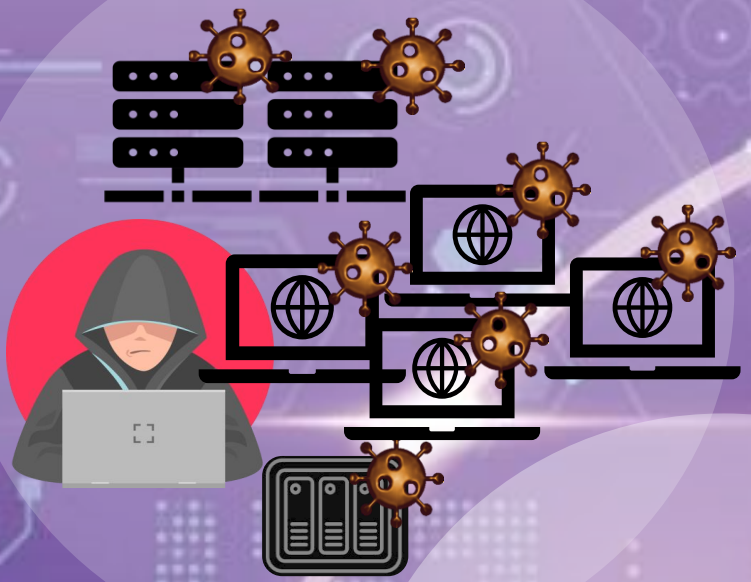
香港校董學會

「網絡安全探討：應對網絡罪行與私隱保護實踐」

研討會



如何應對資料外洩事故及提升數據安全

陳鐵威先生
高級個人資料主任
（資訊科技）

2025年2月28日

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

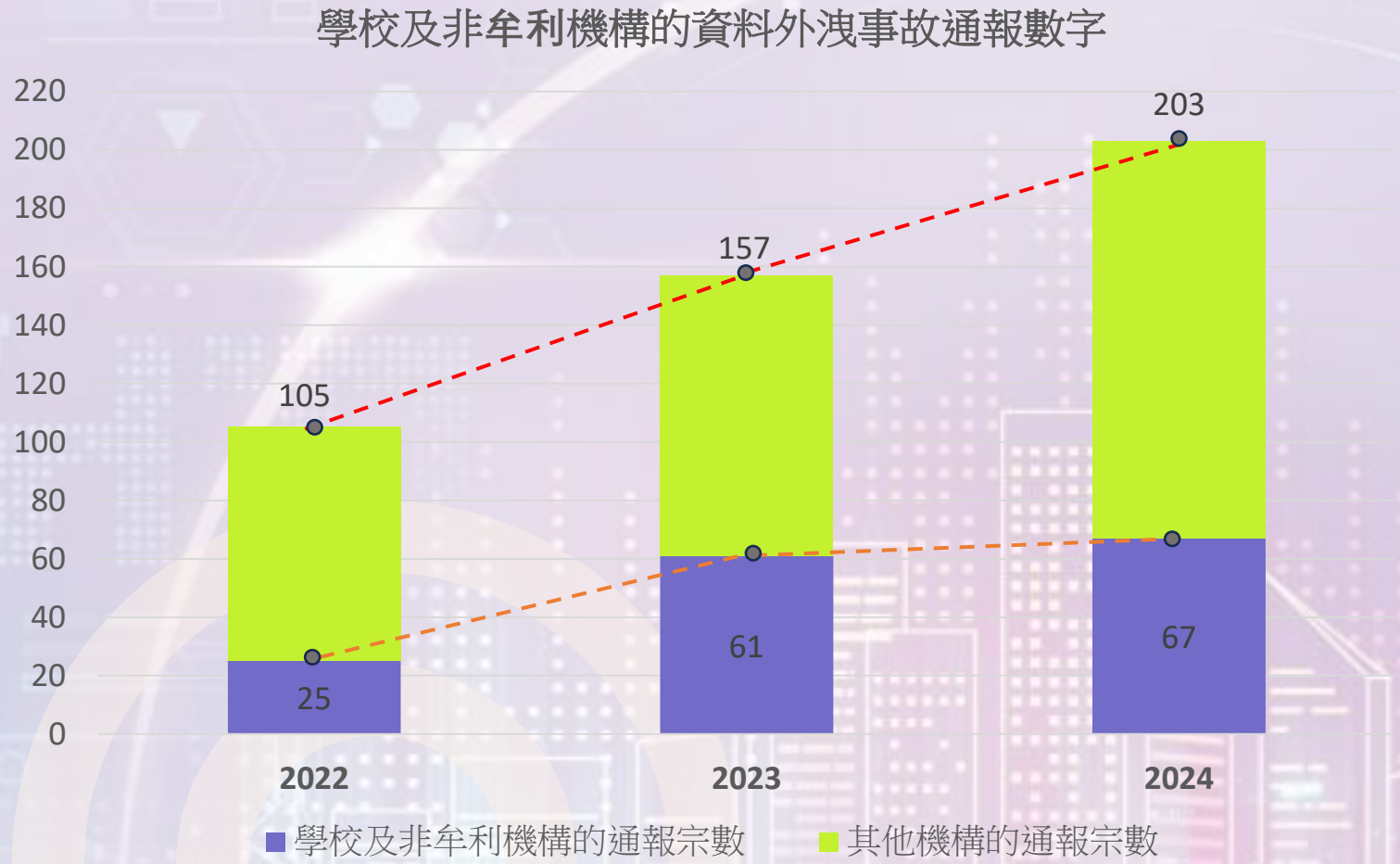
- **遺失**載有個人資料的文件或便攜式裝置
- 資訊系統**配置錯誤**
- 載有個人資料的資訊系統被**非法侵入**或被未經授權的第三方查閱
- 經郵件或電郵**錯誤發送個人資料**
- 第三方以**欺騙**手法從資料使用者取得個人資料
- 在電腦**安裝檔案分享軟件**而導致資料外洩

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

資料外洩事故通報趨勢



- 私隱專員公署於2024年共接獲203宗資料外洩事故通報
- 當中來自學校及非牟利機構的個案佔67宗（約33%），比2023年的61宗上升約10%，較2022年的25宗上升超過1.6倍

《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）

一間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（1）

一間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

該學會違反《個人資料（私隱）條例》的保障資料第4（1）原則有關個人資料保安的規定

個案分享（1）

一間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（2）

一間教育機構因密碼管理欠佳而導致學生和家長的個人資料被未獲授權查閱

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（2）

一間教育機構因密碼管理欠佳而導致學生和家長的個人資料被未獲授權查閱

- 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須加強警惕，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

個案分享（3）一個專業團體的電郵系統遭未獲授權查閱

一個專業團體向私隱專員公署通報，表示一名員工點擊釣魚電郵內的連結，並在連結中的釣魚登入頁面輸入電郵帳戶的登入憑證，令黑客成功盜用其帳戶，並向約2,700人發送釣魚電郵，導致再多兩個員工的電郵帳戶被盜用，黑客其後利用盜用的帳戶查閱載有超過17,000人的電郵地址的文件

補救措施

該團體已為所有帳戶重設密碼及採用雙重認證，亦採用地理位置檢查以阻止使用來自已知涉及黑客活動國家的IP位址的登入。該團體承諾對所有員工進行加強網絡安全意識的培訓

個案分享（3）一個專業團體的電郵系統遭未獲授權查閱

- 員工成為網絡釣魚攻擊的受害者可能會對機構造成嚴重後果
- 為了防止此類攻擊，機構應讓員工了解網絡釣魚相關的風險，並提供有關如何識別和避免網絡釣魚的定期培訓
- 機構應在電郵系統中實施完備的偵測和過濾系統來加強保安措施。機構亦應實施多重認證功能和定期更改密碼，以降低機構被未經授權存取資料的風險

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

範疇主要包括

- 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

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

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

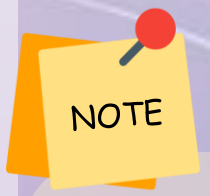
傷害程度取決於不同情況，例如:

- 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，及發生的可能性
- 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

PCPD.org.hk

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

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**

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

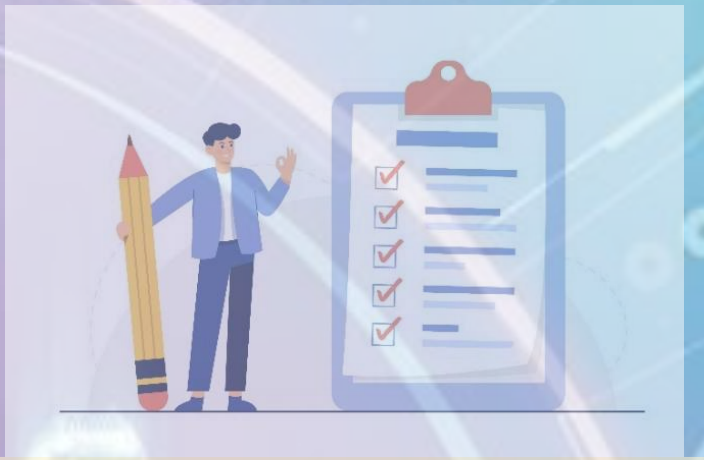
下載指引

下載小冊子

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（如首席私隱官）、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，定期和及時地覆檢與修訂政策及程序，並可考慮將「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

資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

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

- 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

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

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

資訊及通訊科技的資料保安建議措施

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

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

自攜裝置

- 盡可能避免資料使用者收集的個人資料存儲在自攜裝置設備內
- 控制對儲存在自攜裝置設備內的個人資料的存取

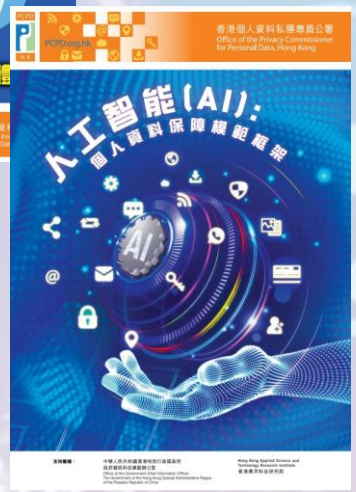
便攜式儲存裝置

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
- 使用後妥善地刪除便攜式儲存裝置中的資料

公眾教育

- 就不同個人資料私隱議題發布指引及單張



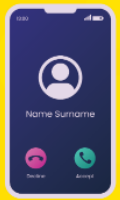
其他資訊科技相關指引及報告

- 雲端運算指引
- 人工智能 (AI): 個人資料保障模範框架
- 資料外洩事故的處理及通報指引
- 《電子點餐的私隱關注》報告
- 《數碼時代的私隱保障：比較十大網購平台的私隱設定》報告
- 社交媒體私隱設定大檢閱
- 開發及使用人工智能道德標準指引
- 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

www.pcpd.org.hk

下載有關指引及資料單張

「數據安全」套餐 “Data Security” Package

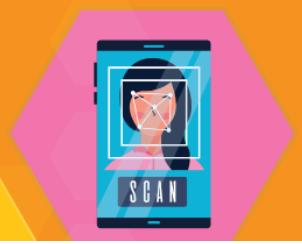


數據安全熱線
Data Security Hotline
2110 1155

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



PCPD HK

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

「數據安全」套餐 “Data Security” Package

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

數據安全快測

截止日期：4月30日

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

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!