安全管理規範(113.01 版)

1 資安環境

1.1 資安認證標準

1.1.1 本公司已通過並持續維護 ISO 27001 認證，其認證範圍涵蓋運算雲。

1.2 資安作業原則

1.2.1 運算雲開發、維運之資訊安全相關作業，遵循公司資安相關作業規範與程序。

1.2.2 如因內、外部或其他標準要求，於遵循公司管理原則下，將另訂細部作業規範，以符合作業需求。

1.3 風險管理

1.3.1 運算雲之資訊資產，如因應內、外部或其他標準要求，得依據「弱點威脅模板 - 雲端版」進行雲端風險評鑑，並記錄於「資訊資產清冊 - 雲端版」。

1.3.2 如因管理需求，雲端風險評鑑可另訂風險可接受等級，但風險可接受等級，不得超過公司資訊安全委員會決議之風險可接受等級。

1.4 稽核活動

1.4.1 本公司對運算雲之稽核準則，包含資訊安全管理制度所有正式文件、ISO27001 國際標準、雲端認證標準（如：「資訊安全稽核查驗表 - 雲端版」)、相關內部管理規範與外部法令法規。

1.5 實體及環境安全

1.5.1 機房內之重要設備設置具有即時告警功能之環境監控系統，具有 7*24 小時值班人員與網管中心，該系統定期檢測，以確保系統運作可靠度。

1.5.2 機房與各安全區域由管理權責單位依屬性制訂設備安置與保護管理作業規定，以符合實體與環境安全管理要求。

1.6 合規性

1.6.1 針對所提供的雲端服務之合規性，運算雲已取得 ISO27001、ISO27017、ISO27018、CSA 及 PIMS 等國際標準認證，用戶如有其他需要協助的部分，可洽詢專屬業務人員或撥打全天 24 小時免費服務專線 0809-000-809。

2 安全管理事項

2.1 資訊安全政策

2.1.1 雲服務之規劃、建置、審查及持續改善，基於雲服務特有安全風險，參考國際標準規範與實務準則，強化相關安全管控機制，以降低雲服務安全風險。管理事項包含如下：

2.1.1.1 適用於雲服務設計與建置的資安基準要求。

2.1.1.1.1 本公司已通過並持續維護 ISO 27001 認證，其認證範圍涵蓋運算雲。

2.1.1.1.2 運算雲服務位於台灣固網通過 ISO 27001/27011 資安國際認證的雲端機房，實體層安全有保障。並且通過 ISO 27017、ISO 27018 及 CSA 的雲端安全認證。

2.1.1.2 內部人員風險、存取控制與保護雲服務客戶資料。

2.1.1.2.1 所有與運算雲服務設計、規劃、建置、運維等相關內部人員，皆於人力任用時即告知應負的法律責任與義務。

2.1.1.2.2 相關內部人員均了解並簽署保密切結文件，以對機密性與敏感性資料的控管。

2.1.1.2.3　每年依人力資源單位規劃、執行雲服務安全管理相關課程，以提升並確保相關人員具備所需之能力。

2.1.1.2.4　內部人員對相關系統資訊存取，以最小權限、最少資訊為原則，並以帳號申請與角色分類控管權限。

2.1.1.2.5　平台運維人員僅限定特定人員可註冊申請平台系統存取權限，非必要之人員不得提出需求。

2.1.1.3　多租戶雲服務之間隔離。

2.1.1.3.1　運算雲服務為多租戶公有雲平台，每一租戶皆可享有獨立虛擬化使用空間，於部署 VM 服務和使用時，不與其他租戶間的服務資源互相影響。

2.1.1.4　與雲服務客戶的溝通。

2.1.1.4.1　運算雲服務如需進行平台優化、異動調整等可能影響服務時，將主動提前通知用戶。

2.1.1.4.2　變更管理前後或變更期間，用戶皆可透過全天 24 小時免費服務專線 0809-000809 由專人為您處理運算雲服務任何相關問題。

2.1.1.5　虛擬化安全。

2.1.1.5.1　運算雲服務位於台灣固網通過 ISO 27001/27011 資安國際認證的雲端機房，實體層安全有保障。並且通過 ISO 27017、ISO 27018 及 CSA 的雲端安全認證。

2.1.1.5.2　於網路層，客戶需自行設定防火牆，以確保您的資訊安全。此外，客戶亦可透過 SSH 或是 VPN 加密連線至您的 VM 進行管理，以確保連線安全。

2.1.1.5.3　運算雲服務提供客戶透過實體電路走 Private VLAN 連線至 VM，我們亦提供各類實體電路連線之管道；詳情請洽台灣大哥大商務服務客服專線 0809-000809 或您的直銷業務。

2.1.1.6　雲服務客戶帳戶的生命週期管理。

2.1.1.6.1　請參閱運算雲服務契約「租用與終止」章節。

2.1.1.7　溝通違規行為與資訊共享指引，以幫助調查與取證。

2.1.1.7.1　請參閱運算雲服務操作手冊「使用明細說明」章節，運算雲平台提供所有申裝資源的新增、異動、退租等所有操作時間歷史紀錄。

2.1.1.7.2　運算雲為保障平台服務安全性，針對用戶於平台上的介面操作行為予以進行紀錄。

2.1.1.7.3　上述紀錄保存期間皆依內部安全管理規範進行留存。

2.2　資產管理

2.2.1 為確保資料安全，依據運算雲架構，鑑別運算雲重要資料，並評估其風險，以進行適當管控，針對以下資料或介面存取，優先採加密或其他安全方式處理。

2.2.1.1　客戶使用介面連線。

2.2.1.2　系統管理介面連線。

2.2.1.3　維運機敏資料。

2.2.1.3.1　架構圖。

2.2.1.3.2　Data flow 流程圖。

2.2.1.3.3　文件內容超過運算雲平台 IP 相關訊息大於等於 10 筆。

2.3 設備安全汰除或再使用管理

2.3.1 運算雲設備中，須報廢之儲存媒體依據其機密等級，需進行銷磁、低階格式化、清除資料或進行實體破壞，確保資料已被銷毀。

2.3.2 設備與媒體（含紙本與電子媒體）進行銷毀時，於專人監督下進行銷毀。若需外送銷毀時，將由簽訂保密同意書之合格廠商處理。相關銷毀記錄及廠商簽訂之保密協定需留存備查，公司內資訊安全官可視需要進行抽檢。

2.3.3 協助運送銷毀媒體之廠商則需與本公司簽訂保密協定，嚴禁銷毀媒體內之資訊外洩。

2.4 資源容量管理

2.4.1 運算雲服務具備內部維運監控系統，監控平台資源使用率，以確保有足夠可用資源能提供予客戶使用。

2.4.2 運算雲服務平台資源容量監控系統具備告警水位，到達設定水位時，運算雲平台維運將啟動容量擴容程序，以避免資源可用容量短缺導致客戶服務受影響的情形發生。

2.5 密碼管理

2.5.1 運算雲之網站憑證，使用 2048 位元以上之加密安全金鑰 SSL 憑證，憑證簽章演算法為 SHA256RSA，且提供 TLS1.2 高安全性之傳輸通道，以確保資料在網路傳輸過程中的安全性。

2.5.2 運算雲之客戶使用金鑰管理，請詳參【運算雲操作手冊】之 VPN 管理功能章節。

2.5.3 運算雲使用者於首次登入時，提供一次性簡訊驗證，以強化使用者管理身分安全性。另於往後每次登入使用者管理中心時，可選擇透過多因子驗證(multi-factor authentication)發送簡訊認證碼至使用者綁定手機號碼，始得登入使用。

2.6 運作安全

2.6.1 運算雲與內部系統之介接，經由需求單位提出申請經核准後，始可提供必要資料交換。

2.6.2 為確保運算雲互通性和可攜性，客戶可登入雲平台自行下載客戶所屬之虛擬機映像檔，操作步驟可詳參【運算雲操作手冊】。

2.6.3 禁止使用自攜式設備進行運算雲之維運管理，僅允許透過公司資安政策管理作業規範內之加密外部連線方式。

2.7 系統獲取、開發及維護

2.7.1 如需變更運算雲入口網站程式，需提出申請，經核准後，系統開發單位依據申請內容，進行程式開發作業，待測試完成後，由運算雲維運單位進行上線程序。

2.7.2 運算雲之系統獲取、開發及維護，得參考安全標準(如：OWASP)，與設計、開發、上線與測試時納入考量，以降低資安風險。

2.8 供應者關係

2.8.1 運算雲之委外廠商，執行委外作業時，如接觸公司密級(含以上)資料，每年對廠商進行資安抽查（如：廠商保密切結、廠商資安教育訓練等）。

2.8.2 運算雲之委外廠商服務內容，得依專案需要進行審查，審查項目可包括技術能力、規格滿足度、交付時程符合度及保密作業之遵循等。

2.9 資訊安全事故管理

2.9.1 運算雲如遇障礙，將依據障礙通報流程，通知受影響客戶，並協助客戶因應，以降低影響與衝擊。

2.9.2 運算雲如遇資訊安全事件，經查明確認且問題發生之責任歸屬於本公司，本公司應於 24

小時內通知客戶，通知時間不包含不可控之因素，如火災、風災、地震、戰爭、政治、國際傳染疫情等。

2.9.3 運算雲如遇資訊安全事件且影響至客戶時，得向客戶提供以下文件：

2.9.3.1 資訊安全事件的影響範圍。

2.9.3.2 檢測資訊安全事件的影響程度。

2.9.3.3 發生資訊安全事件的時間範圍。

2.9.3.4 資訊安全事件通知程序。

2.9.3.5 處理與資訊安全事件有關的問題的聯繫資訊。

2.9.3.6 發生資訊安全事件時可能適用的任何補救措施。

2.9.4 當重大資安事件發生需對外說明時，本公司資訊安全委員會視需要主動指派專人向主管機關陳報，並協助公司發言人對外說明情況與處置方式。

2.9.5 用戶如遇資訊安全相關事件時，亦可主動透過全天 24 小時免費服務專線 0809-000809 由專人為您處理運算雲服務相關問題。

2.10 營運持續管理之資訊安全層面

2.10.1 針對運算雲所提供之服務，依據「營運流程衝擊分析表」中之適用評估項目，進行營運衝擊分析，以判別關鍵營運流程。

2.10.2 依據營運流程衝擊分析判斷營運流程與其相關之重要資訊資產對運算雲營運的衝擊程度，並考量其影響與最大可容忍中斷時間。

2.10.3 運算雲營運持續計畫之判定、發展及維護包含以下三個主要事項：

2.10.3.1 依據關鍵營運作業流程，分析可能導致營運中斷之潛在威脅，並評估其發生之

可能性。

2.10.3.2 分析評估關鍵營運流程中斷時，可能發生之財務與商譽損失，並研判關鍵營運流程之最大容忍中斷時間。

2.10.3.3 就衝擊分析之結果，考量成本效益因素，進行因應方案之可行性分析，再根據評估結果，制定營運持續計畫與啟動時機。

2.11 遵循性

2.11.1 運算雲服務營運及儲存地點均建置於中華民國境內，地點範圍受本國司法管轄，適用中華民國法律，為自營服務，安置於自有機房，未使用其他雲服務或場所。

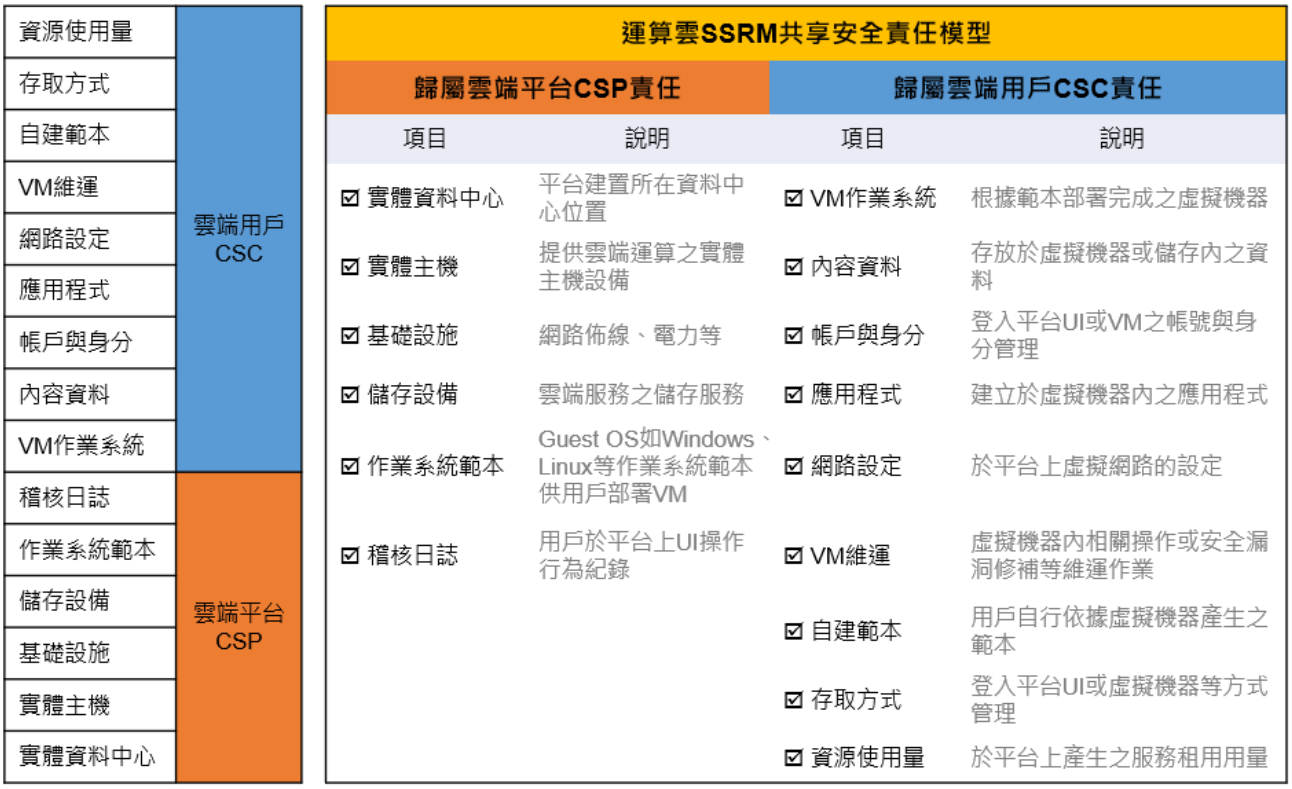
2.11.2 為確保服務品質與客戶權益，運算雲之服務契約具有版本控制，並每年進行審查內容適切性。

3 共享安全責任模型

3.1 台灣大哥大運算雲為 IaaS 服務型態，本服務提供虛擬化環境及其基礎設施，如作業系統範本、用戶管理中心、維持雲服務相關之實體伺服器、實體網路基礎設施、儲存設備及所在機房實體安全。

3.2 用戶透過用戶管理中心所租用之虛擬主機、安裝於虛擬機內的作業系統層更新及漏洞修補、其他應用程式及資料、運營之業務合規性及資訊安全為用戶負責。

3.3 以下圖表定義雲端服務於雲端提供商和客戶之間如何共享責任：



3.4 如上圖所示，雲端提供商須對基礎網路和基礎架構負責，用戶則須對存取政策和資料安全負責。