	ISO 27001：A.5		制定日期	104年05月29日
	文件編號	DAE00BA23	修訂日期	110年10月28日
	文件名稱	資通安全政策	第3.1版	總頁次：4

1. 目的

隨著醫療機構資訊化作業及電子病歷系統之推動，及個人資料保護法、資通安全管理法等法規之實施，為確保病歷資料安全性，建置完善資通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大林慈濟醫院（以下簡稱本院）資通系統服務正常且安全穩定的運作，特制定【資通安全政策】（以下簡稱本政策）以作為規範本院之資通安全管理制度最高指導方針，以建立安全、可信賴之資通系統服務，並確保本院之資通資產之機密性、完整性、可用性、適法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，進而保障本院資通系統服務使用者之權益及電子病歷安全。同時建立資通安全人人有責之觀念，共同遵循本院資通安全相關規範。

2. 適用範圍

2.1 適用範圍為資訊室、資訊機房暨核心資通系統(HIS&PACS)、影像醫學科聯網醫療影像之醫療儀器與網路安全維運管理。

2.2 參照ISO 27001/CNS 27001本文、附錄資訊安全要項及資通安全管理法，本院之資通安全要項涵蓋14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，導致資通資產不當使用、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：

- 2.2.1 資通安全政策
- 2.2.2 資通安全的組織
- 2.2.3 人力資源安全
- 2.2.4 資產管理
- 2.2.5 存取控制
- 2.2.6 密碼學
- 2.2.7 實體及環境安全
- 2.2.8 運作安全
- 2.2.9 通訊安全
- 2.2.10 系統獲取、開發及維護
- 2.2.11 供應商關係
- 2.2.12 資通安全事件管理
- 2.2.13 營運持續管理
- 2.2.14 遵循性管理

2.3 適用人員

於本院服務之員工、約聘人員及外包供應商。

3. 定義

3.1 資通安全

保存資訊的機密性、完整性、可用性、適法性；此外亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質；亦避免因人為或自然災害等風險，運用系統化之控制措施，以確保資通安全管理制度範圍內之資通資產受到妥善保護。

3.2 資通資產

凡與本院資訊(Information Technology, IT)及醫療儀器(Operational Technology, OT)、基礎工程設施(水、電、空調)等相關之資訊網路及資通系統之資產，如文件、人員、軟體、硬體、服務與建築等皆屬之。

3.3 資通安全異常事件

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

3.4 資通系統

凡與本院資訊(IT)、醫療儀器(OT)等相關之資訊系統。

4. 相關文件

4.1 資訊安全管理作業程序書【DAE00BA21】

4.2 資訊安全組織作業程序書【DAE00BA24】

4.3 醫療志業資訊保密辦法【AAG00A003】

4.4 CNS 27001：2014【ISMS-0-001】。

4.5 個人資料保護法【ISMS-0-008】。

4.6 著作權法【ISMS-0-010】。

4.7 醫療法【ISMS-0-011】。

4.8 資通安全管理法【ISMS-0-027】。

5. 作業說明

5.1 權責

5.1.1 資通發展暨安全管理委員會

本院資通系統發展暨安全管理階層決策組織。

5.1.2 資通安全推動組

本院、機房、資通系統及網路維運作業之資通安全管理制度規劃、建立、實施、維護、審查與持續改善，並將資通安全相關議題於資通發展暨安全管理委員會提報。

5.1.3 所有員工、約聘人員及外包供應商

皆應遵循本資通安全政策，共同維護本院資通安全。

5.2 通則

5.2.1 應考量相關法律規章及營運要求，進行資通資產之資通風險評鑑，確定資通作業安全需求，採取適當資通安全措施，確保資通資產安全。

5.2.2 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通安全教育訓練及宣導。

5.2.3 定期執行資通安全稽核作業，檢視資通安全管理制度之落實。

5.2.4 資通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。

5.2.5 違反本政策與資通安全相關規範，依相關法規或本院人事規定辦理。

5.2.6 建立資通安全事件通報及應變程序，以確保本院資訊服務能持續運作。

5.2.7 訂定業務持續計畫並定期演練，以確保重大資安事件發生時，能妥善回應。

5.2.8 依據個人資料保護法、醫療法、著作權法與資通安全管理法等相關規定，審慎處理及保護醫療電子紀錄、個人資訊與著作權。

5.2.9 為確保本院同仁皆知悉本院資通安全要求，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「同仁保密切結」（應用表單6.1）或以書面方式於「同仁聘任合約書」（應用表單6.2）中簽署亦可。

5.2.10 辦理資通安全宣導課程，強化員工資通安全之認知，建立資通安全人人有責之觀念。

5.3 目標

5.3.1 維持本院營運資通系統服務持續順暢正常運作。

5.3.2 保護本院資通資產，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，以保障病歷及個人資料等資通資產之機密性、完整性、可用性。

5.3.3 建立本院資通系統服務之標準作業程序，避免人為作業疏失及意外，加強同仁資通安全意識。

5.3.4 辦理本院資通安全目標之規劃、量測、審查及改善，依照本院【資通安全管理作業程序書】辦理，以因應不同資通安全之要求與期望，力求達成資通安全管理之目標。

5.4 審查

5.4.1 本政策應至少每年審查一次，以反映相關法令、技術及資訊服務等最新發展現況，並予以適當修訂；如遇重大變更，得隨時招開資通發展暨安全管理委員會進行審查。

5.4.2　本政策經本院資通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所有員工及提供資訊服務之相關廠商與關注方，修正亦同。

5.4.3　本辦法經院部核可後公告實施，修正時亦同。

6. 應用表單

6.1　同仁保密切結(電子表單)

6.2　同仁聘任合約書【E9A1226403-xx】