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