[中文譯本僅供參酌。若中、英文版本間有任何歧異，應以英文為準。]

APEX 資訊安全性措施附錄

APEX 服務託管於您的場所或主機託管站點上，並且通常不涉及在受 Dell 管理之資料中心的伺服器上託管客戶內容，因此這些服務採用共同承擔安全性責任模型，您和 Dell 在此模型中各自承擔一定的責任。適用的服務產品說明中訂明了您的責任。

Dell 已實施並將維持以下針對 APEX 服務的企業安全性措施。這些措施，連同適用的服務產品說明中所述的安全性措施，是 Dell 對 APEX 服務安全性所承擔的唯一責任。除非本文件中另有定義，否則本文件中使用的所有詞彙均具有 APEX 協議中為其賦予的含義。

職能	措施
資訊安全性計畫	Dell 已實施並將維護資訊安全性計畫 (包括採用內部政策和標準)，旨在： (a) 就用於提供 APEX 服務的 Dell 企業資料中心、伺服器、網路設備、防火牆和主機軟體系統 (下稱「**Dell 網路**」) 的任何部分，識別可合理預見的安全性風險 (如果有)，以及 (b) 用商業上合理的努力，以 Dell 認為適當的方式，減輕已識別的 Dell 網路安全性風險，包括執行定期風險評估和測試。 Dell 已任命一名或多名安全性專員負責協調、監控和執行資訊安全性計畫。 Dell 將持續進行一項威脅和漏洞管理計畫，以持續監控 Dell 網路中的漏洞。用於識別漏洞的來源/方法有許多種，其中可能包括供應商、安全性研究人員、漏洞掃描、紅隊演練、滲透測試和員工報告。公開發佈的第三方漏洞會接受有關 Dell 環境中適用性的審查。漏洞掃描和評估是在 Dell 的應用程式基礎結構上例行和定期執行的。這些流程旨在實現對漏洞的主動識別和補救，並支援 Dell 的合規和法規要求。
安全開發生命週期和漏洞回應	Dell 已實施並維護安全開發生命週期計畫，以定義必須採取的步驟，來幫助確保其產品在具有已定義安全開發生命週期的正式管制計畫結構下，得到適當評估、開發和封裝。此計畫連同 Dell 的資訊安全性計畫，有助於解決 APEX 系統整個開發和維護生命週期的安全性問題。Dell 採用嚴格的流程來持續評估和改進其安全開發和漏洞回應做法，並且 Dell 定期將這些做法與行業標準做法對照。 在調查和驗證 APEX 系統中報告的漏洞後，Dell 將根據 Dell 發佈的漏洞回應政策 (目前位於 https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy) 嘗試確定、開發和約束適當的救濟措施。 Dell 透過安全性公告向其客戶傳達救濟措施 (如適用)。Dell 努力在商業上合理的時間內提供救濟措施 (如適用)。回應時間表將取決於許多因素，例如：嚴重性、救濟措施的複雜性或受影響的元件。
資產管理	Dell 追蹤和管理 Dell 網路的實體和邏輯資產。Dell 可能追蹤的資產及可能實施的控制措施範例包括：

	(a) 軟體資產，如應用程式和系統軟體， (b) 實體資產，如伺服器、桌上型電腦/筆記型電腦、備份/封存磁帶、印表機和通訊設備，以及 (c) 資訊資產，如資料庫、災難回復計畫、業務持續性計畫、資料分類和封存資訊。 Dell 根據業務關鍵性和/或資料分類敏感性對資產進行分類。此類分類可使對此等資產的存取受到適當的限制。
人力資源安全性	作為僱傭流程的一部分，Dell 員工必須在受聘時簽署保密契約，並遵循和依照適用法律接受檢測程序。儘管 Dell 保留自行決定審查其政策和實施人員安全性的權利，但根據現行政策並遵照當地法律和當地可用性，Dell 會進行以下一項或多項就業檢測：藥物篩檢、社會保障追蹤、刑事犯罪記錄搜尋、教育和就業驗證，以及就業資格驗證。Dell 努力達到 Dell 所在行業同類公司的當前行業標準，但 Dell 無法為滿足特定客戶的特定期望而相應調整其人員安全性或檢測流程。 第三方或外部約聘人員會經由 Dell 按照合約條件進行檢測，或由約聘人員按照 Dell 批准的檢測流程進行驗證。 Dell 維持一套紀律程序，對不遵守其資訊安全性計畫要求的人員採取行動，包括但不限於為滿足安全性、可用性和保密性承諾和要求而實施相應紀律程序。 Dell 為所有適用人員提供年度安全性意識教育訓練，並要求適用的分包商為其人員提供此類教育訓練。
實體安全性	Dell 維護相關政策和控制措施，限制只有授權人員可進出 Dell 網路實體組件所在場域，以防止未經授權進入場域。 Dell 網路實體組件所在的場域 (例如資料中心) 採用基於風險的控制措施。進出控制措施可能包括保全人員、安全性記錄、監控、警報、限制進出安全區域、進出路徑保護、視訊監控、鑰匙卡和/或雙重因素驗證。 此規定適用於 Dell 管理的主機託管站點。
網路安全性	Dell 可根據需要以電子方式存取 Dell 網路以提供 APEX 服務。Dell 將維護各政策和存取控制措施，以管理允許從每個連線對 Dell 網路存取的權限，包括使用防火牆和身份驗證控制措施。 Dell 透過實施基於風險的控制措施，防止 Dell 網路中對資產的惡意使用以及惡意軟體。此類控制措施可能包括但不限於：安全性政策；限制性存取控制措施；分隔開發和測試環境；在伺服器、桌上型電腦和筆記型電腦上進行的惡意軟體偵測；電子郵件附件惡意軟體掃描；系統合規掃描；入侵防禦監控和回應；記錄和提醒重大可疑事件；基於資料類型、電子商務應用程式和網路安全性的資訊處理程序；使用外部資產；以及系統和應用程式漏洞掃描。 Dell 要求根據其資訊安全性計畫，在需要時對傳輸中和待用資料進行加密。在透過開放網路遠程存取客戶系統時，Dell 採用加密技術和適當的通訊協定 (例

	如 TLS)。Dell 將其非使用中的加密金鑰儲存在經過批准的解決方案中，這類解決方案旨在提供獲行業接納的金鑰管理做法。
存取控制	Dell 實施適當的存取控制措施，旨在防止未經授權存取 Dell 網路。為降低有意或無意濫用的風險，存取按照「最低權限」和「須知」的原則受到控制。Dell 可能使用的存取控制措施包括審查存取、維護服務帳戶及對應用程式的特殊權限存取、在系統級別設定存取，以及產生存取相關報告。 Dell 利用行業標準做法來識別和驗證 Dell 網路使用者，這些做法包括雙因素驗證 (如適用)。Dell 要求在整個 Dell 網路中使用高強度密碼。Dell (a) 禁止 Dell 網路使用者在任何系統上共享、寫下、透過電子郵件傳送、以即時訊息發出或儲存未加密的密碼，並且 (b) 在連續多次輸入錯誤密碼的嘗試後鎖定帳戶。 Dell 利用行業標準做法來加強存取控制措施，包括： (a) 處於閒置時，使用者工作階段會自動逾時， (b) 需要驗證身份和輸入密碼才能重新開啟， (c) 透過獲接納的行業標準防火牆防止外部存取，並且防火牆與網際網路的連線 (如適用) 由 VPN 連線保護； (d) 視情況在顯示或輸入密碼時加上遮罩；以及 (e) 傳輸時採用適當的行業標準密碼加密技術。
事件管理	Dell 利用事件回應框架來準備、應對、管理安全性事件並將其影響降至最低。此框架包括發生安全性事件時應遵循的程序，當中涉及： (a) 一個內部事件回應團隊，其中設一名回應負責人； (b) 一個調查團隊，負責分析根本原因並確定受影響的各方； (c) 內部報告和通知程序； (d) 記錄應對行動和補救計畫；和 (e)事件事後審查。
業務持續性管理	Dell 維護業務持續性計畫 (下稱「**BCP**」)，以便在合理可行的情況下盡快從業務中斷的狀況中恢復，並繼續正常的業務營運。如果出現對您的 APEX 服務產生重大影響的業務中斷，Dell 將根據情況作出合理且及時的努力，來嘗試與您聯繫。