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

數據安全快測

下載報告

日期: 2025年10月10日

參考編號: TK251010115127534

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。

整體風險水平: 很低至低

第一部：資料管治和機構性措施

問題1的風險水平： 很低至低

問題：

貴機構有沒有一套有關資料管治及 / 或資料保安的政策和程序？

你的答案：

- (•) 有
- ( ) 沒有

問題：

如答案為「有」，下列哪個項目包含在有關政策和程序中？（可選擇多於一個）

你的答案：

- [x] 員工分別在維護資訊及通訊系統和保障資料安全的角色和責任
- [x] 資料保安風險評估
- [x] 資訊及通訊系統中資料的查閱和輸出
- [x] 外判資料處理及資料保安工作
- [x] 應付資料保安事故，包括事故應變計劃和通報機制
- [x] 銷毀不再為收集資料時所訂明的目的或相關目的而需要保留的資料

你的風險水平是： **很低至低**

建議

貴機構在資料管治及 / 或資料保安有明確的政策或程序。

建議行動：

在未來，貴機構應根據當時的情況，例如行業內的新標準和對資料保安的新威脅，定期和及時地檢視與修訂其相關政策和程序。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》 第3.1部
- ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

問題2的風險水平： 很低至低

問題：

貴機構有沒有委任領導人物（例如首席資料官或首席私隱官）負責資料保安？

你的答案：

- (•) 有
- ( ) 沒有

問題：

如答案為「有」， 貴機構有沒有一套指引列出有關人員的角色和責任？

你的答案：

- (•) 有
- ( ) 沒有

問題：

如答案為「有」，以下哪個項目包含在指引中？（可選擇多於一個）

你的答案：

- [x] 機構處理個人資料的整個資料周期
- [x] 獲委任負責個人資料保安的各個人員的角色和責任
- [x] 決策的權力分配
- [x] 有關查閱和轉移個人資料的問責和監督權

你的風險水平是： 很低至低

建議

貴機構有委任合適的領導人物負責資料保安，亦有全面的指引列明有關人員的角色和責任。

建議行動：

在未來，貴機構應根據當時的情況，定期和及適時檢視與修訂有關指引和人手配置。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》 第3.1部

問題3的風險水平： 很低至低

問題：

貴機構有沒有為工作人員提供有關《私隱條例》的培訓？

你的答案：

- (•) 有
- ( ) 沒有

你的風險水平是： 很低至低

建議

貴機構有為工作人員提供培訓，以確保他們熟悉《私隱條例》的規定。

建議行動：

在未來，貴機構應繼續定期為工作人員提供培訓，並根據當時的情況（例如相關資料私隱法例的修訂），適時檢視和更新培訓計劃。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》 第3.1部
- 私隱專員公署有關《私隱條例》的專題網頁
- 《私隱條例》

問題4的風險水平： 很低至低

問題：

貴機構有沒有就機構的資料保安政策及程序為工作人員提供培訓？

你的答案：

◉ 有

○ 沒有

問題：

如答案為「有」，有關培訓包含以下哪一個項目？（可選擇多於一個）

你的答案：

☑ 有效的密碼管理

☑ 加密軟件的使用

☑ 便攜式儲存裝置和遙距存取工具的使用

☑ 將資料永久銷毀的原則和相關工具的用法

☑ 可疑超連結、二維碼及附件帶來的風險

☑ 社交工程、詐騙電子郵件、勒索軟件或虛假網站所帶來的風險

☑ 只使用經機構內部核准的軟件

☑ 社交媒體和互聯網的適當使用

你的風險水平是： 很低至低

建議

貴機構有為工作人員提供全面的培訓，以確保他們熟悉機構的資料保安政策及程序。

建議行動：

在未來，貴機構應繼續定期為工作人員提供培訓，並根據當時的情況（如對資料保安的新威脅、推行新措施或採用可能影響資料保安的新工具），適時檢視和更新培訓計劃。

為加強並鞏固員工的警覺性，貴機構可以考慮將網絡安全和資料保安「演習」納入培訓。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》 第3.1部

第二部：風險評估

問題5的風險水平： 很低至低

問題：

貴機構有沒有在啟用新系統及／或新應用程式前進行資料保安風險評估？

你的答案：

- ◉ 有
- ○ 沒有
- ○ 不適用

問題：

如答案為「有」，以下哪一項是正確的？（可選擇多於一個）

你的答案：

- ☑ 在啟用後會定期重複進行風險評估
- ☑ 會向高級管理層匯報風險評估的結果
- ☑ 及時處理在風險評估中發現的保安風險

你的風險水平是： 很低至低

建議

貴機構會在啓用新系統及／或新應用程式前進行資料保安風險評估，並採取適當的跟進行動。

建議行動：

在未來，貴機構應繼續在啓用新系統及／或新應用程式前進行資料保安風險評估，並採取適當的跟進行動。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》 第3.2部

第三部：技術上及操作上的保安措施

問題6的風險水平： 很低至低

問題：

有關實施技術上及操作上的保安措施，貴機構有沒有採取以下措施？（可選擇多於一個）

你的答案：

- ☑ 保護電腦網絡 — 例如採納存取控制措施、使用防火牆、使用端點保安軟件，以及定期對網絡和系統保安進行掃描和審核
- ☑ 存取管控 — 例如限制存取權限、實施密碼管理、制訂帳戶鎖定閾值策略，以及定期覆檢存取權限並適時刪除不必要的帳戶和存取權限（例如在職員離職時）
- ☑ 防火牆和反惡意軟件 — 例如使用域名系統（DNS）防火牆、對資訊及通訊系統進行保安漏洞評估，以及使用反惡意程式軟件
- ☑ 加密 —例如加密傳輸中和儲存的資料、有效管理加密密鑰、為流動裝置及便攜式儲存裝置的資料進行加密、代號化和雜湊資料
- ☑ 電郵 — 例如鼓勵使用以密件副本功能（bcc / blind carbon copy）而非副本功能（cc / carbon copy）發出電郵、過濾濫發的、帶有惡意附件或鏈結的電郵
- ☑ 檔案傳送 — 使用端點保安軟件防止未獲批准的資料轉移、為載有敏感個人資料的檔案添加數碼水印
- ☑ 安全地銷毀資料，令資料無法恢復，及 / 或將不必要的或過期的個人資料匿名化

你的風險水平是： 很低至低

建議

貴機構實施了全面的技術上及操作上的保安措施，以保護所控制或持有的個人資料和資訊及通訊系統。

建議行動：

《私隱條例》保障資料第4(1) 原則規定資料使用者須採取所有切實可行的步驟，以確保其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，尤其須考慮(a) 該資料的種類及如該等事情發生便能做造成的損害；(b) 儲存該資料的地點；(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

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。保安措施是否足夠取決於每宗案件的具體情況。

在未來，貴機構應根據當時的情況（例如貴機構在營運上的改變、新的資料保安威脅等），定期檢視和更新實施中的保安措施。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》 第3.3部
- 私隱專員公署與新加坡個人資料保護委員會共同製作的《資訊及通訊科技系統的貫徹數據保障設計指引》(只有英文版)
- 香港政府的政府資訊科技總監辦公室維護的「網絡安全資訊站」及「資訊安全網」網站
- 香港電腦保安事故協調中心發出的《物聯網保安最佳實踐指引》
- 香港電腦保安事故協調中心發出的《數據保護指引》

第四部：資料處理者的管理

問題7的風險水平：不適用

問題：

貴機構有沒有聘用第三方（例如雲端服務供應商和資料分析服務供應商）處理資料？

你的答案：

○ 有

◉ 沒有

你的風險水平是：不適用

建議

貴機構沒有聘用第三方處理資料。

相關原則：

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。保障資料第 4(2) 原則亦規定，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。

為充分保障個人資料安全，貴機構可考慮在聘用資料處理者之前及之時，採取以下行動：

- 實施政策及程序以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；
- 資料處理合同應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；及
- 進行現場審核以確保資料處理者遵守資料處理合同，並對資料處理者違反合同的行為施加後果。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》 第3.4部
- 私隱專員公署發出的《外判個人資料的處理予資料處理者》資料單張

第五部：資料保安事故發生後的補救措施

問題8的風險水平： 很低至低

問題：

貴機構有沒有建立一套資料保安事故應變計劃（即一套包括程序、規程及指引在內的計劃，以助機構應對資料保安事故並從中恢復，務求將損害減至最低）？

你的答案：

◉ 有

○ 沒有

問題：

如答案為「有」，以下哪一項是貴機構在發生資料保安事故時會採取的補救措施？（可選擇多於一個）

你的答案：

☑ 立即停止受影響的資訊及通訊系統，並將其與互聯網和資料使用者的其他系統的連接中斷（如切實可行）

- [x] 立即更改涉嫌導致資料保安事故的用戶的密碼，或中止其存取權限
- [x] 立即更改系統的配置，以管制對受影響系統的存取
- [x] 在沒有不當延誤的情況下通知受影響的人士，並向他們建議保障自己的可行辦法
- [x] 在沒有不當延誤的情況下通知私隱專員公署及其他執法機構 / 監管機構
- [x] 適時修補保安漏洞
- [x] （在不影響未來調查取證分析的情況下）掃瞄系統，以查找任何其他未知的保安漏洞

你的風險水平： **很低至低**

建議

貴機構有一套全面的資料保安事故應變計劃。

建議行動：

《私隱條例》保障資料第 4(1)原則規定，資料使用者須採取所有切實可行的步驟以保障由其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，其中尤其須考慮，該資料的種類及如該等事情發生便能造成的損害。

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。保安措施是否足夠取決於每宗案件的具體情況。

在未來，貴機構應定期檢視及更新資料保安事故應變計劃，以確保計劃仍然有效和符合《私隱條例》的相關規定和任何相關的法例。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》第3.5部
- 私隱專員公署發出的《資料外洩事故的處理及通報指引》

第六部： 監察、評估及改善

問題9的風險水平： 很低至低

問題：

貴機構有沒有既定機制以監察資料保安政策和程序的遵從情況，以及評估它們的成效？

你的答案：

- (•) 有
- ( ) 沒有

問題：

如答案為「有」，貴機構有沒有採取行動去處理該機制以發現的違反政策的行為或成效不彰的措施？

你的答案：

- ○ 有
- ○ 沒有
- ◉ 在評估後，沒有發現違反政策的行為或成效不彰的措施

你的風險水平是： **很低至低**

建議

貴機構有既定機制以監察資料保安政策和程序的遵從情況，以及評估它們的成效，該機制並沒有發現違反政策的行為或成效不彰的措施。

建議行動：

日後如該機制發現違反政策的行為及 / 或保安措施成效不彰，貴機構應及時採取改善行動以減低保安風險。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》第3.6部

第七部：雲端服務、自攜裝置、以及便攜式儲存裝置

問題10的風險水平：不適用

問題：

貴機構有沒有使用第三方雲端服務供應商所提供的運算和資料儲存服務？

你的答案：

- ○ 有
- ◉ 沒有

你的風險水平是：不適用

建議

貴機構沒有使用第三方雲端服務供應商所提供的運算和資料儲存服務。

相關原則：

雲端服務供應商一般屬於資料處理者。資料使用者仍須為其採用雲端服務供應商代其持有的個人資料之保安負主要責任。

資料使用者應在使用雲端服務時採取以下措施，以確保雲端環境和個人資料的保安：

- 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；及
- 檢視雲端的現有保安功能，並啟用合適的保安功能，不要只依賴預設的保安設置。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》 第3.4部及3.7部
- 私隱專員公署發出的《雲端運算》資料單張

問題11的風險水平： 很低至低

問題：

貴機構有沒有實施自攜裝置政策，允許員工使用屬於其個人的電子裝置（例如智能電話或手提電腦）查閱貴機構的系統和處理貴機構持有的資料？

你的答案：

◉ 有

○ 沒有

問題：

如答案為「有」，貴機構採取了以下哪一項有關實施自攜裝置政策的保安措施？（可選擇多於一個）

你的答案：

☑ 我們盡可能避免資料使用者收集的個人資料儲存在自攜裝置設備內

☑ 我們控制對儲存在自攜裝置設備內的個人資料的存取（例如，除了員工智能電話的屏幕鎖之外，再需要另外登入才能查閱）

☑ 我們使用並非自攜裝置設備內建的加密方法來加密存儲在其中的個人資料

☑ 我們在自攜裝置設備上安裝軟件，以便在丟失自攜裝置設備時可遙距刪除存儲在其中的資料

你的風險水平是： 很低至低

建議

貴機構實施自攜裝置政策時，採取了全面的保安措施。

建議行動：

實施自攜裝置政策時，資料使用者實際上是把資料從保安良好的企業系統轉移至安全程度較低、亦較難以有效控制的員工設備上。在這情況下，資料使用者仍須為轉移到員工設備的個人資料完全負上遵守《私隱條例》的責任。

因此，資料使用者應設立行政和技術性措施以確保此類個人資料受到保障，亦應通過明文政策和培訓，藉以加強這些措施的成效。

在未來，貴機構應定期檢視及更新所採取的保安措施，以確保措施仍然有效和符合《私隱條例》的相關規定。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》第3.7部
- 私隱專員公署發出的《自攜裝置》資料單張

問題12的風險水平： 很低至低

問題：

貴機構有沒有允許使用便攜式儲存裝置來儲存和轉移個人資料？

你的答案：

◉ 有

○ 沒有

問題：

如答案為「有」，貴機構採取了以下哪一項有關使用便攜式儲存裝置的保安措施？（可選擇多於一個）

你的答案：

☑ 我們制訂了政策，列明允許使用便攜式儲存裝置的情況；可轉移到便攜式儲存裝置上的個人資料的類別及數量；使用便攜式儲存裝置的批准程序；及轉移到便攜式儲存裝置的資料的加密要求等

☑ 我們使用端點保安軟件防止資料從機構的系統轉移到不安全（例如沒有加密功能）或未獲批准使用的便攜式儲存裝置上

☑ 我們保存便攜式儲存裝置的清單，並追蹤其使用和下落

☑ 我們規定在每次使用便攜式儲存裝置之後妥善地刪除當中的資料

你的風險水平是： **很低至低**

建議

貴機構實施了全面的有關使用便攜式儲存裝置的保安措施。

建議行動：

當資料使用者使用便攜式儲存裝置時，由於可以簡單且快速地複製和轉移大量個人資料至普遍來說有較佳保安的公司系統以外的地方，因而增加了資料保安事故的風險。資料使用者應在切實可行範圍內避免使用便攜式儲存裝置來儲存個人資料。

如資料使用者使用便攜式儲存裝置，為遵從《私隱條例》規定的資料保安規定，應實施足夠的保安措施。

在未來，貴機構應定期檢視及更新現有的保安措施，以確保措施仍然有效和符合《私隱條例》的相關規定。

有用的參考資料：

- 私隱專員公署發出的《資訊及通訊科技的保安措施指引》第3.7部
- 私隱專員公署發出的《使用便攜式儲存裝置指引》資料單張

多謝完成自我評估。如要下載報告，請點擊右上角的「下載報告」按鈕。