香港社會服務聯會
資料外洩事故的處理及通報指引
研討會及分享會

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12月17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**載有個人資料的可攜式裝置
- **不當處理**個人資料
- 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

資料外洩的常見原因

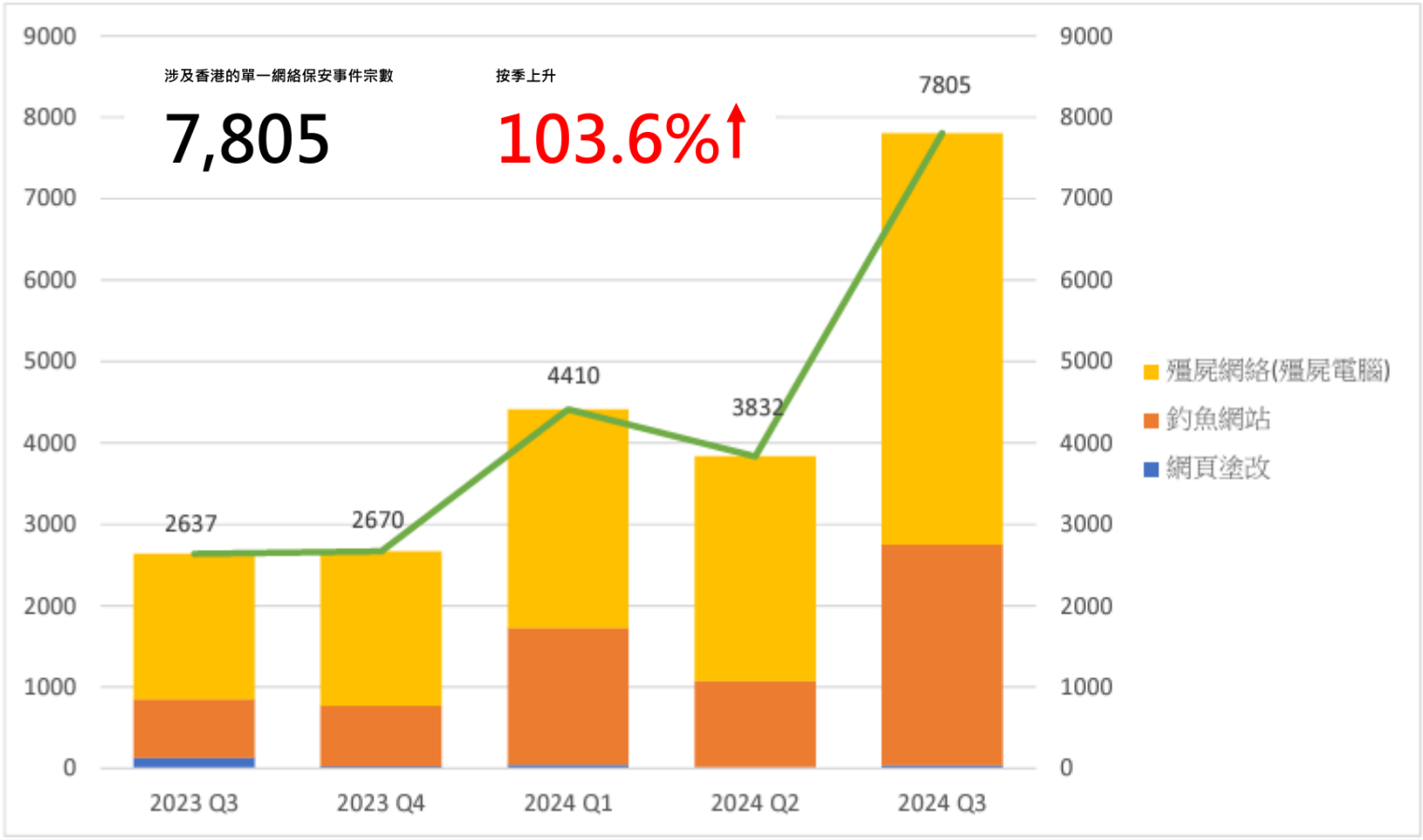
主要技術風險

- 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

網絡安全風險與日俱增

全球趨勢

- 電訊公司Verizon的2023資料外洩調查報告顯示於2013至2022年間，資料外洩事故大幅增加逾三倍
- 市場調查公司Forrester 2023年的研究顯示77%的受訪機構表示於過去一年曾遭受至少一次網絡攻擊



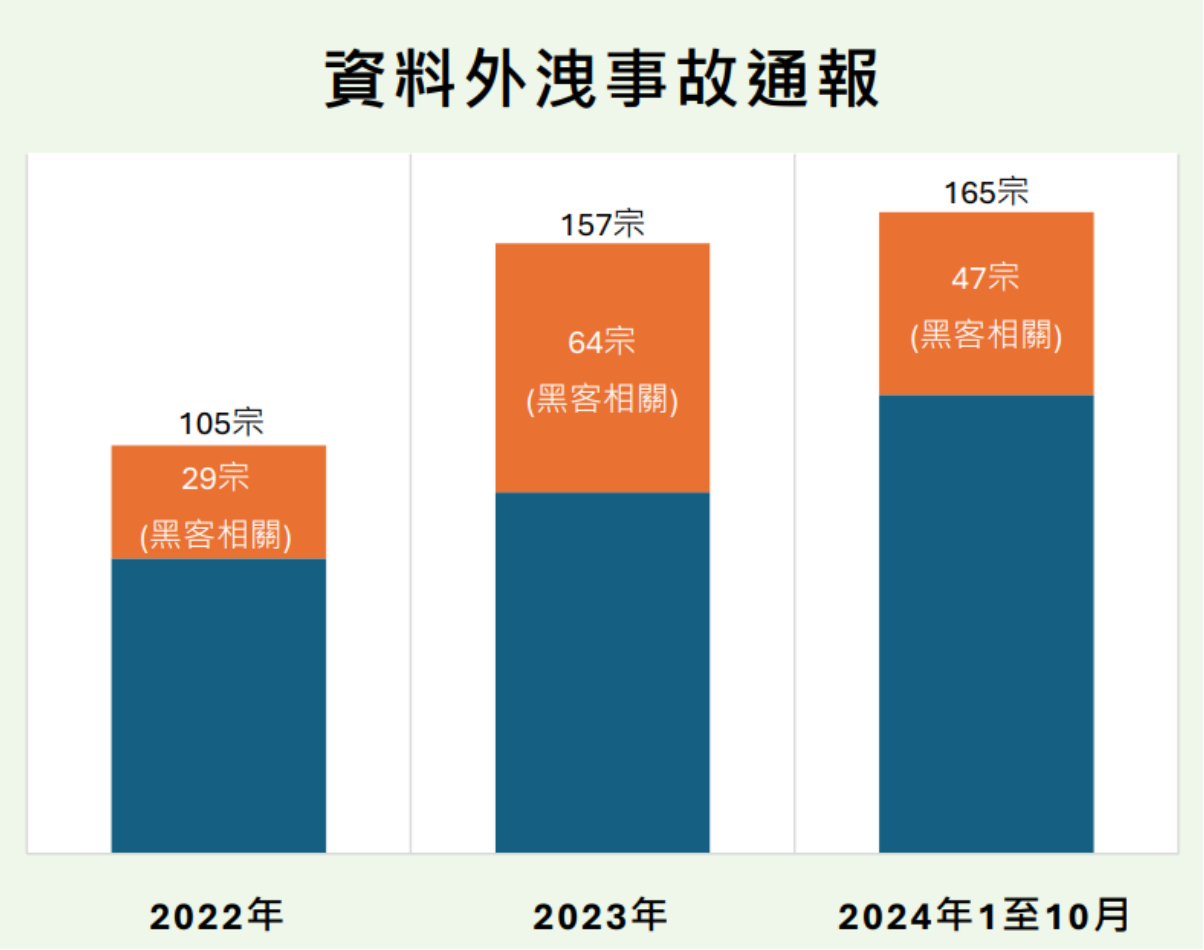
本港趨勢

根據《香港保安觀察報告》[1]，2024年第三季度涉及香港的網絡保安事件宗數比上季上升103.6%，比去年同季更上升196%

殭屍網絡（佔整體案例64.7%）是本地網絡保安事故的主要原因；其次為釣魚網站（佔整體案例34.7%）

[1]《香港保安觀察報告》（2024年第三季）：https://www.hkcert.org/f/report/912892/916161/2024Q3%20HK%20SecurityWatchReport%20(Chinese).pdf

公署接獲的資料外洩事故通報



- 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10個月已接獲165宗通報，接近2023年全年總宗數約105%
- 於2023年涉及黑客入侵的資料外洩事故共64宗（佔全年事故的41%），比2022年的29宗（佔全年事故的28%），大幅增加逾一倍
- 於2024年首10個月，涉及黑客入侵的資料外洩事故共47宗

《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）– 醫療集團的醫療紀錄遭意外棄置

- 一間醫療集團向私隱專員公署作出資料外洩通報，表示旗下一間醫務中心意外棄置了一個載有病人醫療紀錄的紙箱。集團表示，一名清潔員工錯誤地將載有病人醫療紀錄的紙箱當作廢物處理並棄置。
- 涉及接近300名病人的個人資料，包括他們的姓名、電話號碼、香港身份證號碼、地址、出生日期、診斷紀錄、使用藥物紀錄及實驗室結果等。

調查結果發現三項缺失：

1. 員工的個人資料保障意識欠奉
2. 欠缺有效的政策及程序
3. 欠缺員工培訓

個案分享（1）– 醫療集團的醫療紀錄遭意外棄置

執行通知

- 對有關個人資料保障方面的所有書面政策、標準操作程序 / 指引進行全面檢視及更新，以提供具體的政策及操作程序 / 指引
- 制訂有效措施，以確保員工依循更新後的有關個人資料保障的書面政策、標準操作程序 / 指引
- 制訂有效措施，監督員工及任何負責在醫務中心執行清潔工作的第三方遵守清潔守則的規定
- 為員工提供個人資料保障方面的培訓，並妥善記錄培訓進度，以及就員工培訓的參與及有效程度作出評估

個案分享（2）
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。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（2）
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
- 為員工制定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）
一間公司的資訊系統遭勒索軟件攻擊

- 一間公司的電腦系統及檔案伺服器遭受到勒索軟件攻擊及惡意加密。黑客組織要求公司支付贖金，為已被加密的檔案解鎖。

涉及超過13,000名受影響人士，當中約四成受影響人士為求職者及已離職僱員。受影響的個人資料包括姓名、身份證號碼及／或副本、護照號碼及／或聯絡資料，以及部分人士的財務資料、健康資料、照片、出生日期、僱傭資料、社交媒體帳戶資料及／或學歷資料及屬數名人士的信用卡資料等。

個案分享（3）
一間公司的資訊系統遭勒索軟件攻擊

調查結果發現五項缺失：

1. 資訊系統欠缺有效的偵測措施
2. 沒有為遠端存取資料啟用多重認證功能
3. 對資訊系統進行的保安審計不足
4. 資訊保安政策有欠具體
5. 個人資料被不必要地保留

個案分享（3）
一間公司的資訊系統遭勒索軟件攻擊

執行通知

- 徹底檢視載有個人資料的資訊系統的安全及其保安措施，確保該些系統沒有已知的惡意軟件及保安漏洞，以及具備有效的偵測措施
- 為所有會存取載有個人資料的資訊系統的遙距使用者實施多重身分認證，並定期檢視遙距存取的權限
- 聘請獨立的資訊保安專家對資訊系統進行最少每年一次的風險評估及保安審計
- 制訂清晰及全面的資料系統保安政策及程序，涵蓋防範、偵測及應對網絡攻擊的各種管控措施，及進行風險評估及保安審計的要求
- 從資訊系統銷毀所有逾期保留的個人資料
- 制訂清晰的資料保留政策，訂明每個系統內個人資料的保留期限，及制訂刪除已屆保留期限的個人資料的執行細節
- 制訂並實施有效措施以確保員工遵循上述資訊系統保安政策及程序，以及資料保留政策

個案分享（4）
學會的伺服器遭勒索軟件攻擊

- 一間學會向私隱專員公署作出資料外洩通報，表示學會名下六台載有個人資料的伺服器遭勒索軟件攻擊及惡意加密，黑客威脅學會將該些伺服器內的檔案上載至互聯網，並要求學會支付贖金，為已被加密的檔案解鎖。

涉及超過13,000名會員及約10萬名非會員的個人資料，當中包括姓名、聯絡資料、僱主名稱及職位，部份人士的身份證號碼、信用卡號碼（不包括卡驗證碼）、出生日期、專業認證詳情及考試結果。

個案分享（4）
學會的伺服器遭勒索軟件攻擊

調查結果發現三項缺失：

1. 資料保安風險管理欠佳
2. 資訊系統管理有欠妥善
3. 未適時啟用多重認證功能

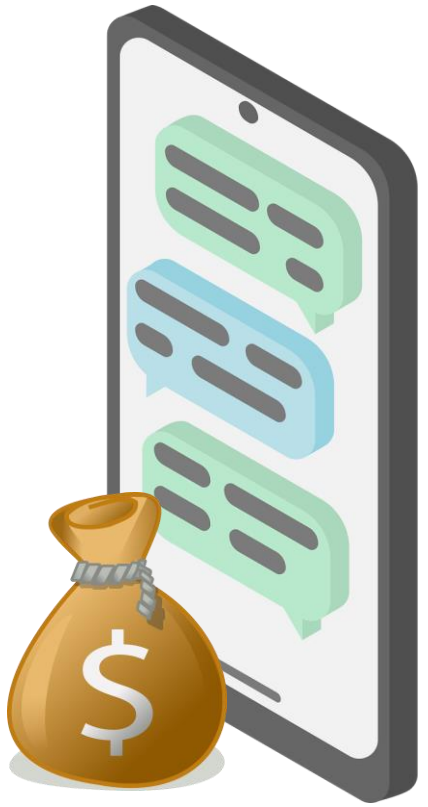
個案分享（4）
學會的伺服器遭勒索軟件攻擊

執行通知

- 徹底檢視學會載有個人資料的系統保安，確保該些系統沒有已知的惡意軟件及保安漏洞
- 聘請獨立的資料保安專家對學會的系統保安（包括載有個人資料的伺服器）進行定期檢視及審核
- 修訂系統保安政策，明確訂定學會對其網絡設備（包括防火牆及伺服器）定期進行漏洞掃描
- 修訂系統保安政策，明確訂定修補程式的管理政策及要求，並採取措施確保有關員工及提供系統保養服務的服務提供者依循相關政策及要求

個案分享（5）
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（5）
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；
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（5）
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

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

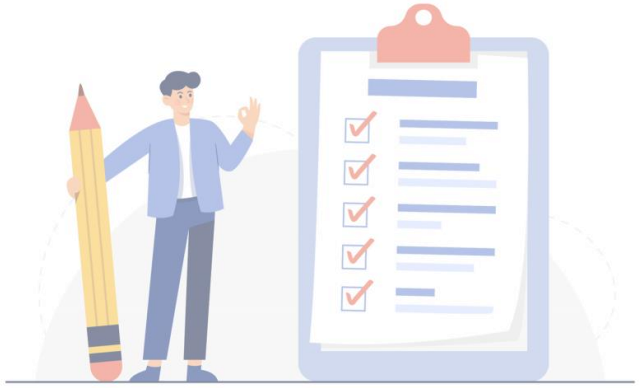
1. 立即收集重要資料
2. 遏止事件擴大
3. 評估事件可造成的損害
4. 考慮作出資料外洩通報
5. 記錄事故

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

資料使用者必須**迅速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，包括：

- 事故於**何時**發生？
- 事故在**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**？



NOTE

最先發現事故的職員應考慮是否依從資料外洩事故應變計劃所訂的程序向專責應變小組／高級管理層／保障資料主任通報事故。

步驟 2：遏止事件擴大

機構可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。

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

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

私隱專員公署的「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》

資料保安建議措施 *七大建議措施一覽*

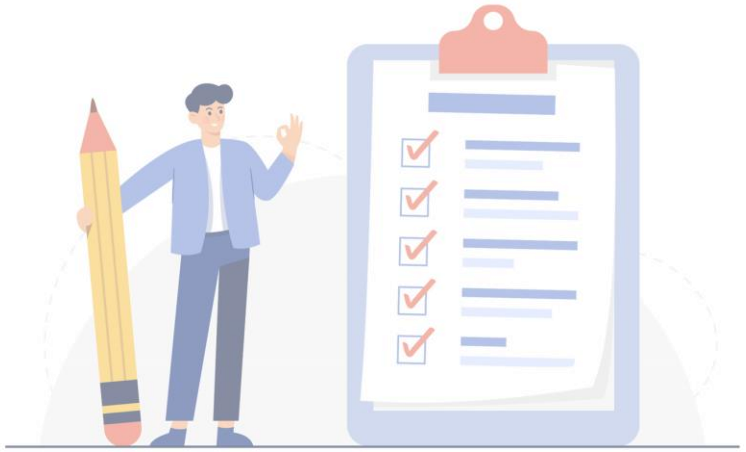
1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

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 *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

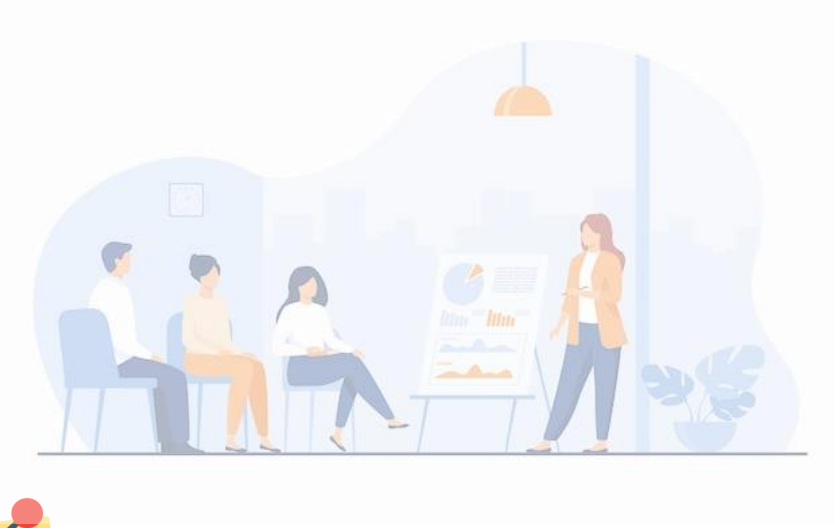
資料使用者亦要注意員工的審慎態度及誠信，以免因人為錯誤或內部攻擊而引致資料外洩。

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

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

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，可參閱私隱專員公署的《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

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，可參閱私隱專員公署發出的《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，請參閱私隱專員公署發出的《使用便攜式儲存裝置指引》

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

下載有關指引及資料單張

PCPD.org.hk

有用連結

數字政策辦公室(DPO)	網絡安全資訊站 https://www.cybersecurity.hk/tc/index.php 資訊安全網 https://www.infosec.gov.hk/tc/
香港電腦保安事故協調中心(HKCERT)	最新網絡保安警報 https://www.hkcert.org/tc/security-bulletin
香港互聯網註冊管理有限公司(HKIRC)	網絡安全員工培訓平台 https://www.hkirc.hk/zh-hant/public-mission/cybersec-training-hub/hkirc-cybersec-training-hub/
香港警務處	「守網者」 https://cyberdefender.hk/

「數據安全」套餐 “Data Security” Package

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

免費名額參加研習班及講座
Free quotas to join professional workshop and seminars

「數據安全」套餐 “Data Security” Package

https://www.pcpd.org.hk/Toolkit/tc/

數據安全快測

完成數據安全快測後，請將閣下的參考編號及機構名稱，電郵至 training@pcpd.org.hk

參考編號: TK241112177527910

學校、非牟利機構及中小型企業：

如欲透過「數據安全」套餐換領五個免費參加由私隱專員公署舉辦的專業研習班及專題講座名額^，請將閣下的**參考編號**（如上）及**機構名稱**，電郵至training@pcpd.org.hk .

^註：五個免費參加由公署舉辦的專業研習班及專題講座的名額有效期至2025年12月31日。

謝謝！Thank you!