



文件編號	ISMS-M-003	文件名稱	雲端服務資通安全管理政策		
機密等級	一般	版 次	V1.0	頁次	1 / 8

管理系統文件

文 件 類 別	第 一 階 文 件
文 件 編 號	ISMS-M-003
文 件 名 稱	雲端服務資通安全管理政策
發 行 單 位	誠雲科技股份有限公司
發 行 日 期	114 年 06 月 01 日
版 次	V1.0

[illegible]

文件編號	ISMS-M-003	文件名稱	雲端服務資通安全管理政策		
機密等級	一般	版 次	V1.0	頁次	3 / 8

1. 目的

1.1 雲端服務採用對應的安全控制政策，目的在提高對雲端服務中託管「客戶資訊」在機密性、完整性和可用性的保護，以降低任何未經授權的處理活動（例如資料丟失或非法破壞）的影響；並要求所有相關人員（包括員工、承包商和臨時員工）遵守本政策及其它服務規範內資訊安全實作要求，以持續改進、強化和落實各項安全管控。

1.2 雲端服務按照符合 ISO/IEC 27001、ISO/IEC 27017 及 ISO/IEC 27018 資訊安全、網宇安全及隱私保護之資訊、雲端安全及雲端隱私控制措施運行，建立全面的控制措施並管理適用於本公司所提供之雲端服務的安全領域以及客戶對雲端服務的使用，採用全面的資訊安全方法，實施多層防禦安全策略，其中網路、作業系統、資料庫和軟體安全實作通過完善的內部控制、治理和監督。

1.3 對於允許客戶配置安全狀況的雲端服務，除非另有說明，否則客戶負責配置、運作、維護和保護這些非本公司提供的雲端服務（包括您的資料）的作業系統和其他關聯軟體。客戶有責任維護自己的資料的適當安全、保護和備份，其中可能包括使用加密措施保護資料免受未經授權的存取和對日常儲存檔案的技術，

2. 安全管理政策及措施

2.1 資訊安全策略

資訊安全策略建立並管理適用於提供之雲端服務和客戶雲端服務使用的安全區域，員工必須遵守公司資訊安全政策以及管理其委外提供服務的任何其他政策，考慮風險因素（包括網路和安全因素）的各項文件化規範，並有效執行管控措施，確保託管客戶雲端服務中資訊的機密性、完整性、隱私性、連續性和可用性，通過有效的安全管理執行和控制，每年由資訊安全暨個人資料保護推動委員會進行審核，並根據需要進行更新。

2.2 實體安全防護(本項不適用於自行提供實體環境及設備之客戶)

採取的措施在防止未經授權的人員存取託管客戶資訊的實體設施，例如使用安全人員、保護建築物和指定的資料中心場所，本公司管理的辦公地點和雲基礎設施受到保護，另外要求供應商使用類似的

文件編號	ISMS-M-003	文件名稱	雲端服務資通安全管理政策		
機密等級	一般	版 次	V1.0	頁次	4 / 8

安全設施來託管客戶的資訊，相關措施：

2.2.1 實體環境及設施存取需要授權並受到監控。

2.2.2 所有員工、分包商和授權訪客在現場時必須明顯佩戴官方身份證明。

2.2.3 訪客必須註冊，並且必須由本公司人員陪同進入設施。

2.2.4 監控鑰匙/門禁卡的擁有情況以及存取實體位置的能力，離職員工必須歸還鑰匙/卡。

2.3 系統存取控制：

應採用多因子認證進行身份驗證、授權控制和存取日誌記錄等控制措施。授權存取客戶資訊人員對雲網路的所有遠端存取，均利用多因子認證的虛擬專用網路來限制。並在授予人員存取雲網路的許可權之前，執行設備組態檢查並進行適當的控制，例如利用跳板主機，禁止（通過策略和技術控制）使用個人設備存取雲網路及雲端服務。

2.4 資料存取控制：

對於管理的服務元件，客戶資料的存取權限僅限於獲得授權的員工，對於存取雲端服務的人員（包括駐留在雲端服務中客戶的資料），實施基於角色的存取控制（RBAC）並採用「需要知道」、「最低權限」和「職責分離」的存取管理原則和措施，供客戶管控使用者對雲端服務及資料的存取。

2.5 外部連接的用戶加密：

通過所提供的安全通訊協定存取雲端服務，如果通過啟用傳輸層安全性（TLS）的連接進行存取，則該連接將協定為 SHA256 位加密，TLS 已部署的所有基於 Web 的應用程式實施或組態，建議使用最新的可用瀏覽器來連接到雲端服務，每個雲端服務版本的推薦瀏覽器清單將透過存取的入口或在雲端服務的相應服務描述中提供，當客戶使用與雲端服務集成的第三方網站（例如社交媒體服務）可能不接受加密連接，對於允許與第三方網站建立 HTTP 連接的雲端服務，除了 HTTPS 連接之外，將啟用此類 HTTP 連接。

2.6 輸入控制

客戶應負責相關輸入控制事項，並自行管理。

文件編號	ISMS-M-003	文件名稱	雲端服務資通安全管理政策		
機密等級	一般	版 次	V1.0	頁次	5 / 8

2.7 資料和網路隔離

客戶資料透過帳號分權方式進行邏輯隔離，確保各客戶僅能存取其授權範圍內的資料與資源。雲端服務平台使用權限控管與身分驗證機制，避免未授權存取其他客戶資料。所有雲端環境亦與本公司內部企業網路分離，確保營運網路與雲端資源之安全隔離。

2.8 保密和訓練

所有員工受保密協議的約束，並在進入公司時完成資訊安全訓練，並根據適用的安全和隱私政策定期完成訓練。

2.9 資產管理

遵循資產的管理程序，定期審查和授權，並維護資產清單，客戶所控制、使用雲端服務或與整合的資產應由客戶負責，包含確定資料的適當資訊分類，以及雲端服務提供的記錄控制是否適合。

2.10 軟體安全性保證

執行軟體安全性保證，在產品的設計、構建、測試和維護中構建安全性的方法，無論這些產品是客戶在本地使用還是經由雲端服務交付。

2.11 安全日誌

記錄作業系統、應用程式、資料庫和網路設備上的部分與安全相關的活動，系統配置為記錄預設安全活動、對資訊或程式的存取、系統事件（如警告、主控台事件和系統錯誤），定期審查安全日誌以進行安全事件調查，識別出的異常活動將回饋到安全事件管理流程中，安全日誌以原生、未更改的格式存儲在安全資訊和事件管理系統（或等效系統）中，並根據內部規範進行保留，安全日誌保留至少 1 年，保留日誌並將其用於內部安全運營作業。

2.12 其他與客戶安全相關的義務

2.12.1 實施整合安全、運營政策、標準和程序規範。

2.12.2 執行完整性和安全性檢查，例如在將資料和文件導入或上傳到雲端服務之前掃描其漏洞、病毒和惡意軟體，以及設定和管理雲端

文件編號	ISMS-M-003	文件名稱	雲端服務資通安全管理政策		
機密等級	一般	版 次	V1.0	頁次	6 / 8

服務環境。

2.12.3 根據策略和安全實施維護自行管理的帳戶。

2.13 內部安全審查和執行

採用內部流程來定期測試、評估、評估和維護本政策中描述的技術和組織安全措施的有效性。

2.14 外部稽核

定期委請第三方進行資訊安全及雲端服務控制措施之稽核（任何此類稽核的範圍可能因服務和國家/地區而異），並視情況進行其他獨立的第三方安全測試，以審查管理和技術控制的有效性。

3. 變更管理

3.1 對雲端硬體基礎設施、作業軟體、產品軟體以及作為雲端服務的一部分提供的支援應用程式軟體進行更改，維護雲端服務的運營穩定性、可用性、安全性、性能和流通性，客戶同意向本公司提供所有資訊、存取許可權和合作，並採取合理必要的措施，使本公司能夠實施和維護雲端服務機制，遵循正式的變更管理程式來審查、測試和核准變更。

3.2 通過變更管理程式進行的變更包括系統和服務維護活動、升級和更新以及客戶特定的變更，變更管理目的在於在最大限度地減少實施變更期間的服務中斷。

3.3 為可能需要雲端服務在維護期間不可用的變更保留特定的維護期，致力於確保在計劃的維護期間（將提前發出通知）執行變更管理程序，同時考慮低流量時段和地理要求，對於特定於客戶的更改和升級，將在可行的情況下與客戶協調維護期。

3.4 對於預期會導致服務中斷的更改，計劃維護期的持續時間不包括在服務可用性級別的每月測量週期內的計劃外停機分鐘數的計算中（請參閱服務級別協定），會盡業務上合理的努力來最大限度地減少計劃維護的使用，並最大限度地減少導致服務中斷的維護期的持續時間。

文件編號	ISMS-M-003	文件名稱	雲端服務資通安全管理政策		
機密等級	一般	版 次	V1.0	頁次	7 / 8

3.5 對於客戶能夠執行維護活動的雲端服務，客戶應負責設定和維護作系統和其他關聯軟體。

3.6 客戶在使用雲端服務時，需負責妥善管理其帳戶密碼、確保上傳資料的合法與安全、即時通報資安事件，並遵守相關法規與合約義務。

4. 支援服務政策：本政策中描述的支援僅適用於基本雲端服務，並且由本公司根據客戶訂單作為此類服務的一部分提供，本公司可能會提供其他支援服務產品，客戶可以訂購這些服務，但需要支付額外費用

4.1 一般服務：

4.1.1 費用：客戶訂單中將描述本公司支援服務所收取的費用，若需其他支援服務產品，客戶可以訂購這些服務，但需要支付額外費用。

4.1.2 支援期限：雲端服務開始之日提供，並在服務到期或終止時結束（支援期），本公司在支援期結束後不再提供本政策中所述的支援。

4.1.3 技術聯繫人：客戶技術聯繫人是與本公司之間單一的聯絡窗口，負責聯繫協調雲端服務的支援服務，技術聯繫人必須至少接受過初始基本服務培訓，並根據需要接受過適合特定角色或實施階段、專業服務/產品使用和遷移的補充培訓；技術聯繫人必須瞭解雲端服務，以幫助解決系統問題並說明本公司分析和解決服務請求；提交服務請求時，技術聯繫人應該對所遇到的問題有基本的了解，並且能夠重現問題，以說明相關診斷和分類問題；為避免雲端服務的支援中斷，技術聯繫人職責轉移給其他人時，客戶必須通知本公司。

4.2 支援內容：

4.2.1 診斷雲端服務的問題。

4.2.2 解決雲端服務中報告和可驗證的錯誤而做出的合理商業努力，以便雲端服務在所有重大方面都按照相關服務規範中所述運行。

4.2.3 在客戶訂閱期間，本公司於周一至周五 08:30~17:30，透過以下方式提供技術支援：

4.2.3.1 Line 官方帳號：客戶可以透過 line 官方帳號聯繫本公司。

文件編號	ISMS-M-003	文件名稱	雲端服務資通安全管理政策		
機密等級	一般	版 次	V1.0	頁次	8 / 8

4.2.3.2 聯絡電話：04-2359-8490

4.2.3.3 聯絡 E-mail：winvans@cmetech.com.tw

5. 雲端服務暫停和終止策略

5.1 在雲端服務服務協議期限結束後的 3 個月內，仍應將資料保留在雲端服務中，並保持服務系統的可存取性，以便檢索資料。除非雲端服務合約協議和所適用的服務規範的條款中另有規範，應於服務期限結束時，應主動告知客戶使用此類服務的權利將過期。

5.2 對於免費試用版和試用期，將在試用期結束後不再提供內容檢索，在此檢索期間，雲端服務等級協定不適用，並且服務系統不得用於任何新的活動。

5.3 在前述試用檢索期之後，本公司沒有義務保留客戶資料，將依既有規範資料刪除銷毀。

5.4 客戶需要協助來獲取存取權或索取副本時，可在本公司所提供支援服務渠道中提出服務請求。

5.5 停機或維護將提前於雲端服務官方網站上發布公告，並發送郵件通知客戶。

6. 本政策經資訊安全長核准，於公告日施行，並以書面、電子或其他方式通知本公司所屬職員及與本公司連線作業之有關機關（構）、委外廠商，修正時亦同。