

敏惠醫護管理專科學校

「資訊安全管理系統」 資訊安全稽核程序書

機密等級：一般

編號：IS-MHCHCM-02-013

版本編號：1.0

制訂日期：110.12.30

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 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

本程序書由資訊安全執行小組負責維護。

目錄：

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

1 目的

- 1.1 建立敏惠醫護管理專科學校（以下簡稱本校）獨立稽核之規範，以判斷各項作業的控制目標、措施、流程及程序是否符合法規及本校之資訊安全要求。

2 適用範圍

- 2.1 本校施作範圍內之資訊安全稽核作業管理。

3 權責

3.1 資訊安全委員會

- 3.1.1 指派資訊安全稽核小組組長及組員。
- 3.1.2 負責督導資安稽核作業。

3.2 資訊安全稽核小組

- 3.2.1 辦理稽核作業相關事宜。
- 3.2.2 稽核缺失定期追蹤改善情形並加以記錄。

3.3 資訊安全稽核小組組長

- 3.3.1 確保稽核業務依本程序書確實執行。
- 3.3.2 協調提供稽核所需資源。
- 3.3.3 編製資訊安全稽核計畫。
- 3.3.4 召開資訊安全稽核小組準備會議。
- 3.3.5 召開稽核啟始及結束會議。

3.3.6 負責報告稽核執行情形及成果。

3.3.7 列管「資訊安全內部稽核報告」及所附相關查核資料。

3.4 資訊安全稽核小組組員：配合資訊安全稽核小組組長指示，執行稽核作業、完成各項紀錄及查證矯正與持續改善措施執行情形。

3.5 受稽部門：受稽部門之主管於稽核期間應指派人員接受稽核，並協助調閱有關紀錄、報告或文件。對於稽核發現缺失應提出並執行矯正與持續改善措施。

4 名詞定義

4.1 資安稽核：一種有系統且獨立的資訊安全檢查，以決定各項活動及相關結果是否與所計畫的安排相符，以及安排是否有效執行及達成目標。

4.2 稽核類別：

4.2.1 內部稽核：由資訊安全稽核小組針對本校之資訊安全控制、風險評鑑與營運持續運作計畫等作業，進行定期查核，以確保其成效。

4.2.2 外部稽核：由本校以外單位所進行的資訊安全稽核。

4.2.3 專案稽核：專案稽核得視特定目的需求（例如：資訊安全事件調查），以不定期之專案方式進行。

5 作業說明

5.1 稽核頻率

5.1.1 每年定期辦理資訊安全內部稽核作業。

5.1.2 視需要不定期執行專案稽核。

5.2 稽核人員之要求

5.2.1 資訊安全稽核小組之組長與組員由資訊安全委員會指派。為確保稽核過程的客觀性與獨立性，稽核之執行應由非受稽人員擔任稽核員。稽核人員資格要求如下：

5.2.1.1 資訊安全稽核小組組長：須由接受資安相關稽核訓練者擔任。

5.2.1.2 資訊安全稽核小組組員：須由接受資安相關稽核訓練者擔任。

5.3 稽核計畫

5.3.1 為達稽核之有效性，資訊安全稽核小組組長應事前規劃並編製「資訊安全管理制度內部稽核計畫」，以作為執行稽核指導綱要，內容應包括：稽核範圍、項目、人員、時程、程序等，並經資訊安全委員會核准後執行。

5.4 稽核準備

5.4.1 資訊安全稽核小組組長應依據『ISO 27001:2013』條文要求，研擬規劃「資訊安全管理制度內部稽核表」，並召開小組準備

會議，提示稽核要點、協調分工及排定時程。

5.4.2 資訊安全稽核小組組長需於查核前通知受稽部門。

5.4.3 受稽部門於接獲稽核通知後，應配合準備稽核所需相關資料。

5.5 稽核執行

5.5.1 資訊安全稽核小組組長應於稽核前，召集資訊安全稽核小組、受稽部門召開啟始會議，說明稽核範圍、時程、配合事項等。

5.5.2 資訊安全稽核小組組員於稽核時，應依抽樣之原理收集足夠之客觀證據，以研判該稽核項目與相關規範之符合性。稽核時應保存適當之稽核軌跡。

5.5.3 資訊安全稽核小組組員依「資訊安全管理制度內部稽核表」執行稽核，逐項填寫稽核結果。「資訊安全管理制度內部稽核表」內容若須增修，需經資訊安全稽核小組組長同意。

5.5.4 受稽部門應尊重及支持資訊安全稽核小組，誠實答覆稽核人員所提問題，並接受調閱有關紀錄、報告及文件。

5.6 稽核報告

5.6.1 資訊安全稽核小組組員應於資訊安全稽核小組內部會議討論、彙整稽核發現，並由資訊安全稽核小組組長提出稽核報告。

5.6.2 資訊安全稽核小組組長應於稽核完成後召開稽核結束會議，由資訊安全稽核小組組長報告稽核發現，並對疑義進行澄清，稽

核報告應請受稽代表簽名。

5.6.3 受稽部門於接獲稽核報告後，應依據「矯正及持續改善管理程序書」之規定，將該單位之缺失分析原因及擬採行之矯正與持續改善措施填列於「矯正處理單」內，並經主管核定後回覆資訊安全稽核小組。

5.7 矯正及持續改善措施

5.7.1 稽核缺失之後續追蹤應依據「矯正及持續改善管理程序書」辦理。

5.8 稽核技巧與工具保護

5.8.1 系統稽核工具（如：弱點掃描系統等）之存取應由授權的人員於授權範圍內操作，並留有存取、操作紀錄，以防止任何可能之誤用或破解。

5.8.2 系統稽核工具應由專人保管，以防止不當操作造成其他系統之損害。

5.9 相關法令之要求

5.9.1 本校執行業務時，應遵守相關法令、法規之要求。資訊安全稽核小組亦應於每次進行資安稽核時檢視其符合性。

6 相關文件

6.1 『ISO 27001:2013』。

6.2 資訊安全管理制度內部稽核計畫。

6.3 資訊安全管理制度內部稽核表。

6.4 資訊安全內部稽核報告

6.5 矯正處理單。