[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。]

Dell APEX 合作夥伴資料處理補充協議

本協議之 Dell APEX 合作夥伴資料處理補充協議 (下稱「**合作夥伴 DPA**」) 適用於協議雙方在履行其義務時交換個人資料的情況，包括 Dell 根據本協議提供服務 (下稱「**服務**」) 時。若本合作夥伴 DPA 和協議相牴觸，則就本補充協議標的事項應以本合作夥伴 DPA 為準。

1. 定義。

此處未定義的術語將採用協議中規定的含義。本合作夥伴 DPA 中的下列詞語具有以下含義：

1.1 「協議」係指 Dell APEX 經銷商協議、Dell APEX 代理商協議，或 Dell 在提供服務時所依據之實質相近似之協議。

1.2 「控制者」係指單獨或與他人共同決定個人資料處理目的和方式的實體。

1.3 「GDPR」係指《一般資料保護規則》(EU) 2016/679。

1.4 「示範條款」的含義如下 (如適用)：

(i) 當從歐洲經濟區 (下稱「**EEA**」) 傳輸至第三國時，係指個人資料傳輸的標準合約條款 (歐盟第 2021/914 號決議)，含其可能不時的修訂或替換；

(ii) 當從英國 (下稱「**英國**」) 傳輸至不受 UK GDPR 適足性認定約束的國家/地區時，係指適用於國際資料傳輸之歐盟委員會標準合約條款的國際資料傳輸附錄或國際資料傳輸協議，均根據《2018 年資料保護法》第 119A 條發布；或

(iii) 當從瑞士傳輸至第三國時，係指個人資料傳輸的標準合約條款 (歐盟第 2021/914 號決議)，含其可能不時的修改或替換，並根據《瑞士聯邦資料保護法》(根據瑞士聯邦資料保護與資訊委員會於 2021 年 8 月 27 日公布之修正案) 進行特別修改以供使用。

1.5 「個人資料」係指凡雙方在履行協議時處理的資訊，且該資訊與已識別或可識別自然人有關或為隱私權法律所定義之「個人資料」或「個人資訊」。

1.6 「個人資料違規」係指導致意外或非法破壞、遺失、變更、未經授權揭露或存取根據本合作夥伴 DPA 處理之個人資料的安全漏洞。

1.7 「隱私權法律」係指協議一方受其約束且適用於所提供之服務的任何資料保護和隱私權法律，包括適用的 GDPR、UK GDPR、加州消費者隱私保護法 (下稱「CCPA」) 和其他類似法律。

1.8 「處理」係指對個人資料或個人資料集合執行的任何操作或操作集合，無論是否透過自動方式，例如蒐集、記錄、組織、構建、儲存、改編或變更、擷取、諮詢、使用、透過傳輸揭露、散布，或以其他方式提供、調整或組合、限制、刪除或銷毀。

1.9 「處理者」係指代表控制者處理個人資料的實體。

1.10 「出售」或「銷售」係指企業以口頭、書面、電子或其他方式，向另一企業或第三方出售、出租、發布、揭露、散布、提供、轉讓，或以其他方式交流消費者的個人資訊，以獲取金錢或任何其他非金錢的有價對價。「銷售」不包括揭露控制者為履行雙方就本協議之義務，而共用個人資料或將個人資料傳輸給接收控制者。

1.11 「轉包處理者」係指為了根據本合作夥伴 DPA 處理個人資料，受任何一方聘請擔任處理者的第三方 (包括但不限於關聯公司及/或分包商)。

1.12 「UK GDPR」係指在英國退出歐盟後根據英國國內法保留的 GDPR，搭配《2018 年英國資料保護法》一起解釋，含其可能不時的修訂。

2. 法規遵循

雙方同意遵守本協議所預期關係適用的所有相關隱私權法律規定的各自義務，並僅在遵守適用的隱私權法律的情況下處理個人資料。在向他方揭露、傳輸或以其他方式提供個人資料前，各方均有責任遵守有關個人資料處理合法性的隱私權法律，且應已獲得向他方揭露個人資料所需的所有權利和授權，包括但不限於發出適當的通知，並在必要時獲得資料主體的同意 (根據隱私權法律) 揭露其與協議相關的個人資料。

3. 控制者對控制者

若作為控制者之一方 (下稱「揭露控制者」) 向他方揭露個人資料，以便同樣以控制者的身分 (下稱「接收控制者」) 進行處理，則將適用以下義務：

3.1 除非雙方另有書面約定，否則接收控制者將僅為履行其在協議中的義務，並根據適用的隱私權法律處理個人資料。除非隱私權法律明確允許，否則接收控制者不得為任何活動或目的處理個人資料；

3.2 僅出於履行其在協議項下義務之目的，將個人資料提供予接收控制者。除依本協議履行服務而於協議約定的款項外，對於存取或以其他方式處理個人資料，揭露控制者不提供任何金錢或其他非金錢的有價對價；

3.3 若揭露控制者出於讓接收控制者傳送行銷通訊之目的揭露個人資料，則揭露控制者同意獲得相關資料主體的事前同意，以便接收控制者進行此類揭露和使用；

3.4 各方應及時履行其義務，回應資料主體的請求，根據隱私權法律行使其對個人資料的相關權利 (包括其撤回同意、存取、限制、更正、刪除和攜帶的權利)。接收控制者將及時處理來自揭露控制者或資料主體與個人資料相關的所有合理詢問，包括請求存取或更正個人資料，以及有關接收控制者的作法、程序及/或投訴流程的資訊；

3.5 關於根據本協議處理的個人資料，若一方收到第三方 (包括資料保護監管機構) 的請求或通知或法院命令，則應立即通知他方，提供所有相關細節。雙方應合理地相互合作以回應此類請求或通知。除非法律要求且按照他方書面指示進行，否則任一方均不得代表他方回應任何請求或通知；

3.6 若發生與本協議有關的個人資料違規，發生個人資料違規的一方應在知悉後立即通知他方。各方應相互合作，並協助他方處理、減輕及/或解決個人資料違規。雙方應在相互商議後，遵守隱私權法律規定的所有適用義務，通知相關監管機構及/或資料主體；

3.7 若依協議目的或適用法律另有規定而不再需要保留個人資料，則接收控制者應在協議終止後刪除及/或銷毀個人資料；

3.8 接收控制者不得：(i) 出售任何個人資料；(ii) 出於履行本協議義務之特定目的以外的任何目的保留、使用或揭露個人資料，包括但不限於出於履行本協議義務以外之商業目的保留、使用或揭露個人資料；及 (iii) 在揭露控制者和接收控制者間直接業務關係以外保留、使用或揭露個人資料；以及

3.9 接收控制者聲明並保證，其瞭解本合作夥伴 DPA 中概述關於個人資料使用以及所有其他處理活動和相關目的的禁止事項與限制 (尤其是第 3.8 節)，並將遵守這些規定。

4. 控制者對處理者

若作為控制者之一方向他方揭露個人資料，以便代表其作為處理者或轉包處理者進行處理，則作為處理者或轉包處理者之一方應：

4.1 除非適用法律要求，否則僅可依照控制者的指示處理個人資料。本合作夥伴 DPA 中未包含的額外或替代處理指示必須由雙方書面同意，包括遵守此類指示的相關費用 (若有)。任一方均不負責確定控制者的指示是否符合適用法律。但是，若任何一方認為控制者指示違反適用的隱私權法律，則該方應在合理可行的情況下盡快通知他方，且無須遵守

此類違法指示。處理協議事項的詳細資訊、持續時間、性質和目的，以及個人資料和資料主體的類型，悉如本協議和附件二中所述；

4.2 僅在履行協議義務所必要的範圍內處理控制者提供的個人資料；

4.3 除非必要且僅用於以下目的，否則不得向第三方 (關聯公司或轉包處理者除外) 揭露個人資料：

(a) 遵守控制者的指示；

(b) 遵守本合作夥伴 DPA；或

(c) 遵守法律或政府機構具有約束力的命令。除非違反法律或政府機構具有約束力的命令，否則處理者將通知控制者本條款提及的法律要求或命令；

4.4 於知悉個人資料違規後，(i) 不無故拖延並及時 (任何情形下均應在 72 小時內) 通知控制者；(ii) 在處理者當時已知或可得之範圍內，提供個人資料違規的書面詳細資訊；(iii) 盡合理努力協助他方在可能的情況下減輕個人資料違規的不利影響；以及 (iv) 在發生此類個人資料違規時，實施隱私權法律要求的所有措施；

4.5 根據合理的事先書面請求，向控制者提供根據適用法律可能合理必要的資訊，以證明處理者遵守本合作夥伴 DPA；

4.6 經合理的事前通知，向控制者提供合理要求的協助，以在隱私權法律要求的範圍內，就該方作為處理者對個人資料之處理行為，進行資料保護影響評估及/或事先商議；

4.7 及時通知控制者，並與控制者合作解決個人或相關資料保護主管機關提出且與根據協議處理個人資料有關的請求，包括依據相關隱私權法律尋求行使權利之人的請求。除非法律強制要求，否則未經控制者事前授權，處理者不得直接回覆此類通訊；

4.8 在協議到期或終止時，或由控制者選擇 (可能以書面形式要求)，在合理可行的情況下盡快刪除所有個人資料，或將所有個人資料返還予控制者，但是，若適用法律要求處理者保留副本時，除適用法律要求的範圍外，處理者將限制和保護該個人資料免於進一步處理；

4.9 若任一方在 CCPA 範圍內處理個人資料，則該方應僅能代表他方處理個人資料，並且，除本合作夥伴 DPA、協議規定之目的以及 CCPA 或任何後續法律允許之目的外，不得出於任何目的保留、使用、共用或揭露該個人資料。在任何情況下，任一方均不得與第三方共用任何個人資料 (根據後述第 5 條與轉包處理者分享者除外) 或出售任何個人資料。各方聲明其知悉並將遵守對其個人資料處理的所有限制，包括避免可能導致他方被視為是 CCPA 所謂出售個人資料或個人資訊的任何行為。就本段而言，此處的處理者將被視為 CCPA 第 1798.140(v) 節中定義的服務提供者；以及

4.10 經他方合理的事前書面請求 (即根據本協議條款提出此類請求)，提供合理必要的資訊，以證明遵守本合作夥伴 DPA 規定的處理者義務，並允許和協助稽核，包括由他方或該方授權其他稽核員進行的查核。

5. 轉包處理者。

5.1 轉包處理者之使用。

任一方均可以(並取得他方之一般同意)使用轉包處理者，雙方可指定和使用轉包處理者來處理與協議所規定之服務相關的個人資料，前提是在任何情況下，應就每個轉包處理者提供的服務與該轉包處理者簽訂相關的書面合約，並且據該合約，轉包處理者應 (i) 充分保證會實施適當的技術和組織措施，以及 (ii) 遵守與本合作夥伴 DPA 賦予 Dell 的權利和/或義務實質上相似的條款。轉包處理者可能包括第三方或一方的關聯公司。若轉包處理者未能履行上述規定的資料保護義務，則聘請該轉包處理者的相關處理者應對他方承擔履行該轉包處理者義務的責任。

5.2 轉包處理者清單。

Dell 為支援其服務提供而任用的轉包處理者清單已由 Dell 提供於 www.dell.com/subprocessors。

6. 安全性。

6.1 技術和組織安全性措施。

各方將確保其已採取適當的技術和組織措施，以合理地確保處理個人資料所涉及的處理系統和服務的安全性、機密性、完整性、可用性和復原能力與此類個人資料相關的風險相稱，並防止個人資料違規。雙方同意，附件一 (下稱「**資訊安全性措施**」) 中描述的技術和組織安全性措施，為保護個人資料提供適當的安全層級，以滿足本合作夥伴 DPA 的要求。各方將定期 (i) 測試和監控其保障措施、控制措施、系統和程序的有效性，以及 (ii) 識別可合理預見的個人資料安全性、機密性和完整性的內部和外部風險，並確保解決這些風險。

6.2 技術進步

資訊安全性措施受技術進步和發展的影響，且 Dell 得修改這些措施，前提是對於根據協議處理的個人資料而言此類修改不會降低其整體安全性。

6.3 存取權。

雙方應確保授權存取個人資料的人員 (包括關聯公司或授權的轉包處理者) 負有保密義務，並將尊重和維護個人資料的機密性和安全性，並已承諾保密或承擔適當的法定保密義務。

7. 國際傳輸。

雙方均獲授權，於根據本合作夥伴 DPA 處理個人資料時，或在正常業務過程中，在全球範圍內將個人資料傳輸給各自的關聯公司和/或轉包處理者。在進行此類傳輸時，各方應確保採取適當的保護措施，以保護根據本協議傳輸或與本協議相關的個人資料。若雙方履行本協議義務涉及將個人資料從歐洲經濟區 (下稱「EEA」) 或英國或瑞士轉移至 EEA 或英國或瑞士以外的國家/地區 (不受隱私權法律規定之適用性認定約束)，雙方同意將使用示範條款，以及根據適用的隱私權法律的適當補充措施或其他適當資料傳輸機制，尤其是，此類傳輸應遵守：(a) 各方與其可能存取個人資料的關聯公司簽訂的集團內部協議，且該協議應納入相關示範條款；以及 (b) 各方均與其轉包處理者簽訂的協議，且酌情納入相關示範條款。若協議雙方在根據協議履行義務時牽涉到跨越其他國際邊界傳輸個人資料，並且需要根據適用的隱私權法律建立一個或多個額外的個人資料傳輸合規機制，則雙方同意將根據隱私權法律和/或相關的資料隱私權監管機構的規定，使用適當的合約條款或其他指定的機制和/或措施，確保跨國際邊界傳輸個人資料的合規性。

8. 存續。

各方在本合作夥伴 DPA 下的義務，於合作夥伴 DPA 和協議終止後繼續有效，且只要該個人資料繼續由接收控制者持有或控制，即繼續有效。

附件一

資訊安全性措施

Dell 非常重視資訊安全性。此資訊安全性概述適用於保護 Dell 集團公司間處理和傳輸個人資料的 Dell 企業控制措施。Dell 的資訊安全性計畫讓員工能夠瞭解其職責。有些客戶解決方案可能有替代的保護措施，此等措施將概述於與每位客戶商定的工作聲明中。

安全性實踐

Dell 實施了企業資訊安全性實踐和標準，旨在保護 Dell 企業環境和解決：(1) 資訊安全性；(2) 系統和資產管理；(3) 開發；以及 (4) 治理。這些實踐和標準由 Dell 資訊長核准，並每年進行一次正式審查。

組織安全性

組織中的每個人均有責任遵守這些實踐和標準。為了促進企業遵守這些實踐和標準，資訊安全性的職能會提供：

1. 對各項政策/標準和法規的策略和法規遵循性、意識和教育、風險評估和管理、合約安全性要求管理、應用程式和基礎結構諮詢、保證測試，並推動公司的安全指引。
2. 安全性解決方案的安全性測試、設計和實施，以確保在整個環境中均採用安全性控制措施。
3. 實施安全性解決方案、環境和資產的安全性作業，並管理事故應對。
4. 安全性作業、法律、資料保護和調查人力資源的取證調查，包括電子蒐證 (eDiscovery) 和電子取證 (eForensics)。

資產分類與管控

Dell 的作法是追蹤和管理實體和邏輯資產。Dell IT 可能追蹤的資產範例包括：

- 資訊資產，如已識別的資料庫、災難回復計畫、業務持續性計畫、資料分類、封存的資訊。
- 軟體資產，如已識別的應用程式和系統軟體。
- 實體資產，如已識別的伺服器、桌上型電腦/筆記型電腦、備份/封存磁帶、印表機和通訊設備。

根據業務重要性分類資產，以確定機密性要求。處理個人資料的業界規範提供了技術、組織和實體保障的框架。這些可能包括存取管理、加密、記錄和監控以及資料銷毀等控制措施。

人員安全性

在聘雇流程中，員工要接受適用於當地法律的審查程序。Dell 的年度法規遵循教育訓練包含要求員工完成線上課程，並通過涵蓋資訊安全性和資料隱私權的評估。安全意識計畫亦可能提供某些工作職能專用的資料。

實體和環境安全性

Dell 在其實體安全性計畫中使用多種技術和操作方法來降低風險。保安團隊與每個據點密切合作，以確定是否確實執行適當的措施，並持續監控實體基礎結構、業務和已知威脅的任何變化。同時亦監控業界同行所使用的最佳實踐措施，並謹慎選擇既能滿足業務實踐的獨特性又能滿足 Dell 整體期望的方法。

Dell 透過考慮包括體系架構、操作和系統在內的控制元素來平衡其安全性方法。

通訊和營運管理

IT 組織透過集中的變更管理計畫，管理對公司基礎結構、系統和應用程式的變更，其中可能包括測試、業務影響分析和管理核准 (如適用)。

具有針對安全和資料保護事故的事故應對程序，其中可能包括事故分析、遏制、應對、補救、報告和恢復正常運作。

為了防止惡意使用資產和惡意軟體，可以根據風險實施額外的控制。此類控制可能包括但不限於資訊安全性實踐和標準；限制存取；指定的開發和測試環境；伺服器、桌上型電腦和筆記型電腦上的病毒偵測；電子郵件附件病毒掃描；系統法規遵循性掃描；入侵防禦監控和應對；記錄和提醒關鍵事件；根據資料類型、電子商務應用程式和網路安全性的資訊處理程序；以及系統和應用程式漏洞掃描。

存取控制

根據不同程序，限制對公司系統的存取，以確保有適當的核准。為了降低蓄意或其他濫用的風險，會根據職責分離和最低權限提供存取權限。

遠端存取和無線運算能力受到限制，並要求同時具備使用者和系統的安全措施。

集中蒐集來自關鍵裝置和系統的特定事件記錄檔，並在異常情況下通報，以啟用事故應對和取證調查。

系統開發與維護

審查公開發布的第三方漏洞在 Dell 環境中的適用性。根據對 Dell 企業和客戶的風險，有預先確定的補救時限。此外，根據風險，亦針對全新和關鍵的應用程式和基礎結構進行漏洞掃描和評估。在生產前的開發環境中使用程式碼檢閱和掃描程式，以根據風險主動地偵測編碼漏洞。這些流程可以主動識別漏洞和法規遵循性。

法規遵循

資訊安全、法律、隱私權和法規遵循部門致力於確定適用於 Dell 公司的地區法律和法規。這些要求涵蓋公司和我們客戶的智慧財產權、軟體授權、員工和客戶個人資訊保護、資料保護和資料處理程序、跨境資料傳輸、財務和營運程序、與技術相關的監管出口管制，以及取證要求等領域。

如資訊安全性計畫、隱私管理委員會、內部和外部稽核/評估、內部和外部法律顧問諮詢、內部控制評估、內部滲透測試和漏洞評估、合約管理、安全意識、安全諮詢、政策例外審查等機制和風險管理相結合，共同推動遵循這些要求。

附件二
資料處理說明

1. 處理主題和持續時間。

處理主題和持續時間均應依據本協議。

2. 處理目的。

處理個人資料係出於履行本協議義務之目的。

3. 處理性質。

個人資料將依要求處理，以滿足雙方於本協議的義務。

4. 資料主體類別。

資料主體是雙方的最終使用者、員工、承包商、供應商，以及與本協議雙方關係有關的其他第三方。

5. 個人資料類型。

可能提交的個人資料類型有：

- 聯絡方式：可能包括姓名、地址、電子郵件地址、電話和其他聯絡方式。
- 最終客戶的詳細資訊：可能包括聯絡方式、發票和信用相關資料。
- IT 系統和運作資訊：可能包括個人識別碼、語音、影片和資料記錄、使用者 ID 和密碼詳細資料、電腦名稱、電子郵件地址、網域名稱、使用者名稱、密碼、IP 位址、權限資料 (根據工作職能)、通訊服務的帳戶和授權資訊、個別信箱和目錄、聊天通訊資料、軟體和硬體清單、有關軟體和網際網路使用模式的追蹤資訊 (例如 cookie)，以及為運作及/或教育訓練目的而記錄的資訊。
- 資料主體的電子郵件內容和流量/傳輸資料；線上互動和語音通訊 (例如部落格、聊天、網路攝影機和網路工作階段)；支援服務 (附隨性存取可能包括存取電子郵件通訊的內容，以及與傳送、路由和交付電子郵件相關的資料)。
- 其他：一方向他方提交的任何其他個人資料。