在家工作安排下的個人資料保障指引：機構篇

引言

1. 2019冠狀病毒病疫情期間，機構需不時實施在家工作安排。就此，機構或許有需要透過僱員的家居網絡及個人電子裝置查閱或傳送資料及文件。相對於由專業人員管理的公司網絡及電子裝置，僱員的家居網絡及個人電子裝置的保安較弱，資料保安及個人資料私隱的風險無可避免會上升。

2. 本指引旨在為機構（包括業務實體）提供實用建議，以提升在家工作安排下的資料保安及個人資料私隱的保障。

在家工作安排的基本原則

3. 不論是在辦公室或在家工作，個人資料的保安以及保障個人資料私隱的標準是相同的。機構在實施在家工作安排時應遵守以下原則：

   (1) 為在家工作安排下的資料處理（包括個人資料）制定清晰的政策[1]；以及

   (2) 採取所有合理切實可行的步驟確保資料安全，特別是當涉及使用資訊及通訊科技以便利在家工作，或涉及將資料和文件轉移予僱員[2]。

給機構的實用建議

4. 機構作為資料使用者及僱主，在確保資料安全及保障僱員的個人資料私隱方面負有主要責任。因此，機構應落實以下的措施以體現上述在家工作安排的基本原則。

風險評估

5. 對很多機構而言，在家工作是前所未有或是全新的安排。因此，機構應評估有關安排對資料保安及僱員個人資料私隱構成的風險，從而制定合適的保障措施。

政策及指引

6. 機構應按照風險評估的結果，審視現有政策及常規，作出適當的修訂，以及為僱員提供充足的指引。有關的政策及指引可包括以下方面：

   (1) 將資料及文件轉移離開機構的處所及公司網絡的安排；

   (2) 遙距接達公司網絡及存取資料的安排；

   (3) 刪除及銷毀非必要的資料的安排；以及

   (4) 資料外洩事故的處理。

僱員培訓及支援

7. 機構應為在家工作的僱員提供足夠培訓及支援，以確保資料安全。相關的培訓及支援可包括以下方面：

   (1) 資料保安的方法，例如密碼管理、資料加密以及安全地使用 Wi-Fi；以及

   (2) 對網絡保安威脅及趨勢的意識，例如網絡釣魚、惡意軟件及電話騙案。

8. 機構應指派專責的職員解答僱員的疑問和提供適切的支援。

電子裝置管理

9. 機構如為在家工作的僱員提供電子裝置（例如智能電話和手提電腦），應採取以下措施確保儲存於電子裝置內的資料（包括個人資料）安全：

   (1) 安裝適合的防惡意程式軟件、防火牆及最新的保安修補程式；

   (2) 定期更新電子裝置系統；

   (3) 確保儲存於電子裝置內、與工作有關的資料已進行加密處理；

---

1 《個人資料（私隱）條例》（香港法例第486章）附表1的保障資料第5原則

2 保障資料第4原則

(4) 設定嚴格的存取控制，例如要求使用高強度密碼（包含英文字母、數字及符號的組合）、要求定期更改密碼以及使用多重身份認證，並且限制登入失敗的次數；

(5) 防止從公司的裝置轉移資料至個人電子裝置；

(6) 開啟遙距資料抹除功能，當電子裝置遺失時可刪除儲存在裝置內的資料；以及

(7) 避免在電子裝置上顯眼地展示機構的名稱、標誌及其他標識，以免引起不必要的注意。

虛擬私人網絡 (VPN)

10.VPN是在家工作安排中一樣重要和普及的工具，因為VPN可讓僱員遙距地以及比較安全地接達公司網絡。為確保VPN的安全，機構應採取以下措施：

(1) 連接VPN時使用多重身份認證；

(2) 及時更新VPN平台的保安設定；

(3) 採用握手協議（handshake protocol）（例如互聯網安全協定（IPSec）、保密插口層（SSL）、傳輸層保安（TLS）等）以為僱員電子裝置與公司網絡之間建立安全通訊渠道；

(4) 在可行情況下選擇全隧道VPN（只在必要的情況下選擇分割隧道VPN，例如當頻寬不足時）；以及

(5) 封鎖不安全的電子裝置。

遙距接達

11.除了使用VPN外，機構應對公司網絡的遙距接達採取進一步保安措施。實際措施可包括：

(1) 採用網絡分段將整個網絡區分成不同的網段或子網絡，以減低資料外洩事故的風險和嚴重程度，並提升對重要和敏感資料的保護；

(2) 按實際需要給予僱員存取權限，例如採用以職能為基礎的存取控制（role-based access control）；

(3) 開啟帳戶鎖定功能，封鎖多次登入失敗的帳戶；以及

(4) 檢視遙距接達的紀錄以識別可疑活動。

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

私隱公署網頁

查詢熱線 : (852) 2827 2827
傳真 : (852) 2877 7026
地址 : 香港灣仔皇后大道東248號陽光中心13樓1303室
電郵 : communications@pcpd.org.hk

下載本刊物

二零二零年十一月初版

在家工作安排下的個人資料保障指引：僱員篇

引言

1. 2019冠狀病毒病疫情期間，機構需不時實施在家工作安排。就此，僱員或許有需要透過家居網絡及個人電子裝置查閱或傳送僱主的資料及文件。相對於由專業人員管理的公司網絡及電子裝置，僱員的家居網絡及個人電子裝置的保安較弱，資料保安及個人資料私隱的風險無可避免會上升。

2. 本指引旨在為僱員提供實用建議，以提升在家工作安排下的資料保安及個人資料私隱的保障。

在家工作安排的基本原則

3. 不論是在辦公室或在家工作，資料保安以及保障個人資料私隱的標準是相同的。僱員在家工作期間應遵守以下原則：

   (1) 遵守僱主有關資料處理（包括個人資料）的政策。

   (2) 採取所有合理切實可行的步驟確保資料安全，特別是當涉及使用資訊及通訊科技以便利在家工作，或在工作過程中涉及資料和文件轉移[1]。

給僱員的實用建議

4. 在家工作期間，僱員或需要遙距接達公司網絡，亦可能會將電子及紙本文件帶回家工作。僱員應採取以下措施確保資料安全。

電子裝置管理

5. 在可行情況下，僱員應只使用公司裝置處理公事，同時應採取以下保安措施以保護電子裝置及其內的資料：

   (1) 設定高強度密碼，並定期更改密碼。不要在不同的電子裝置和帳戶使用相同密碼；

   (2) 不應在公司裝置上安裝個人設備（例如個人USB記憶體），因個人設備存有惡意程式或保安漏洞的機會較高；

   (3) 如需使用便攜式儲存裝置傳輸及儲存資料，應將裝置內的資料加密；

   (4) 不要與家人共用公司裝置；

   (5) 無須使用電子裝置時，將其關掉或鎖上；以及

   (6) 遺失公司裝置時應立即通知僱主。

工作環境

6. 僱員應避免於公眾場所工作，以免意外地將個人資料或限閱資料洩露給第三方。

7. 如無可避免需在公眾場所工作，僱員應—

   (1) 在電子裝置的螢幕上貼上防窺濾片以保障螢幕上顯示的資料；以及

   (2) 不要使用公共Wi-Fi。僱員如因工作需要而要將其他電子裝置連接到互聯網，可使用手提電話的熱點分享功能。

Wi-Fi 連接

8. 一般而言，使用網線連接上網比使用Wi-Fi較為安全。因此僱員在家工作時應盡可能利用網線連接上網。如需使用Wi-Fi，應採取以下措施加強連接的安全：

   (1) 採用最新安全協定，例如 WPA3 或 WPA2 以加密傳輸的資料及抵禦攻擊；

   (2) 為Wi-Fi網絡設定高強度密碼並定期更改密碼。不要使用Wi-Fi路由器預設的登入名稱及密碼；

   (3) 及時更新Wi-Fi路由器的固件；以及

[1] 《個人資料（私隱）條例》（香港法例第486章）附表1的保障資料第4原則

(4) 定期檢視連接至Wi-Fi網絡的電子裝置，以便識別並移除可疑裝置。

電子通訊

9. 電子通訊如電郵及即時通訊可讓僱主與僱員於在家工作期間有效地溝通。為確保電子通訊的安全，僱員應—

(1) 避免使用個人電郵帳戶或個人即時通訊程式辦公；

(2) 只用公司電郵帳戶傳送和接收與工作有關的文件和資料；

(3) 將載有個人資料和限閱資料的電郵及／或附件加密；

(4) 發送電郵和即時訊息前小心覆檢收件人的名字，尤其是當電郵和訊息載有個人資料和限閱資料；以及

(5) 提防釣魚電郵及惡意電郵，切勿點擊可疑鏈結或開啟可疑文件。當收到可疑電郵和訊息時，應透過其他渠道（例如電話）與發送者核實。

紙本文件管理

10. 在可行的情況下僱員應避免從辦公室帶走紙本文件，特別是載有個人資料或限閱資料的文件。如僱員有必要將紙本文件帶回家中工作，應採取以下措施：

(1) 取得上司的批准；

(2) 在可行的情況下，離開辦公室前先將紙本文件中的個人資料、限閱資料以及其他非必要資料遮蓋或移除；

(3) 備存清單，記錄帶回家中的文件；

(4) 攜帶紙本文件途中應份外小心，慎防遺失；

(5) 在家中應將紙本文件鎖進安全的儲物櫃或抽屜，防止未經授權的取閱；

(6) 將不再需要的紙本文件盡快送回辦公室；以及

(7) 切勿於家中棄置載有個人資料或限閱資料的工作文件。有關文件應按既定程序於辦公室銷毀。

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

PCPD 私隱公署

私隱公署網頁

下載本刊物

查詢熱線 : (852) 2827 2827
傳真 : (852) 2877 7026
地址 : 香港灣仔皇后大道東248號陽光中心13樓1303室
電郵 : communications@pcpd.org.hk

二零二零年十一月初版

在家工作安排下的個人資料保障指引：使用視像會議軟件

引言

1. 2019冠狀病毒病疫情期間，機構需不時實施在家工作安排，舉行視像會議因而成為新常態。使用視像會議軟件日趨普遍，為資料保安及個人資料私隱帶來新的風險[1]。

2. 本指引旨在為機構及其僱員提供實用建議，以提升他們使用視像會議軟件時的資料保安及個人資料保障。本指引亦適用於其他視像會議軟件的使用者，例如教師及學生。

使用視像會議軟件的實用指引

3. 機構（包括業務實體）應審視及評估不同視像會議軟件在保安及保障個人資料私隱方面的政策和措施，並按需要選用合適的軟件。例如，機構若無可避免要透過視像會議討論機密事宜，應考慮使用提供端對端加密的視像會議軟件。

4. 使用視像會議軟件時，應留意以下的保安措施：

   (1) 妥善管理帳戶，設定高強度密碼並定期更改密碼。如視像會議軟件提供多重身份認證功能，應啟用有關功能；

   (2) 確保視像會議軟件是最新版本，並安裝最新的保安修補程式；以及

   (3) 連接安全可靠的網絡以進行視像會議。

5. 為確保視像會議期間的保安及保障個人資料私隱，會議主持人應—

   (1) 為每個會議設定獨特的會議登入編號，以及高強度、獨特的密碼。會議登入編號及密碼只提供予與會者。在可行情況下以不同方式（例如電郵及短訊）向與會者分別發送會議登入編號及密碼；

   (2) 在可行情況下，在負責主持會議的人以外，安排多一位副「主持人」，負責管理視像會議，並協助處理技術問題及其他突發事件；

   (3) 使用虛擬等候室功能，在准許與會者加入會議前先核實他們的身份。當所有與會者進入會議後，將會議「鎖上」，防止其他人士擅自加入會議；

   (4) 只允許有需要作匯報的與會者分享屏幕及文件；

   (5) 如需錄影會議，應在開始錄影前明確通知與會者，並取得他們的同意，禁止其他與會者在會議期間進行錄影；以及

   (6) 所有與會議相關的紀錄（例如會議的錄影檔案及與會者的對話訊息）應妥善儲存（例如以密碼或加密方式保護）。當不再需要有關紀錄時，應盡快刪除。

[1] 《個人資料（私隱）條例》（香港法例第486章）附表1的保障資料第4原則訂明，資料使用者須採取所有切實可行的步驟，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。

6. 與會者應採取以下措施保障自己的個人資料私隱：

(1) 留意自己身處地方的背景，因為有關背景可能被拍攝到，從而將一些個人資料或敏感資料披露予其他與會者。如有需要可使用虛擬背景；

(2) 在無需發言時，應關閉麥克風，甚或攝錄機；

(3) 在可行的情況下避免在視像會議期間討論涉及個人的或敏感的資料；以及

(4) 開啟電腦桌面分享功能前，應關閉非必要的文件及視窗（例如電郵視窗），以免被其他與會者看到敏感資料。

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

私隱公署網頁

查詢熱線 : (852) 2827 2827
傳真 : (852) 2877 7026
地址 : 香港灣仔皇后大道東248號陽光中心13樓1303室
電郵 : communications@pcpd.org.hk

下載本刊物

二零二零年十一月初版