Complete Security

信賴帶來力量

- 強大的企業安全框架可以降低風險、遵循現代最佳作法，並以全球性的規模進行運營
- 涵蓋資訊安全管理的所有面向，包含企業持續營運、災難恢復、廠商管理、事故管理、運用第三方滲透測試進行弱點管理，以及與專屬資料隱私專員一同進行的資訊隱私計畫
- 由全球跨國客戶與第三方針對安全性與合規性定期稽核

資訊安全團隊

我們擁有專屬的全球資訊安全團隊，具備超過 100 年以上的業界經驗，以及專業的資訊安全認證，包含 ISO 27001, ISO 10012, CBCP, CISSP, CISA, CISM, CEH, GCIH, GCIA, GAWN, GPE, GXPN, GSEC, GREM, GCC, GNFA, SSCP, CAPM, GSE, OSCP, GPEN, 以及 GWAPT.

資料中心

實體安全性的多個層級，包含保全、相機與生物辨識，限制我們機構的人員進出。

- 拉斯維加斯
- 多倫多
- 倫敦
- 法蘭克福
- 巴黎
- 蘇黎世
- 香港
- 上海
- 東京

為了提供安全的客戶體驗，以符合我們全球客戶所需，Consilio 投資並部署了強大的全球企業安全框架，與採用的技術、基礎架構與團隊進行完全整合。

Consilio 安全性認證

我們的電子蒐證解決方案完整套件實際位於經過認證的安全資料中心。

- 經 ISO/IEC 27001:2013 認證
- 經 HITRUST 認證
- 符合 ITAR 規範
- 經 Cyber Essentials Plus 認證
- 符合 GDPR 規範
- 符合 CCPA 規範
- 符合歐盟-美國與瑞士-美國的隱私護盾原則*

安全性重點

- 機構已獲得 ISO 27001/SAS 70 或 Type II/SSAE 16 認證，並受全天候保護措施、警報裝置、動作偵測、生物識別、防盜門與上鎖的鐵欄所保護
- 環境控制可保護資料中心免受火災、水災或自然災害的破壞
- 在每個地理區之中，災難恢復機構中都具備近乎即時的資料複製功能
- 使用嚴格的最低權限原則控制資料中心、網路與系統的存取
- 所有資料按照客戶與專案，以有邏輯的方式區分
- 靜態資料：AES-XTS 256 位元加密
- 傳輸中資料：僅有 TLS 1.2 與 1.3，以及對稱加密演算法的 128 位元/256 位元密碼
- 多層級、多廠商，且額外涵蓋範圍不包含 MITRE ATT&CK 框架的重疊安全模型
- 雇用前的背景查核與保密協議
- 年度員工安全訓練，以及持續舉辦的網路釣魚意識測試
- 運用強化遠端使用者安全的多重要素驗證，來保護虛擬文件審閱的基礎架構

即使歐盟不再使用隱私護盾原則，美國商務部仍要求美國的實體遵循該原則的規範。請查閱 privacyshield.gov 中的常見問答集。

Consilio
法律諮詢與服務的全球領導者
hk.consilio.com

Consilio
hk.consilio.com

Consilio 提供電子蒐證、文件審閱、風險管理以及法律諮詢服務。我們協助跨國法律公司與企業運用合法與合規的產業專業知識與專門工具。Consilio 的 Complete Security 套件包含合格的安全專家團隊遵循經認證的最佳作法。

規則： Consilio 經 ISO/IEC 27001:2013 標準認證，並且符合其極為嚴格的要求，能夠妥善處理敏感資料。Consilio 所有的設備共管資料中心皆由 ISO 27001 或 SOC 2 Type 2 認證。Consilio 遵循 ITAR 規範、歐盟-美國與瑞士-美國的《隱私護盾原則》（在美國仍適用）、歐盟的《一般資料保護規範》(GDPR)、《加州消費者隱私保護法》(CCPA)，以及其他許多在全球流通的資料隱私規則。Consilio 目前正在進行取得 2021 年 HITRUST 認證的流程，我們也已經與 HITRUST 的廠商一同完成差距評估的階段。

資訊安全計畫與政策： 如 ISO 27001 認證所要求，Consilio 提供全面且首要的安全政策與程序，在全球據點為我們的安全性態勢標準化。企業資訊安全政策與程序由管理階層謹慎審閱，並提供給 Consilio 的員工。政策與程序經由 Consilio 的資訊安全控管委員會 (ISGC) 核可，傳達給所有員工，並且每年進行審閱。我們的政策確保所有儲存於 Consilio 的資料，處理方式皆按照當地的資料保護規則，並且也遵循世界各地不同據點的不同法規與契約要求。內部與外部人員，包含 ISO 的稽核人員，會定期監控並稽核是否遵循這些要求。

我們的認證要求政策涵蓋所有安全領域，與我們保護的資料相關聯，包含風險管理、事故管理、廠商管理、災難恢復/企業持續營運、網路安全、存取控制、人力資源安全、評估管理、變更管理等等。

資訊安全架構 Consilio 的首席資訊安全人員帶領我們的高品質資訊安全團隊，負責管理機構的所有安全性活動。在資訊安全團隊之中，又細分為不同的小隊，專門負責安全營運、合規性與風險等內容。我們也與第三方安全管理提供者合作，獲得進階的安全功能，而我們的員工也會依照歐盟規範，針對與歐盟相關的合法及合規考量，提供額外的專業知識。Consilio ISGC 同樣也監督並支援資訊安全倡議，團隊包含來自多個 Consilio 單位的管理人員。ISGC 團隊兩年進行一次會議，以審閱並稽核 Consilio 的資訊安全性態勢。

廠商風險管理： 風險管理是 Consilio 在安全相關全面性作法的其中一環。我們所有廠商作為 Consilio 的廠商管理計畫的其中一部分，都必須經過審查，確保不會為 Consilio 或我們的客戶帶來非必要的安全風險。Consilio 災難恢復的稽查與企業持續營運的計畫會按照預約的時程定期舉行。Consilio 的全球資訊安全團隊負責進行內部稽查。資料備份會持續不斷更新，並且儲存於我們的次要資料中心內，該中心與主要的資訊中心距離遙遠。

網路安全： Consilio 的運算網路具有非軍事區 (DMZ) 與多個防火牆，將網路可存取的區域以及敏感資料的儲存位置進行區分。我們的網路具備極嚴格防火牆、第三方監控服務、入侵檢測與預防軟體、防毒軟體，及嚴謹存取控制政策的保護。使用者許可流程遵循最低權限原則，而每個網路區塊的存取都必須取得相應機關的正式授權。IT 基礎架構的變更遵循正式的變更管理流程。軟體漏洞會定期且及時修補，在執行之前須通過正式審閱與核可。

資料儲存： 所有客戶的資料與 Consilio 企業的資料，皆以實體且有邏輯的方式區分，而客戶資料也會依照客戶與專案區分。資料儲存的時間長度是依照客戶合約而定，而專案終止時，Consilio 會依照適當的資料銷毀政策來處理資料。在銷毀資料前，正式的資料銷毀或形式轉變都須經客戶簽名同意，而在資料銷毀之後，Consilio 會提供資料銷毀的認證。

資產管理： 所有設備皆透過 Consilio 的資產管理政策進行追蹤與控管。對於所有客戶的設備與媒體，均遵循文件的監管鏈與控制。客戶的媒體內容儲存在受保護且上鎖的區域，只有獲得授權的資料管理人員可以存取。

認證與合規

Consilio 經 ISO/IEC 27001:2013 標準認證，並且符合其極為嚴格的要求，能夠妥善處理敏感資料。Consilio 所有的設備共管資料中心皆由 ISO 27001 或 SOC 2 Type 2 認證。Consilio 遵循 ITAR 規範、歐盟-美國與瑞士-美國的《隱私護盾原則》* (在美國仍適用)、歐盟的《一般資料保護規範》(GDPR)、《加州消費者隱私保護法》(CCPA)，以及其他許多在全球流通的資料隱私規則。Consilio 目前正在取得 HITRUST 的認證，我們也已經與 HITRUST 的廠商一同完成差距評估的階段。我們預期於 2021 年完成 HITRUST 認證。

*請注意：即使歐洲聯盟法院判定歐盟-美國隱私護盾框架無效，Consilio 仍會在原框架適用的時機點，持續實踐所有與隱私相關的契約要求。若建立有新的適用規則取代隱私護盾框架，Consilio 會遵循所有適用的法規。

隱私

Consilio 的隱私政策與作法遵循國際資訊安全最佳作法，且通常表現更佳。我們的企業隱私架構與政策，依據每個專案與資料的地點判斷，確保我們符合國際與當地隱私規則要求。其包含的法規如：GDPR、HIPAA、ITAR、CCPA 以及其他類似的規範。

合格的資料隱私專員監管我們隱私標準的執行狀況。Consilio 的資訊分類政策確保所有資料根據敏感度區分，受到妥善的保護。客戶的資料存取限制永遠遵循客戶的要求，且符合當地法規與客戶合約要求。

實體安全

Consilio 的設備共管資料中心經 ISO 27001:2013 標準認證，或已經完成 SOC 2 Type 2 保證的稽核 (依據中心的地點有所不同)。Consilio 在世界各地的多個地點皆設有設備共管資料中心，可以處理我們客戶在當地的資料安全要求。Consilio 和設備共管資料中心的營運廠商一同執行嚴格的契約及保密協議，確保資料與設備的安全性與機密性。

在資料中心中執行嚴格的實體與邏輯控制，確保 Consilio 的資產與其他存放於資料中心裡的資產確實做出區隔，而其他客戶的資產也與其他資產妥善區分。Consilio 的伺服器在設備共管機構之中，存放於專屬的 Consilio IT 設備鐵籠中，與外界區隔，唯有獲得認證的 Consilio IT 團隊員工，才能實際進入伺服器所在的區域。Consilio 資訊中心伺服器室的任何進出活動都存有紀錄，也可以追蹤。攝影機會持續紀錄建築與周邊區域的實體活動，而監視器也安裝於多個地點。

在設備共管資料中心機構衡量的實體安全性包括：

- 周邊區域的安全，包含柵欄與大門。
- 全天候待命的保全人員。
- 設施與設備室的大門會控制進出，門鎖由密碼鎖與生物辨識系統鎖定。
- 在資料中心之中，Consilio 的 IT 設備單獨放至在架上的上鎖鐵籠裡。
- 閉路電視監視器與影片片段的儲存備份。
- 訪客管理流程將會：
  - 禁止未經授權的人員進入資料中心。
  - 要求訪客預先經過核可，並且在進入資料中心時由經過授權的人員陪同。
- 環境控制如不斷電系統 (UPS)、空氣調節系統 (HVAC)、制火系統與備用發電機。

資料安全

Consilio 的客戶資料處理政策確保資料與裝置獲得安全儲存，並且在 Consilio 的保管之下，防止未經授權的存取。所有客戶的資料均為機密，不論該資料含有個人可識別資訊 (PII)、受保護健康資訊 (PHI) 或僅是非公開的資訊，均是如此。

實體且符合邏輯的安全性管理包含嚴格的認證控制、高強度密碼、資料區隔、客戶資料與其他機構資料的區隔，以及根據最低權限原則的角色存取權。同意存取客戶專案資料的內部程序，根據 Consilio 與客戶企業互動的獨特性質、客戶的合約要求、符合當地法規，以及對於特定狀況的安全性考量，都會有所不同。客戶資料的存取權只會開放給獲得合理授權，且須申請存取權以履行工作職責的員工。客戶對於資料與專案存取權的開放對象擁有完整的決定權。

安全資料處理政策會在電子蒐證專案的完整生命週期中全程執行，包含：維護資料的有效監管鏈，直到將資料歸還給客戶或銷毀資料為止。專案開始時，Consilio 會收集資料、執行資料擷取、在我們專屬的系統中處理，並且在 Consilio 或客戶的監管之下，於安全裝置進行文件審閱。專案結束後，客戶可以決定要求歸還資料或銷毀資料 (包含實體媒體資料)，銷毀後會提供證明。技術、運作與管理控制皆已部署，確保在資料生命週期之中遵守資料安全的要求。

Consilio 並不會混合客戶的資料。我們在安全技術基礎架構中，建立專屬於特定客戶與專案的虛擬伺服器。我們只會依循客戶合約中的時間長度儲存客戶資料，接著會銷毀資料，或將資料歸還給客戶，一切依照客戶指示進行。

網路安全

所有網路可存取的系統，皆存放於安全防火牆後的非軍事區 (DMZ) 網路之中。所有的客戶資料存放於另一相似防火牆後的安全網路之中。兩個防火牆都設定為僅允許極少數的存取。來自網路的流量並不允許直接進入安全網路。這些網路之間的通訊傳播使用 256 位元 SSL 加密技術進行加密，保證沒有資料 (包含登入憑證) 會以無加密的方式，透過公用網路傳輸。

Consilio 的網路安全控制包含以下內容：

1. 所有連結網路的地點皆受防火牆、入侵偵測與預防系統 (IDS/IPS) 基礎架構的保護，而安全資訊與事件管理 (SIEM) 軟體則以完全額外的設定進行部署。所有進入或離開 Consilio 網路的流量皆須穿過受控制的安全進入點。

2. 網路安全協定如 BGP、MPLS 與 IPSec 皆已啟用，確保網路流量安全穿過 Consilio 的網路、伺服器，以及終端使用者的位置。Consilio 針對網路/網路服務、資料庫以及儲存活動，將網路與伺服器層級設備的系統做出區隔。

3. 高強度的驗證控制 (如高強度密碼、多重要素驗證、資料區段劃分，及以角色為基礎的存取) 皆於 Consilio 的網路環境中執行，確保妥善控制客戶資料的存取。內部認證是針對 Active Directory LDAP 伺服器來執行。

    1. 所有使用者務必使用獨特的用戶名稱與高強度的密碼。

    2. Consilio 使用第三方工具，針對 Active Directory 的帳號遵守密碼政策。第一次使用時，務必變更或移除廠商預設的密碼/帳號。

4. Consilio 使用標準加密技術演算法，包括 AES、3DES、RSA 與 IDEA 來保護靜態資料 (AES-XTS 256 位元認證加密技術) 以及傳輸中資料 (僅有 TLS 1.2 與 1.3 以及對稱加密技術演算法的 128 位元/256 位元密碼)。每個 Mozilla 的中繼相容性標準皆有設定密碼套件。

5. 為確保未使用的端口維持鎖定，而連接的字串僅在已知的伺服器與服務中建立，Consilio 的所有系統皆依據 Consilio 的基線加強政策進行加強。

6. 所有 Consilio 的伺服器與工作站皆已核可安裝防毒與防惡意軟體。進階的端點威脅偵測軟體與行動裝置管理解決方案在所有 Consilio 的端點上執行。

7. 在生產環境中執行之前，所有與資訊科技及應用發展相關的變更，都會妥善審閱與授權。
8. 應用、網路弱點評估與滲透測試會定期執行。內部與外部弱點掃描與滲透測試由值得信賴的第三方團隊每兩年執行一次，並且由內部團隊更頻繁地進行。
9. Consilio 的軟體發展生命週期包含安全發展框架。發展、測試與生產環境皆進行區隔，以確保我們系統與資料的安全與完整。

文件審閱

Consilio 透過我們的安全虛擬審閱 (SVR) 平台，提供現場與遠端的安全文件審閱服務。Consilio 文件審閱專案的所有使用者 (不論是在現場或遠端都務必經由 Consilio 的安全虛擬環境認證，該環境運用嚴格的安全控制，在自己的網路設定中區隔：

- 文件審閱系統在區隔的 VLAN 環境中執行。
- 審核機構提供可靠的鎖定精簡型客戶系統，設定為僅允許專為該文件審閱專案設定的軟體公共設施使用。
- Consilio 可靠的文件審閱系統限制網路內容、影印與電子郵件能力，遵循客戶專案的規格。
- Consilio 可靠的文件審閱系統不允許使用 Wi-Fi、即時訊息工具、可移除的媒體硬碟或印表機存取，除非專案客戶有特別要求，或是安全虛擬審閱所需要。
- 以使用者為主的團隊存取政策套用於文件審閱者帳號，限制僅有已經認證的文件審閱系統可以存取。
- 以角色為主的存取控制政策套用於文件審閱者，若客戶要求，也會提供多重要素認證。

員工

Consilio 的所有員工與承包商在受僱之前，都需要完成背景篩選的手續。Consilio 的員工必須要：

- 在入職時簽署保密與機密協議。
- 在入職時與每一年都需要完成資訊安全意識訓練。
- 同意遵循 Consilio 的安全性政策。
- 維持與工作職責相關聯的訓練。
- 在受僱過程中，符合職位的資格要求，並且具有適合的學歷。

Consilio
hk.consilio.com

廠商風險管理

Consilio 的廠商風險評估政策要求 Consilio 的廠商與第三方供應商在開始和 Consilio 合作之前，需要通過適當的審查與核可，並且定期接受 Consilio 的安全性稽核。Consilio 與廠商的合約協議包含機密性條款，保護 Consilio 與客戶的資訊。Consilio 至少每年執行一次廠商風險評估。

Consilio 也監控廠商出現的供應鏈弱點，並且在發現新問題時持續追蹤廠商狀況。

事故管理

Consilio 的事故管理政策確保我們採取積極措施，以預防並報告安全性事故，並且降低影響。Consilio 依據客戶合約要求的時間範圍，揭露任何包含客戶資料的事故。視情況而定，Consilio 的事故回應程序也涵蓋內部的升級協定，包含升級的流程，以及針對管理階層、客戶與外部管理機構的通知。

Consilio 的事故回應團隊由全天候運行的安全營運廠商支援，因此可以針對緊急狀況立刻行動。在發現潛在的事故後，廠商可以立即區隔有問題的端點/使用者，以便預防事故的影響擴散至可能受波及的端點。

災難恢復與企業持續營運

Consilio 的災難恢復與企業持續營運政策要求 Consilio 為災難情境做出準備，這些災難可能會中斷我們的資料中心或辦公室的業務運作。計畫涵蓋的狀況包含自然災害、疫情狀況、公用措施中斷使用、員工資源短缺，以及其他可能會影響人力或企業資源的情形。

Consilio 的災難恢復計畫涵蓋災難後的最初回應與評估階段，包含與員工和客戶的動員和溝通、服務的恢復、正常運作的認證、業務的重新開始、過渡期的運作，並且回歸正常運作。Consilio 的災難恢復與企業持續營運計畫處理相關的風險管理、法規與規範要求，以及在災後重新開始服務客戶的方式。

Consilio 的文件恢復時間目標在各個 IT 評估與應用中都不相同。特定應用、資料或專案的特定恢復時間目標，可以透過 Consilio 客戶服務代表，依據個別專案來取得。所有資產與應用的恢復時間目標會進行紀錄與追蹤，且會在 Consilio 的年度災害恢復與企業持續營運測試中進行考核。

資料備份

Consilio 的資料備份政策要求我們執行資料複製的合併、每日遞增的備份，以及每週針對重要資料的完整備份。Consilio 首要與次要的資料中心機構之間的距離至少有 25 英里，確保萬一其中一個中心發生災害，也不會影響到另一個次要中心的營運。

PM.FS0134.HK.20220524