德明財經科技大學

伺服器代管規定

機密等級：一般

文件編號：Takming-ISMS-B-016

版　次：V 1.2

初版日期：108.10.30

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	108.10.30	N/A	執行小組	初版
1.1	114.02.08		推動小組	修改目的內容，新增集中化管理與虛擬伺服器
1.2	115.06.10	2,3	推動小組	新增雲端服務項目

伺服器代管規定					
文件編號	Takming-ISMS-B-016	機密等級	一般	版次	1.2

1. 目的

德明財經科技大學 (以下簡稱本校)為遵循資安法規範，集中化管理本校資通系統，提供非電子計算機中心(以下簡稱本中心)管轄之伺服器申請放置本中心機房機架空間或申請伺服器代管，特訂定本校伺服器代管規定(以下簡稱本規定)。

2. 適用範圍

本規定所指伺服器係指本校各行政及學術單位用以提供網際網路服務之各式伺服器。

3. 名詞定義

無。

4. 權責

4.1. 各單位建置伺服器時，基於資源整合運用與校園資安考量，請會同本中心先行評估，若確有購置必要者，得於年度或相關經費內編列預算採購，惟採購經費來源屬專案計畫者，不在此限。

4.2. 本中心進行評估時，以可使用虛擬伺服器運作為優先考量；若所申請者不適用虛擬伺服器，才選擇採購實體伺服器。

4.3. 各單位購置伺服器時，應將採購規格(含服務軟體與硬體設備) 會請本中心審查，基於資安要求，一律置於本中心機房，委託本中心管理(主機代管)。

4.4. 各單位委託本中心代管之伺服器，須提供系統管理者帳號與密碼，由本中心代為執行系統管理與資訊安全相關作業，惟網路服務或服務軟體之使用與管理仍須由各單位指定專人或由委外廠商負責。

4.5. 各單位伺服器管理人員應為本校專任之教職員，不得為兼任教師或學生，人員異動時，應主動通知本中心，並更新相關資料。

5. 要求事項

5.1. 提供各單位伺服器代管內容及範圍如下：

5.1.1. 由本中心提供機房機架空間及必要之空調、電力、學術網路等基礎設施， 供申請單位放置伺服器等設備。

5.1.2. 各申請單位放置之設備以機架型伺服器為原則，放置地點原則上為本中心機房。

5.1.3. 各申請單位須遵守本校「校園網路使用規定」及「資訊安全政策(ISMS) 」規定。

5.1.4. 本中心不提供作業系統、資料庫等相關軟體授權(License)，申請單位須自行準備。

5.1.5. 本中心不提供委外開發軟體系統及其配合開發元件之安裝、功能修改，各申請單位須自行作業。代管之伺服器如有維護需求，請提出「軟硬體需求服務申請表」由電算中心與廠商簽訂維護合約。

5.1.6. 各申請單位之伺服器系統發生遭經由網路入侵、破壞、竊取資

料等情形 所衍生之損失，本中心不負賠償責任。

5.1.7. 各申請單位之伺服器硬體、系統、資料，因天災、停電、電信業者線路障礙等不可抗力因素造成損失，本中心不負責賠償責任。

5.1.8. 停電時本中心機房不斷電系統(UPS)僅能暫時提供停電期間之緊急用電，無法長時間供應伺服器主機持續運作所需之電力，各申請單位需自行判斷伺服器之處置方式。

5.2. 申請本校機房伺服器代管，悉依下列規定及程序辦理：

5.2.1. 由需求申請單位填寫「伺服器代管申請書」，提出書面申請，本中心得考量機房相關設施容量狀況，決定是否接受申請。

5.2.2. 各申請單位之伺服器須黏貼校內財產標籤。

5.2.3. 伺服器移入機房時，各申請單位人員須與本中心管理者於現場核對其型號、規格、數量及財產編號等資料。

5.3. 雲端服務

5.3.1. 獲取雲端服務

5.3.1.1. 需求評估：業務單位應定義雲端服務需求，包括資料儲存、安全性及擴展性要求。電算中心應協助進行服務提供者的技術可行性與安全性評估。

5.3.1.2. 風險評估：進行雲端服務風險評估，包括資料安全、服務中斷及法律合規性風險。特別針對 Google 雲端硬碟等工具，評估其共享功能和跨境資料傳輸風險。

5.3.1.3. 供應商選擇：優先選擇符合安全標準（如 ISO 27001、SOC 2）的供應商。確保協議中涵蓋資料刪除、災害復原及責任分界條款。

5.3.2. 使用雲端服務

5.3.2.1. 存取與權限管理

5.3.2.1.1. 使用者帳號與存取權限：所有使用者帳號應綁定組織電子郵件，並啟用多因子驗證（MFA）。

5.3.2.1.2. 將權限分層：基礎使用者、管理員、超級管理員。定期審核帳號的活躍狀態及權限分配，移除多餘或未授權的存取權限。

5.3.2.1.3. 資料共享控制：將檔案共享功能限制為組織內部使用為預設值，特例共享需經管理員審核。禁用「任何有連結者可存取」的設定，並記錄所有外部共享的審核流程。

5.3.2.2. 資料分類與安全配置

5.3.2.2.1. 資料分類：將資料分為機密、內部使用、公用，並根據分類設定不同的存取控制和加密

要求。將高機密資料儲存於具備更高安全性的雲端儲存解決方案中。

5.3.2.2.2. 安全配置：啟用服務中的安全功能（如 Google 雲端硬碟的活動記錄與審核日誌）。使用端點管理工具（如 Google Workspace Admin Console），集中管理所有設備和服務存取。

5.3.3. 管理與監控

5.3.3.1. 日誌與活動監控

5.3.3.1.1. 活動記錄：開啟日誌記錄功能，追蹤所有檔案的存取、編輯、刪除及共享操作。對於可疑行為（如大批量下載或未授權設備存取），自動觸發警報。

5.3.3.1.2. 定期審核：每季度進行雲端服務的安全配置與共享檔案清單審查，確保符合政策要求。

5.3.3.2. 資料備份與復原

5.3.3.2.1. 備份策略：使用第三方備份工具對雲端儲存的關鍵資料進行定期備份，避免資料丟失。備份應包括 Google 雲端硬碟的關鍵檔案、Google 表單的回應資料等。

5.3.3.2.2. 災害復原計畫：定義資料復原目標時間（RTO）與目標復原點（RPO）。進行年度災害復原演練，確保服務中斷期間資料可快速回復。

5.3.4. 退出雲端服務

5.3.4.1. 資料轉移與刪除

5.3.4.1.1. 資料導出：終止雲端服務前，將所有資料導出至內部系統或其他雲端平台，確保資料完整性。Google 雲端硬碟的檔案可透過 Google Takeout 工具進行批量導出。

5.3.4.1.2. 資料刪除要求：供應商應按照協議刪除所有組織資料，並提供刪除證明。特別對於儲存於 Google 雲端的共享檔案或表單回應，需檢查刪除後是否存在備份痕跡。

5.3.5. 文件與記錄

5.3.5.1. 雲端服務風險評估報告。

5.3.5.2. 帳號與權限清單。

5.3.5.3. 雲端資料刪除證明文件。

5.3.5.4. 共享檔案與日誌審查報告。

5.3.6. 定期審查與改進

5.3.6.1. 每年至少審查一次，特別針對服務使用的風險變化及法律規範的更新進行修訂。若發生重大安全事件，需即時檢討並更新相關程序。

6. 參考文件

6.1 軟硬體需求服務申請表。

6.2 伺服器代管申請書。