

# 敏惠醫護管理專科學校

## 「資訊安全管理系統」 資訊安全政策

**機密等級：一般**

**編 號：IS-MHCHCM-01-001**

**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。



目錄：

1	目的 .....	3
2	適用範圍 .....	3
3	定義 .....	3
4	目標 .....	3
5	責任 .....	4
6	審查 .....	4
7	實施 .....	4

## 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，確保所屬之資訊資產的機密性、完整性及可用性，以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，特定此政策規範。

## 2 適用範圍

2.1 本校所有單位。

## 3 定義

3.1 無。

## 4 願景與目標

4.1 資訊安全政策願景：

強化人員認知、避免資料外洩

落實日常維運、確保服務可用

4.2 依據資訊安全政策願景，擬定資訊安全目標如下：

4.2.1 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。

4.2.2 保護本校業務活動資訊，避免未經授權的存取與修改，確保其正確完整。

4.2.3 定期進行稽核作業，確保相關作業皆能確實落實。

4.2.4 確保本校關鍵核心系統維持一定水準的系統可用性。

4.3 應針對上述資訊安全目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間以及結果評估方式與評估結果，相關監督與量測程序，應遵循本校「監督與量測管理程序書」辦理。

4.4 資訊安全執行小組應於管理審查會議中，針對資訊安全目標有效性量測結果，向資訊安全委員會召集人進行報告。

## 5 責任

5.1 本校的管理階層建立及審查此政策。

5.2 資訊安全執行小組透過標準和程序以實施此政策。

5.3 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。

5.4 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。

5.5 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。

## 6 審查

6.1 本政策應至少每年審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本校永續運作及資訊安全實務作業能力。

## 7 實施

7.1 任何機關單位因業務需求取得本校機敏性資訊或個人資料時，應負起

資料保密責任及妥善運用，並遵守國家相關之法令及本校之相關資訊安全規定。

7.2 若因機關單位疏失造成資料外洩或資安事件，應負相關法律責任。

7.3 資訊安全政策配合管理審查會議進行審核。

7.4 本政策經「資訊安全委員會」進行會審後，由召集人核定後實施，修訂時亦同。