以下翻譯僅供參考。若本翻譯版本與最後更新的英文版本之間有歧異、不一致或衝突（包括因翻譯延遲所造成者），則應以英文版本為準。

本政策內容得依下列規定進行變更。依需要儲存此版本之副本以供內部記錄使用。

AMAZON 供應商安全性政策

最後更新日期：2024 年 9 月 11 日

1. 範圍。供應商須遵守這些安全性要求（下稱「安全性政策」）。 本安全性政策不會限制供應商的任何其他合約或法律義務。若本安全性政策與供應商和 Amazon 簽訂的其他協議之間有所衝突，供應商須遵守加強保護 Amazon 資訊的更嚴格的要求。供應商與 Amazon 之間的其他協議中提及第三方安全性要求的地方，均應視為引用本安全性政策。

2. 更新。

2.1 Amazon 可能不時對本安全性政策進行商業上合理之更新，該更新內容將於本安全性政策「最後更新日期」後 30 天生效。供應商同意在更新生效後遵守更新後的安全性政策。

2.2 若供應商希望在更新生效前事先收到更新通知，則供應商得使用本安全性政策網頁上所提供之訂閱表單進行訂閱，以便接收更新通知。供應商須確保為接收訂閱更新通知而提供的所有供應商聯絡資訊隨時保持最新狀態且準確。透過電子郵件傳送更新通知時，無論供應商是否實際收到該更新通知，均視為已收到更新通知。

3. 許可用途。

3.1 **明確授權。**供應商僅可處理本協議明確授權的 Amazon 資訊，且僅限用於按照本協議提供產品或服務之用途（下稱「許可用途」）。

3.2 **資料保留**。供應商僅可基於許可用途以及在必要期間內保留 Amazon 資訊。

3.3 **明確限制**。供應商不會以其他方式：(a) 處理任何 Amazon 資訊，即使該資訊已匿名化；(b) 轉讓、租賃、交換、交易、銷售、借出、出租或以其他方式向任何第三方散佈或提供任何 Amazon 資訊，即使該資訊已匿名化；或 (c) 使用 Amazon 資訊開發、訓練或改善任何人工智慧 (AI) 或機器學習 (ML) 模型，即使該資訊已匿名化。

4. 最低安全性要求。供應商須維持符合產業最佳實務之實體、管理和技術保護措施（包括國際標準化組織（以下簡稱「ISO」）標準 27001 和 27002、國家標準和技術研究所（以下簡稱「NIST」）網路安全架構或其他
類似標準）。供應商維持之保護措施須包括以下第 4.1 至 4.18 節所述之最低要求。

4.1 **成文的資訊安全計劃**。供應商須具備成文的資訊安全計劃，該計劃：(a) 包括符合本安全性政策所述要求之適當政策、程序和標準；(b) 指定負責溝通和管理安全性問題（包括安全性事件）之安全聯絡人；(c) 至少每年審核一次且視需要更新；及 (d) 適用的工作人員。供應商須監控及執行其資訊安全計劃及處理違規行為。

4.2 **修補程式管理**。供應商須利用最新的升級、更新、錯誤修正和新版本維持所管控的資訊系統之最新狀態。供應商須針對無法修補之資產實施緩解措施。

以下翻譯僅供參考。若本翻譯版本與最後更新的英文版本之間有歧異、不一致或衝突（包括因翻譯延遲所造成者），則應以英文版本為準。

4.3 **日誌記錄。** 供應商須蒐集、管理及保留稽核、事件及安全性日誌記錄，包括：(a) 就許可用途提供給供應商的 Amazon 帳戶或憑證之所有使用情形（包括授權及未授權）的日誌資料，及 (b) 任何冒充或試圖冒充 Amazon 人員或可存取 Amazon 資訊或所管控的資訊系統之工作人員的日誌資料。此類日誌須包含足夠的資料，以利識別每個已記錄事件的以下資訊：(i) 發起事件的工作人員或帳戶，(ii) 事件的時間，以及 (iii) 受影響的系統、資料或其他資源。供應商須定期分析此類日誌，以利偵測、調查未經授權之活動及恢復正常運作。

4.4 **惡意軟體防護。** 供應商須 (a) 對所有所管控的資訊系統部署反惡意程式軟體或相等的安全性控制；(b) 維持反惡意程式軟體或相等的安全性控制更新、簽章和設定；以及 (c) 設定系統以便偵測、預防和修復惡意或未經授權之程式的安裝、散佈和執行。

4.5 **風險管理計劃。** 供應商須具備成文的資訊安全風險管理計劃，定義風險分析、風險處理、風險接受和例外情況的流程。

4.6 **安全意識培訓**。供應商須在聘雇工作人員時及此後至少每年一次，為工作人員提供資訊安全和資料隱私相關培訓。供應商亦須確保及時向工作人員通知供應商安全性和資料隱私政策之更新。

4.7 **資料清冊。** 供應商須記錄並維護有關 (a) 其正在處理的 Amazon 資訊，以及 (b) Amazon 資訊的處理方法和處理地點的資訊（例如，在最新的架構圖中）。若 Amazon 提出要求，供應商須向 Amazon 提供這些資訊。

4.8 **安全性測試。**

4.8.1 供應商每年均須執行測試，以確保符合本安全性政策的要求。

4.8.2 供應商至少須每年執行一次供應商安全性防護滲透測試。滲透測試須包括：(a) 供應商網路內部和外部測試，(b) 社交工程（例如網路釣魚模擬），以及 (c) 無線網路安全性測試。供應商須根據其漏洞管理計劃處理所發現的漏洞。若 Amazon 提出要求，供應商須向 Amazon 提供該滲透測試及漏洞補救的結果。

4.9 **網路安全性。** 供應商須限制未經授權的網路存取，尤其是來自外部網路者，以保護所管控的資訊系統。供應商須維護和設定防火牆或其他同等安全控制措施，以防止系統遭受未經授權存取，且至少每年審查防火牆規則集，以確保所有規則均是依據有效且記錄在案的業務案例。

4.10 **合適的環境**。供應商須僅在適合其目的之環境中處理 Amazon 資訊，且除非本協議許可，否則不會在測試環境中處理 Amazon 資訊。

4.11 **加密**。供應商須根據產業最佳實務，對靜態存儲及透過外部網路傳輸的所有 Amazon 資訊進行加密。如果 Amazon 資訊使用內部供應商網路傳輸，則應使用符合產業最佳實務的加密協定進行傳輸。供應商須根據產業最佳實務管理和保護加密金鑰。

4.12 **管理權限之控制使用**。供應商須依照 NIST Cybersecurity Framework 或 ISO 27002 執行管理職能。供應商應至少將管理帳戶與標準帳戶分開，而且管理帳戶僅限使用執行管理職能所需的功能。供應商應記錄所有管理帳戶的操作，並確保相關記錄可追溯至個別使用者。授予標準帳戶的管理權限應遵循最少權限原則，並記錄相關操作，確保可追溯至個別使用者。

4.13 **存取控制。**

以下翻譯僅供參考。若本翻譯版本與最後更新的英文版本之間有歧異、不一致或衝突（包括因翻譯延遲所造成者），則應以英文版本為準。

4.13.1 **唯一識別碼**。供應商會為擁有 Amazon 資訊或所管控的資訊系統存取權限之工作人員（包括擁有管理權限的帳戶）指派唯一的個人識別碼。

4.13.2 **僅限「必要知悉」。** 供應商須限制對 Amazon 資訊及所管控的資訊系統的存取權限，僅提供給為執行許可用途而「必要知悉」的工作人員。

4.13.3 **使用者存取審查**。 供應商應至少每 90 天一次，審查擁有 Amazon 資訊及所管控的資訊系統存取權限的工作人員與服務，並移除不再需要存取權限的帳戶。

4.13.4 **單一登入 (SSO)。**需要驗證 Amazon 人員身分的任何供應商服務必須整合 Amazon 身分識別供應商（例如 Amazon Federate）來進行相關驗證。此類服務不得使用供應商提供或供應商管理的憑證進行驗證。

4.14 **密碼管理。**

4.14.1 **高強度密碼**。 供應商不得在任何所管控的資訊系統上使用製造商提供的預設值作為系統密碼及其他安全參數。供應商應強制執行並確保所有所管控的資訊系統均依照 NIST SP 800-63B 所述之最佳實務，使用系統強制執行的「高強度密碼」。供應商應要求所有密碼及存取憑證均須保密，且工作人員之間不得共用。

4.14.2 **帳戶鎖定。**帳戶連續錯誤輸入密碼超過十 (10) 次時，供應商須透過停用可存取 Amazon 資訊或所管控的資訊系統的帳戶來維護和強制執行「帳戶鎖定」。

4.15 **遠端存取；多重要素驗證**。對於遠端存取任何供應商網路、系統、應用程式或其他資產的行為，供應商須實施多重要素驗證（即至少需要兩項要素來驗證使用者）。

4.16 **「大量」存取**。 就本節而言，「大量」存取是指透過資料庫查詢、報告產生或任何其他大量資料傳輸來存取資料。

4.16.1 除本協議或 Amazon 以書面明確規定者外，供應商不會也不允許「大量」存取 Amazon 資訊，無論 Amazon 資訊是儲存在 Amazon 或供應商控制的資料庫中，或是使用任何其他方式儲存，包括儲存在檔案式封存檔（例如純文字檔案）。

4.16.2 若 Amazon 授權「大量」存取，供應商須：(a) 限制此類存取權，僅提供給「必要知悉」的指定工作人員，及 (b) 根據第 4.3 條規定要求明確授權和記錄此類存取。若經 Amazon 要求，並配合第 10 節的安全性審查或第 11 節安全性事件之規定，供應商應向 Amazon 提供本節所述「大量」存取的所有日誌記錄。

4.17 **資料隔離**。供應商須隨時以物理或邏輯方式將 Amazon 資訊與供應商及任何第三方的資訊隔離。若無法進行隔離，供應商須確保 Amazon 資訊能與其他資訊清楚區分，以利進行日誌記錄、刪除及安全性事件應變。

4.18 **供應商工作人員安全**。

4.18.1 供應商須採取一切合理的預防措施，確保獲准存取 Amazon 資訊的工作人員維持資訊的機密性並且依照許可用途使用資訊。這些預防措施必須包括透過保密協議或供應商政策實施保密要求。

以下翻譯僅供參考。若本翻譯版本與最後更新的英文版本之間有歧異、不一致或衝突（包括因翻譯延遲所造成者），則應以英文版本為準。

4.18.2 對於 (a) 不再需要存取 Amazon 資訊或 (b) 不再符合供應商工作人員資格的任何工作人員，供應商須在 24 小時內終止其對 Amazon 資訊和所管控的資訊系統之存取權。若任何工作人員在 (a) 或 (b) 發生後超過 24 小時仍保有對 Amazon 資訊或所管控的資訊系統的存取權，供應商必須於得知該持續存取情況後 24 小時內，透過電子郵件 security@amazon.com 通知 Amazon。

5. 付款安全性要求。若供應商可存取或將處理持卡人資料，供應商須遵守最新版支付卡產業資料安全標準 (PCI DSS)。

6. 分包商。

6.1 未經 Amazon 事先書面同意，供應商不得將本安全性政策下的任何義務分包或委託給任何第三方（統稱「分包商」）。無論是否存在任何分包或委派的情形或其相關條款，供應商仍然有責任全面履行本安全性政策所規定的所有義務。本安全性政策之條款及細則對供應商之分包商及分包商工作人員具有拘束力。

6.2 如果供應商使用任何分包商管控的資訊系統，供應商須對分包商管控的資訊系統及其安全控制措施進行安全性審查，而且，經 Amazon 要求，須向 Amazon 提供關於分包商管控的資訊系統安全控制措施的定期報告（例如《鑑證業務準則公告第 16 號》(SSAE 16)）。

7. 存取 Amazon 管理的資訊系統。Amazon 可以授權供應商透過入口網站、其他非公開網站或外部網路（統稱「Amazon 管理的資訊系統」）處理 Amazon 資訊，但僅限於許可用途。若 Amazon 允許供應商使用 Amazon 管理的資訊系統處理任何 Amazon 資訊，供應商及其工作人員必須遵守以下要求：

7.1 **帳戶**。供應商須確保其工作人員僅使用 Amazon 為其個別指定之 Amazon 管理的資訊系統帳戶，並要求其妥善保管存取憑證並不得共用。

7.2 **系統**。供應商及其工作人員存取 Amazon 管理的資訊系統所使用的運算或處理系統或應用程式必須符合以下條件：(a) 執行由供應商管理之作業系統，並使用全磁碟加密；以及 (b) 滿足第 4.2 節（修補程式管理）、第 4.4 節（惡意軟體防護）和第 4.9 節（網路安全性）的要求。

7.3 **限制。** 除非經 Amazon 事先書面核准，否則供應商及其工作人員不得下載、鏡像複製或永久儲存任何 Amazon 管理的資訊系統存放在任何媒體上的任何 Amazon 資訊。

7.4 **帳戶終止**。若任何工作人員 (a) 不再需要存取 Amazon 管理的資訊系統，或 (b) 不再符合供應商工作人員資格（例如該供應商工作人員離職），供應商須立即（最多 24 小時內）終止該工作人員對 Amazon 管理的資訊系統之存取權限，或通知 Amazon 移除該存取權限。

8. AMAZON 網域或網址。 供應商提供給 Amazon 專門使用的任何網域或 URL，自協議終止後至少 5 年內不得分發給任何第三方或由任何第三方重複使用。

9. 資料歸還和刪除；媒體鑑識銷毀。

9.1 **資料歸還和刪除**。經 Amazon 要求，供應商須立即（但不得超過 72 小時）根據 Amazon 要求歸還和/或刪除的通知，將所有 Amazon 資訊歸還給 Amazon，並永久且安全地刪除該資訊。供應商亦須於許可用途完成或協議終止或到期日（以較早者為準）後 30 天內，永久且安全地刪除所有即時存取（在線上或可透過網路存取）的 Amazon 資訊。若 Amazon 要求，供應商須以書面方式證明所有 Amazon 資訊皆已刪除。為免疑義，本節不適用第 9.3 節所述之歸檔副本。

以下翻譯僅供參考。若本翻譯版本與最後更新的英文版本之間有歧異、不一致或衝突（包括因翻譯延遲所造成者），則應以英文版本為準。

9.2 資料清除。供應商應依據 NIST SP 800-88 修訂版 1《媒體清理準則》（2014 年 12 月 18 日，附錄 A）中關於相關裝置類型的最低清除建議，刪除所有 Amazon 資訊。如 NIST SP 800-88 未提供特定裝置類型的指引，供應商須依下列其中一種方式銷毀含有 Amazon 資訊的設備：(a) 依 NIST SP 800-88 所定義進行清除；(b) 依 NIST SP 800-88 所定義進行銷毀；或(c) 依 Amazon 依據 Amazon 資訊之分類及敏感性所要求的其他標準執行。

9.3 歸檔副本。 如法律要求供應商保留 Amazon 資訊的歸檔副本，供應商不得將歸檔的 Amazon 資訊用於任何其他用途，且
仍須遵守本安全性政策規定之所有義務。所有歸檔的 Amazon 資訊均應加密並儲存在所管控的資訊系統中，但是託管或儲存加密 Amazon 資訊的系統不能擁有加密金鑰副本的存取權限。任何離線備分或「冷備份」（即無法即時或透過互動操作存取）必須存放於具備物理安全保護的設施內。

9.4 **媒體鑑識銷毀**。在處置任何包含或曾經包含 Amazon 資訊的硬體、軟體或任何其他媒體之前，供應商須依據 NIST SP 800-88 附錄 A，對該硬體、軟體或其他媒體進行完整的鑑識銷毀。此銷毀要求不適用於供應商無法存取或控制其實體的儲存媒體。在這種情況下，供應商須確保不再需要 Amazon 資訊時會按照產業最佳實務安全地刪除。

> 9.4.1 除非供應商事先獲得 Amazon 的明確書面同意，否則供應商不得出售、轉售、捐贈、翻新或以其他方式轉讓任何曾經含有 Amazon 資訊的硬體、軟體或其他媒體，惟已根據本節進行鑑識
> 銷毀者除外。

10. **安全性審查**。 應 Amazon 要求，供應商須：(a) 完成 Amazon 風險評估，(b) 提供 Amazon 要求的證據，以證實供應商遵守本安全性政策，(c) 允許 Amazon 或其指定的第三方審查供應商對本安全性政策之遵循情形，和/或 (d) 以開放網路安全模式框架 (Open Cybersecurity Schema Framework，OCSF) 格式，向 Amazon 提供第 4.3 節所述之所有日誌記錄。若供應商要求任何證據必須親自或以實地稽查方式審查，而非以遠端方式提供此類證據供 Amazon 審查，供應商須負擔與此類現場稽查相關的差旅和其他費用。若任何評估或審查發現問題，供應商須自行承擔所有費用，並立即採取所有合理必要之行動，在雙方協議的時限內依 Amazon 合理滿意的標準完成補救。

11. **安全性事件。**

11.1 **安全性事件通知**。供應商須在知悉或合理認為 Amazon 資訊或所管控的資訊系統發生未經授權之存取、蒐集、獲取、使用、傳輸、揭露、損壞或遺失事件（「安全性事件」）後，盡快但不得遲於 24 小時內通知 Amazon，並將安全性事件通知發送至 security@amazon.com。

11.2 **事件應變計劃**。供應商須備有一份成文的事件應變計劃，且應要求提供一份副本給 Amazon。供應商須遵照供應商成文的事件應變計劃和產業最佳實務，及時進行每宗安全性事件的補救工作。供應商須至少每年審查、測試和（如有需要）更新計劃內容。

11.3 **與 Amazon 合作**。 供應商須 (a) 協助 Amazon 調查安全性事件；(b) 協助推進與涉及安全性事件或應變工作之工作人員和其他人的訪談；(c) 保留供應商安全性事件調查及應變之書面詳細資訊；及 (d) 向 Amazon 提供所有相關的記錄、日誌、檔案、資料報告、鑑識報告、調查報告，以及 Amazon 要求的其他資料。

以下翻譯僅供參考。若本翻譯版本與最後更新的英文版本之間有歧異、不一致或衝突（包括因翻譯延遲所造成者），則應以英文版本為準。

11.4 **第三方通知**。除非法律另有規定，供應商須獲得 Amazon 事先書面同意，方能：(a) 向任何第三方（包括任何監管機構或客戶）通知任何安全性事件；或 (b) 在有關任何安全性事件的任何通知或公開聲明中提及 Amazon。除非法律另有規定，Amazon 有權決定是否向任何第三方發出安全性事件通知以及通知的形式、時間點及相關內容。

12. **法律程序通知**。法律程序通知。 除非法律禁止，如果為回應法律程序或其他適用法律而查詢 Amazon 資訊，供應商須充分提前通知 Amazon，以便 Amazon 尋求保護令或其他適當的救濟措施。

13. **定義。**

13.1「**協議**」指任何引用本安全性政策的協議。

13.2「**Amazon**」是指 Amazon.com, Inc. 及其關係企業。

13.3「**Amazon 資訊**」是指：(a) 所有 Amazon 機密資訊（如雙方任何其他協議中所定義）；(b) 供應商或其關係企業從 Amazon 處或代表 Amazon 以任何形式獲取、存取、收集、接收、儲存或維護的所有資料、記錄、檔案、內容或資訊，或其他與本協議相關的資訊；(c) 源自(a) 或 (b) 的資訊，即使已匿名化。

13.4「**匿名化**」指對任何資料或資訊（包括 Amazon 資訊）進行處理，使其不具備 Amazon、任何使用者、裝置識別碼、來源、產品、服務、內容或品牌的識別資訊，亦無法從中識別這些資訊，更無法據此推斷其中關聯性。

13.5「**所管控的資訊系統**」指供應商用來處理 Amazon 資訊的任何系統。

13.6「**工作人員**」指供應商或分包商的員工、代理人、分包商及其系統和網路資源的其他授權使用者。

13.7「**處理**」是指對資料進行任何操作，例如存取、使用、收集、接收、儲存、更改、傳輸、傳播或以其他方式提供、刪除或銷毀。

13.8「**供應商**」指協議中定義的每個供應商、賣方或承包商，以及須遵守協議規範的任何其他提供者。