資訊保安工作坊 - 保護訊息資產 提升同工資訊保安意識

2023年3月28日

資訊及通訊科技的保安措施指引

譚嘉榮先生
個人資料主任（資訊科技）

《私隱條例》的相關規定

《私隱條例》的相關規定

《私隱條例》的規定　1) 有關資料保安的規定

保障資料第4原則:

4 保安措施 Security

資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

NOTE

在發生資料外洩的情況下，資料使用者有責任證明他們已採取所有合理地切實可行的步驟以保障個人資料的安全，而「合理地切實可行」的步驟將視乎每個個案的案情而定。

《私隱條例》的相關規定

《私隱條例》的規定　2)《私隱條例》其他相關規定

資料收集

就「**收集最少量資料**」這一基本原則，**保障資料第1(1)原則**訂明，資料使用者只應為收集資料目的**收集足夠但不超乎適度的資料**。

NOTE

一般而言，資料使用者最初收集或保留的資料越少，日後的安全風險便越低。

資料保存

保障資料第2(2)原則要求資料使用者採取「所有切實可行的步驟」，以確保個人資料的**保存時間不超過所需**。

《私隱條例》第26條亦要求資料使用者採取「所有切實可行步驟」**刪除不再為使用目的而需要**的個人資料。

NOTE

資料使用者持有的資料越少，受攻擊或出現漏洞的風險便越低。

資料保安建議措施

資訊及通訊科技的資料保安建議措施

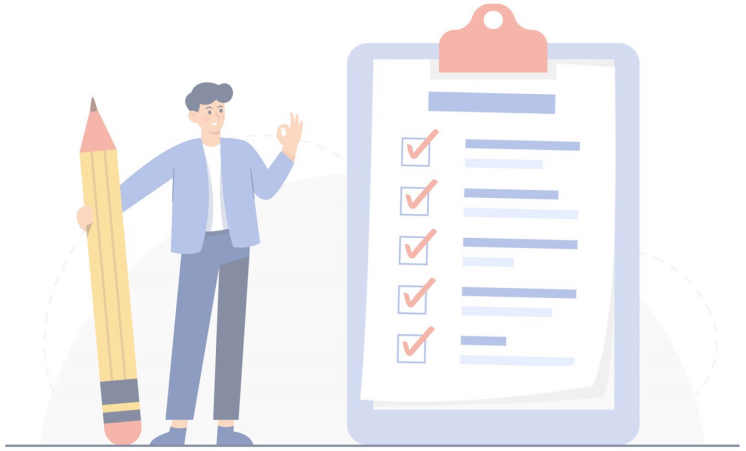
資料保安建議措施 *七大建議措施一覽*

1. 資料管治和機構性措施 (Data Governance & Organisational Measures)
2. 風險評估 (Risk Assessments)
3. 技術上及操作上的保安措施 (Technical and Operational Security Measures)
4. 資料處理者的管理 (Data Processor Management)
5. 資料保安事故發生後的補救措施 (Remedial Actions in the event of Data Security Accidents)
6. 監察、評估及改善 (Monitoring, Evaluation and Improvement)
7. 其他考慮 (Other considerations)

資訊及通訊科技的資料保安建議措施

1) 資料管治和機構性措施 *政策及程序*

資料使用者應制訂明確針對**資料管治**和**資料保安**的**內部政策**和**程序**，並涵蓋:



NOTE

資料使用者應根據當時情況（如業內新標準、資料保安新威脅等），定期和及時地覆檢與修訂政策及程序。

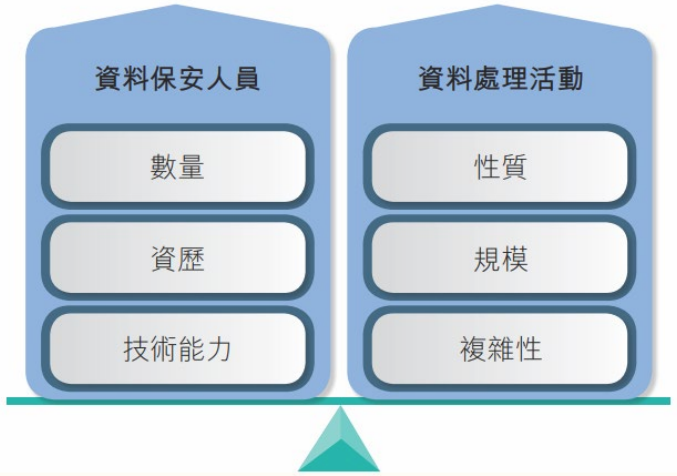
資訊及通訊科技的資料保安建議措施

1) 資料管治和機構性措施 *人手*

資料使用者應:

- 委任合適的領導人物負責個人資料保安（如首席資料官、首席私隱官等）
- 提供適當的人手配置
- 制訂指引列出:
  ① 處理的個人資料從收集到銷毀的**整個資料周期**
  ② 有關人員的**角色和責任**
  ③ 決策的**權力分配**
  ④ 有關查閱和轉移個人資料的**問責和監督權**

資料保安人員的配置應與資料處理活動合乎比例



NOTE

資料使用者亦要注意員工的審慎態度及誠信，以免因人為錯誤或內部攻擊而引致資料外洩。

在適當情況下，資料使用者可考慮在僱傭合約中加入保密責任。

資訊及通訊科技的資料保安建議措施

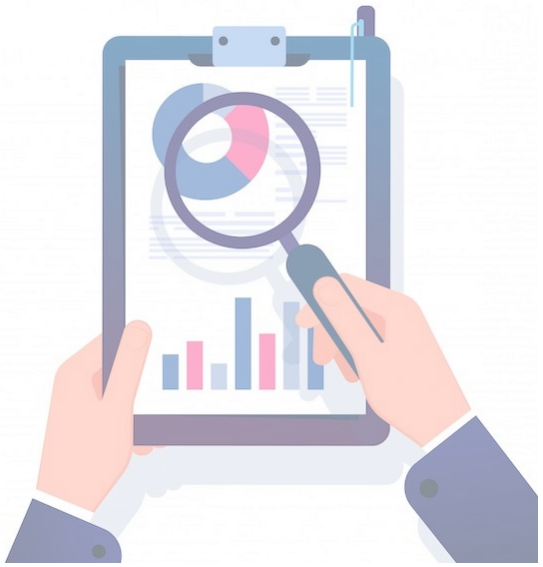
1) 資料管治和機構性措施 *培訓*

工作人員應在入職時及往後**定期接受足夠培訓**，培訓類型可包括:

NOTE

企業可考慮將「演習」納入資料保安培訓（例如模擬的網絡騙案），以提高員工的警覺程度。

資訊及通訊科技的資料保安建議措施



NOTE

風險評估的結果應定期向高級管理層匯報，而發現的保安風險亦應及時處理。

2) 風險評估

資料使用者應:

- 在啟用新系統和新應用程式前，以及在啟用後**定期進行資料保安風險評估**
- 就控制的個人資料**備存清單**，並評估有關資料的性質，以及它們被洩露的潛在損害
- 在收集敏感資料前作慎重考慮，確保**只收集必要的資料**並**提供更穩妥的保障**（例如以加密的形式儲存在獨立安全的資料庫中）

➢ *缺乏相關專業知識的中小企應考慮聘用第三方專家，以進行安全風險評估*

資訊及通訊科技的資料保安建議措施

3) 技術上及操作上的保安措施 *保護電腦網絡 (非詳盡)*

資料使用者應:

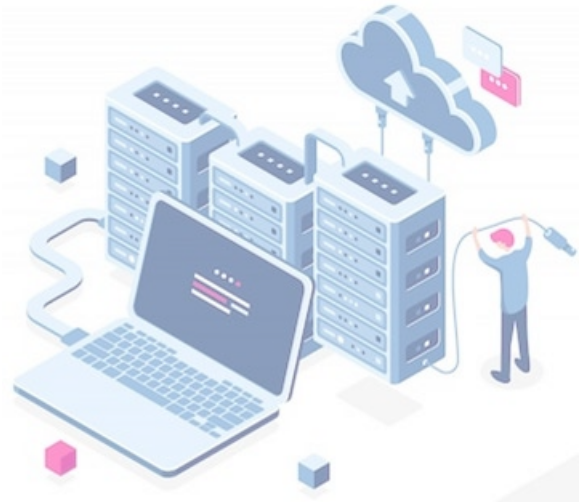
- **採納實體存取控制措施**來限制處所、房間和資訊設施的進出及使用
- **使用保安裝置或軟件**（如防火牆或防毒程式）來保護電腦網絡，並**定期更新軟件**來偵測新威脅
- **使用端點保安軟件**以防止用戶在網絡執行未獲授權的、並會對網絡帶來風險的應用程式或操作
- 定期對網絡、伺服器等**進行漏洞掃瞄**，並適當跟進
- **記錄系統活動**，以用於偵測和調查資料保安事故

資訊及通訊科技的資料保安建議措施

3) 技術上及操作上的保安措施 *資料庫管理*

資料使用者應:

- **利用防火牆將資料庫伺服器與網絡伺服器分開**，以在網絡伺服器受到威脅時保護內部伺服器
- **備存並定期更新個人資料清單**，以便實施適當的保安措施
- **資料集的分區** — 根據資料既定的屬性（如敏感屬性）將資料集分割成更小的子集（故即使主要資料庫的資料遭洩露，被分割的資料也不會受到影響）
- **數碼水印** — 在資料上添加水印，例如能夠識別資料集的始發者和證明檔案真實性的加密電子簽署
- 禁止使用真實的資料進行測試



資訊及通訊科技的資料保安建議措施

3) 技術上及操作上的保安措施 *存取管控 (非詳盡)*

資料使用者應:

- **採取「最小權限」原則**，授予用戶盡可能少的存取權限
- **實施密碼管理以管理用戶密碼**，包括強制密碼長度、複雜性和歷史紀錄
- **制訂帳戶鎖定閾值策略**來限制資訊及通訊系統**允許登入失敗的次數**，並在達到次數上限時封鎖帳戶一段特定的時間
- **對高風險的活動**（如遙距登入系統／存取敏感資料庫）**實施多重身份驗證**或更高程度的存取管控
- **定期覆檢存取權限**並適時刪除不必要的帳戶和存取權限（例如在職員離職或重新調配職位時）

資訊及通訊科技的資料保安建議措施

3) 技術上及操作上的保安措施 *防火牆和反惡意軟件*

資料使用者應:

- **使用域名系統（DNS）防火牆**，防止資訊及通訊系統或其用戶連接到惡意網站
- 定期對系統**進行保安漏洞評估及滲透測試**
- **使用反惡意程式軟件**為系統提供實時保護

保護網絡應用程式

- 避免於線上存儲不必要的個人資料
- 當含有個人資料的系統已過時，將它們的**網絡連接切斷**。

資訊及通訊科技的資料保安建議措施

3) 技術上及操作上的保安措施 *加密*

資料使用者應:

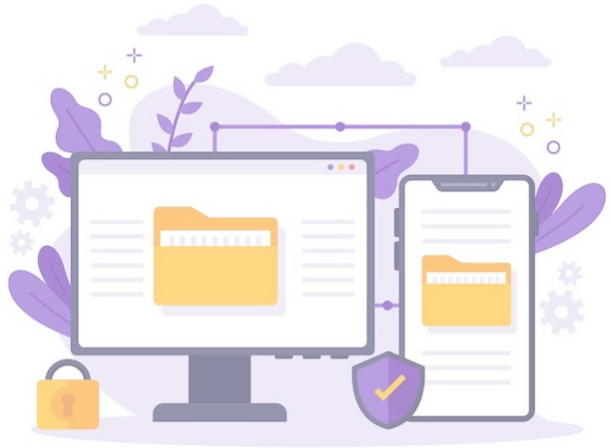
- **正確地加密**傳輸中和存儲中的資料，並有效地管理和保護加密密鑰
- 為**流動裝置**（例如智能電話）及**便攜式儲存裝置**（例如USB記憶體 及外置硬碟）的資料進行加密
- **代號化** — 將識別符及屬性轉換成只有已獲授權的用戶才能理解的數值（這適用於以後需要使用實際值的資料字段，例如個人的姓名）
- **雜湊資料** — 使用算法得出的數值來取代敏感數值，這適用於毋須恢復實際值的資料字段，例如密碼（雜湊與一般加密不同，經雜湊的資料**無法通過解密還原成原始資料**）

資訊及通訊科技的資料保安建議措施

3) 技術上及操作上的保安措施 *電郵及檔案傳送*

資料使用者應:

- **以密件副本功能（bcc / blind carbon copy）而非副本功能（cc / carbon copy）**發出電郵，使收件者的資料（電郵地址或姓名）不會被其他收件者看見
- **安裝工具**（例如資料外洩預防工具）確保任何可能屬高風險（例如有敏感資料）的郵件在發送之前已被仔細檢查
- 過濾濫發的、帶有惡意附件或鏈結的電郵
- **使用端點保安軟件**防止資料從資料使用者的電腦轉移到未獲批准使用或不設加密功能保障的便攜式儲存裝置上
- **為載有敏感個人資料的檔案添加數碼水印**，以防止資料喪失、被不當使用及未經授權地分享



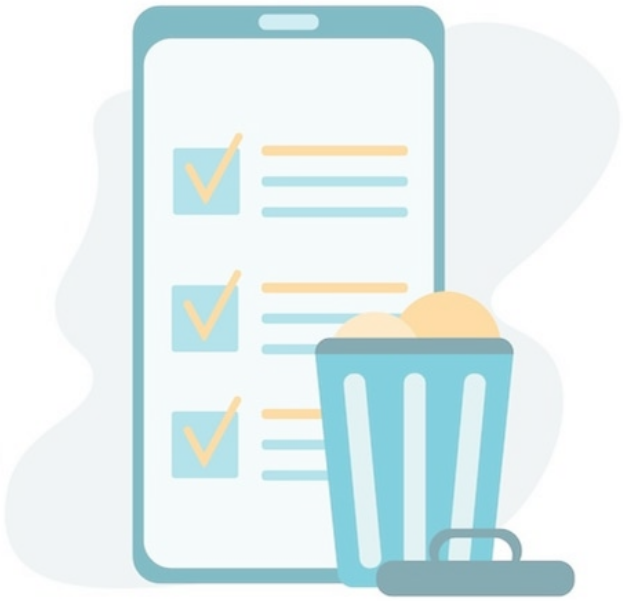
資訊及通訊科技的資料保安建議措施

3) 技術上及操作上的保安措施 *資料備份、銷毀及匿名化*

資料使用者應:

- **備份含有必要資料的系統**，並且**確保恢復機制**能有效地恢復失去的或因惡意/勒索軟件而無法存取的資料
- **適時地銷毀或匿名化**不必要的或過期的個人資料

➢ *為安全地刪除資料，可以採用 NIST 800-88 R1 (Guidelines for Media Sanitization) 的清除操作（當中技術令資料被清除後，即使採用先進的實驗室技術也無法恢復）*



資訊及通訊科技的資料保安建議措施

NOTE

根據《私隱條例》第65(2)條，資料使用者有可能需對其代理人（包括資料處理者）的有關行為負責

有關管理資料處理者的更多資訊，可參閱私隱公署的《外判個人資料的處理予資料處理者》資料單張

4) 資料處理者的管理 *(非詳盡)*

資料使用者在聘用資料處理者時可考慮:

- 實施政策及程序確保**只聘用稱職且可靠**的資料處理者
- 進行評估**確保只有必要的個人資料轉移**至資料處理者
- 於合同**明確規定**資料處理者須採取的**保安措施**
- 要求資料處理者在發生資料保安事故時**立即作出通知**
- **進行現場審核**以確保資料處理者遵守資料處理合同

資訊及通訊科技的資料保安建議措施

5) 資料保安事故發生後的補救措施

資料使用者在資料保安事故發生時可採取的補救措施:

- 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

NOTE

資料使用者亦應從資料保安事故中汲取經驗及教訓，覆檢和加強其整體資料治理和資料保安措施。

有關如何處理資料外洩的詳細指引，可參閱私隱公署發出的《資料外洩事故的處理及通報指引》

資訊及通訊科技的資料保安建議措施

NOTE

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

6) 監察、評估及改善

資料使用者可委派獨立的專責小組（如內部或外部審計隊），並負責:

- 定期**監察**資料保安政策的**遵從情況**
- 定期**評估**資料保安措施的**成效**

資訊及通訊科技的資料保安建議措施

7) 其他考慮 — *雲端服務*

資料使用者在使用雲端服務時應:

- **評估**雲端服務供應商的**能力**，要求他們為雲端環境的保安管控**提供正式的保證**
- 於雲端環境**設立穩固的查閱管控和認證程序**，例如嚴格的密碼政策、多重身份驗證、妥善的紀錄保存，以及定期覆檢存取權限
- **檢視雲端的現有保安功能**，並啟用合適的保安功能，而非依賴預設的保安設置

自攜裝置

實施自攜裝置政策的資料使用者可考慮:

- **避免儲存**個人資料
- **容許遙距刪除**資料
- **控制**個人資料的**存取**
- 為個人資料**進行加密**

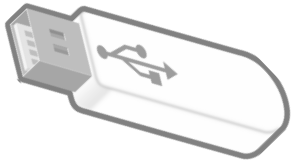
有關自攜裝置的更多資訊，可參閱私隱公署發出的資料單張《自攜裝置(BYOD)》

資訊及通訊科技的資料保安建議措施

7) 其他考慮 *便攜式儲存裝置*

如有必要使用便攜式儲存裝置，資料使用者應考慮:

- 在政策中列明可使用便攜式儲存裝置的情況
- 使用端點保安軟件
- 保存便攜式儲存裝置的清單並進行追蹤
- 在使用後刪除便攜式儲存裝置中的資料



NOTE

由於可以簡單且快速地複製和轉移大量個人資料至公司系統以外的地方，便攜裝置因此會增加資料保安事故的風險

有關使用便攜式儲存裝置的詳細指引，請參閱私隱公署發出的《使用便攜式儲存裝置指引》

謝謝!

下載《資訊及通訊科技的保安措施指引》