HP 安全措施概要

為保護客戶資料，HP 遵守一套穩健的資訊安全控制措施，包括政策、實踐、程序和組織結構，以保護其自身資訊和其客戶資訊（包括 HP 的客戶和資料處理附錄中定義的個人資料）的保密性、完整性和可用性。以下概述了 HP 在整個公司實施的技術/組織安全措施。

1. 安全政策

   HP 維護旨在保護 HP 和客戶資料的全球適用的政策、標準和程序。HP 安全政策的細節屬於保密資訊，用於保護 HP 資料和系統的完整性。但是，我們的主要政策摘要如下。

2. 資訊安全組織

   HP 的資訊安全計畫，旨在指導和維護組織的資訊安全策略和控制措施。此系統確保企業全面遵循 HP 的安全政策和控制措施，並符合其客戶的安全要求。該框架依據業界標準的網路安全框架、法律和法規進行結構化，並每年審查以適應 HP 不斷變化的威脅環境。

3. 網路安全風險管理

   HP 的網路安全風險管理計畫旨在維護其資訊資產的機密性、完整性和可用性。該計劃提供一致的方法來識別、評估、優先排序、處理、補救、跟蹤和報告網絡安全風險。HP 將其風險承受能力定義為可接受的損失暴露程度，將風險容忍度定義為與此承受能力的偏差程度。風險是使用既定的方法進行評估，使 HP 能夠將資訊安全風險降低到可接受的水平。此計畫符合 HP 的企業風險管理流程。

4. HR 安全性

   HP 人力資源安全政策透過建立設施、資訊系統及其他資產的存取流程，確保員工生命周期中的資訊安全。這包括通過保密和非披露協議獲得書面確認，以及進行背景篩選程序。所有應徵 HP 職位的候選人必須根據相關法律、法規和倫理進行背景核查。

5. 資產管理

   HP 設有一套流程來識別技術資訊資產、分類關鍵資產，並為每種資訊分類類型（包括包含個人資料的類型）維護文件化的處理程序。這些程序涵蓋存儲、傳輸、通信、存取、記錄、保留、銷毀、處置、事件管理和違規通知。HP 的安全政策和標準還要求安全處置媒體。

上次更新時間：2024 年 9 月

6. 資料安全性

HP 的數據安全計劃概述了必須實施的安全措施和技術控制，以保護數據的機密性、真實性和完整性。法律要求、價值、未經授權披露或修改的關鍵性和敏感性是決定資訊在 HP 資料安全政策下如何分類的幾個因素。除了數據處理程序外，該政策還概述了數據加密、刪除、收集和處理、保留、備份和數據丟失防護。

7. 存取控制

HP 採用最小權限原則進行邏輯存取控制，透過唯一的使用者 ID 和密碼提供使用者存取權限。密碼政策定義了複雜性、強度、有效性和密碼歷史控制。存取權限會定期檢查，並在人員離職時撤銷。在專案執行期間，實施已商定的使用者帳戶建立和刪除程序，以授予和撤銷對客戶系統的存取權限。

8. 密碼學

HP 已經定義了一套強健的加密過程，以確保資訊資產的機密性、完整性和可用性。核准的協議要求對某些資產進行加密，包括那些包含個人資料的資產。我們的加密計畫涉及使用數學技術來保護信息和通信，確保只有授權方能夠存取數據。HP 資訊安全計劃的一個關鍵組成部分是保護數據免受未經授權的存取和篡改。

9. 實體及環境安全

HP 設施透過各種實體和電子存取控制措施來確保安全，包括保全人員、電子存取控制以及閉路電視 (CCTV)。設施也配備了必要的基礎設施支持，包括溫度控制和電力備援，使用不斷電系統和/或柴油發電機來支持關鍵服務。所有 HP 人員均須註冊並攜帶適當的識別證。

10. 營運管理

HP 已建立技術基礎設施的最低強化要求，包括工作站、伺服器和網路設備。這些設備使用預先強化的作業系統映像，具體要求因作業系統和實施的控制措施而異。此外，HP 已部署網路入侵偵測/防護系統 (NIDS/NIPS)，並進行 24/7 監控和管理。

11. 通訊安全性

通信安全確保公司網路內資訊的保護。這包括網路安全元件的安裝和管理（例如防火牆）、網路隔離，以及網頁過濾和電子郵件處理控制。此外，這涉及監控和管理通訊渠道，以偵測和防止未經授權的存取或資料洩漏。

12. 系統安全性

HP 的政策要求在系統和軟體的整個生命週期中採用安全的開發方法。軟體開發生命週期涵蓋啟動、開發/採購、實施、運營和處置。所有系統元件皆會被評估其對整體安全性的影響。HP 已建立應用服務交易的控制措施，包括使用者憑證驗證、數位簽章、加密、安全通訊協議，以及在適當的網路安全區域內儲存交易詳情。內部弱點掃描也會定期執行。

上次更新時間：2024 年 9 月

13. 第三方與分包商

HP 擁有選擇符合全面合約安全要求的分包商的流程。對於處理 HP 或客戶數據，或存取 HP 網絡的適用供應商，HP 網路安全會進行風險評估，以驗證具有物理、技術和管理保障措施的信息安全計劃。在供應商可以存取 HP 資訊之前，必須進行此評估。

14. 資訊安全事件管理

HP 擁有一套全面的網路事件管理流程，概述了目的、範圍、角色、責任、管理承諾、組織協調、實施程序和合規檢查。此流程每年審查並更新。網路事件應變小組，包括接受過事件應變和危機管理訓練的 HP 資安人員，定期進行流程及任何事件或活動的桌上演練檢討。

15. 業務持續管理

HP 的全球業務連續性計劃透過協作、標準化和文件化的規劃流程，確保端到端的連續性。公司定期執行其業務連續性計劃，以確保其有效性，並至少每年測試和更新所有計劃。此外，所有參與業務連續性計劃的人員都會接受適當的培訓。

16. 合規性

合規性塑造了 HP 在滿足法律、合同和內部期望方面對有效資訊安全計劃的做法。定期的資安審查確保協議整合到每個業務群組的運作中。審查過程還會使文件保持更新，以反映隨著要求變化的當前法律義務。

17. 支付卡產業

支付卡產業 (PCI) 框架指導 HP 達成 PCI 合規的方式，概述與 PCI DSS 對齊的業務責任和安全控制。透過安裝和維護像防火牆這樣的網路安全控制措施，HP 確保其符合 PCI 合規性要求。

18. HP 產品安全性

HP 產品安全包含確保 HP 產品安全的基本實踐，例如程式碼簽署、管理產品安全漏洞、發布安全公告和報告產品安全問題。這些措施確保 HP 產品對使用者而言保持安全和可靠。在 HP，產品安全性至關重要，因為此舉有助於維護客戶信任並防範潛在威脅。

19. HP 服務安全性

HP 服務安全涵蓋確保提供給 HP 客戶的服務安全的基本實踐。此政策涵蓋服務安全的各個領域，包括 HP 基礎設施託管、第三方託管、合作夥伴託管和客戶託管環境。這些措施確保 HP 服務對用戶而言保持安全和可靠。HP 通過實施強大的安全措施，確保其產品和服務的安全性和完整性，為所有用戶創造一個安全且值得信賴的環境。

上次更新時間：2024 年 9 月