佛教慈濟醫療財團法人

台中慈濟醫院

ISO 27001 :2022
資通安全政策

機密等級：一般

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
V1.0	113 年 10 月 18 日	All	楊嘉琪	ISO 27001:2022 改版發行。
V1.1	114 年 07 月 11 日	All	蕭志豪	1. 目的新增: 台中慈濟醫院及相關受託醫院 2. 適法性改為法律遵循性 3. 5.3.8 均依循適當之通報機制向上反應，改為均依循主管機關之通報機制向上反應。 4. 條文 3.3 原「凡因人為或天然災害因素，造成本院資通系統服務中斷」新增「超過可容忍時間」敘述。 5. 相關文件新增「4.5 資通安全維護計畫」 6. 名詞「醫療資訊系統」改為「核心資通系統」。 7. 條文 5.1.3 原本僅有避免未經授權的修改，改為增加「新增」與「刪除」 8. 名詞「委外服務廠商」該為「委外廠商」。 9. 條文 5.2.3 裡的「訪客」改為「利害關係者」。 10. 條文 5.3.3 原:應符合主管機關之要求，依員工職務責任提供適當之資通安全相關訓練。改為「應符合主管機關之要求，全院員工應接受適當之資通安全教育訓練」。 11. 條文 5.3.8 原為「依循適當之通報機制向上反應」改為「依循主管機關之通報機制向上反應」

	ISO 條文：27001		制定日期	113 年 10 月 18 日
	文件編號	GAE00A001	修訂日期	114 年 07 月 11 日
	文件名稱	資通安全政策	第 1.1 版	總頁次：4

1. 目的：

為確保佛教慈濟醫療財團法人台中慈濟醫院及相關受託醫院（以下簡稱「本院」）所屬之資訊資產的機密性、完整性及可用性，以符合「資通安全管理法」等相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，特訂定本政策。

2. 適用範圍：

2.1 本政策適用範圍為本院之全體同仁、委外服務廠商、資料使用者(含保管者)與訪客等。

2.2 資通安全管理範疇涵蓋組織、人員、實體及技術等 4 大領域，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，對本院造成各種可能之風險。

3. 定義：

3.1 資通安全

保存資訊的機密性、完整性、可用性、法律遵循性；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，以確保資訊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 Information Technology(IT)資訊及 Operational Technology(OT)醫療儀器、基礎工程設施(油、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

凡因人為或天然災害因素，造成本院資通系統服務中斷超過可容忍時間，或本院資訊資產遭竄改、刪除或竊取等，皆屬之。

3.4 資通安全事件

系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

3.5 核心資訊系統

泛指與醫院臨床治療與照護服務之資通系統，如醫療資訊系統(HIS) 、電子病歷(EMR) 、醫療影像儲存傳輸系統(PACS)，子功能資工系統如:醫囑，護理、檢驗、檢查、藥局、病歷管理及影像儲存傳輸等均屬之。

4. 相關文件：

4.1 資通安全管理法 (GAE0034)。

4.2 個人資料保護法施行細則(GAE0019)。

4.3 CNS 27001:2023(GAE008)。

4.4 醫療志業資訊保密辦法(AAG00A003)。

4.5 資通安全維護計畫。

5. 作業內容：

5.1 目標：

為維護本院資訊資產之機密性、完整性、可用性與法律遵循性，並保障使用者資料隱私之安全，藉由本政策之實施以達成下列目標：

5.1.1 建立安全及可信賴之資通作業環境，確保本院電腦資料、系統、設備及網路之安全，以保障本院業務永續運作。

5.1.2 保護本院業務服務之安全，確保資通系統及相關資訊需經授權人員才可存取資訊，以確保其機密性。

5.1.3 保護本院業務服務之安全，避免未經授權的新增、修改、刪除，以確保其正確性與完整性。

5.1.4 建立本院業務永續運作計畫，以確保本院資通業務服務之持續運作。

5.1.5 確保本院各項業務服務之執行須符合相關法令或法規之要求。

5.1.6 為保護本院業務相關個人資料之安全，免於因外在威脅或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。

5.1.7 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。

5.2 責任：

5.2.1 本院應成立資通安全組織統籌資通安全事項推動。

5.2.2 管理階層應積極參與及支持資通安全管理制度，並透過適當的標準和程序以實施本政策。

5.2.3 本院全體同仁、委外廠商、資料使用者(含保管者)與利害關係者皆應遵守本政策。

5.2.4 本院全體同仁、委外廠商及資料使用者(含保管者)均有責任透過適當通報機制，通報資通安全事件或弱點。

5.2.5 任何危及資通安全之行為，將視情節輕重追究其民事、刑事及行政責任，或依本院「工作規則」第七章第四十條、第四十一條之資通安全獎懲規範及本院之相關規定進行議處。

5.3 管理指標：

5.3.1 為評量資通安全管理目標達成情形，本院應訂定相關管理指標，並定期監控、評估及改善。

5.3.2 應定期審查本院資通安全組織人員執掌，以確保資通安全工作之推展。

5.3.3 應符合主管機關之要求，全院員工應接受適當之資通安全教育訓練。

5.3.4 應加強本院資訊資產之環境安全，採取適當之保護及權限控管機制。

5.3.5 應確保資訊不被透漏給未經授權之第三者。

5.3.6 應加強存取控制，防止未經授權之不當存取，以確保本院資訊資產已受適當之保護。

5.3.7 本院資訊系統開發應考量安全需求，並定期稽核安全弱點。

5.3.8 應確保所有資通安全事件或可疑之安全弱點，均依循主管機關之通報機制向上反應，並予以適當調查及處理。

5.4 管理審查：

本政策應每年至少審查 1 次，以反映政府法令、技術及業務等最新發展情況，確保本院資通業務永續運作之能力。資通安全組織、主管機關(或法令、法規要求)、或專家學者等利害關係者如有資通安全相關回饋事項，應將列入管理審查會議之討論議題。

5.5 實施：

本政策經「資通發展暨安全管理委員會」核定後實施，修訂時亦同。

6. 應用表單：無。