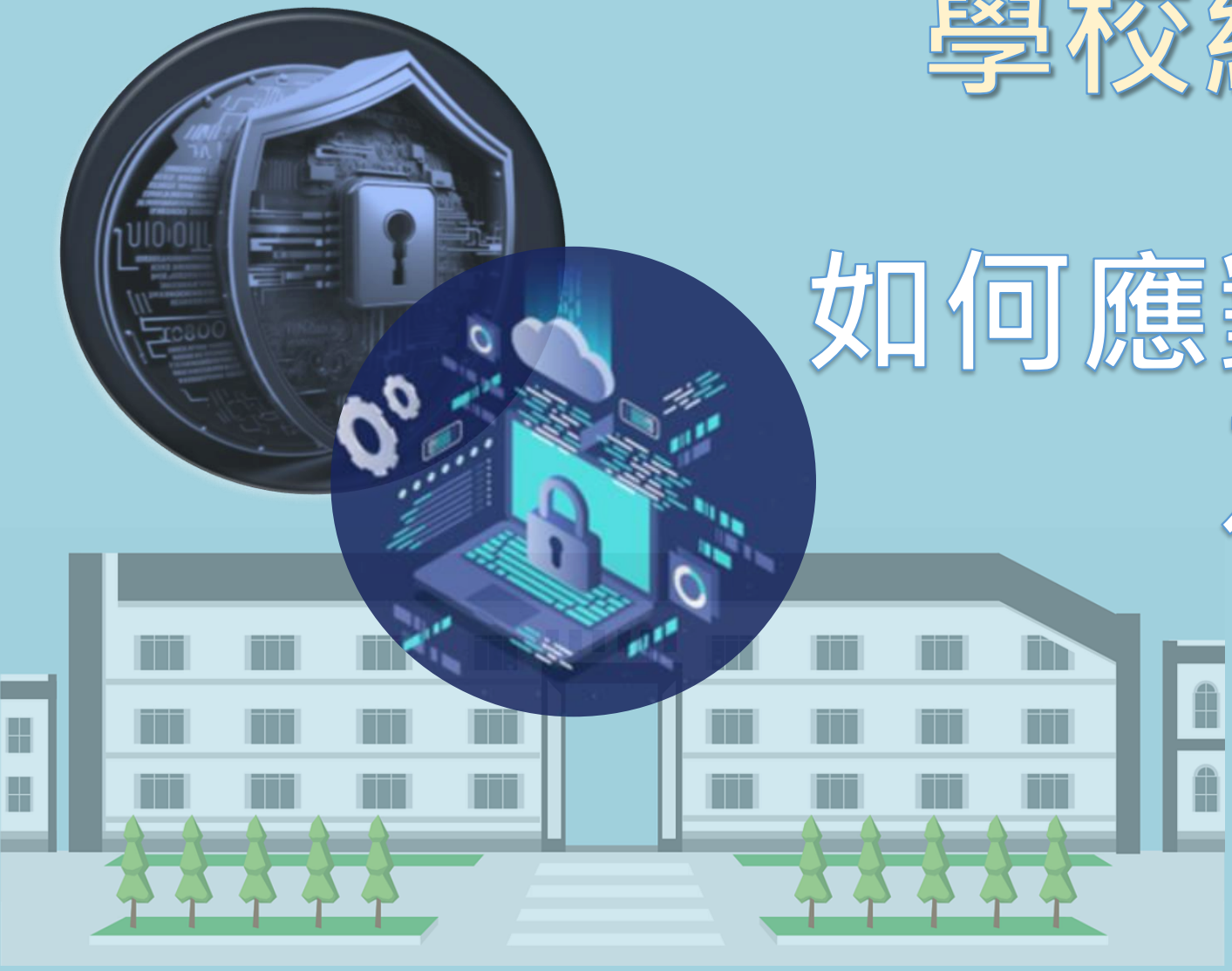
學校網絡安全研討會



如何應對資料外洩事故及提升數據安全

文靄怡女士
署理高級個人資料主任
（合規及查詢）

2024年6月29日

資料外洩事故

甚麼是資料外洩事故?

一般指**資料使用者**持有的個人資料懷疑或已經遭到外洩，令有關資料當事人的個人資料有被**未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險**

例子

- **遺失**載有個人資料的文件或便攜式裝置
- **資訊系統配置錯誤**
- 載有個人資料的資訊**系統被非法侵入**或**被未經授權的第三方查閱**
- **經郵件或電郵錯誤發送個人資料**
- 第三方以**欺騙手法**從資料使用者取得個人資料
- 在電腦**安裝檔案分享軟件**而導致資料外洩

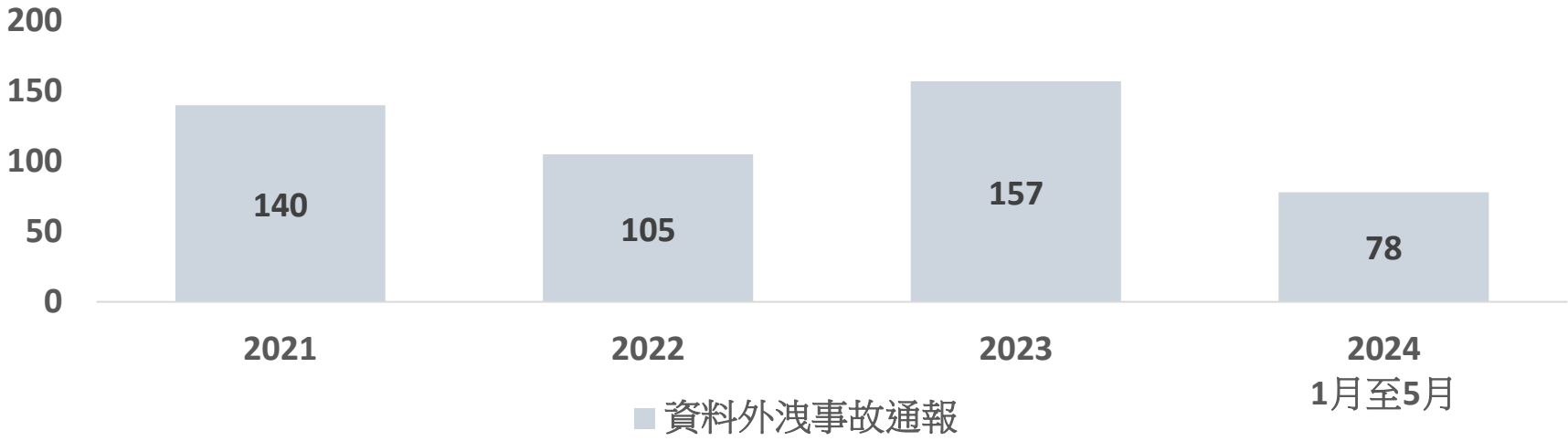
資料外洩事故

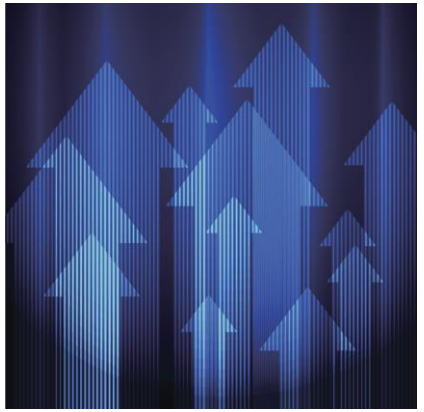
主要技術風險

- 網絡釣魚
- 未修補保安漏洞
- 低強度密碼
- 過時的操作系統和應用程式
- 植入惡意軟件

公署接獲的資料外洩事故通報

- 私隱專員公署於2023年共接獲157宗資料外洩事故通報，比2022年的105宗上升近五成：





- 公署於2024年首5個月共接獲78宗資料外洩事故通報，已達2023年全年資料外洩事故通報數字的一半。
- 涉及黑客入侵的資料外洩事故由2022年的29宗（佔2022年資料外洩事故的28%），大幅增加逾一倍至2023年的64宗（佔2023年資料外洩事故的41%，當中包括即時通訊軟件被騎劫個案）。在2024年首5個月，涉及黑客入侵的資料外洩事故亦佔整體資料外洩事故近三成。

《私隱條例》的相關規定

資料外洩事故可構成違反《私隱條例》 附表1的保障資料第4原則

保障資料第4(1)原則

資料使用者須**採取所有切實可行的步驟**，確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響

保障資料第4(2)原則

如資料使用者聘用（不論是在香港或香港以外聘用）**資料處理者**，以代該資料使用者處理個人資料，該資料使用者須採取**合約規範方法**或其他方法，以防止轉移予該資料處理者作處理的個人資料被未獲准許或意外地被查閱、處理、刪除、喪失或使用

個案分享

個案分享（1）
因密碼管理欠佳導致學生和家長的個人資料未獲授權查閱

一間教育機構的資訊管理系統遭黑客利用暴力攻擊獲取了管理員密碼，並建立了具有管理權限的新帳戶，以查閱當中的個人資料。事件影響超過24,000名家長及學生用戶的個人資料。調查後發現是次事故源於密碼管理欠佳，未有採取行業最佳做法保護管理員帳戶所致。

補救措施

該機構為其資訊管理系統採用雙重認證功能為系統帳戶提供額外的保護、設定高強度密碼、定期清理不必要的帳戶，以及透過加強培訓提高員工的資料保障意識。

個案分享（1）
因密碼管理欠佳導致學生和家長的個人資料未獲授權查閱

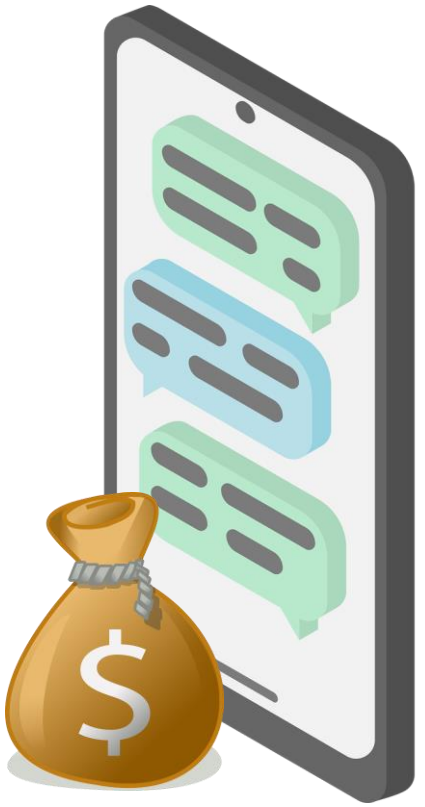
- 當教育機構利用資訊科技帶來方便的同時，不應忽視隨之而來的私隱風險，特別是關乎兒童及青少年的個人資料。

- 機構管理個人資料系統需加強警惕，制定適當的系統安全政策、措施和程序（例如善用多重認證功能及採用合適的密碼管理政策），以減低個人資料遭未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險。

借鑑

個案分享（2）
學校的即時通訊軟件帳戶遭騎劫

- 一所學校獲悉有家長收到由該校的即時通訊軟件發出要求轉賬的訊息，因而懷疑該帳戶遭騎劫。
- 事件共涉及約370名人士的個人資料，包括學生姓名及其家長的電話號碼，以及教職員的姓名和電話號碼，其中部分學生及教職員已離校。



個案分享（2）
學校的即時通訊軟件帳戶遭騎劫

1. 為所有即時通訊軟件帳戶啟用雙重認證功能；
2. 就使用即時通訊軟件制訂指引，並於教職員入職時及每年向所有教職員傳閱，以加強教職員保障個人資料私隱的意識；及
3. 從該手提電話刪除已離校學生、家長及教職員的個人資料，並承諾定期檢視及適時刪除即時通訊軟件內儲存的通訊資料。

補救措施

個案分享（2）
學校的即時通訊軟件帳戶遭騎劫

- 即時通訊軟件為通訊帶來便利，但機構須小心因即時通訊軟件帳戶遭騎劫及盜用而引致的騙案。
- 機構應定期向員工提供資訊科技安全培訓，指導員工正確使用即時通訊軟件和保障帳戶安全的方法，包括啟用相關雙重認證功能，定期檢查已連結的裝置，登出不再使用或不明的裝置連結及提醒員工使用即時通訊網頁版時須留意網頁連結。
- 機構亦應制訂資料保留期限，確保適時刪除不再需要的個人資料。

借鑑

個案分享（3）
一間公司的電郵系統遭入侵

- 一間公司的六個員工電郵帳戶遭黑客入侵，導致客戶發送至該些電郵帳戶的電郵被轉發至兩個不明的電郵地址。該事件涉及超過1,600名客戶的個人資料，當中包括姓名、職稱、電郵地址、公司名稱、電話號碼及信用卡資料。

調查結果發現該公司的四項缺失：

1. 薄弱的密碼管理
2. 保留已過時的電郵帳戶
3. 電郵系統欠缺針對遠端存取的保安措施
4. 欠缺針對資訊系統的保安措施

個案分享（3）
一間公司的電郵系統遭入侵

執行通知

- ✓ 修訂資訊保安政策，加入並詳細說明強密碼管理政策、定期刪除已過期或不再使用的電郵帳戶機制，及訂立系統以定時監察及審核（包括內部審核）電郵帳戶的使用情況
- ✓ 制訂有效措施以確保員工依循已修訂的資訊保安政策
- ✓ 聘請獨立的資料保安專家對公司的系統保安，包括電郵系統進行定期檢視及審核
- ✓ 為員工制訂最新的資訊保安培訓，並妥善記錄培訓進度，以及對培訓的參與及有效程度作出評估

個案分享（3）
一間公司的電郵系統遭入侵

- 設有客戶個人資料電郵系統的機構需加強警惕，以防止網絡攻擊影響其電郵系統。
- 機構應制訂適當的系統安全政策、措施和程序，並涵蓋以下領域：
  1. 設立個人資料私隱管理系統
  2. 委任保障資料主任
  3. 訂定電郵通訊政策
  4. 制定足夠保安措施
  5. 培養工作場所的私隱友善文化

借鑑

如何處理資料外洩事故

資料外洩事故應變計劃

載列機構一旦發生資料外洩時會**如何應對的文件**

有助機構快速應對及有效管理事故

資料外洩事故應變計劃應：

① 概述發生事故後**須執行的程序**

② 資料使用者由事故開始到完結就**識別**、**遏止**、**評估**以至**管理**事故所帶來的影響的策略

資料外洩事故應變計劃

計劃涵蓋範疇（非詳盡）

- 描述構成資料外洩事故的要素
- 內部事故通報程序
- 指明專責應變小組成員的角色及責任
- 聯絡名單
- 風險評估工作流程
- 遏止策略
- 通訊計劃
- 調查程序
- 保存紀錄的政策
- 事後檢討機制
- 培訓或演習

如何處理資料外洩事故

步驟

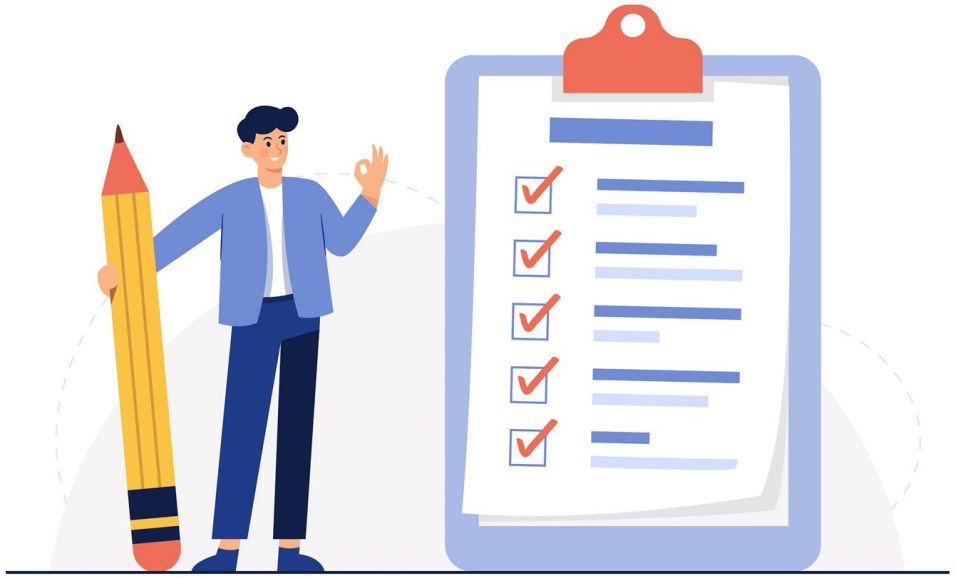
1. 立即收集重要資料
2. 遏止事件擴大
3. 評估事件可造成的損害
4. 考慮作出資料外洩通報
5. 記錄事故

下載《資料外洩事故的處理及通報指引》

步驟 1：立即收集重要資料

收集事故的所有相關資料，以評估對資料當事人的影響及找出適當的緩和措施：—

- 事故於**何時**發生及在**哪裏**發生？
- 事故**如何被發現**及由**誰人發現**？
- 導致事故的**原因**是甚麼？
- 涉及**甚麼種類**的個人資料？
- **有多少個**可能受影響的資料當事人？
- 可能對受影響人士造成甚麼**傷害**？



步驟 2：遏止事件擴大

視乎所涉及個人資料的類別及事故的嚴重性，考慮採取以下的遏止措施：

- **徹底搜尋**載有個人資料的遺失物品
- 要求錯誤接收有關電郵 / 信件 / 傳真的人士**銷毀或交回誤發的文件**
- **關閉或隔離**受損 / 遭破壞的系統 / 伺服器
- **修復**導致事故的**漏洞或錯誤**
- **更改用戶密碼及系統配置**
- **移除**涉嫌造成或引致資料外洩的**用戶的查閱權**
- 如已發生或可能發生身份盜竊或其他犯罪活動，應通知有關執法部門

步驟 3：評估事件可造成的損害

資料外洩事故可導致的損害：

- 人身安全受到威脅
- 身份盜竊
- 財務損失
- 受辱或喪失尊嚴、名譽或關係受損
- 失去生意或聘用機會

傷害程度取決於不同情況，例如:

- 外洩個人資料的**種類**、**敏感程度**及**數量**
- 資料外洩的情況
- 傷害的性質
- **身份盜竊**或**詐騙**的可能性
- 遺失的資料**有否備份**
- 外洩資料有否進行足夠的**加密**、**匿名化**或其他保障措施
- 資料外洩**持續的時間**

步驟 4：考慮作出資料外洩通報

資料使用者在決定是否把事故通知受影響資料當事人、私隱專員公署及其他執法部門時，應考慮：

- 事故可能對受影響人士造成的影響
- 影響有多嚴重或重大
- 發生的可能性
- 不作出通知的後果

如資料外洩事故相當可能對受影響資料當事人有構成實質傷害的風險，資料使用者應在知道發生資料外洩後在切實可行的情況下盡快通知**私隱專員公署**及**受影響資料當事人**。

步驟 4：考慮作出資料外洩通報

如何通報？

通知資料當事人

- 透過電話、書面、電郵或親身向資料當事人作出通報
- 如直接的資料外洩通報不切實可行，可發出公告、報章廣告，或於網站或社交媒體平台發出帖文

通知私隱專員公署

- 經私隱專員公署**網頁**、傳真、親身或郵寄方式遞交「**資料外洩事故通報表格**」
- **不接受口頭通報**

NOTE

不論資料使用者有否作出通報，公署可就資料外洩事故展開調查。

資料外洩事故通報表格

資料外洩事故一般指資料使用者持有的個人資料外洩，令此等資料承受未獲准許的或意外的查閱、處理、刪除、遺失或使用的風險。視乎個案的情況而定，資料外洩事故可構成違反《個人資料（私隱）條例》（《私隱條例》）的保障資料第 4 原則。

雖然《私隱條例》沒有規定資料使用者必須就資料外洩事故作出通報，但個人資料私隱專員公署（私隱公署）建議資料使用者在資料外洩發生後盡快向私隱公署、受影響資料當事人及相關機構作出通報。

資料使用者可使用此通報表格向私隱公署通報資料外洩事故，需時大約 10-15 分鐘。你可參考私隱公署的「處理資料外洩事故的實務建議」（見附錄）以獲取更多資訊。

收集個人資料聲明

請注意，你可自願向私隱公署提供你的個人資料。你提供的所有個人資料只會用於與是次資料外洩事故通報及個人資料私隱專員行使規管權力及職能直接有關的用途。

你有權要求查閱及改正私隱公署所持有你的個人資料。查閱或改正該等資料，可用書面向保障資料主任提出，地址為香港灣仔皇后大道東 248 號大新金融中心 12 樓。

你所提供的個人資料可能轉移給私隱公署因處理本個案而接觸的人士或機構，包括獲授權收取有關資料以作出執法或起訴行動的人士或機構。

❑ 本人明白上述內容，並代表資料使用者提交資料外洩事故通報。*

*必須填寫　*請圈出適用者

資料使用者的基本資料

資料使用者機構：❑ 私營機構　❑ 公營機構

公司／機構名稱*：

香港辦事處的聯絡地址：

聯絡人資料

作出此通報的人士的姓名*：

職位：　電郵地址*：

國家編號（非香港電話號碼）：

聯絡電話號碼*：

你是否你所屬公司／機構的資料保障主任？* 是／否

1

公署的「資料外洩事故通報表格」

步驟 5：記錄事故

- 資料使用者必須**完整地記錄事故**，包括事故的**詳情**、**影響**，**資料使用者所採取的遏止措施和補救行動**
- 機構如須依從其他司法管轄區的法例及規例，亦應留意有關法例及規例下的**強制記錄要求**
- **檢討資料外洩事故，從中汲取教訓，改善其處理個人資料的做法。**

NOTE

例如歐洲聯盟的《通用數據保障條例》規定資料控制者記錄所有資料外洩事故並保存有關紀錄

資料保安建議措施

《資訊及通訊科技的保安措施指引》

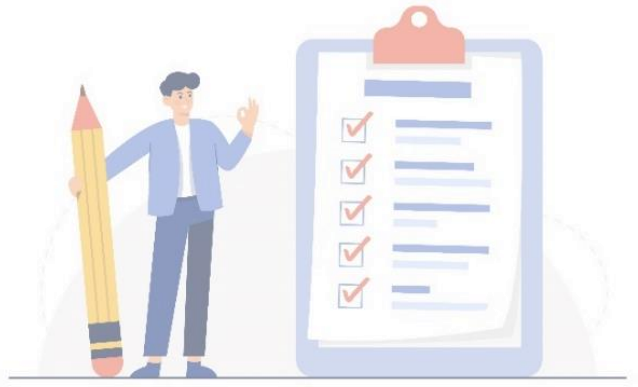
1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

下載《資訊及通訊科技的保安措施指引》

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

- 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**
- 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及制訂指引
- 工作人員應在入職時及往後**定期接受足夠培訓**



NOTE

資料使用者應根據當時情況（如行業內的新標準、資料保安新威脅等），定期和及時地覆檢與修訂政策及程序，並機構可考慮將「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）

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
- 資料庫管理
- 存取管控
- 電郵及檔案傳送
- 防火牆和反惡意軟件
- 保護網絡應用程式
- 加密
- 資料備份、銷毀及匿名化

資訊及通訊科技的資料保安建議措施

4) 資料處理者的管理

NOTE

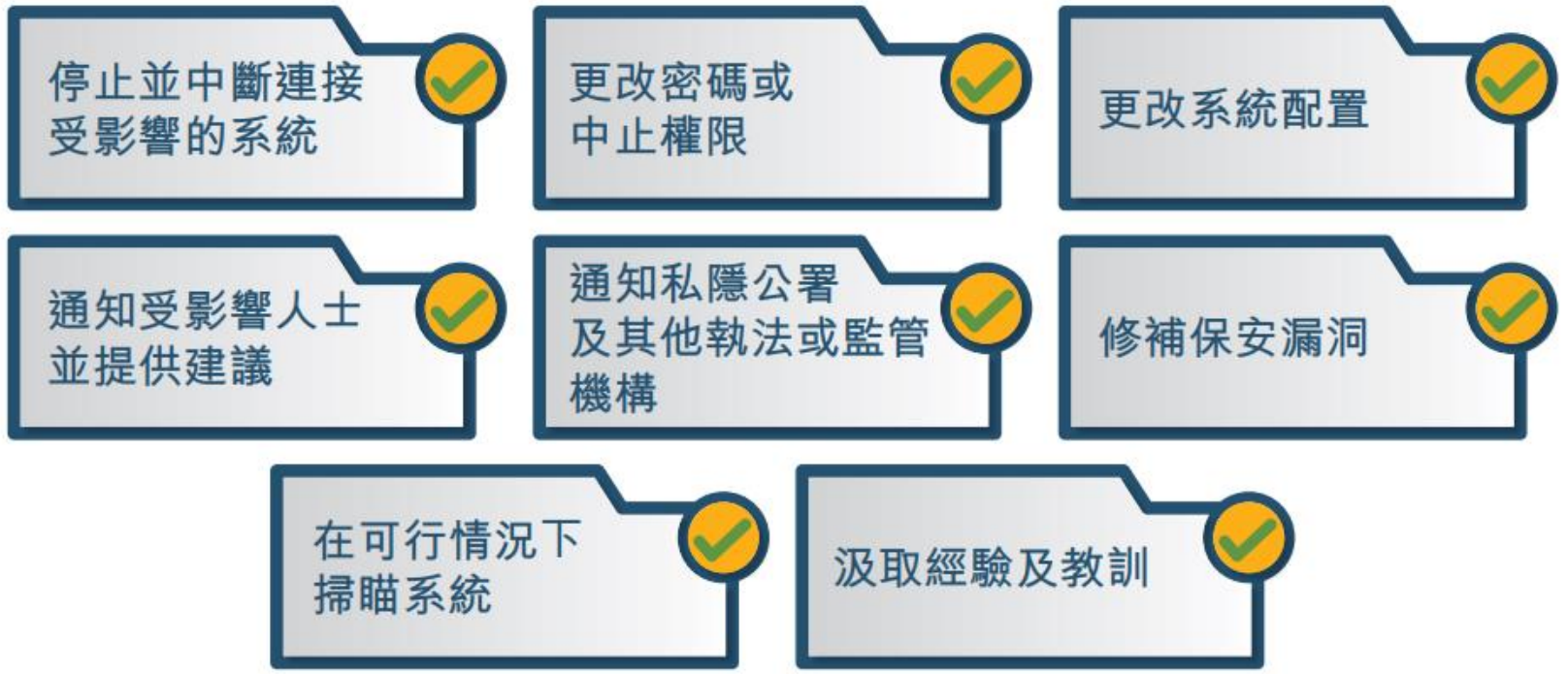
根據《私隱條例》第65(2)條，資料使用者有可能需對其代理人（包括資料處理者）的有關行為負責

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

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:



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

雲端服務及自攜裝置

雲端服務

- 檢視雲端的現有保安功能及評估雲端服務供應商的能力
- 設立穩固的查閱管控和認證程序

自攜裝置

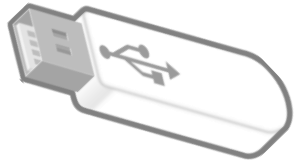
- 控制對儲存在自攜裝置設備內的個人資料的存取
- 使用並非自攜裝置設備內建的加密方法及安裝適合的軟件

便攜式儲存裝置

如有必要使用便攜式儲存裝置，應：

- 制訂政策
- 使用端點保安軟件
- 保存便攜式儲存裝置的清單使用
- 使用後妥善地刪除便攜式儲存裝置的資料

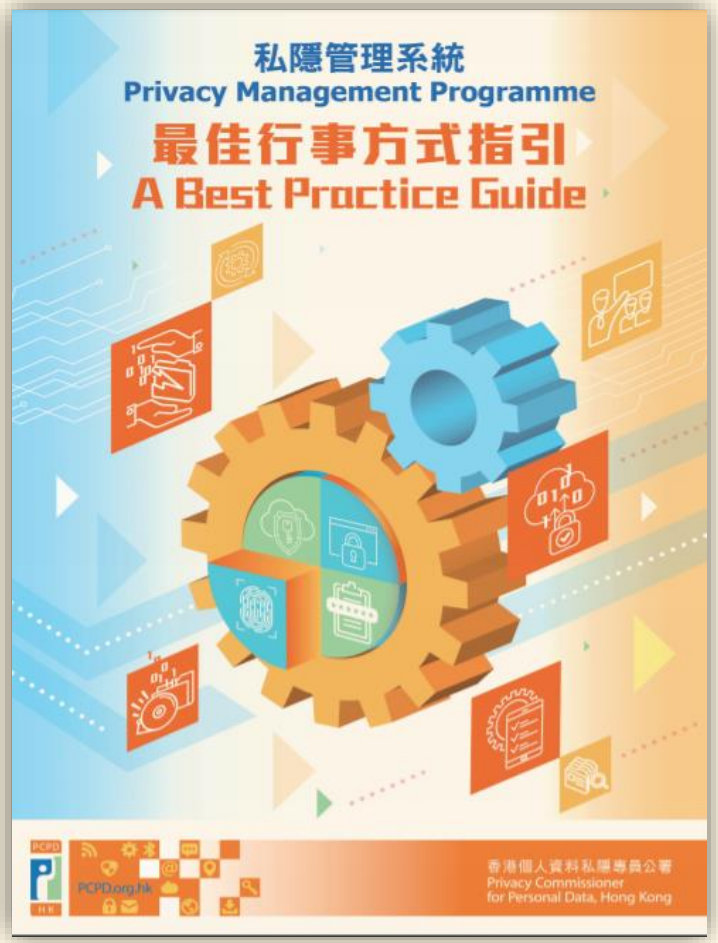
有關使用便攜式儲存裝置的詳細指引，請參閱私隱公署發出的《使用便攜式儲存裝置指引》



私隱管理系統

私隱管理系統

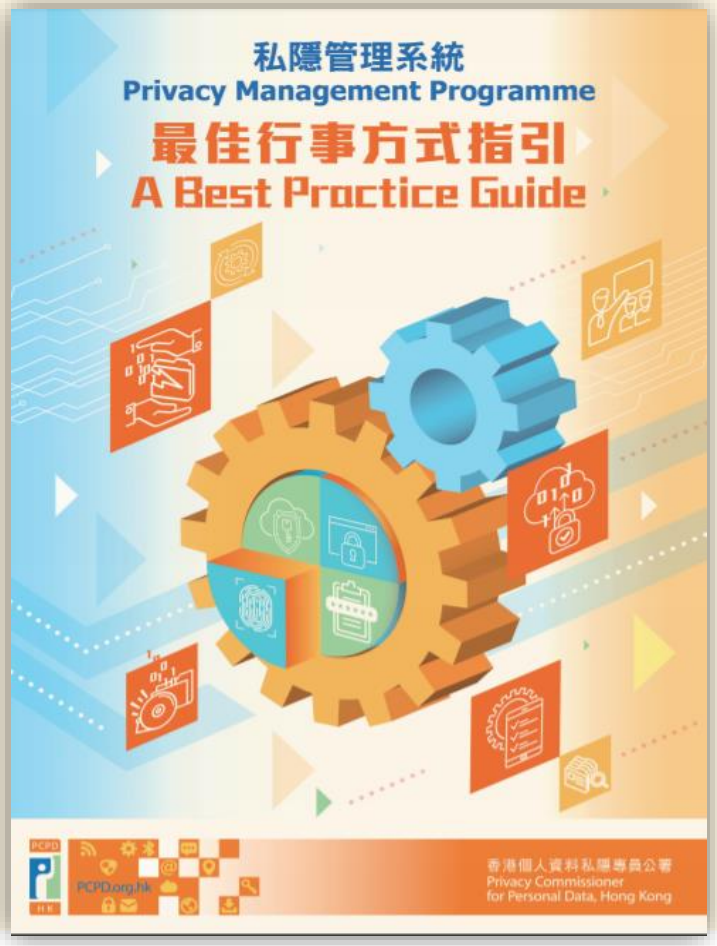
建立私隱管理系統，由最高管理層做起，將個人資料保障視為其企業管治責任，並將之納入處理業務中不可或缺的一環，由上而下貫徹地在機構中執行有關保障個人資料的政策。



下載《私隱管理系統最佳行事方式指引》

私隱管理系統

- **私隱管理系統的主要部分：**
  - **機構的決心：**最高管理層的支持、委任保障資料主任 / 設立部門及建立匯報機制
  - **系統管控措施：**建立個人資料庫存、處理個人資料的內部政策、培訓及教育推廣等
  - **持續評估及修訂：**制訂監督及檢討計劃、評估及修訂系統管控措施



下載《私隱管理系統最佳行事方式指引》

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

其他資訊科技相關指引及資料單張

- 人工智能 (AI): 個人資料保障模範框架
- 開發及使用人工智能道德標準指引 – 指引資料
- 保障個人資料私隱 – 使用社交媒體及即時通訊軟件的指引
- 資訊及通訊科技系統的貫徹數據保障設計指引
- 經互聯網收集及使用個人資料：以兒童為對象的資料使用者注意事項
- 開發流動應用程式最佳行事方式指引
- 使用便攜式儲存裝置指引
- 經互聯網收集及使用個人資料：給資料使用者的指引
- 個人資料的刪除與匿名化指引

PCPD.org.hk

PCPD HK

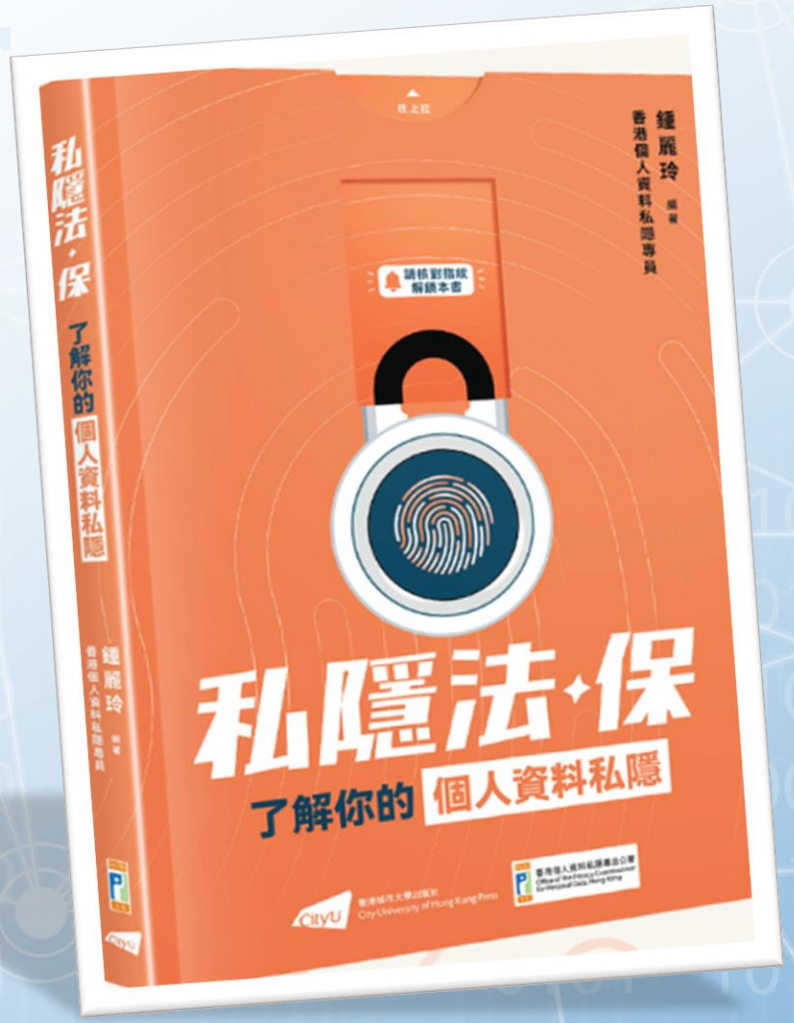
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

數據安全熱線
Data Security Hotline
2110 1155

數據安全快測
Data Security Scanner
https://www.pcpd.org.hk/Toolkit/tc/

數據安全專題網頁
Data Security Webpage
https://www.pcpd.org.hk/tc_chi/data_security/index.html

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



編著：
鍾麗玲
私隱專員

訂購表格

謝謝！Thank you!