

敏惠醫護管理專科學校

「資訊安全管理系統」 組態管理作業說明書

機密等級：一般

編號：IS-MHCHCM-03-012

版本編號：1.0

發行日期：

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

組態管理作業說明書					
文件編號		機密等級	普通	版本	1.0

目錄

1	目的	1
2	適用範圍	1
3	權責	1
4	名詞定義	1
5	作業說明	1
6	相關文件	4
7	附件	4

組態管理作業說明書					
文件編號		機密等級	普通	版本	1.0

1 目的

為確保敏惠醫護管理專科學校（以下簡稱本校）硬體、軟體、服務及網路於所要求安全設定下正常運行，避免配置不會因未經授權或不正確的更改而改變，以及協助本校建立書面紀錄、實作、監視並審查硬體、軟體、服務及網路之組態（包括安全組態），特訂定組態管理作業說明書（以下簡稱本作業說明書）。

2 適用範圍

本校資訊安全實際範圍相關硬體、軟體、服務及網路之安全組態，如下：

2.1 硬體：伺服器主機、核心交換器、防火牆、IPS。

2.2 軟體：核心系統、伺服器作業系統、伺服器應用程式、作業系統、應用程式、瀏覽器。

2.3 網路及服務：ADSL 服務、無線網路。

3 權責

3.1 本校相關資訊系統管理人員、個人電腦使用者、委外人員：遵守本作業說明書之相關規定，以確保本局相關軟體與資料等資訊資產之安全。

3.2 組態擁有者：確認組態基準，審核組態查檢結果，以及定期審查組態清冊及組態例外清單內容。

4 名詞定義

4.1 標準組態基準

由國家標準與技術機構(NIST)或我國資通安全中央主管機關公告之資訊安全組態基準。

4.2 自訂組態基準

由本局授權自行或委外定義並建置之資訊安全組態基準。

5 作業說明

5.1 建立組態基準

組態管理作業說明書					
文件編號		機密等級	普通	版本	1.0

5.1.1 標準組態基準

5.1.1.1 本校建立標準組態基準時，應依照下列原則與注意事項進行之。

5.1.1.1.1 使用依據開發商所提供之操作指引或公開說明書。

5.1.1.1.2 宜考量機關之資通安全等級與保有之資料進行設定。

5.1.1.2 宜考量機關之資訊安全政策、法令法規要點指引及其他安全要求事項。

5.1.1.2.1 宜考量在組織全景中，標準組態基準之可用性與適用性。

5.1.1.3 本校應考量新型威脅弱點、系統更新或硬體更新，必要時更新標準組態設定。

5.1.1.4 本校應定期審查標準組態設定之妥適性。

5.1.1.5 本校於設定標準組態基準時，應依照下列原則與注意事項進行之。

5.1.1.5.1 將具有特權或系統管理員等級之存取權限的身份數量減至最少。

5.1.1.5.2 停用不必要、未使用或不安全的身份。

5.1.1.5.3 停用或限制非必要的功能和服務。

5.1.1.5.4 限制對強效公用程式和主機參數設定之存取權限。

5.1.1.5.5 鐘訊同步。

5.1.1.5.6 安裝後，立即變更廠商預設鑑別資訊，如預設密碼，並審查其他重要的預設安全相關參數。

5.1.1.5.7 應設定無動作逾時自動登出機制。

5.1.1.5.8 查證是否為授權使用。

5.1.1.6 標準組態基準可參照「政府組態基準」之說明文件或指引。

5.1.2 自訂組態基準

組態管理作業說明書					
文件編號		機密等級	普通	版本	1.0

5.1.2.1 應最大限度符合本局系統獲取開發與維護作業規範，並留下開發與版次變更紀錄。

5.1.2.2 本校自行或委外建置組態基準，應可實作硬體、軟體、服務（含雲端服務）、網路、新安裝之系統以及運作中之系統，並符合安全系統發展生命週期(SSDLC)之要求。

5.1.3 組態基準應經過組態擁有者確認，已確認之組態基準由系統管理者記錄於「組態清冊」中。

5.1.3.1 「組態清冊」宜包含下列內容：

5.1.3.1.1 組態 ID 及名稱

5.1.3.1.2 版本

5.1.3.1.3 參照之標準組態來源

5.1.3.1.4 最後組態變更日期

5.1.3.1.5 相關資產

5.1.3.1.6 組態擁有者或聯絡窗口資訊

5.2 管理組態

5.2.1 組態變更管理（組態異動）

5.2.1.1 組態欲實施變更時，應依「系統開發與維護程序書」中變更管理程序辦理。

5.2.2 組態備份

5.2.2.1 針對組態應實施備份。

5.2.2.2 當組態項目首次設定或變更時需執行備份作業。

5.2.2.3 每季至少一次的完整組態備份作業，至少保留四代。

5.2.3 例外管理

5.2.3.1 公務機關應符合「政府組態基準」所要求之組態設定，如有例外排除項目應另外記錄於「組態例外清單」。

5.3 監控組態

組態管理作業說明書					
文件編號		機密等級	普通	版本	1.0

5.3.1 組態查檢

5.3.1.1 系統管理者應**每季**至少一次的執行組態查檢，並填寫「**組態查檢紀錄表**」或「**網路或系統檢查紀錄表**」經組態擁有人審核。

5.3.1.2 如有發生以下狀況並與組態相關，需執行組態查檢，並填寫「**組態查檢紀錄表**」經組態擁有人審核。

5.3.1.2.1 系統變更。

5.3.1.2.2 發生資安事件。

5.3.1.2.3 上級機關要求異動。

5.3.1.2.4 稽核缺失。

5.3.1.3 當組態查檢發現異常時，應依據「**矯正管理程序書**」辦理矯正作業。

5.3.2 組態審查

5.3.2.1 「**組態清冊**」應**每年**至少一次由組態擁有人審查一次（如有「**組態例外清單**」則須包含「**組態例外清單**」）。

5.3.2.2 組態擁有人審查「**組態清冊**」時，應留意紀錄內容跟實際設定是否相符。

6 相關文件

6.1 組態清冊

6.2 組態例外清單

6.3 組態查檢紀錄表

7 附件

7.1 無。