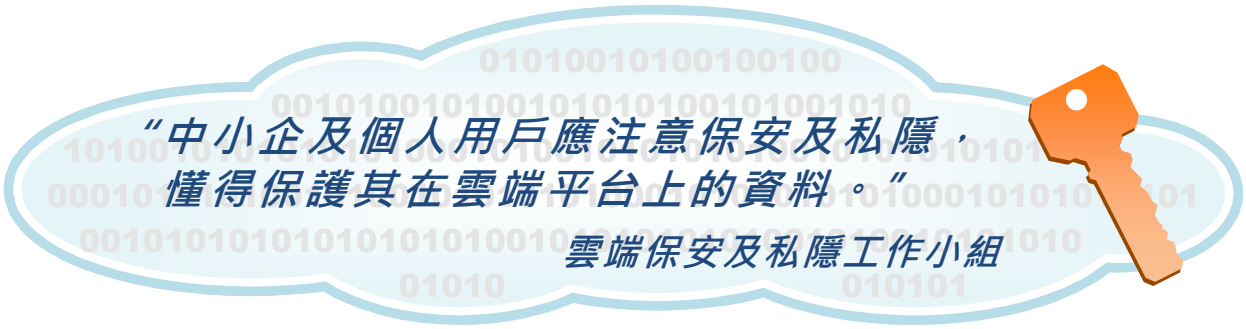
雲端服務用戶
的資訊保安備忘事項



目的

雲端服務無遠弗屆、方便使用、具成本效益，故愈來愈多工商機構及個別人士使用。本文件載列了資訊保安方面的三份備忘事項，以供用戶在考慮使用或在使用雲端服務時參考。

目標對象

本文件的主要目標對象是雲端服務用戶，包括中小型企業（下稱“中小企”）及個人用戶。

討論範圍

本文件的重點集中在雲端用戶服務上，當中涉及用戶儲存及分享自己的資料；以及經互聯網或其他網絡連接方式，接達第三方服務供應商擁有或營運的遠端伺服器，從而使用已安裝的雲端應用程式。當使用這些雲端服務的基本功能時，一般都是免費的，但一些進階服務則可能須向用戶收取費用。雲端服務的例子包括網上電郵、社交網站、資料儲存、照片分享網站、聯絡人管理、文件管理及其他應用程式。這些服務通常屬“軟件即服務”，即透過寄存在中央雲端平台上的軟件提供服務，而相關資料，亦會寄存在中央雲端平台上。

雲端服務用戶關注的保安問題

很多人因擔心服務中斷、資料遺失、私隱、帳戶遭黑客入侵和法例問題而對使用雲端服務有戒心。對熟悉應用資訊科技的企業而言，他們很可能具備技術和資源，以監察服務供應商的服務水準，評核服務供應商是否符合保安規定，或自行採取額外保安措施保護其資料。

另一方面，一般雲端服務用戶及中小企用戶可能忽略本身的權利及責任，也可能不清楚如何選擇可信靠的雲端服務供應商，以及可能不肯定在使用雲端服務時，其資料是否充分受到保護。

雲端服務用戶應注意哪些事項？

雲端服務用戶透過雲端平台處理或儲存的資料，可能包含有價值、敏感和牽涉個人的資料。用戶要保護這些資料，單靠雲端服務供應商所採取的保安措施並不足夠。對中小企用戶而言，他們需要懂得在選擇雲端服務供應商和使用雲端服務時要考慮什麼保安措施。對所有雲端服務用戶（包括商業和個人用戶）而言，他們需要深入了解在雲端平台上保護其資料所遇到的困難和考慮。

中小企在選擇雲端服務供應商的備忘事項

服務條款及保安和私隱政策

- 中小企公司須閱讀服務供應商的服務條款及保安和私隱政策，並應注意：
  - 公司可如何使用雲端服務（即使用限制條款、使用權或使用限制）；
  - 資料是如何儲存及受到保護；
  - 服務供應商是否可以存取你的公司資料。如果可以的話，此類存取是怎樣被限制的；
  - 如何舉報保安事故；
  - 如何終止服務，以及在終止服務後，如何處理仍然保留在相關雲端平台上的資料；
  - 服務供應商會否在更改服務條款前預先發出通知；
  - 私隱政策是否遵從《個人資料（私隱）條例》[1]的保障資料原則；以及
  - 條款可適用於哪些司法管轄區（香港特別行政區或其他地區）。
- 如不接納某些服務條款，應與服務供應商洽談。如物色不到能夠滿足所訂要求的服務供應商，應重新考慮是否需要使用雲端服務。
- 了解帳戶資料會否在用戶不知情或未經用戶同意的情況下作“次要用途”，例如儲存在雲端平台上的資料可能會被用來製作切合用戶需要的廣告。

資料擁有權

- 查核服務供應商是否保留權利，可使用、披露或公開用戶所擁有的資料。
- 查核用戶能否保留所擁有資料的知識產權。
- 查核即使資料從雲端平台上被刪除後，服務供應商會否保留使用該些資料的權利。
- 了解用戶能否按本身意願把資料及服務轉移至另一服務供應商，以及是否有容易用的資料匯出功能供用戶使用。
- 從雲端平台上刪除資料或停止使用該服務時，應檢查這些資料（包括任何儲存備份資料）是否可被永久刪除。

選擇服務供應商時的其他考慮因素

- 了解使用雲端服務所涉及的風險和公司可接受的風險程度。
- 選擇服務水準協議與你的業務重要性相符的服務供應商。
- 選擇能清楚說明提供哪些保安功能的服務供應商，有獨立資訊保安管理認證（例如ISO/IEC 27001）者為佳。
- 選擇不曾發生重大保安事故，或即使曾發生保安事故但能清楚解釋事發原因及補救辦法的服務供應商。
- 選擇能透過以下途徑確保用戶資料得以保密的服務供應商：
  - 使用加密功能（例如保密插口層(SSL)）以傳送資料；以及
  - 使用加密功能以保護儲存資料。（如供應商沒有提供加密功能，用戶應自行為資料加密，然後才儲存在雲端平台上，並須安全保管加密密碼匙。）
- 選擇設有簡單清晰通報機制的服務供應商，以供舉報服務問題、保安事故和侵犯私隱事宜。
- 選擇能定期提交服務管理報告及保安事故報告的服務供應商。

中小企在使用雲端服務的備忘事項

身分識別和認證

- 如雲端服務有提供的話，應使用嚴謹的認證方式，例如雙重認證，用戶可以使用其本人的特徵(例如指紋)、擁有的憑證(例如數碼證書)和所知的資料(例如密碼)的其中兩項進行認證。
- 帳戶應使用難被猜中的密碼。
- 不同的帳戶應使用不同的密碼。
- 不同的員工應使用不同的帳戶。
- 定期更改密碼。
- 出現人事變動時，應即時刪除有關用戶帳戶或更改密碼。

雲端平台管理

- 就雲端服務的使用制訂一套簡單的帳戶政策。
- 制訂簡單的使用政策供員工遵守。
- 指派一名合適的員工(對雲端服務有基本認識)擔任雲端服務管理員。
- 定期檢討員工對雲端平台上資料所擁有的存取權。
- 為使用雲端服務的員工提供基本保安認知培訓。

資料保護

- 了解並記錄儲存於雲端平台上資料的種類。
- 遵從《個人資料(私隱)條例》[1]以保護個人資料。
- 透過以下途徑避免把資料分享給非預定人士：
  - 如用戶擬透過雲端平台上與他人分享敏感資料，確保只有指定收件人才可存取；
  - 確保任何運行於用戶裝置用作接達雲端服務的應用程式，只可把有關裝置與雲端平台之間的許可資料同步；以及
  - 替檔案或文件夾預設合適的存取權限。
- 了解資料(包括備用副本)的儲存位置(及所屬司法管轄區)，並評估不同的法規遵行要求對保安程序是否有影響。

服務的持續性

- 向服務供應商索取有關服務支援的聯絡資料(特別是保存可以用作通報電腦保安事故的電話號碼清單)。
- 評估雲端服務中斷、資料遺失或資料被他人擅自存取對公司造成的潛在損害。
- 制訂持續業務運作計劃和替代方案，以應對雲端服務停用或資料不能被讀取的情況。
- 擬訂退出策略，確保有關終止程序允許把資料傳送回公司。
- 定期為儲存在雲端服務中的資料備份。
- 為重要資料進行備份至公司，即使服務供應商暫時(例如網絡發生故障)或永久不能提供服務，有關資料仍可供使用。

個人用戶在雲端平台上保護其資料的備忘事項

服務條款及保安和私隱政策

- 個人用戶須閱讀服務供應商的服務條款及保安和私隱政策，並應注意：
  - 資料是如何儲存及受到保護；
  - 如何舉報保安事故；以及
  - 如何終止服務，以及在終止服務後如何處理仍然保留在相關雲端平台上的資料。
- 如不同意服務條款和政策，可以不使用有關服務。應留意服務條款和政策定期作出的修訂。

資料保護

- 審慎考慮是否必需把敏感資料儲存於雲端平台上，並評估這些資料一旦披露所造成的影響。
- 避免在不確定對方身分的情況下分享資料，做法如下：
  - 如用戶擬透過雲端平台上與他人分享敏感資料，應確保只有指定收件人才可存取；
  - 確保任何運行於用戶裝置用作接達雲端服務的應用程式，只可把有關裝置與雲端平台之間的許可資料同步；以及
  - 檢查使用中的檔案或文件夾的預設存取權限是否合適。例如，一個預先安裝的“圖片”文件夾可能被預設為開放任由他人存取，這種設定不利於資料保護。
- 為重要資料進行備份至公司，即使服務供應商暫時（例如網絡發生故障）或永久不能提供服務，有關資料仍可供使用。
- 透過以下途徑確保服務供應商令資料得以保密：
  - 使用加密功能（例如保密插口層(SSL)）以傳送資料；以及
  - 當儲存資料時，使用加密功能。（如供應商沒有提供加密功能，用戶應自行為資料加密，然後才儲存在雲端平台上，並須安全保管加密密碼匙。）

登入帳戶保安[2]

- 帳戶應使用難被猜中的登入密碼。
- 不同的帳戶應使用不同的登入密碼。
- 透過下列方法保護用戶名稱及密碼：
  - 放在安全的地方；
  - 避免與他人分享；
  - 關閉瀏覽器和應用程式的密碼儲存功能；以及
  - 避免以純文字方式把密碼儲存於裝置上。
- 確保以上保安措施實施在任何運行於電腦或流動裝置上用作接達雲端服務的應用程式，亦實施以上保安措施。
- 當完成工作後，登出雲端服務。

存取裝置保安[3]

- 只使用可信靠的存取裝置接達雲端服務。切勿使用公用電腦處理雲端平台上的敏感資料。
- 保護存取裝置免被他人擅用。
- 啟動電腦或流動裝置的屏幕鎖定功能。
- 切勿破解存取裝置（即移除生產商所設定的使用和存取限制）。
- 定期為電腦及流動裝置的操作系統、瀏覽器和電腦應用程式進行更新和安裝最新的保安修補程式。
- 小心謹慎瀏覽互聯網，特別不要點擊來歷不明的連結。

參考資料

1. 參考 http://www.pcpd.org.hk/chinese/ordinance/ordglance1.html#dataprotect
   有關《個人資料(私隱)條例》的保障資料原則
2. 參考 http://www.infosec.gov.hk/tc_chi/yourself/account.html
   有關帳戶及密碼的處理
3. 參考 http://www.infosec.gov.hk/tc_chi/virus/geninfo_common.html
   有關保護你的電腦從而更有效地對抗電腦病毒與惡意程式碼攻擊的最佳作業實務

「雲資訊網」是一站式入門網站，由雲端運算服務和標準專家小組建立，方便市民和企業（特別是中小企）有效取得有關雲端運算技術的資訊和資源。該網站提供用例、相關指引和良好作業模式，讓市民和企業在採用雲端運算模式時達到預期效益。

雲端運算服務和標準專家小組由香港特區政府屬下的政府資訊科技總監辦公室成立，透過廣納業界、學術界、專業團體及政府的專業知識，推動香港雲端運算的應用和發展，以及促進本港雲端運算專家彼此交流及與內地專家互相交流。雲端保安及私隱工作小組是一個在專家小組轄下設立的工作小組。

此文件由雲端保安及私隱工作小組發表，載述了有關雲端保安及私隱的良好作業模式和指引。工作小組成員透過通力合作，制訂有關措施，以推動並促進本地業界，更廣泛應用雲端運算和安全使用雲端服務。