# 敏惠醫護管理專科學校

# 「資訊安全管理系統」
# 組織全景與範圍程序書

**機密等級：一般**

**編號：IS-MHCHCM-02-020**

**版本編號：2.0**

**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 | 110.12.30 | 資訊安全執行小組 | 初版發行 | 召集人 |
| 2.0 | 112.10.30 | 資訊安全執行小組 | 將「組織全景分析手冊」從一階文件改為「組織全景與範圍程序書」二階文件<br>修訂頁首、頁尾及作業說明 | 召集人 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

本程序書由資訊安全執行小組負責維護。

目錄：

## 1 目的

1.1 敏惠醫護管理專科學校（以下簡稱本校）為強化資訊安全管理，確保資訊安全管理制度執行之範圍，期使本制度達成既定之目標，以維護資訊業務運作之安全。提供本校之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此程序規範。

## 2 適用範圍

2.1 本校各行政單位之資訊安全相關業務作業流程。

## 3 權責

3.1 本校資訊安全管理委員會建立及審查此程序及其相關內容。

3.2 資訊安全管理委員會透過適當的程序以實施此程序及其相關內容。

3.3 本校人員和委外供應商均需依相關安全管理程序以維護程序及其相關內容。

## 4 名詞定義

4.1 關注者：可影響、受其所影響、抑或自認會受到決策或活動影響的個人或組織。

4.2 內外部議題：

組織為尋求達成其目標所處之內外部環境，可能影響組織目標與範圍定義之風險因素。

4.3 資訊資產：係指為維持本校資訊業務流程運作之硬體、軟體、服務、文件及人員。

4.4 營運持續運作之資訊環境：係指為維持本校各項業務正常運作所需之電腦作業環境。

5 作業說明

5.1 關注方需求與期望鑑別

5.1.1 應識別對本校資訊安全有所需求與期望之關注者，並蒐集其需求與期望，相關作業程序如下：

5.1.1.1 應決定可能影響資訊安全管理系統之外部與內部議題，及辨識其利害相關者與對資訊安全相關之要求事項，並將分析結果填寫於「利害相關者與議題一覽表」中。

5.1.1.2 確認年度議題

5.1.1.2.1 應決定與本校目標及資訊系統、服務或流程相關，並會影響達成資訊安全管理系統預定成果的外部與內部議題，並將所擬定之議題填寫於「利害相關者與議題一覽表」中。

5.1.1.2.2 此等議題應包含法令、法規以及契約要求。

5.1.1.2.3 依據 ISO 31000 要求，內、外部議題可參考下列範圍。

5.1.1.2.3.1 外部議題

5.1.1.2.3.1.1 與本校相關的法令、法規、契約新增與異動。

5.1.1.2.3.1.2 同產業、機構、體系所引用的新技術、作業流程。

5.1.1.2.3.1.3 可供本校借鑒之任何資訊安全事項。

5.1.1.2.3.1.4 與外部利害相關者之關係互動與其對於組織之價值。

5.1.1.2.3.2 內部議題：

5.1.1.2.3.2.1 治理、組織結構、角色和責任。

5.1.1.2.3.2.2 政策、目標、及在不同階層實現這些目標的策略。

5.1.1.2.3.2.3 能力、資源和知識方面的理解（如資金、時間、人員、流程、系統和技術）。

5.1.1.2.3.2.4 內部關注者、組織的文化、觀念和價值的關係。

5.1.1.2.3.2.5 資訊系統、資訊流和決策過程（包括正式和非正式的）。

5.1.1.2.3.2.6 被組織所採用的標準、指引和模型。

5.1.1.2.3.2.7 契約關係的形式和範圍。

5.1.1.3 關注者需求與期望蒐集

5.1.1.3.1 應透過訪談與主動資料蒐集方式，蒐集關注者對本校資訊安全之需求與期望，依據系統進行分類，並填寫於「利害相關者與議題一覽表」中。

5.2 需求與期望項目鑑別

5.2.1 應鑑別關注者需求與期望項目類別屬於「風險項目」或是「機會項目」，並填寫於「利害相關者與議題一覽表」中。

5.2.2 若屬於「風險項目」則應納入資訊流程風險評鑑作業，進一步識別該風險等級。

5.2.3 若屬於「機會項目」則應納入資訊流程機會評鑑作業，進一步識別現有資源與施作效益，評估實作可能性與適切性。

5.2.4 相關風險處理與機會實作作業，應依據「風險評鑑與管理程序」辦理。

5.3擬定組織資訊安全範圍

5.3.1 活動間的介面及相依性分析

5.3.1.1 組織應於每年定期組織全景分析作業時，分析組織的各項資訊系統、服務或流程是否完全或部份由其他組織所提供，若是，則應分析其介面及相依性，並填入「利害相關者與議題

一覽表」，以作為組織擬定資訊安全範圍之依據。以反映政府法令、技術及業務等最新發展現況，以確保本校營運持續運作及提供學術網路服務之能力。

5.3.1.2 相依性評估依據如下：

| 相依性程度 | 評估標準 |
|---|---|
| 高 | 1. 系統完全由其他組織提供，且系統中斷服務時將影響組織營運。<br>2. 系統部份活動由其他組織提供，但該部份活動停止服務時，將導致系統中斷，且系統中斷服務時將影響組織營運。 |
| 中 | 1. 系統完全由其他組織提供，且系統中斷服務時會降低組織營運效率。<br>2. 系統部份活動由其他組織提供，但該部份活動停止服務時，將導致系統中斷，且系統中斷服務時會降低組織營運效率。 |
| 低 | 1. 系統完全由其他組織提供，且系統中斷服務時對組織營運影響甚微。<br>2. 系統部份活動由其他組織提供，但該部份活動停止服務時對組織營運影響甚微。 |

5.3.2 組織應依據內、外部議題分析討論、關注者需求與期望、活動間的介面及相依性分析結果，分析並評估組織現有資訊安全管理範圍是否須調整，並於管理審查會議上報告分析結果，並取得管理階層之核准。

## 6 責任

6.1 本校的管理階層需週期性更新並審查資訊安全全景與範圍。

6.2 資訊安全委員會透過適當的標準和程序定義並透用。

6.3 所有人員和委外服務供應商均須依照相關安全管理程序以維護資訊安

全政策。

6.4所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。

6.5任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行懲處。

## 7 實施

7.1資訊安全委員會每年召開資訊安全管理及審查會議，進行資訊安全政策審核。

7.2本政策經「資訊安全委員會」核定後實施，修訂時亦同。

## 8 相關文件

8.1利害相關者與議題一覽表。

8.2資訊安全組織成員表。

8.3外部單位聯絡清單。