臺北榮民總醫院

資通安全管理政策

文件編號：TVGH-I-01-01
機密等級：普通
版　　次：1.1
發行日期：115年8月27日

文件制/修訂紀錄

版次	制/修訂日期	制/修訂說明	作者	備註
1.0	113.09.01	● 文件重新改版發行 ● 文件版次、格式調整修正 ● 法規遵循內容修正	許保全	
1.1	115.08.27	● 依據數發部資安事件統計，「資訊蒐類」資安事件統計數量最高，且近年生成式AI技術更被用於自動產製釣魚郵件及偽冒身分，故增列3.1.3 、3.1.4，以深化本院全體同仁資安防護文化及因應新興科技風險。	楊啟仁	

1. 目的

確保臺北榮民總醫院(以下簡稱「本院」)所屬之資訊資產之機密性、完整性及可用性，並符合相關法令法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，以保障本院所屬利害關係人之權益。透過建立制度化、文件化及系統化之管理機制，持續監督及審查管理績效，以落實資通安全管理及業務持續營運之理念，特訂定本資通安全管理政策。

2. 適用範圍

2.1 本政策適用範圍為本院之全體同仁(含約聘僱人員及工讀生)、委外服務廠商、資料使用者(含保管者)與訪客…等。

2.2 資通安全管理制度(以下簡稱「ISMS」)所涵蓋範圍內皆適用。

2.3 資通安全管理涵蓋相關管理事項，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。管理事項如下：

2.3.1 資通安全管理政策制定及評估。

2.3.2 資通安全組織之職責與分工。

2.3.3 人力資源安全。

2.3.4 資訊資產管理。

2.3.5 存取控制。

2.3.6 實體與環境安全。

2.3.7 作業安全。

2.3.8 通訊安全。

2.3.9 資訊系統獲取、開發及維護。

2.3.10 委外作業管理。

2.3.11 資通安全事件管理。

2.3.12 營運持續管理。

2.3.13 法規遵循性。

3. 政策內容

3.1 本政策旨在讓本院於日常工作執行過程中涉及資訊相關作業時有一明確指導原則，以確保本院所有資料、資訊系統、設備及網路之安全維

運，並期許全體同仁(含約聘僱人員及工讀生)、委外服務廠商、資料使用者(含保管者)與訪客…等均能了解、實施與維持，以達下列資通安全目標：

3.1.1 落實資通安全，強化服務品質。

3.1.2 加強資安韌性，確保持續營運。

3.1.3 提升資安意識，維持安全文化。

3.1.4 健全安全治理，因應新興風險。

3.2 本院各項資通安全管理規定必須遵守政府相關法規(如：資通安全管理法及其施行細則、刑法、國家機密保護法、醫療法及其施行細則、醫師法、醫療機構電子病歷製作及管理辦法、專利法、商標法、著作權法、個人資料保護法及其施行細則…等)之規定。

3.3 成立資通安全管理組織負責ISMS之建立及推動事宜。

3.4 為能有效確保本院整體資通安全，應針對各資通安全領域訂定資通安全管理規範。

3.5 對於資通安全事件須有完整的通報及應變措施，以確保資訊系統及重要業務的持續運作。

3.6 訂定內部稽核計畫，定期檢視本院推行ISMS範圍內所有人員及設備使用情形，依稽核報告擬訂及執行矯正預防措施。

3.7 本院之全體同仁(含約聘僱人員及工讀生)、委外服務廠商、資料使用者(含保管者)與訪客均負有維持資通安全之責任，且應遵守相關之資通安全管理規範。

3.8 辦理資通安全教育訓練及宣導，促使全體人員瞭解資通安全的重要性，各種可能的安全風險，以提高資通安全意識並熟悉工作中之資通安全職責，促其遵守資通安全規定。

4. 實施

本政策經資通安全長核准，於公告日施行，並以書面、電子或其它方式通知本院所屬同仁及必要之外部人員，修正時亦同。