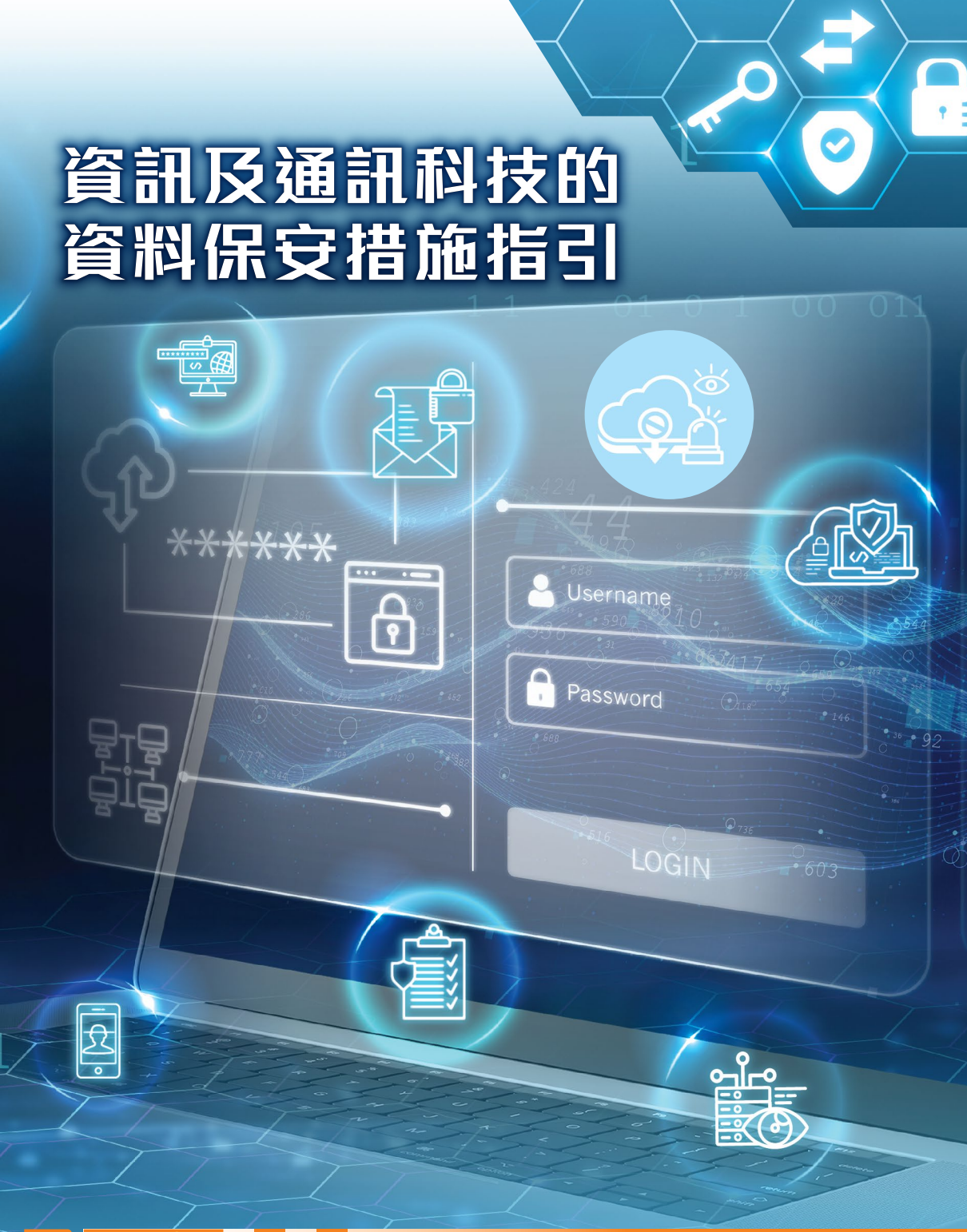
資訊及通訊科技的資料保安措施指引



PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

引言

《資訊及通訊科技的資料保安措施指引》（指引）就資訊及通訊科技方面的資料保安措施向資料使用者提供建議，以協助他們遵從《個人資料（私隱）條例》（香港法例第 486 章）（《私隱條例》）的相關規定。指引同時在加強資料保安系統方面，向資料使用者建議良好的行事方式。本小冊子涵蓋指引中的重點建議。

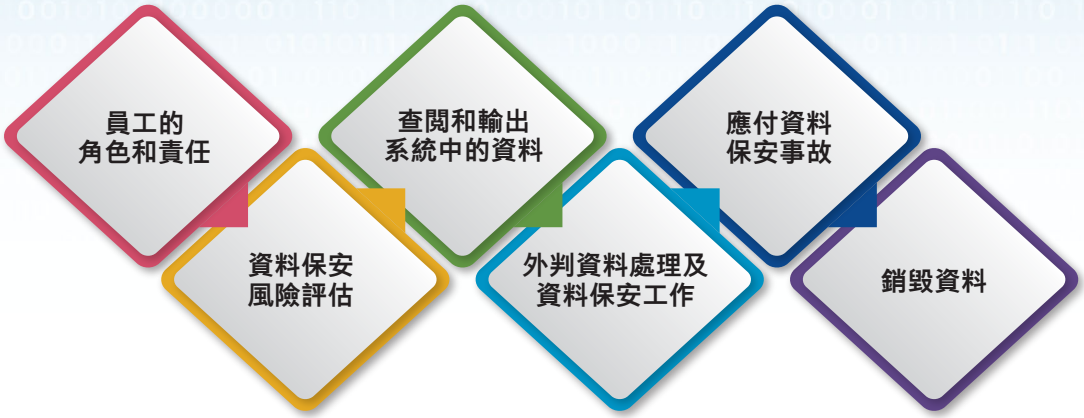
向資料使用者建議的資料保安措施可歸納於 7 大範疇：

- 資料管治和機構性措施
- 風險評估
- 技術上及操作上的保安措施
- 資料處理者的管理
- 資料保安事故發生後的補救措施
- 監察、評估及改善
- 其他考慮

資料管治和機構性措施

- **政策及程序**

  資料使用者應制訂針對資料管治和資料保安的政策和程序，並涵蓋以下範疇：



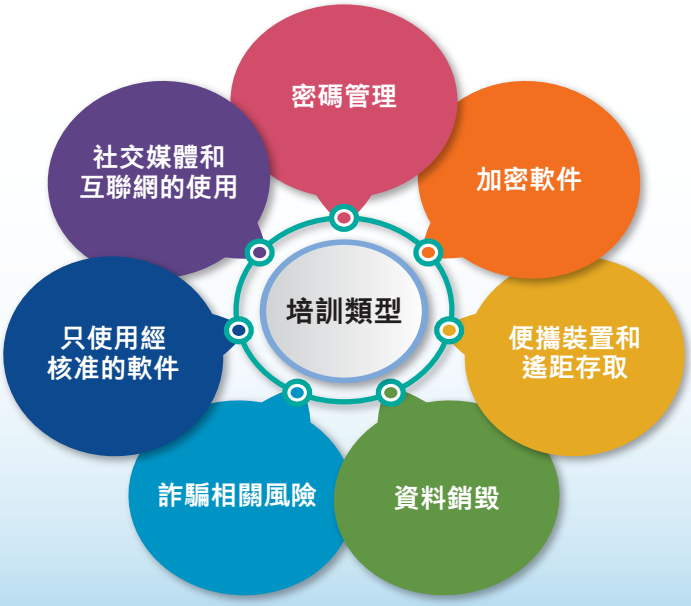
- **人手**

  委任合適的領導人物負責資料保安

  負責資料保安人員的數量、資歷及技術能力應與資料處理活動的性質、規模、複雜性，以及資料保安風險合乎比例

- **培訓**

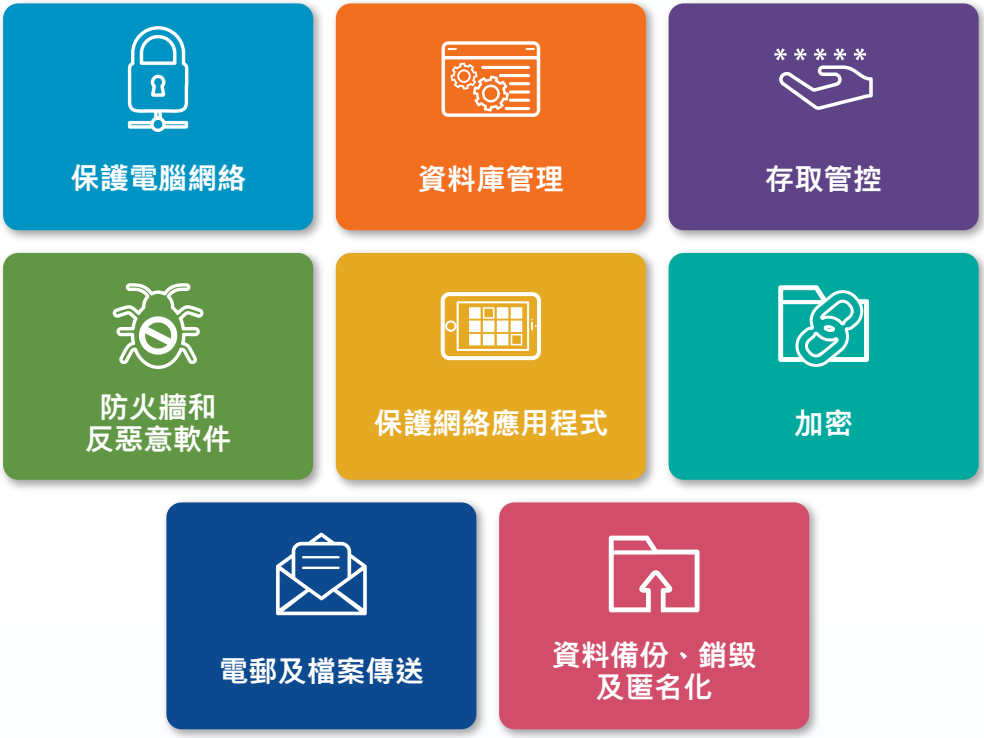
  工作人員應在入職時及往後定期接受培訓：



風險評估

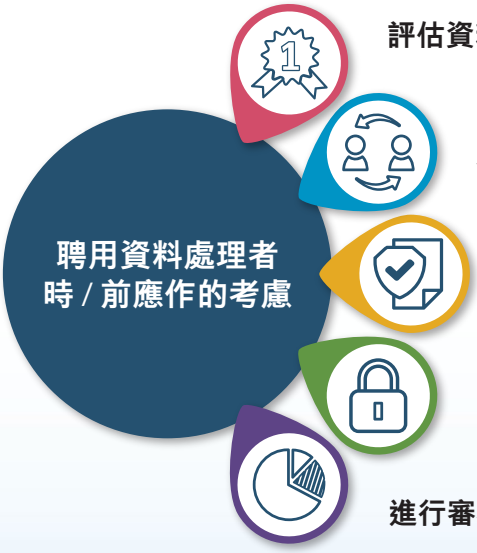
- 啟用新系統和新應用程式前，先進行資料保安風險評估 — 如有需要，可聘用第三方專家
- 定期向高級管理層匯報風險評估的結果
- 及時處理發現到的保安風險

技術上及操作上的保安措施



資料處理者的管理

根據《私隱條例》保障資料第 4(2) 原則，資料使用者須採取合約規範方法或其他方法，以防止轉移予資料處理者作處理的個人資料在未獲准許或意外的情況下被查閱、處理、刪除、喪失或使用。



- 評估資料處理者的稱職及可靠程度
- 只把最少及必要的資料轉移至資料處理者
- 在合同中訂明須採取的保安措施
- 要求通報資料保安事故
- 進行審核，以確保合同獲得遵從

發生資料保安事故後可採取的補救措施

資料使用者在資料保安事故發生後採取及時和有效的補救措施，可能減低個人資料被未獲准許的或意外的查閱、處理或使用的風險，從而減輕對受影響人士可能造成的傷害。

- 停止並中斷連接受影響的系統
- 更改密碼或中止權限
- 更改系統配置
- 通知受影響人士並提供建議
- 通知私隱公署及其他執法或監管機構
- 修補保安漏洞
- 在可行情況下掃瞄系統
- 汲取經驗及教訓

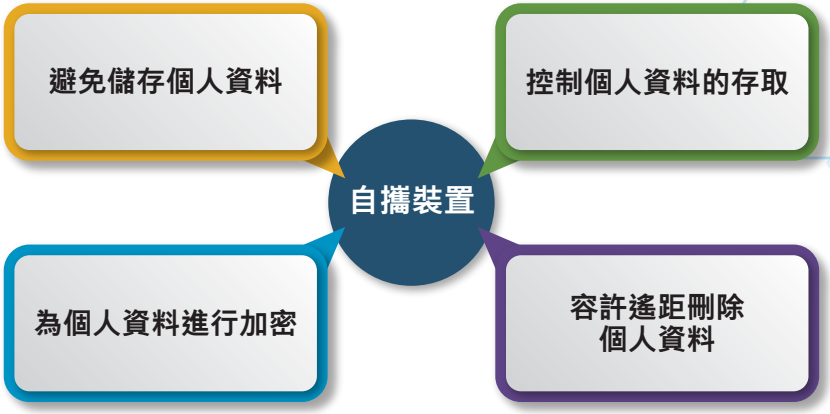
監察、評估及改善

- 委派獨立的專責小組（例如內部或外部審計隊）負責定期監察資料保安政策的遵從情況，以及定期評估資料保安措施的成效
- 如發現違反政策的行為或保安措施成效不彰，應採取改善行動

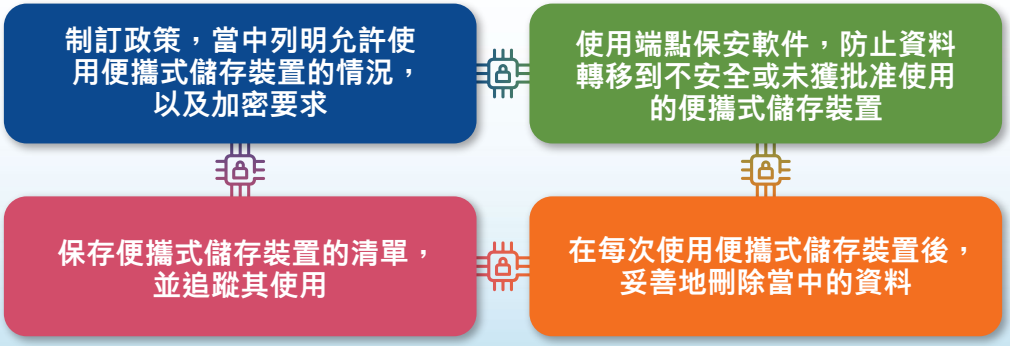
其他考慮

- 使用雲端服務時的考慮因素

- 實施自攜裝置政策時可採取的保安措施



- 使用便攜式儲存裝置時可採取的保安措施



PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

下載本刊物

下載指引

香港灣仔皇后大道東248號大新金融中心13樓1303室

電話：2827 2827
傳真：2877 7026
電郵：communications@pcpd.org.hk
網站：www.pcpd.org.hk

二零二三年二月初版

環保紙印刷