

## 前言：

鑑於近年來電腦及網際網路應用之普及，為確保本院有關資料、資訊系統、設備及網際網路之安全，特訂定資訊安全管理作業規範，作為本院有關資訊安全管理組織權責分工、人員教育訓練、電腦軟硬體、網路及實體環境管理之準則。

## 壹、 資訊安全政策

一、 目標：本院資訊安全管理目標如下

- (一) 維護資訊系統持續運作。
- (二) 防止駭客、病毒等入侵及破壞。
- (三) 防止人為意圖不當及不法使用。
- (四) 避免人為疏忽意外。
- (五) 維護實體環境安全。

二、 範圍：本作業規範之範圍包括人員、應用系統、硬體設備及網路設施等部分。

(一) 人員：適用本院正式人員（含約聘、契約人員）與其他人員（含替代役、實習生）及使用本院資訊資源之委外廠商。

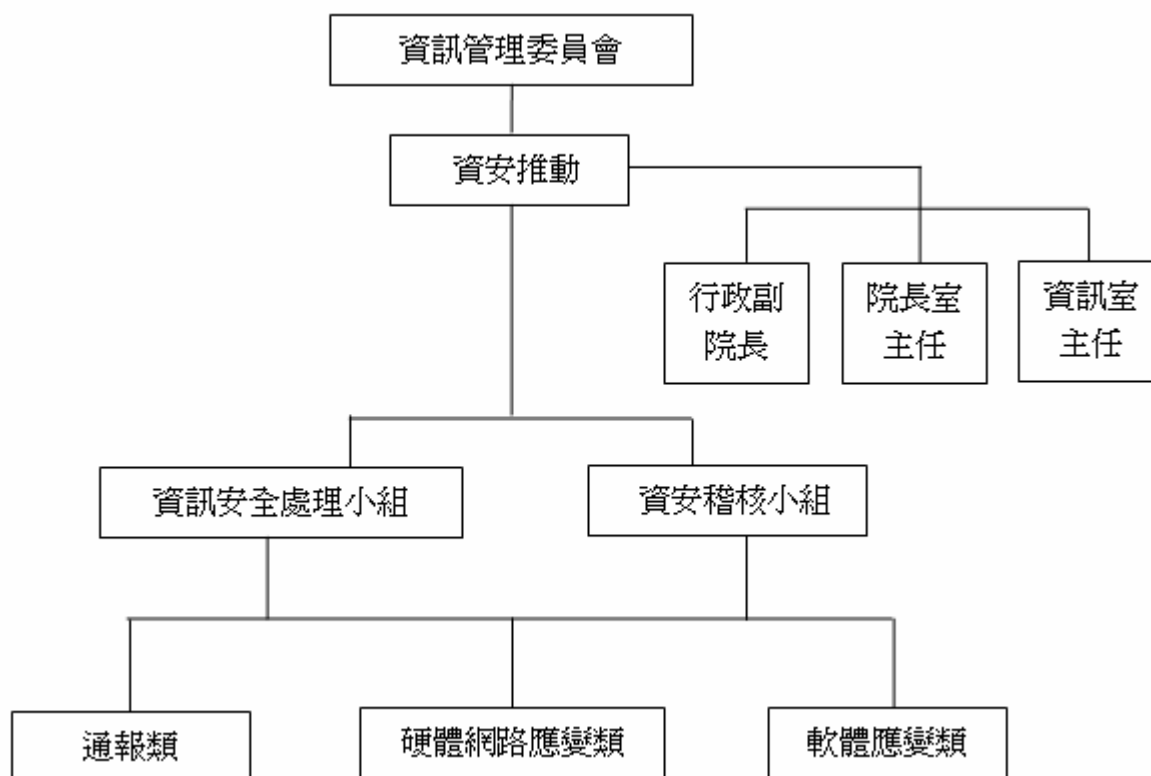
(二) 應用系統：1.本院醫療資訊系統。2.影像資訊系統。3.網頁及郵件資訊系統。4.本院行政管理資訊系統。

(三) 硬體及其設施：各式主機、伺服器、工作站及個人電腦。

(四) 網路設施：本院區辦公室內部網路（Intranet）及網際網路（Internet）及其相關設施。

## 貳、 資訊安全之組織與工作執掌

組織圖如下：



### 參、存取控制

- 一、 資訊單位對存取之程式，應依承辦人員之執掌，設定存取權限，除通行碼外，需配發執行密碼，並每三個月須變更密碼一次。
- 二、 對於識別碼閒置六個月以上未曾使用者，主管配發人員應瞭解後刪除。
- 三、 對進出系統之人員、時間，電腦應保留一年以上紀錄，進出紀錄應不定期稽核。
- 四、 程式安裝完畢後，應將廠商所預設的通行碼變更，並啟動反脅迫機制，禁止廠商以遠距控管方式執行維修作業。

### 肆、系統開發及維護

- 一、 系統委外開發者，應於合約書明定著作權歸屬及保密條款。
- 二、 進入系統作業人員應由單位主管視業務需要，申請通行密碼及識別碼，資訊單位核配後，使用者應立即變更密碼。
- 三、 系統應定期偵測病毒碼、木馬程式及間諜軟體，掃描處理結果並應做成紀錄呈核備查。

### 伍、考核

- 一、 資訊系統及程式進出管理紀錄應留存必要紀錄一年以上，俾供考核。
- 二、 各終端機使用人不得擅自安裝非法軟體，或將機密性資料存置於資料庫內。
- 三、 各資訊單位稽核小組每年執行稽核乙次，稽核結果彙整後，提資訊安全處理小組報告。

陸、本政策奉核後實施，修正時亦同。