敏惠醫護管理專科學校

「資訊安全管理系統」
矯正及持續改善管理程序書

機密等級：一般

編號：IS-MHCHCM-02-014

版本編號：1.1

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	110.12.30	資訊安全執行小組	初版發行	執行秘書
1.1	112.10.30	資訊安全執行小組	修訂頁首、頁尾，新增預防措施定義	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 針對敏惠醫護管理專科學校（以下簡稱本校）資訊安全管理制度（ISMS）運作過程中發生之缺失及潛在之風險，採取相關的矯正及持續改善措施，以防止類似事件發生，進而達成持續改善之目標。

2 適用範圍

2.1 本校資訊安全管理制度（ISMS）各項作業流程發生之缺失、發生資訊安全事件及潛在之風險處理事項。

3 權責

3.1 資訊安全委員會：負責矯正與持續改善措施之管理審查。

3.2 缺失權責單位：負責稽核所發現缺失、資訊安全事件（含重大異常事件）或自行發現缺失之原因分析，決定優先順序與處理時限，提出矯正或持續改善措施並實施。

4 名詞定義

4.1 矯正措施：為防止不符合資訊安全管理制度（ISMS）實施、操作及使用之事項重複發生，所採取之措施。

4.2 預防措施：為預防不符合資訊安全管理制度（ISMS）實施、操作及使用之事項發生，所採取消除未來不符合事項發生原因之措施。

4.3 缺失：不符合資訊安全管理制度（ISMS）實施及操作事項者。依影響程度分為：

4.3.1 主要缺失：未執行資訊安全管理制度（ISMS）之要求，或多個次要缺失集中於同一控制措施者。

4.3.2 次要缺失：未能完全遵循資訊安全管理制度（ISMS）之要求，但為單一事件者。

4.3.3 觀察事項：發現可能對資訊安全管理制度（ISMS）造成影響的事實及事件，但未有足夠證據顯示會影響資訊安全政策及目標的達成，卻因未來可能成為缺失而需要再覆核。

4.3.4 建議事項：發現可能對資訊安全管理制度（ISMS）造成影響的潛在問題，可提出建議之改善措施，以持續改善未來發生之可能性。

4.4 潛在風險：尚未發生但未來有可能發生之不確定事件。

4.5 暫時性對策：能控制缺失的擴大或消除單一事件的影響之措施。

4.6 永久性對策：能消除缺失或潛在風險的根本原因之措施。

4.7 缺失權責單位：矯正及持續改善措施之實際執行單位。

4.8 追蹤人：進行矯正或持續改善措施執行狀況之追蹤，可由資訊安全稽核小組組長、組員或相關權責人員負責，但不可由該矯正或持續改善措施處理人員擔任。

5 作業說明

5.1 執行時機

5.1.1 內部或外部稽核發現缺失時，缺失權責單位需提出矯正措施，並填寫於「矯正處理單」。

5.1.2 發生資訊安全事件（含重大異常事件）或自行發現缺失時，應執行矯正或持續改善措施，並填寫於「矯正處理單」。

5.2 原因分析

5.2.1 防制缺失權責單位應分析問題發生之原因及影響程度，決定優先順序與處理時限。

5.3 矯正與持續改善措施評估

5.3.1 缺失權責單位提出矯正與持續改善措施時，得區分為暫時性對策及永久性對策，防止類似事件發生。

5.3.2 評估措施時須考慮成本效益及可行性。

5.4 追蹤執行狀況

5.4.1 矯正與持續改善措施之執行狀況，應由缺失權責單位依據「矯正處理單」確實執行。

5.4.2 有關執行狀況之追蹤，由資訊安全稽核小組組長、組員或相關權責人員負責。

5.4.3 追蹤人最遲應於收到「矯正處理單」後，依據所提預計完成日

期進行追蹤，並應於「矯正處理單」上留存追蹤軌跡。

5.5 管理審查

5.5.1 缺失權責單位應彙整相關矯正及持續改善措施之執行狀況，於管理審查會議提出報告。

6 相關文件

6.1 矯正處理單