資訊安全政策

版本 3.1

中華民國 107 年 09 月 20 日

文件編號	ISMS-007	資訊安全政策	文件類別	一般
版　　次	V3.1		發布日期	107/09/20

文件編號	ISMS-007	資訊安全政策	文件類別	一般
版　　次	V3.1		發布日期	107/09/20

1. 目的

為建立【澄清綜合醫院中港分院】（以下簡稱本院）資訊安全管理制度最高指導方針，以確保本院資訊資產之機密性、完整性、可用性，進而降低資訊作業風險，確保資訊系統安全穩定的正常運作，以符合相關法規之要求及保障使用者之權益，特制定此政策規範。

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，且資訊機房為本院資訊系統服務之重要基礎架構，故將資訊室與資訊機房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擴展至其他範圍。

2.2 資訊室與資訊機房之資訊安全管理事項總計涵蓋 14 項，避免因人為疏失、蓄意破壞或天然災害等因素，導致資訊資產被不當使用、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 人力資源安全。
2.2.4 資訊資產。
2.2.5 存取控制。
2.2.6 密碼。
2.2.7 實體及環境安全。
2.2.8 作業的安全。
2.2.9 通訊安全。
2.2.10 資訊系統獲取、開發及維護。
2.2.11 供應商關係。
2.2.12 資訊安全事故。
2.2.13 業務持續。
2.2.14 遵循性。

3. 權責

3.1 【資訊管理委員會】

本院資訊發展暨安全管理階層決策組織。

3.2 【資訊安全長】

由本院【資訊室主任】擔任、負責資訊室與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【資訊管理委員會】提報。

3.3 資訊室同仁、資訊系統服務使用者、委外人員

3.3.1 配合資訊安全管理制度活動。

3.3.2 遵守相關資訊安全管理制度規範。

4. 定義

4.1 資訊安全

保存資訊的機密性、完整性及可用性；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。

4.2 資訊資產

對組織有價值的任何事物，如資訊、人員、軟體、硬體、服務與建築與保護類設施等皆屬之。

5. 本院資訊安全政策

S：Strength and Stability

致力於建置更堅固的資安機制，以確保資訊系統的穩定性。

A：Accessibility and Accuracy

努力防範各種資安威脅，提高系統的可存取性與準確性。

F：Feasibility and Flexibility

以資安政策為最高指導原則下，致力研究各種可行性方案，以提供醫務服務最安全、最有彈性的資訊系統。

E：Effectiveness and Efficiency

從管理到技術，從政策到落實，以最有效的資安管理機制，達到最高效率的資訊安全目標。

6. 瞭解組織及其全景

本院應依決定與其目的有關且影響達成其資訊安全管理系統預期成

果能力者之內部及外部議題，包含相關法律要求，及院、主管機關政策需求，並建立『組織全景策略表』（詳附件一）以作為鑑別及執行之依據，並據以確認 ISMS 之範圍符合性。『組織全景策略表』需於每年管理審查會議時進行確認及必要之修訂。

7. 溝通規劃

本院決定相關於資訊安全管理系統之內部及外部溝通或傳達的需要，規劃於『ISMS 溝通規劃表』（詳附件二），包括下列事項：

7.1 溝通或傳達事項。
7.2 溝通或傳達時間。
7.3 溝通或傳達對象。
7.4 溝通或傳達人員。
7.5 進行有效溝通或傳達所採用過程。

8. 資訊安全目標規劃

維護本院資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標，每年定期由資訊安全工作組，從資訊安全政策及下列項目挑選適合作為衡量之項目，彙整於『資訊安全目標規劃表』(詳附件三)，每季填寫於『資訊安全目標統計表』(詳附件四)，並依目標需求，確認各作業程序是否規範適當，以及達成目標之作業方式，包含：要做什麼、需要什麼資源、誰要負責、何時完成，經由【資訊安全長】審核後，進行作業管制。

8.1 資訊安全政策：

8.1.1 對資訊相關職務及工作，應進行安全評估，並於人員晉用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

8.1.2 針對管理、業務及資訊等不同工作類別之需求，不定期辦理資訊安全教育訓練及宣導，建立同仁資訊安全認知，提升資訊安全水準。

8.2 資訊安全組織管理：

8.2.1 成立之資訊安全工作組，負責推動資訊安全。

8.2.2 資訊安全工作組需不定期舉辦資訊安全會議，確保資安措施正常運作。

8.2.3 專案遵循資訊安全規範，考量資訊資產機密、完整、可用性之適切性，以確保專案之資訊安全。

8.3 人力資源安全管理：

8.3.1 各部門增補人員應依政府規定之相關勞動法規、本院理念與守則，定義聘僱員工的條款與條件，到職當天均要求詳讀保密條款，並簽訂之，離職當日，亦應歸還、接所有業務範圍內之資訊、資料、保管之資產。

8.3.2 被管理階層授權之資訊安全工作組，肩負資訊安全認知教育訓練。

8.4 資訊資產管理：

8.4.1 機房資產應有效彙整統一管理，並明定資產所有人及資產保管人等角色，並進行標示、分級。

8.4.2 電子媒體含可攜式媒體皆應經過申請，核准後始可使用，相關儲存媒體於汰除時，亦應移除敏感性資料。

8.5 存取控制管理：

8.5.1 系統存取應依人員職務或角色，訂定相關權限。

8.5.2 離(調)職人員，應取消各項資訊資源之所有權限，並列入離(調)職之必要手續。

8.5.3 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新週期。

8.5.4 對於必要之遠端登入方式進行系統維護行為，應加強安全控管，課其相關安全保密責任。

8.5.5 建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

8.6 密碼管理：

8.6.1 依據資訊安全管理制度要求就驗證範圍，本院藉由加密、身分驗證及存取控制方式適當的保護資訊的機密性、鑑別性或完整性。

8.6.2本院使用醫事人員/醫事機構憑證 IC 卡。

8.7 實體與環境安全管理：

8.7.1就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。

8.7.2實體與環境進行安全維護、安全汰除或再使用，並包括消防器材與資訊資產之定期保養等設備安全管理。

8.8 作業的安全管理：

8.8.1系統開發應區隔開發、測試、營運環境，並規範開發、測試、驗收之相關權責。

8.8.2營運日誌應妥善保存，並維持其正確性、可信度，以作為分析資安事件之資料來源。

8.8.3為預防資訊技術弱點造成重大資安事故，應定期執行弱點掃描與修補作業。

8.9 通訊安全管理：

8.9.1經由網際網路連線作業之資訊系統，應視資料及系統之重要性及價值，採用連線加密、身分鑑別及防火牆等適當之技術或措施，防止資料及系統被入侵、破壞、竄改、刪除及未經授權之存取。

8.9.2利用網際網路及全球資訊網公布及流通資訊，應實施安全監控，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布及傳播。

8.10 資訊系統獲取、開發及維護管理：

8.10.1自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入評估，考量不當軟體、後門及電腦病毒等危害系統安全。

8.10.2對軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍。

8.11 供應商關係管理：

8.11.1委外服務交付協議中之安全管控、委外服務之定義、委外廠商之監控審查及服務變更管理。

8.11.2於採購合約中明定與第三方服務的範圍與內容，並載明雙方之權利與義務。

8.12 資訊安全事故管理：

8.12.1各項資訊安全活動或服務過程之意外與緊急事故鑑定。

8.12.2資訊安全緊急事故通報。

8.12.3資訊安全意外與緊急事故應變之演練。

8.12.4持續監控、管理及改善資訊安全。

8.13 業務持續管理：

8.13.1為確保關鍵營運業務能及時恢復，應於適當之風險評估基礎上，進行災害及系統中斷影響分析，識別營運中斷之關鍵因素及其影響。

8.13.2應採取適宜之測試方法，對業務持續管理計畫進行測試及演練。

8.13.3於業務持續規劃時，需考量備援設備之充足性。

8.14 遵循性管理：

8.14.1每年應針對資訊安全管理系統進行內部稽核，須包含與系統相關之所有單位，確保所有資訊安全程序及流程正確無誤，且符合資訊安全政策與標準。

8.14.2定期審查範圍內的資訊技術遵循性、相關資安法規，及其有效性，以保持遵循法律、法規之最新版本。

8.14.3要求同仁對客戶資料之管理與保護，須嚴格遵循個資保護相關法規，以防止遺失或洩漏個人資料之風險。

9. 資訊資產分類、等級及評鑑原則

9.1 分類

依據各項作業內容特性，將資產分為人員、資訊、軟體、硬體(一般類、建築與保護類)，以及服務等類別。

9.2 風險評鑑

根據營運項目之機密、完整、可用之可能風險、並依其威脅及衝

擊，評鑑其風險等級。經分級與評鑑後，依其所具備之價值，施以適當程度之安全控管。

9.3 不可接受風險等級

執行風險評鑑後，將資產區分為不同風險等級，其中屬於不可接受風險之資產，應執行風險回應及處置，據以監督控管，並落實執行追蹤控制。

10. 適用性聲明書

依據「ISO 27001 資訊安全管理系統-要求」製作產出『適用性聲明書』，以書面方式列舉資訊資產是否適用其標準所列之控制措施，及其不適用之原因。當組織架構、人員、設備、實體環境等變動時，資訊安全工作組應重新定義控制措施之適用性。

11. 審查

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。

12. 實施

12.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

12.2 本政策經【資訊管理委員會】核准，於公告日施行，並以書面、電子或其他方式通知資訊室、全院所有員工及提供資訊室資訊服務之廠商，修正亦同。

13. 相關資料

無。

14. 附件

14.1 附件一、組織全景策略表。

14.2 附件二、ISMS 溝通規劃表。

14.3 附件三、資訊安全目標規劃表。

14.4 附件四、資訊安全目標統計表。