

# 新光吳火獅紀念醫院

## 資通安全政策

— 僅限本院同仁參閱 —

[illegible]

# 新光醫療財團法人新光吳火獅紀念醫院

文件編號	ISMS-1-01	文件名稱	機密等級	版本	3.0
制訂單位	資訊部	資通安全政策	內部使用	頁數	1/2

## 1 目的

為加強資訊安全管理，新光吳火獅紀念醫院（以下簡稱本院）特訂定資通安全政策（以下簡稱本政策）。本政策旨在確保資訊資料、系統、設備及網路通訊的安全，降低因人為疏失、蓄意行為或天然災害等風險，避免資訊資產遭竊、不當使用、洩漏、竄改或毀損。依據國際標準執行各項資訊安全措施，持續改善以降低風險。未規定事項則依政府其他資訊安全法規辦理，以達成資訊的機密性、完整性、可用性與適法性。

## 2 名詞解釋

本政策所稱資通安全係保護資訊資產避免遭受各種不當使用、洩漏、竄改、竊取、破壞等事故威脅，並降低可能影響及危害業務運作之損害程度。

機密性(Confidentiality)指確保只有經過授權的人才能存取資訊資產。

完整性(Integrity)指確保資訊資產其處理方法的準確性及完整 (Completeness)。

可用性(Availability)指確保授權的使用者在需要時，可以使用資訊資產。

適法性(Legality)符合本國相關法令規範。

## 3 適用範圍

3.1 基於本院以保護資通資產機密性、完整性、可用性為目標，資訊機房為本院資通系統服務之重要基礎架構，故將資訊部及資訊機房優先納入資訊安全管理系統(ISMS)範圍，展現負責之經營管理理念，期日後將資訊安全管理系統(ISMS)拓展至其他範圍。

3.2 資訊部及資訊機房之資訊安全管理系統(ISMS)涵蓋 ISO 27001(CNS 27001)標準之管理事項，並符合資通安全管理法，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本院帶來各種可能之風險及危害。

## 4 依據

本政策係依據「資通安全管理法」及其子法，ISO 27001 資訊安全管理系統標準，考量業務需求，訂定資通安全政策及相關標準作業程序，以建立資訊安全管理機制、強化資訊安全防護，提昇資訊安全之水準。

## 5 組織

為統籌資通安全管理等事項之規劃、執行、稽核及矯正活動，特成立跨單位之資通安全推

# 新光醫療財團法人新光吳火獅紀念醫院

文件編號	ISMS-1-01	文件名稱	機密等級	版本	3.0
制訂單位	資訊部	資通安全政策	內部使用	頁數	2/2

動組織，並依「ISMS-1-02\_資通安全組織章程」辦理。

## 6 實施目標與內容

相關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效(量測指標)，實施程序參見「ISMS-2-02\_資通安全實施程序書」。

- 6.1 各項資通安全管理規定必須遵守政府相關法規(如：刑法、國家機密保護法、著作權法、個人資料保護法、資通安全法等)之規定。
- 6.2 負責資通安全制度之建立及推動事宜。
- 6.3 定期實施資通安全教育訓練，宣導資通安全政策及相關實施規定。
- 6.4 建立資訊硬體設施及軟體之管理機制，以統籌分配、運用資源。
- 6.5 為考量各專案管理之資訊安全，應於研擬專案作業計畫或系統變動前，將資訊安全納入考量因素，防範發生危害系統安全之情況。
- 6.6 建立電腦機房實體及環境安全防護措施，並定期實施相關保養。
- 6.7 明確規範資訊系統之使用權限，防止未經授權之存取動作，必要時得採行加解密及身分鑑別機制，以加強資通資產之安全。
- 6.8 訂定資訊安全內部稽核計畫，定期檢視驗證推行資訊安全管理系統範圍內所有人員及設備使用情形，依稽核報告擬定及執行矯正措施。
- 6.9 訂定資訊安全之業務持續運作計畫並實際演練，確保業務持續運作。
- 6.10 本院所有人員均有維持資訊安全之責任，且應遵守相關之資訊安全管理規定。
- 6.11 建立本院資通系統之標準作業程序，避免人為作業疏失及意外，加強同仁資通安全意識。
- 6.12 建立連網醫療設備之資通安全管理機制。

## 7 實施與修正

本政策應至少每年評估一次，以反映政府相關法令、技術、醫療業務等最新發展現況，以確保維持營運和提供民眾適當服務的能力。本政策陳資安長核准後公告實施，修正時亦同。