重於管理某一特定系統的政策問題。它只會處理一個系統。程式層面政策及問題特定政策兩者則會處理廣泛層面上的問題，通常涵蓋整個機構。

(d) 選擇制訂哪一種保安政策乃視乎學校的需要。然而，最重要的是政策必須定出可行的方向。下面的流程圖是保安政策制訂周期的鳥瞰圖。



(e) 資訊保安政策應涵蓋學校對適當使用其電腦及網絡資源的期望，以及防止和應付保安事故的程序。在草擬政策時，應要考慮校本保安需求。草擬政策時應考慮以下範疇：

- 學校目標及方向
- 現行政策、守則、規條及香港特區政府的法例
- 學校本身的要求和需要
- 推行、分發及執行事宜

2.4.3 制訂及推行管理及行政程序

(a) 根據保安政策所定的方向和範圍，設定管理及行政程序以支持政策的推行。這些是主要的管理及行政活動：

- 委派任務及職責
- 指引及標準
- 保安認知和培訓
- 落實執行
- 各方持續參與

(i) **委派任務及職責**：制訂資訊科技保安政策需要來自多個職級及職務單位人士的積極支持和持續參與。因此，學校必需明確界定責任及適當委派職責，以保護學校的資訊及系統資產，並會視乎運作需要和環境而涉及以下職務：

✧ **學校管理層（辦學團體／法團校董會／校董會／校長／副校長）**

- 指揮及落實制訂保安措施
- 提供推行保安措施所需資源
- 確保各級管理、行政、技術及操作人員參與資訊科技保安工作，並向他們提供一切支援
- 確保保安策略能配合學校的保安要求
- 代表管理層批核就事故向公眾發布的回應口徑

✧ **資訊科技負責人**

- 制訂適當的保安監管程序，以評估、指導、監察及傳達學校內有關資訊科技保安的工作
- 帶領制定、維持及推行資訊科技保安的政策、標準、指引及程序
- 向學校內的負責人傳達由香港電腦保安事故協調中心 (HKCERT)就即將及已經發生的威脅所發出的保安警報
- 確保進行所需的資訊保安風險評估和審計
- 就違反保安事故主動展開調查並作出修正
- 全面監督及協調處理學校內所有資訊系統的資訊保安事故
- 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
- 因應事故對學校運作的影響，在適當情況下啟動學校的運作復原程序
- 代表管理層批核為事故處理程序投放的資源
- 報告資訊保安事故，供學校作記錄及採取所需的跟進行動
- 決定資料的保密類別、授權資料的用途，以及保護資料的相應保安要求

✧ **資訊科技委員會成員**

- 監察、覆檢和改善資訊科技保安管理工作的效益和效率
- 就保安政策的制訂及覆檢提出建議
- 履行學校內的所有保安職責
- 促進學校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訊
- 提高學校的保安意識

✧ **技術支援人員（TSS）**

- 負責學校內部電腦系統和網絡的日常管理、運作及配置工作
- 根據學校制訂的程序／指引，推行保安機制
- 協助帶領處理、監察和協調學校內的資訊科技保安事宜
- 協助找出系統的保安漏洞

- 執行系統保安的管理工作
- 管理資料與系統的控制及接達規則
- 稽查及管理審計記錄

✧ **用戶（教師／職員／學生／訪客）**

- 用戶須為自己的一切活動負責
- 用戶的責任包括：

  - 盡量了解、認識、遵從及運用一切可行及可用的保安機制。
  - 防止其所保管的資料外泄和遭他人在未獲授權的情況下接達。
  - 盡力安全地保管電腦和儲存裝置，防止他人在未獲授權的情況下接達或惡意攻擊裝置。
  - 報告任何不正常事故或故障。

(ii) **指引及標準**：指引及標準是推行保安政策的工具。由於政策可能在一個廣泛的層面上擬訂，故必需制訂有關標準、指引和程序，以給予用戶、管理人員、電腦人員及高層管理人員一個較為清晰的方法去推行保安政策及達成學校的保安要求。

(iii) **保安認知和培訓**：保安意識對於確保有關各方能了解風險、接受和採納良好保安作業模式是十分關鍵的。培訓和教育可以為校長、資訊科技負責人、技術支援人員、用戶及其他有關各方，提供推行保安措施所需的技術和知識。

除非用戶或有關方面作出承諾和溝通，否則政策不可視作已落實推行。這是指用戶及有關方面：

- 已透過簡報或簡介會知悉有關政策
- 已獲邀參與制訂政策建議書
- 已按政策所需接受技術培訓
- 認為保安措施是為他們的利益而制訂
- 獲定期提醒有關最新的保安問題
- 已簽署確認
- 已獲得政策指引

(iv) **落實執行**：這是指推行政策的權力，以及糾正侵犯此等權力的工作。學校應制定程序，為調查違反系統保安的事宜上提供及時的協助。成立學校事故管理小組和設定保安事故處理程序，均能改善保安政策的效能。

(v) **各方的持續參與**：一個有效的保安政策亦有賴學校各方之間的不斷交流資訊、諮詢、協調和合作。從有關方面引入標準、方法、操作守則及其他資訊科技保安方面的專門知識，將有助保持保安政策追上時代和切合需要。

2.4.4 選擇及推行技術措施

(a) 除了管理和行政程序外，推行保安政策可能會透過選擇和應用合適的技術和產品而涉及技術措施。這些技術措施應在正式操作前進行適當的測試。

(b) 以下是給學校的建議：

- 選擇及推行有關技術及產品的措施，如：
  - ✧ 抗惡意軟件
  - ✧ 接達控制系統
  - ✧ 防火牆
  - ✧ 入侵偵測系統
  - ✧ 加密技術
  - ✧ 密碼匙的管理及密碼匙分發系統
  - ✧ 網絡管理系統及保安管理系統
- 採取適當的操作程序，如：
  - ✧ 採取適當程序來管理帳戶及個人數據
  - ✧ 採取適當程序來處理事故
  - ✧ 採取適當程序來追蹤系統活動和警告
  - ✧ 採取適當程序來監察保安基建的健全狀況
  - ✧ 採取適當程序來處理及控制變動

2.5 監察及記錄

2.5.1 在透過推行及維護來提供穩妥的保安架構的同時，還要恆常地進行監察及記錄，以便在處理保安事故時能夠作出適當安排。

2.5.2 日常運作如用戶在使用資源或資訊時的接達嘗試及活動，也要妥善監察、審計和記錄。例如，個人用戶身份識別需要包含在審計記錄中，以加強個人責任。每位用戶在使用學校資源時應了解其責任，並為本身的行為負責。

2.5.3 主要恆常記錄活動應包括：

(a) 維持保安事故處理及匯報程序

(b) 維持主要系統及重要應用程式的審計追蹤

(c) 維持適當的帳戶權限分配及更新記錄

(d) 維持操作系統的事件記錄及誤差記錄

(e) 維持進入學校網絡的訪客或嘉賓的進入記錄

(f) 維持記錄以追蹤接達及進行重要活動的授權情況

2.6 覆檢及改善

2.6.1 覆檢及改善是持續性檢討以找出需要改善的地方。這是一系列對於遵守情況的周期性覆檢和重新評估，確保能適當地執行保安措施以達至保安要求，並應對技術和環境上的急劇轉變。它亦需要持續的回饋和監察。可以透過定期的保安審計來進行檢討工作，在一個持續性的基礎上進行監察和檢討保安作業模式及策略。

2.6.2 保安審計是一個重複性的檢測過程，以確保在任何時候保安措施均被妥善地執行。保安審計較保安風險評估進行得更為頻繁，旨在找出目前環境是否按照既定的保安政策而受到安全保護。

2.6.3 保安審計的目的

(a) 提供遵守保安政策的證據

(b) 檢查及分析系統及操作環境的防護

(c) 評估保安設計的技術及非技術性推行情況

(d) 確認所有保安功能是否適當或不適當地整合及操作

2.6.4 審計步驟

(a) 界定審計範圍及活動

(b) 規劃

(c) 收集審計數據

(d) 進行審計測試

(e) 匯報審計結果

(f) 保護審計數據及工具

(g) 改善及跟進

2.6.5 應積極及定期監察和覆檢審計服務供應商及用戶的保安控制遵行情況，並保留權利以審計服務水平協議所界定的責任及安排獨立第三方進行審計。

2.6.6 為了確保有效及全面地進行檢討，學校須保存最新及準確的詳細清單，包括：

(a) 一份載有服務內所有的伺服器和系統的清單，以及那些伺服器／系統會儲存敏感或個人資料；

(b) 一份第三方服務供應商支援人員的名單，包括授予個別支援人員的用戶帳戶和接達權限；及

(c) 一份已移交給第三方服務供應商的資料（尤其是敏感或個人資料）之清單。