資訊安全政策

版本 5.0

中華民國 102 年 07 月 30 日

文件編號	ISMS-002	資訊安全政策	文件類別	一般
版　　次	V 5.0		發布日期	102/07/30

文件編號	ISMS-002	資訊安全政策	文件類別	一般
版　　次	V 5.0		發布日期	102/07/30

1. 目的

確保安泰醫療社團法人安泰醫院(以下簡稱本院)資訊系統服務正常且安全穩定的運作，規範本院資訊室及資訊機房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，並確保資訊室及資訊機房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，維持業務持續運作，降低資訊作業風險，進而保障資訊系統服務使用者之權益。

2. 範圍

2.1 基於本院以保護資訊資產機密性、完整性、可用性為目標，資訊機房為本院資訊系統服務之重要基礎架構，故將資訊室、資訊機房及 HIS、EMR 系統之維運優先納入資訊安全管理範圍，展現負責之經營管理理念，期日後將資訊安全管理制度拓展至其他範圍。

2.2 資訊室及資訊機房之資訊安全管理涵蓋 11 項管理事項，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，對本院帶來可能之風險及危害。管理事項如下：

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

3. 權責

3.1 E 化委員會

本院資訊發展暨安全管理階層決策組織。

3.2 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 E 化小組提報。

3.3 資訊室所有員工

皆應共同遵守本資訊安全政策。

3.4 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。

4. 定義

4.1 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。

4.2 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。

5. 作業內容

5.1 通則

5.1.1 應考量相關法律規章及營運要求，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。

5.1.2 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訊安全教育訓練及宣導。

5.1.3 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。

5.1.4 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。

5.1.5 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。

5.1.6 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。

5.1.7 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。

5.1.8 依據電腦處理個人資料保護法與智慧財產法之相關規定，審慎處理及保護個人資訊與智慧財產權。

5.1.9 為確保本院同仁皆知悉本院資訊安全要求，另訂定「資訊安

全宣言」（詳附件一）告知本院同仁遵悉。

5.2 政策

5.2.1 符合法規

5.2.2 保障隱私

5.2.3 資料正確

5.2.4 服務不間斷

5.3 目標

5.3.1 維持資訊室及資訊機房業務持續運作。

5.3.2 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。

5.3.3 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。

5.3.4 確保達成營運量測指標

5.3.4.1. 資訊系統服務可用率：99%

計算方式依據維運記錄詳列當月服務中斷之時間，計算服務中斷時間累計之實際值，以當月總分鐘數減去此實際發生服務中斷之時間再除以當月總分鐘數即可得出當月之服務可用率，若大於或等於目標績效值，則達成績效指標得分。資料來源：資訊安全異常事件紀錄。

5.3.4.2. 線上作業用電腦硬體故障排除即時完成率：90%

線上作業用電腦設備故障於規定時間（兩個工作天）內在院內（院外送修者不計算在內）完修之比率。計算方式：統計當月合格件數為分子，除以當月一般硬體故障總件數，即可得到合格率，若大於或等於目標績效值，即達成績效指標。資料來源：（請修報銷系統）修繕申請單及 E-MAIL 紀錄。

5.3.4.3. 線上電腦設備良率：95%

以線上單位資訊設備 總數減去當月設備硬體障礙次數累計值，再除以線上資訊設備總數所得之比率，若大於或等於目標績效值，即達成績效指標得分。資料來源：（請修報銷系統）修繕申請單（資訊設備包括：電腦主機、印表機、螢幕、印表機、網路設備、讀卡機）。

5.3.5 確保達成資訊安全管理量測指標

5.3.5.1. 資訊安全事件 4 級不得有。

5.3.5.2. 資訊安全事件 3 級每半年不得超過一件（含一件）。

5.3.5.3. 資訊安全事件 2 級每半年不得超過六件。

5.3.5.4. 資訊安全事件 1 級每半年不得超過十二件。

5.3.6 資訊安全機密性量測指標

5.3.6.1. 每半年進行人員作業行為檢驗，執行人員違反作業規範不得超過五件。

5.3.6.2. 每半年進行資訊存取管制檢驗，違反資訊處置作業規範不得超過五件。

5.3.7 資訊安全完整性量測指標

每半年進行資訊安全相關紀錄、報告、查詢資料或備份資料之檢驗，資料錯誤或是短缺不得超過五件。

5.3.8 資訊安全符合法規量測指標

每半年進行管理制度作業檢驗，因嚴重違反本院管理規章、相關法規、個資法不得發生。

5.4 審查

5.4.1 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。

5.4.2 本政策經 E 化委員會核准，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。

6. 相關資料

6.1【資訊安全管理作業流程及程序】。

6.2【資訊安全組織管理作業流程及程序】。

7. 附件

7.1 附件一、資訊安全宣言。

安泰醫療社團法人安泰醫院（以下簡稱本院）資訊安全工作之最終目的在於，透過對人員、作業及資訊科技之管理，確保本院醫療資訊處理作業能安全有效地運作，防範醫療資訊處理作業過程，發生影響醫療資訊機密性、完整性及可用性之安全事件，以保障社會大眾個人醫療資訊隱私權益為前提，整合基層醫療資訊系統之服務提供，進而建設醫療體系之全景。

本院之資訊安全政策以下列十七字綱領簡述其概要：

～　符合法規、保障隱私、資料正確、服務不間斷　～

本院之資訊安全工作係以系統化之風險評估及風險管理為基礎，以管理及技術並重作為實施風險控制措施之原則，並由全體同仁落實於日常工作中，共同努力達成下列目標，以實現本院資訊安全工作之目標：

- 醫療資訊與隱私權之保護完全符合法令要求。
- 醫療、行政資訊處理過程與結果之完整正確。
- 資訊系統與資訊處理作業服務之不間斷。

本院同仁在資訊安全應扮演之角色及權責等有關規定，應在程序書、工作說明書或有關作業手冊中詳細載明，經由公告程序，責成作業管理人員於執行職務相關管理作業之前，必須先瞭解與熟悉本院資訊安全相關作業規範，俾益其遵守與實行。

本院所有資訊安全管理相關同仁、約聘人員、委外廠商、系統硬軟體維護之簽約廠商，或與本院有業務往來且涉及資訊資產完整性與隱密性之資訊安全管理範圍者，應簽署保密協議書，使其瞭解於本院工作期間所有取得之資訊皆為本院之資產，且不被允許使用於其他未授權之用途上，以昭示本院維護醫療資訊安全之決心。

若發現未遵循本政策或有行使任何危及本院資訊安全之行為，應依院內相關懲處管理規範處理或訴諸適當之懲罰或法律行動。

為反映政府資訊安全政策、法令、技術及機關業務之最新狀況，本院將適時修訂本宣言，以確保資訊安全實務作業之可行性、有效性及持續改善。