# 佛教慈濟醫療財團法人台北慈濟醫院資訊安全政策

## 目的

隨著醫療機構資訊化作業及電子病歷系統之推動，為確保病歷資料安全性， 建置完善資訊安全系統已成為醫療機構不可或缺之重要措施，因此為確保佛教慈濟醫療財團法人台北慈濟醫院（以下簡稱本院）資訊系統服務正常且安全穩定的運作，特制定資訊安全政策（以下簡稱本政策）以作為規範本院之資訊安全管理制度最高指導方針，以建立安全、可信賴之資訊系統服務，並確保本院之資訊資產之機密性、完整性、可用性及符合相關法規之要求，以期維持本院業務持續運作，降低資訊作業風險，進而保障本院資訊系統服務使用者之權益及電子病歷安全。同時建立資訊安全人人有責之觀念，共同遵循本院資訊安全相關規範。

## 適用範圍

基於保護本院資訊資產機密性、完整性、可用性、適法性及個資性為目標，資訊室、資訊機房、資訊網路及醫療資訊系統為本院資訊系統服務之核心所在，故將其優先納入資訊安全管理範圍，推動建置完善資訊安全管理制度與服務系統，並期於日後將此資訊安全管理制度拓展至本院其他各單位之作業範圍。

參照ISO27001/CNS27001資訊安全要項，資訊室及資訊機房之資訊安全要項涵蓋11項管理事項，其目的在於避免因人為疏失、蓄意或天然災害等因素，導致資訊資產不當使用、洩漏、竄改、破壞等情事發生，進而對本院帶來可能之風險及危害。管理事項如下：

資訊安全政策
資訊安全組織
資訊資產管理
人力資源安全管理
實體與環境安全管理
通訊與作業管理
存取控制管理
資訊系統獲取、開發及維護管理
資訊安全事故管理
業務持續管理
遵循性管理

## 定義

資訊安全

係避免因人為或自然災害等風險，運用系統化之控制措施，以確保資訊安全管理制度範圍內之資訊資產受到妥善保護。

資訊資產

凡資訊室及資訊機房之資產，如文件、人員、軟體、硬體、服務與建

築等皆屬之。

資訊安全異常事故

凡因人為或自然災害因素，造成本院資訊系統服務中斷，或本院資訊資產遭竄改、刪除或竊取等，皆屬之。

資訊安全異常事故分級

資訊安全異常事故A級：資訊安全異常事故影響全院範圍，使本院資訊系統服務完全停頓超過一小時(含)，業務無法繼續;本院資訊系統服務遭竄改、刪除或竊取嚴重影響本院聲譽與民眾權益，造成嚴重財務損失。

資訊安全異常事故B級：資訊安全異常事故影響部分範圍，使本院資訊系統服務部分中斷超過半小時(含)或完全停頓低於一小時，影響業務效率;本院資訊系統服務遭竄改、刪除或竊取影響本院聲譽與民眾權益，造成輕微財務損失；便於後續追蹤故區分為「本院可自行處理」及「協力廠商處理」

資訊安全異常事故C級：資訊安全異常事故影響部分範圍，使本院資訊系統服務部分中斷低於半小時，可於議定時間修復;本院資訊系統服務遭竄改、刪除或竊取，造成作業不便，但未影響本院聲譽與民眾權益。

## 相關文件

資訊安全管理作業程序
資訊安全組織管理作業程序
醫療志業資訊保密辦法
國家資通安全發展方案
行政院國家資通安全會報
個人資料保護法
著作權法
ISO27001資訊安全管理制度
CNS27001資訊安全管理制度

## 作業說明

權責

資訊發展暨安全管理委員會

本院資訊系統發展暨安全管理階層決策組織。

資訊安全推動組

本院資訊室及資訊機房資訊安全管理制度規劃、建立、實施、維護、審查與持續改善，並將資訊安全相關議題於資訊發展暨安全管理委員會提報。

資訊室所有員工

皆應共同遵守本資訊安全政策。

提供資訊室資訊服務之廠商

皆應共同遵守本資訊安全政策

通則

應考量相關法律規章及營運要求，鑑別本院資訊資產價值，評估其弱點與威脅，以進行資訊資產之資訊風險評估，確定資訊作業安全需求，採取適當資訊安全措施，確保資訊資產安全。
依角色及職能為基礎，建立評估或考核制度，並視實際需要辦理資訊安全教育訓練及宣導。
定期執行資訊安全稽核作業，檢視資訊安全管理制度之落實。
資訊資產存取權限之賦予，應業務需求並考量最小權限與權責區隔。
違反本政策與資訊安全相關規範，依相關法規或本院人事規定辦理。
建立資訊安全事故通報及應變程序，以確保資訊室及資訊機房持續運作。
訂定業務持續計畫並定期演練，以確保資訊室及資訊機房於重大資安事故發生時，能妥善回應。
依據個人資料保護法與著作權法之相關規定，審慎處理及保護個人資訊與智慧財產權。
為確保本院同仁皆知悉本院資訊安全要求，另依據「醫療志業資訊保密辦法」公告本院同仁周知，並要求所有同仁簽署醫療志業資訊保密承諾書（應用表單6.1）。

目標

維持資訊室及資訊機房業務持續運作。
保護資訊室及資訊機房資訊資產，防止人為意圖不當或不法使用，遏止駭客、病毒等入侵及破壞之行為。
建立資訊室及資訊機房之標準作業程序，避免人為作業疏失及意外，加強同仁資訊安全意識。
確保達成營運量測指標
確保達成資訊安全管理量測指標
資訊安全機密性量測指標
資訊安全完整性量測指標
資訊安全符合法規量測指標

審查

本政策應至少每年評估一次，以反映相關法令、技術及資訊室業務等最新發展現況，並予以適當修訂。
本政策經本院資訊發展暨安全管理委員會核准，於公告日施行，並以書面、電子或其他方式通知經資訊室所有員工及提供資訊室資訊服務之廠商，修正亦同。

## 應用表單

醫療志業資訊保密承諾書

〈以上內容摘自本院資訊安全政策**FAE00A001-F6**〉