資訊安防管控需求

1. 簡介

美光的管理部門致力於確保美光資料的安防。

範圍：
這些資訊安防管控需求，適用於所有經手、處理或提供美光資料的供應商。

美光供應商（下稱「**供應商**」）必須實施管理、實體和技術層面的防護措施，針對供應商可存取、獲得或為美光存放的任何實質或非實質美光自有或供應的項目（「**IT 資產和美光資料**」）提供保護，以避免遭受未授權存取、獲得、揭露、銷毀、修改、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、網路安防和隱私權保護－－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。根據此類需求，供應商必須按照下文所論，維護多項管控領域。

2. 定義

「**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）。

「**美光資料**」包括美光自有或第三方交由美光信託的智慧財產和其他機密與專屬文件。

「**個人資料**」係美光資料的一部分，務必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。

「**美光突發事件**」是指實際或可能危及資訊系統或系統持有、存放或傳送的資訊（美光資料）的突發事件，或構成違反或幾近威脅安防政策、安防程序或可接受的使用政策的突發事件。

「**處理**」是建立、收集、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

供應商必須管理與維持一組安防政策和程序文件，藉此管理美光資訊、資產和關聯服務的接收、傳送、處理、管控、發布、擷取、存取、呈現和保護。

供應商必須透過符合 NIST 網路安防框架、ISO27001/27002 或任何替代性業界認證標準或框架的資訊安防政策框架，針對 IT 資產維護全面的保護措施和明確的責任歸屬。

供應商的資訊安防政策和程序至少必須涵蓋以下項目：

a) 供應商對資訊安防的承諾。

b) 資訊分類、標籤和處理，包括從供應商或其客戶的資訊中分隔的美光資料。

c) 可接受的 IT 資產使用方式（例如將資產單獨使用於經過協議的用途且採取管控措施），包括運算系統、網路和傳訊。

d) 資訊安防突發事件管理，包括違規通知及收集證據的合作方式與程序。

e) 主機和網路型安防管控措施，包括防毒軟體、入侵偵測系統／入侵防範系統 (IDS/IPS)、防火牆和系統強化需求。

f) 使用者、管理員和系統的驗證需求。

g) 存取管控，包括遠端存取和定期審核存取權。

h) 記錄和監控供應商的生產環境，包括用於處理或儲存個人資料的 IT 資產的實體和邏輯存取。

i) 向員工提供適當的隱私權和資訊安防訓練。

j) 用於保護待用、轉移中和使用中資料的端點安防、加密技術。

k) 保護實體資產的實體安防和環境安防管控措施。

l) 資料生命週期管理、記錄保留，以及在收到請求時提供相關政策和文書，以便用於美光實務。

美光可向供應商發出合理通知，請求、審核與檢查上述資訊安防政策和程序，並請求對相關計畫作出合理調整。

4. 注意義務之標準

供應商認知且同意，在與美光合作期間，供應商可建立、接收或存取美光資料，包括個人資料。供應商必須遵守本美光資料處理標準所列的條款與條件，並在其管控範圍內負責供應商或第三方對美光資料的未授權或非法處理行為。

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所做的行動或疏失，必須對美光負責且持續負有責任，且保護美光資產的程度，必須至少達到供應商保護自有資料的層級。基於承認上述事項的目的，供應商同意且立約承諾其必須：

a) 採取適於避免未授權存取、使用或揭露的保管層級，維護所有美光資料的嚴格機密性。

b) 不以違法方式建立、收集、接受或使用美光資料。

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標準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) 禁止將美光資料使用於可能導致未授權存取的 AI 聊天機器人、搜尋引擎或工具。

e) 不得未經美光事先書面同意而直接或間接向供應商以外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的義務。

供應商必須以至少每年檢查一次的頻率，維護技術及網路安防風險管理辦法。供應商必須讓風險管理程序維護定期識別、評估和管理美光資料及 IT 資產的風險。

5. 個人資料保護與處理需求

a) **美光個人資料之機密性。**供應商應對與美光業務來往過程中收集的所有個人資料保密。「**個人資料**」是指本身（或與其他資訊結合後）可合理識別特定人士身分的資訊（例如姓名、聯絡資訊、工作地點、購買記錄、描述、偏好設定、相片、語音錄製檔等）。這類資訊合稱為「**美光個人資料**」。

b) **資料最小化與目的限制。**供應商應將美光個人資料的收集與使用限制於在向美光提供商品或服務時，執行其權利與義務所合理必需的合法業務目的。未經美光事先書面允許，美光個人資料不得挪作他用。

c) **傳遞隱私義務。**供應商須定期向經手美光個人資料的員工、承包商或其他第三方指示維護美光個人資料機密性的義務，並將收集與使用限制於向美光提供商品或服務時所必須的處理程序。供應商必須透過合約向所有處理美光個人資料的分包商或委外處理者規範義務，要求遵守相同的資料保護義務。

d) **隱私。**供應商應與美光合作，以即時且透明的方式遵守法定資料主體隱私權請求。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美光個人資料，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。未經美光事先書面授權，供應商不得分享或販售任何美光個人資料。

e) **隱私突發事件公告及合作。**如發生任何美光個人資料的未授權存取、收集、使用、修改、分享、複製或銷毀，供應商需適時通知並配合美光調查。突發事件涉及美光個人資料的資訊時，務須將通知傳送至 security@micron.com。

f) **遵循證明。**供應商在受到美光請求時，應適時提供充足的書面保證，證明遵守相關的個人資料保護及處理需求。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員持有美光個人資料期間，保護美光個人資料的相關義務皆需維持有效。

6. 人力資源安防

供應商必須維護多層次的人力資源安防辦法。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。

供應商必須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。供應商必須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. 系統之獲取、開發與維護

供應商必須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。
供應商必須在系統的獲取、開發和維護過程中，執行以下動作：

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。供應商必須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；並且

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。

8. 資產管理

供應商必須維護專為教育員工瞭解如何分類、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，內容從資訊的建立，涵蓋到資訊的處理、儲存和處置。

供應商必須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。

供應商必須：

a) 維護 IT 資產的清查資料，並管理相關的資產生命週期。確保資產僅可使用於經過協議的用途。

b) 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。

c) 根據國防部、NIST 800-88 或同等標準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。

d) 在供應商與美光的合作結束或終止時，或在美光提出請求時，供應商必須清除敏感資料並以安全的方法銷毀（或在美光請求下歸還至美光）所有美光資訊的副本，無論任何電子或非電子格式，且必須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。

9. 存取管控

供應商必須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），以便確保只有授權人員獲得美光資料的存取權。存取請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。

供應商必須在存取管控措施中採取以下動作：

a) 必須利用識別碼，以邏輯方式限制存取，讓其他供應商用戶端無法檢視或存取美光資料。

b) 在合作終止後，或在內部轉移後經過合理的商務期間，直至該存取權已不再需要的階段，立即撤銷存取權。

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) 收集、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；並且

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。

h) 收集、監控與保留記錄，以便美光資料的存取可供追蹤。

10. 加密技術

供應商所維護的加密政策必須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。

供應商必須維護政策、程序和技術來為轉移中及待用的美光資料加密。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。

供應商必須與美光合作實施可靠且安全的電子資料轉移方法，藉此滿足美光需求。

11. 實體安防與環境安防

供應商必須維護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）、入侵偵測和警示功能、適當的存取管控系統、訪客管理與記錄。基礎建設和環境管控措施可能包括但不限於與當地法律和業界標準相符的電力、溫度和濕度監控、滅火系統、通用電源 (UPS)、緊急或備份系統。

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。供應商在美國境外的營運，必須維護嚴格程度不低於當地法規的管控措施。

12. 營運安防

供應商必須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。供應商必須在該辦法中維持以下安防管控措施：

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) 收集 IT 資產和感測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) 監控與管控員工與網際網路的連線；以及

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。

13. 事業韌性

供應商必須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。供應商必須透過電信通訊、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。供應商維護的復原計畫必須可在事件期間或之後執行，且必須在受到請求時將相關計畫與美光分享，證明遭到連續性事件影響的系統可以復原。為求供應商的業務持續性和災難復原辦法的成果，供應商的復原時間目標（「**RTO**」）和復原點目標（「**RPO**」）必須與美光的 RTO/RPO 相符，並以雙方的服務曾及協議為基礎來運作。

14. 資訊安防突發事件管理

供應商必須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，供應商必須進行以下動作：

a) 評估安防事件和可疑突發事件。

b) 以遏制和減輕突發事件的方式來反應。

c) 確定行動以盡量減少類似突發事件再次發生的風險；以及

d) 依據保留證據的法律需求進行調查。

e) 認識習得的教訓以提高突發事件管理之整體能力。

15. 資料突發事件或外洩通知

如果發生任何漏洞導致美光資料遺失、銷毀、遭致破壞、損毀、無法使用或遭到存取（例如遭到查看、複製、修改、揭露或傳送），供應商必須立即透過 security@micron.com 通知美光，並遵守任何適用的合約或法定需求。供應商必須自行支出費用復原上述美光資料。供應商必須依據適用法律、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安防突發事件、未授權或非法處理後，超過 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。供應商必須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) 促成與供應商的員工、前員工、承包商、委外處理者和其他涉及事件的人員面談；以及

d) 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，不得向任何第三方告知發生任何安防突發事件。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，或經美光獨自裁量，決定是否向任何受影響的個人、監管機構、執法機關或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。

供應商必須負擔執行本節所述義務而產生的所有合理費用。供應商也必須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。供應商同意維護與保留所有與任何安防突發事件相關的文件、記錄和其他資料。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。

16. 通訊安防

供應商必須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。

供應商必須：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。

17. 供應商關係

供應商必須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。供應商對於上述處理或儲存美光資料的提供者所執行的服務負有責任，責任範圍與供應商自行執行服務時相同，且必須與處理或儲存美光資料的提供者成立書面協議，協議需與供應商的資訊安防義務一致，且適用於提供者所執行的服務。

18. 安防保證及評估

在美光的請求下，供應商必須每年以 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。

在美光的書面請求下，為了確認遵守本標準及任何適用法律和業界標準，供應商必須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。供應商必須完全配合相關調查。美光會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必須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 90 天前提供書面通知。供應商所產生的安防評估時數和稽核時數，不得造成美光任何費用。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人員具有無限制的實體存取權。供應商必須派遣安防人員接受美光的合理詢問。美光不得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請求）。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

光和供應商必須立即針對補救計畫取得共識，且供應商必須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。