敏惠醫護管理專科學校

「資訊安全管理系統」
雲端服務資訊安全管理程序書

機密等級：一般

編　　號：IS-MHCHCM-02-017

版本編號：1.0

制訂日期：112.10.30

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說　　明	核准者
1.0	112.10.30	資訊安全執行小組	初版發行	執行秘書

本程序書由資訊安全執行小組負責維護。

目錄：

1 目的

1.1 為防止敏惠醫護管理專科學校（以下簡稱本校）之雲端資料在不安全之網路服務環境下，產生遭到破壞、被竊取之疑慮、或非預期及非經授權之修改，故建立本程序以確保雲端資料之安全性、可用性及完整性。

2 適用範圍

2.1 本校所轄範圍內相關雲端服務及設備之管理。

3 權責

3.1 本校網路與系統管理人員應遵守本程序書之相關規定，以確保雲端之安全。

4 名詞定義

4.1 雲端運算服務

4.1.1 包含基礎設施作為服務(Infrastructure as a Service, IaaS)、平台作為服務(Platform as a Service, PaaS)及軟體作為服務(Software as a Service, SaaS)。

4.2 雲端服務提供者

4.2.1 依據契約、類契約、法令規範或行政命令，提供本校雲端服務之供應商。

5 作業說明

5.1 雲端服務安全規劃作業

5.1.1 本校於選擇雲端服務應評估對本校核心業務與核心系統之風險與衝擊，參考資通安全責任等級辦法附表九進行風險與衝擊評估，並彙整於雲端服務安全等級清冊。

5.1.2 本校應至少每年評估一次雲端服務對本校核心業務與核心系統之衝擊程度，並評估雲端服務提供者提供服務之適切性，確保雲端服務持續受到監督、審查與評估。

5.1.3 前項所示之雲端服務適切性不足時，宜考量進行變更雲端服務提供者，進行資料遷移計畫或資通系統遷移計畫，並依照雲端服務終止管理規定辦理。

5.2 選擇雲端服務提供者

5.2.1 在選擇雲端服務提供者時，應優先考量政府電子採購網共同供應契約平台之雲端服務廠商。評估廠商時，如有必要得要求廠商展示與說明其資安防護部署、個資管理及適法性，或邀請第三方進行獨立評估，或由需求單位依下列內容進行評估：

5.2.1.1 根據產業公認的架構和基礎設施標準提供解決方案；

5.2.1.2 管理雲端服務的訪問控制，以滿足組織的要求；

5.2.1.3 實施惡意軟體監控和保護解決方案；

5.2.1.4 在核可的位置（特定國家或地區）或特定管轄範圍內或受其約束，處理和儲存組織的敏感資訊；

5.2.1.5 在雲端服務環境中發生資訊安全事件時，提供專門支援；

5.2.1.6 確保在雲端服務進一步分包給外部供應商的情況下滿足組織的資訊安全要求（或禁止將雲端服務分包）；

5.2.1.7 支援該組織收集數位證據，同時考慮到不同司法管轄區的數位證據法律和法規；

5.2.1.8 當組織希望退出雲端服務時，在適當的時間範圍內提供適當的支援和服務可用性；

5.2.1.9 根據組織用作雲端服務客戶的雲端服務提供商的能力，提供所需的資料和配置資訊備份，並酌情安全地管理備份；

5.2.1.10 在提供服務期間或終止服務時提出要求時，提供並返回作為雲端服務客戶的組織擁有的資訊，如配置檔案、原始碼和資料。

5.2.2 於使用雲端服務前，應與雲端服務提供者共同商議，以確保符合校雲端服務資安政策，並於資通安全與個資保護上符合校需求。惟雲端服務提供者訂價政策與服務協議無法協商與變更

時，應尋找最符合雲端服務資安目標之雲端服務提供者，並識別風險，擬定對應管理措施。

5.2.3 在契約與服務水準協議可協商情況下，本校應確認契約或服務水準協議中至少包含下列內容：

5.2.3.1 雲端服務內容與保證

5.2.3.2 雲端服務之限制

5.2.3.3 雲端服務中雙方之權利與義務

5.3 雲端服務資安事件與營運持續管理

5.3.1 雲端服務資安事件管理準用資訊安全事件管理程序書，並應加以考量事件責任歸屬與受損範圍，必要時保留不法侵害之證據與受損害事實。

5.3.2 本校宜考量雲端服務之營運持續性，如有事實足認雲端服務可能中斷時，宜納入營運持續演練計畫，包含資料遷移、服務中斷應變作業等。

5.4 雲端服務變更與終止管理

5.4.1 雲端服務變更管理

5.4.1.1 因重大異動須中止雲端服務業者，需填寫「系統及網路變更申請表」，經權責主管同意後進行。

5.4.1.2 調整雲端服務設定需留下完整操作與變更紀錄，且於調整前備份或記錄現行設定。

5.4.2 雲端服務終止管理

5.4.2.1 本校若僅終止一部雲端資源使用，即視為變更，應依循前項雲端服務變更管理執行。

5.4.2.2 本校若終止全部雲端資源使用，應於變更前對受影響關係人與其他相依之營運進行通知，並填寫「系統及網路變更申請表」，經主管同意後使得為之。

5.4.2.3 雲端服務終止後，應於立即刪除在雲端服務平台資料、將資料遷移回校、將資料遷移至另一個雲端服務提供者或在原雲端服務提供者中進行存檔。如未能即時刪除者，應將原因與理由敘明於「系統及網路變更申請表」，經主管同意後使得為之。

5.5 資料備份

5.5.1 各項雲端資料均應由各負責人員訂定備份週期，並依據週期執行系統排程或手動備份，相關備份要求需遵循本校「資訊備份管理說明書」。

5.5.2 應定期於測試雲端資料是否正確。

5.5.3 重要雲端資料應考量建立異地備份機制。

5.6 雲端服務存取控制

5.6.1 雲端服務管理人員準用本校帳號及通行密碼管理規定。

5.6.2 經授權之雲端服務使用者，只能在授權範圍內存取資源。

5.6.3 雲端服務使用者應遵守安全規定，並確實瞭解其應負之責任；如有違反安全情事，應依資訊安全規定，限制或撤銷其雲端服務資源存取權利，並依相關規定處理。

5.6.4 雲端服務使用者不得將自己之登入身分識別與登入密碼交付他人使用。

5.6.5 禁止雲端服務使用者以任何方法竊取他人之登入身分與登入雲端服務通行碼。

5.6.6 雲端服務使用者不得將色情檔案建置在網路，亦不得散播色情文字、圖片、影像、聲音等不法或不當之資訊。

5.6.7 雲端服務使用者不得任意修改雲端服務相關參數。

5.6.8 為維護本校雲端服務安全，管理人員於發現雲端服務使用者之電腦發送異常封包或使用非經允許之服務時，得中斷其雲端服務使用權限。

5.6.9 應定期或不定期檢查支援重要業務之作業系統是否有任何未核

准的檔案或未經授權的修改。

5.6.9.1 應於使用前檢查自雲端下載檔案有無惡意軟體。

6 相關文件

6.1 雲端服務安全等級清冊。

6.2 系統與網路檢查紀錄表。