

供應商資訊安防管控需求

目錄

1. 介紹.....	1
2. 定義.....	2
3. 資訊安防政策.....	2
4. 注意義務之標準.....	3
5. 個人資料保護與處理需求.....	4
6. 人力資源安防.....	4
7. 負責任地使用人工智慧.....	5
8. 系統之獲取、開發與維護.....	5
9. 資產管理.....	6
10. 存取控制.....	6
11. 加密技術.....	7
12. 實體安防與環境安防.....	7
13. 營運安防.....	7
14. 事業韌性.....	8
15. 資訊安防突發事件管理.....	8
16. 資料突發事件或外洩通知.....	9
17. 通訊安防.....	9
18. 供應商關係.....	9

1. 介紹

美光管理階層致力於確保 IT 資產及美光資料（定義如下）的安全性。

範圍：

這些資訊安防管控需求（**資訊安防管控需求**），適用於所有處理、處置或提供 IT 資產與美光資料的供應商，或處理或處置 IT 資產與美光資料之解決方案或平台的供應商。

美光供應商（下稱「供應商」）應實施管理、實體和技術層面的防護措施，保護任任何 IT 資產和美光資料，以避免遭受未授權存取、獲得、揭露、銷毀、變更、意外損失、濫用或損毀，保護方法必須採取嚴格程度不低於業界實務作法的最佳已知方法，包括資訊安防環境和管理措施，且符合國際標準化組織 (ISO) 27001「資訊安防、網路安全和隱私權保護——資訊安防管理系統——需求」的標準或其後繼規範。

這些資訊安防管控需求並不意圖取代供應商的標準政策和程序，而是為了要求供應商在自有的標準政策和程序中制定必要的最低管控度。依據上述需求，供應商應維持多個控制領域，詳情如下文所述。

本文件概述美光與其供應商之間在資訊安防與風險管理上的期望與需求。重點是遵循國際標準——特別是 ISO 27001 及 SOC 2 Type II——可作為實務上符合本文件需求之方式。這些經認可的認證及評估框架均展現出已設立紮實的安防管控、風險管理實務及資料保護措施，以便保衛美光資料，包括涉及第三方業者的時候。本文件進一步詳述持續性安防評估的協定，並強調以合作方式解決並修復已識別的任何風險或缺陷，確保完全符合美光的資訊安防標準。在涉及美光較為敏感資訊的情況下，美光可自行酌情增加額外的安全需求。

2. 定義

- a) 「突發事件」係指實際上或可能危及資訊系統或其所處理之美光資料機密性、完整性或可用性的任何情況，該資料包含對美光營運十分重要的任何內容。這包括任何未經授權存取、使用、揭露、中斷、修改或銷毀美光資料的情形，或任何違反或幾近威脅違反美光安防政策、程序或可接受的使用政策之情形。
- b) 「IT 資產」包括但不限於：美光基於執行美光業務的目的而向其主管、行政人員、團隊成員、承包商和其他第三方供應的電腦設備（例如筆記型和桌上型電腦）、行動裝置（例如手機/智慧型電話、平板電腦）、硬體、軟體、作業系統、儲存媒體、網路資源、身分識別（例如提供電子郵件、線上瀏覽、檔案傳輸協定和其他 IT 服務的權限），以及運算環境（例如開發、測試、展示、生產和備份應用程式環境）。
- c) 「美光資料」包括美光擁有之智慧財產權及其他機密與專屬文件，以及第三方委交給美光的相關資料。
- d) 「個人資料」係美光資料的一部分，指一已識別或可識別的自然人之任何相關資訊；意指此人為得以直接或間接識別者，特別是參考諸如姓名、身分證字號、位置資料、網路識別碼、一或多項其身體、生理、基因、心理、經濟、文化或社會認同等具體因素；以及由資料保護適用法律所定義者。
- e) 「處理」是建立、蒐集、持有、處置、經手、處理、接收、傳送、儲存、保留和揭露美光資料的統稱。

3. 資訊安防政策

持有現行有效之 ISO/IEC 27001 認證及／或 SOC 2 Type II 證明之供應商，於符合下列條件之前提下，得視為已符合美光之部分安防需求，惟該等認證須：

- 由經認可且具公信力之機構核發；
- 持續有效且為最新版本；以及
- 涵蓋與美光服務或資料具重大關聯之適用範圍內系統、流程及控制措施。

美光保留自行酌情評估該等認證充分性之權利。在此情況下，供應商得免於依美光資安評估流程重複提交相關佐證資料。

作為上述之替代方案，供應商應維護並實施明文規定的安防政策及程序，以便規範接收、傳輸、處理、儲存、存取及保護美光資料、IT 資產以及由供應商提供的相關服務之情形。供應商之決策與程序必須符合 NIST 網路安全框架、ISO 27001/27002，或任何後續同級產業認證標準或框架。

這些決策至少須涵蓋以下控制領域：

- 資訊安全治理與責任歸屬
- 資訊分類、標示歸類及處理（包含資料分離）
- 可接受的 IT 系統使用（限於經同意的用途，並採取技術與管理控管）
- 事件偵測、應變與違規通報（包含明確的角色分工、證據保存，以及與美光的合作協定）
- 網路與主機安全生（例如：防毒、防火牆、入侵偵測/入侵防禦系統、系統強化）
- 身分驗證與存取管理（包含定期使用者存取審查）
- 處理美光資料的系統日誌與監控（實體與邏輯層面）
- 員工安防與隱私意識訓練
- 透過加密保護資料（靜態、傳輸中及使用中資料）
- 設施的實體與環境安全性
- 資料保存、棄置及生命週期政策（可依要求提供）

4. 注意義務之標準

供應商知悉且同意，與美光合作期間，供應商可建立、接收或存取美光資料，包括個人資料。供應商應遵守本文件所列的條款與條件，並在其管控範圍內負責供應商或第三方未經授權或非法處理之行為。

供應商對於具有美光資料存取權的使用者、承包商或資料處理者之作為或疏失，必須對美光負責且持續承擔責任；並且，供應商須與所有將可存取美光資料或 IT 資產之各方簽訂書面協議。鑑於上述事項，供應商同意並承諾：

- a) 對所有的美光資料嚴格保密，並採取適當的注意程度，以避免未經授權的存取、使用或揭露。
- b) 不得以違反法律的方式建立、蒐集、接收、存取或使用美光資料。
- c) 使用與揭露美光資料時，僅限於美光資料或其存取權的取得遵守本文件的條款與條件時的用途，且個別情況下皆不得未經美光事先書面同意，即基於供應商本身的目的或美光以外任何人的利益，而使用、販售、租賃、轉移、散布或揭露、提供美光資料。
- d) 限制在 AI 聊天機器人、搜尋引擎或可能導致未經授權揭露的工具中使用美光資料。
- e) 不得未經美光事先書面同意，而直接或間接向供應商員工、承包商及或資料處理者以外的任何人士揭露美光資料，且必須要求供應商所有經手美光資料的承包商或資料處理者以書面同意遵守本文件中的義務。

- f) 確保如果供應商的任何員工或分包商取得對任何美光系統或設施、美光資料或 IT 資產的存取權，此類人員應遵循美光向供應商佈達的所有適用政策及流程，並且，除了提供服務所明確需要者，不得存取或試圖存取任何美光電腦系統、電子檔案、軟體或其他電子服務。如果供應商的員工或承包商被解僱或將不再為美光提供服務，供應商應至少提前二十四 (24) 小時通知美光，以便終止該員工或該承包商對美光資料及 IT 資產的存取權（例：門禁識別證、登入資訊等）。

供應商應維持一套科技與網路安全風險管理計畫，並至少每年進行一次審查。供應商應維持風險管理流程，以定期辨識、評估及管理對美光資料及 IT 資產的風險。

5. 個人資料保護與處理需求

- a) **個人資料之機密性**。供應商應對與美光業務來往過程中蒐集的所有個人資料保密。
- b) **資料最小化與目的限制**。供應商應將個人資料的蒐集與使用，以向美光提供商品或服務時為限，執行其權利與義務所合理必需的合法業務目的。未經美光事先書面同意，不得將個人資料用於其他地方。
- c) **傳遞隱私義務**。供應商須定期向經手個人資料的員工、承包商或其他第三方指示維護個人資料機密性的義務，並將蒐集與使用，以向美光提供商品或服務時為限，所必須的處理程序。供應商應以契約方式，要求所有處理個人資料之次級承包商或次級處理者，遵守相同之資料保護義務。
- d) **隱私**。供應商應及時且以透明的方式配合美光，遵循合法之資料當事人隱私權利要求。供應商應在受到美光的書面指示時，提供其記錄和資料存放庫中的資料副本，或予以修正或刪除，範圍僅限於法定義務所規定需以原始格式保留的個人資料，且如有保留，則僅可保留至法律需求仍有效的時間範圍，之後則須予以刪除。供應商未經美光事前書面授權，不得分享或販售任何個人資料。
- e) **隱私突發事件公告及合作**。如發生任何個人資料的未授權存取、蒐集、使用、變更、分享、複製或銷毀，供應商需適時通知並配合美光調查。突發事件通知若涉及個人資料時，必須傳達 security@micron.com。
- f) **遵循證明**。在美光提出要求時，供應商應適時提供充足的書面保證，證明其遵守本【個人資料保護及處理需求】章節。無論供應商目前是否仍向美光提供商品或服務，在供應商或其代理人持有個人資料期間，保護個人資料的相關義務皆需維持有效。

6. 人力資源安防

供應商應建立並維持多層級的人力資源安全計畫。員工必須配戴獨特形式的識別證（例如徽章）、簽署保密協議，並且每年重審與認知供應商的道德準則或同等效力文件。員工也必須依據法律所允許的範圍，完成全面的背景調查，其中可能包括指紋、犯罪記錄、信用記錄、藥檢和資歷審查。

供應商應要求所有員工完成年度資訊安防訓練，瞭解機密資訊和客戶資料的正確使用和處理方式，且必須保有完成相關訓練的員工名單。供應商應要求所有員工皆認知自身已瞭解且遵守供應商的資訊安防政策。

7. 負責任地使用人工智慧

為確保在美光的業務營運中可靠採用並使用人工智慧（「AI」），關於供應商為支援美光而使用 AI 的任何情形，供應商應遵循以下規定：

- a) 應公開且明確揭露 AI 的使用情形，可能包括對於向美光提供的任何 AI 生成素材或輸出，進行標註或其他清楚的命名。
- b) 處理與美光人力資源作業相關之個人資料時，如果有使用 AI，應事先通知美光。
- c) 對於使用美光資料訓練供應商或其承包商的 AI 模型或豐富供應商或其承包商的資料集，要事先取得美光的書面同意。
- d) 在為美光或使用美光資料分析、處理或開發工作或服務時，僅可利用經美光核可的 AI 工具處理及經手資料，對於美光的機密或非公開資料，供應商將不得利用未經授權或公用的 AI 工具及／或語言模型。如需確認經美光核可的工具最新清單，請聯絡 AI_OPS_CORE@micron.com。
- e) 供應商應就其自身或其承包商之 AI 品質、法規及法規遵循控制措施提供充分透明資訊。在美光的合理要求下，供應商應向美光提供與供應商 AI 品質、法規及法遵管控相關的回應資訊，例如，包括針對偏誤測試、確認偏誤控制、效能監控以及為遵循適用法律、規則或法規可能必要的其他此類管控。

8. 系統之獲取、開發與維護

供應商應維護安全的開發方法，在完整開發週期中融合安防，包括應用程式開發政策、應用程式開發人員安防訓練，以及對供外部使用的網頁應用程式進行安全的程式碼檢核和入侵測試。

作為其系統取得、開發與維護流程之一部分，供應商應進行下列事項：

- a) 基於保護美光資料機密性、完整性和可用性的原則來開發與設定應用程式及資料庫。
- b) 開發網頁應用程式時，遵照安防最佳做法（例如 **Open Worldwide Application Security Project [OWASP] 十大漏洞**），並採取合理步驟驗證該網頁應用程式的設定已針對 OWASP 十大漏洞予以防護。
- c) 另行實作專供生產、開發與測試的環境。
- d) 運用自動掃描工具和手動分析，至少每年實施一次安全的程式碼檢核，包括開放原始碼檢核，以及入侵測試或同等級測試。供應商應確保根據明文規定的政策，按照以風險分級的優先補救措施，確保針對已識別的漏洞進行補救應。
- e) 根據明文規定的程序管理原始程式碼，藉此在部署前限制存取與驗證程式碼完整性。

- f) 如果供應商或其分包商使用網站、入口網站及／或其他技術提供任何服務，供應商應每年自費委託獨立第三方執行入侵測試。供應商應即時修補該第三方發現的任何重大缺失。美光有權驗證該等測試是否已完成，及所有發現事項是否已完成修復。

9. 資產管理

供應商應維護專為教育員工瞭解在資料生命週期全程如何分類、標籤、處理與處置資訊及所有媒體類型而設計的資訊安防辦法。

供應商應指示員工針對個別資訊類型採取適當方法來處理資訊，例如發布、討論、傳送電子郵件、複製、傳真和儲存。

供應商應：

- a) 維護 IT 資產的清查資料，並管理相關的資產生命週期。
- b) 確保 IT 資產僅可使用於經過協議的用途。
- c) 按照業界標準和適用法規來經手、處理與儲存美光資料，包括個人資料。
- d) 根據 ISO 27001 或 CMMC Level 2，或其替代性標準等目前的業界標準，清除媒體中的敏感資訊或以安全的方式銷毀。
- e) 在供應商與美光的合作結束或終止時，或在美光提出要求時，供應商應清除敏感資料並以安全的方法銷毀（或在美光要求下歸還至美光）所有美光資料的副本，無論任何電子或非電子格式，且應提供經供應商行政長官簽署的憑證，以美光可接受的型式，詳細證明資料的歸還或銷毀。

10. 存取控制

供應商應維護合理的存取政策和管控（例如身分識別和存取管理系統及驗證機制），以便確保只有經授權員工擁有美光資料的存取權。存取要求必須透過正式的存取管理系統加以追蹤和授權。存取權的授予必須以最低權限和責任分離的概念為依據，且必須限於具有業務需求的對象。

作為其存取控制措施的一部分，供應商應進行下列事項：

- a) 使用識別碼以進行邏輯性存取限制，確保其他供應商客戶無法檢視或存取美光資料。
- b) 員工或承攬人員離職後，應即時撤銷其存取權限；或於供應商員工內部調職至不再需要該等存取權限之職位時，應於商務上合理期間內撤銷其存取權限。
- c) 定期審核使用者帳戶及其權限，藉此驗證該存取權與職務角色相符，並移除已不再需要的存取權。
- d) 將特權帳戶的使用限於執行系統管理或安防管理活動的授權員工。

- e) 蒐集、監控與保留記錄，以便美光資料的存取可供追蹤。
- f) 將系統帳戶的用途限制為系統對系統的通訊，並將這些帳戶設為防止使用者的互動式登入。
- g) 針對僅限授權人員存取的 IT 資產，實施安全且加密的遠端存取解決方案。

11. 加密技術

供應商所維護的加密政策應符合目前的聯邦資訊處理標準 (FIPS) 140 修訂版，且適用於所有用於保護美光資料與 IT 資產的加密技術。此類技術包括業界標準的演算法和金鑰長度、金鑰生命週期管理的需求，以及金鑰和憑證驗證的需求。

供應商應建立並維持相關政策、流程及技術措施，對傳輸中及靜態的美光資料進行加密。這類手法包括磁帶、卸除式媒體裝置、筆記型電腦、網路檔案傳輸和網路交易。提供加密時必須採取商務級的業界標準加密演算法、通訊協定和金鑰強度。

供應商應與美光合作，實施可靠且安全的電子資料傳輸方式，以符合美光的要求。

12. 實體安防與環境安防

供應商應維持：

- a) 實體安防措施來管控與限制 IT 資產的實體存取，包括全職的專業保全人員、攝影機（範圍所涵蓋的存取點及於處理與儲存美光資料專用的安全及禁止／關鍵空間，以及停車區域）、
- b) 入侵偵測和警示功能、
- c) 適當的存取管控系統、訪客管理與記錄。
- d) 基礎建設及環境管控，以便防範因人為錯誤、潛在環境危害（例如火災及水災）或技術失效導致 IT 資產銷毀、遺失或損壞，可能包括但不限於與當地法律及業界標準相符的電力、溫度及濕度監控、滅火系統、通用電源 (UPS)、緊急或備份系統。
- e) 供應商應確保實體資產至少透過主動監督、鎖具機制及清理辦公桌政策加以保護。

所有用於儲存美光資料的資料中心都必須位於美光核准地理區域的資料中心。即使供應商和美光之間簽署的協議有另訂任何條款，供應商仍可在北美地區以外執行技術支援的服務，包括但不限於軟體開發、後台系統運作、品質確保和生產支援。供應商在美國境外營運時，應維持不低於當地法規之控管措施。

13. 營運安防

供應商應維護適當的安防營運辦法，專門用於保護美光資料和 IT 資產，且該辦法必須經過測試且持續改良。供應商應將下列安防管控措施納入此計畫中加以維護：

- a) 防範資料遺失、惡意軟體、惡意入侵或惡意下載。

- b) 適時更新反惡意軟體和防毒軟體簽章。
- c) 入侵偵測和預防系統 (IDS/IPS)。
- d) 監控未授權存取、連線、裝置和軟體。
- e) 在安防漏洞辦法中納入定期網路漏洞掃描、修補程式管理，以及按照風險程度排序的已識別安防漏洞補救措施。
- f) 蒐集 IT 資產和感應器的安防事件並彼此建立關聯，以便偵測與解決安防事件（亦即安防突發事件和事件管理 [SIEM]）。
- g) 使用標準化的強化版本導入系統和裝置。
- h) 監控與管控供應商員工與網際網路的連線。
- i) 依需求備份美光資料，以便供應商按照測試的備份和復原程序來滿足持續性需求和復原時間目標，並保護備份免於遺失、損毀和未授權存取。
- j) 進行安全的變更管理流程，以安裝、配置、操作及維護存放美光資料及 IT 資產的資訊系統（例如工作站、伺服器、網路和應用程式）。

14. 事業韌性

供應商應維護全方位的業務持續性和災難復原辦法，包括技術與業務營運復原。供應商應透過電信通訊、系統和業務營運的備援措施來預防中斷，以及擬定復原策略來因應資料遺失事件。業務持續性和災難復原辦法必須以供應商身為產品或服務提供者的適用情況，遵守法定和法規需求。

災難復原程序必須包含每年至少一次訓練、規劃和測試關鍵技術及業務營運復原。供應商必須執行業務影響分析，並針對不同威脅情境開發復原策略，將營運場所、人員、技術或供應鏈損失情境都納入考量。供應商應維持可於事件發生期間或發生後執行之復原計畫，並應於要求時提供計畫確實存在的證明。

15. 資訊安防突發事件管理

供應商應維護並定期測試其已成文的整體網路突發事件回應計畫，該計畫專用於識別潛在威脅、評估任何風險暴露、向管理層通報風險，以及保護業務營運。作為其資訊安防突發事件管理計劃的一部分，供應商應進行以下動作：

- a) 評估安全事件和可疑事件。
- b) 以遏制和減輕事件影響為目的採取行動。
- c) 確定行動，以盡量減少類似事件再次發生的風險。
- d) 依據保留證據的法律規定進行調查。

e) 記取教訓，以提高整體事件的管理能力。

16. 資料突發事件或外洩通知

如果發生任何導致美光資料遺失、銷毀、損毀、破壞、無法使用或遭未經授權之個人或實體存取（例如檢視、複製、變更、揭露或傳輸）之漏洞，供應商應立即透過 security@micron.com 通知美光，並遵守任何適用之合約或法定需求。供應商應自行支出費用復原上述美光資料。供應商應依據適用法律、規定或法規通知美光，不得延遲，但任何情況下都不得在發現美光資料的突發事件、未授權或非法處理後，超過七十二 (72) 小時才通知。雙方必須在發生任何美光資料的未授權或非法處理後，立即彼此合作調查事件。

供應商應在美光經手處理事件的過程中與美光合作，包括：

- a) 協助任何調查。
- b) 依情況適當與否，向美光提供任何設施和受影響營運據點的邏輯、實體及遠端存取權。
- c) 提供所有相關記錄、日誌、檔案、資料報告和其他遵守所有隱私權與資料保護需求所需的素材，或美光合理要求的素材。

除非法律或法規要求，否則若供應商未事先取得美光書面同意，不應向任何第三方告知發生任何突發事件。此外，供應商同意美光具備單獨權利，可依據法律或法規要求，或經美光獨自在裁量，決定是否向任何受影響的個人、監管機構、執法機關或其他者通知發生突發事件，包括通知的內容及告知方式；以及可決定是否向受突發事件影響的個人提供任何形式的補救措施，包括該補救措施的性質及範圍。

供應商應負擔執行本節所述義務而產生的所有合理費用。供應商也應補償美光在回應與降低損害時產生的合理費用，補償範圍及於供應商的所為或無為導致的突發事件，包括本節所述的通知和任何補救措施的所有成本。供應商同意維持並保存所有與任何事件相關的文件、紀錄及其他資料。此外，供應商同意自行負擔費用，完全配合美光執行任何訴訟、調查或其他美光認定必需的動作，以便保護美光在使用、揭露和維護美光資料方面的權利。如果供應商無法在美光合理設定的時間內修正或再生成遺失或銷毀的美光資料，則美光得請第三方重建資料，在美光提出要求時，供應商應與該第三方合作。供應商應優先進行此項工作，以確保美光資料遺失不會對美光的業務或供應商提供的服務造成不利影響。

17. 通訊安防

供應商應維護合理的適當網路安防及資訊傳輸管控措施，專門為在公共或無線網路傳遞的資料保護機密性和完整性，確保防護 IT 資產，包括防火牆、入侵偵測和預防系統、反惡意軟體、Proxy 伺服器，以及安全的檔案傳輸技術。

供應商應：依據風險等級，使用多因素驗證保護特定核心基礎結構元件的遠端虛擬私人網路 (VPN) 存取和管理；設計所有網路時，以防火牆或同級技術保護網路完整性和分隔網路區域，以便限制為僅供授權業務流量使用；並且每年檢核防火牆政策。

18. 供應商關係

供應商應維護第三方風險管理辦法，利用衍生自供應商安防政策、ISO 27001 和其他業界標準實務做法的整體風險評估方法，定期對供應商旗下處理美光資料（包括個人資料）的供應商進行審核。

美光認知供應商可能針對供應商和美光簽署的協議所提供的服務，運用與該服務相關聯的雲端服務提供者。

在美光的要求下，供應商應每年以 ISO 27001 認證、SOC 2 Type II 報告或任何替代性或類似標準的報告為形式提供保證，證明已制定適當的資訊安防保護和管控措施。

在美光的書面要求下，為了確認遵守本標準及任何適用法律和業界標準，供應商應立即且準確完成美光或代表美光的第三方提供的資訊安防問卷調查，以便說明供應商針對所有經手的美光資料採取的業務實務做法和資訊技術環境以及／或者供應商向美光提供的服務符合本標準。供應商應完全配合此類調查。美光應將供應商在安防問卷調查所提供的資訊視為供應商的機密資訊。

如果美光對供應商用於提供服務的場址、設施、系統（包括基礎建設、軟體、人員、程序和資料）及系統元件實施現場或遠端安防評估（「安防評估」），對象包括供應商自身的所有供應商、分包商和委外服務組織，美光實施安防評估時將盡可能不在供應商的正常營運時間內造成營運的不便或中斷，頻率不超過每年一次，並至少在九十 (90) 天前提供書面通知。由供應商所產生的安防評估時數，不應由美光支付任何費用。美光不會審核：供應商的其他客戶或用戶資料或資訊、供應商的任何專屬資料（可能對保護供應商及供應商客戶資料的管控措施造成破口的資訊），或與安防評估目的無關的任何其他機密資訊。此外，美光不會重複執行或監視管控措施的測試或執行。

安防評估的持續時間必須合理，評估範圍須經雙方協議，且美光會優先檢視現有 SOC 2 Type II 服務稽核員報告、ISO 27001 憑證或任何替代性或類似標準的報告，證明供應商已採取適當的資訊安防保護和管控措施，以便對用於保障美光資料的管控措施獲得合理擔保。美光對於供應商的網路和系統不得擁有邏輯存取權，也不得對供應商的設施和員工具有無限制的實體存取權。供應商應讓資安人員待命，隨時回答美光合理提出的問題。美光不會請託任何供應商的競爭對手（或供應商在與美光簽署的協議下的任何重要分包商）、供應商的第三方服務稽核員或 ISO 27001 稽核員來實施上述評估。美光的任何第三方代表皆必須簽訂機密和保密協議，並遵守供應商的安防和機密性需求。美光會維護保護措施，至少透過美光在維護自身資訊、資料和記錄時採取的相同程序，防止供應商提供的安防資訊遭到不當揭露。未經供應商事先書面核准，美光不會將供應商提供的任何安防資訊揭露予任何第三方，但法律要求情況下除外（這種情況下，美光會以書面方式向供應商通知該要求）。如果美光在安防評估中發現實質風險或缺陷，且雙方同意該風險需要補救，美光與供應商應立即共同協商制定補救計畫，包括作業時間，且供應商應從商務層面使用合理手法來補救任何已發現的缺陷或實質風險。

此外，在美光的要求下，在任何 SOC 2 報告（或其同等報告）完成至美光財政年度結束期間，供應商將提供一份書面證書，說明在該期間供應商對此類報告主旨的管控、程序及系統所做的變更（如有），以便美光使用此類報告滿足本身的稽核及法遵需求。

萬一美光判定供應商未遵循本文件所載的任何需求，或供應商無法提供任何稽核報告或要求驗證是否遵循這些條款，則美光有權利在不承擔任何罰則及費用的情況下，(i) 進行補充安防評估，以便確認供應商是否遵循這些資訊安防管控需求；及／或 (ii) 暫停或終止服務，或由美光選擇扣留款項，且供應商在此拋棄與此類暫停或終止相關的任何適用終止費用或未結費用。