新光醫療財團法人
新光吳火獅紀念醫院
SHIN KONG WU HO-SU MEMORIAL HOSPITAL

新光吳火獅紀念醫院

資通安全實施程序書

－僅限本院同仁參閱－

新光醫療財團法人新光吳火獅紀念醫院

文 件 名 稱：資通安全實施程序書

文 件 編 號：ISMS-2-02

制 定 單 位：資訊部

制 定 日 期：114 年 05 月 26 日

修 訂 紀 錄			
修訂日期	修訂內容摘要	頁次	版本
111.07.14	初版		1.0
112.04.17	因應本院擴大資通安全層級及範圍調整對應名稱	全	1.1
112.08.09	新增「資通安全量化指標有效性量測表」編號	6	1.2
114.05.26	因應 ISO27001:2022 轉版，相關內容改版		3.0
114.08.04	修正變更管理	9	3.1

新光醫療財團法人新光吳火獅醫院

文件編號	ISMS-2-02	文件名稱	機密等級	版本	3.0
制訂單位	資訊部	資通安全實施程序書	內部使用	頁數	1/7

1 目的：

為摘要說明實施資訊安全管理系統(ISMS)的相關措施，訂定「資通安全實施程序書」(以下簡稱本程序書)。

2 適用範圍：

資訊安全管理系統(ISMS)實施範圍中之員工、專案及委外服務廠商，均屬於本程序書之適用範圍。

3 資訊安全管理系統(ISMS)架構

實施 ISO 27001(CNS 27001)資通安全管理系統(ISMS)分四個階段，並依作業步驟持續進行，其執行單位及主要參考資料說明如下表：

表 1：資通安全管理系統架構

階段	作業步驟	執行單位	主要參考資料
計　畫(P)	1. 資通安全手冊	資通安全管理委員會、資通安全資安組	ISMS-1-01_資通安全政策
	2. 資通安全的組織	資通安全管理委員會	ISMS-1-02_資通安全組織章程
	3. 文件管制	文件組	ISMS-2-03_資通安全管理文件管理程序書
	4. 全景風險評鑑	驗證實施範圍單位	ISMS-2-01_資通安全組織全景管理程序書
	5. 訂定資通安全管理目標及有效性量測	驗證實施範圍單位	管審會議資料 ISMS-2-02_資通安全實施程序書
	6. 風險評鑑	驗證實施範圍單位	ISMS-2-04_資通安全風險評鑑程序書
	7. 業務持續管理	驗證實施範圍單位	ISMS-2-08_營運持續管理程序書

階段	作業步驟	執行單位	主要參考資料
	8. 訂定與審視資通安全管理系統範圍與適用性聲明	資通安全管理委員會、資通安全資安組	ISO 27001 ISMS-1-01_資通安全政策 ISMS-2-15_適用性聲明書 ISMS-2-02_資通安全實施程序書 驗證範圍於規格書或管審會或稽核會議訂定。
執行(D)	9. 執行資通安全	資通安全管理委員會、資通安全資安組	ISMS-2-02_資通安全實施程序書
	10. 人力資源安全	資通安全資安組	ISMS-2-06_人員管理及教育訓練程序書
	11. 資產管理	資通安全資安組	ISMS-2-05_資通資產管理程序書
	12. 存取控制	資通安全資安組	ISMS-3-01_實體與環境安全工作說明書 ISMS-2-12_資訊系統獲取、開發與維護管理程序書
	13. 密碼控制	資通安全資安組	ISMS-2-12_資訊系統獲取、開發與維護管理程序書 ISMS-3-02_系統與網路安全管理工作說明書
	14. 實體與環境安全	資通安全資安組	ISMS-3-01_實體與環境安全工作說明書

階段	作業步驟	執行單位	主要參考資料
	15. 運作管理	資通安全資安組	ISMS-2-02_資通安全實施程序書 ISMS-3-01_實體與環境安全工作說明書 ISMS-2-12_資訊系統獲取、開發與維護管理程序書 ISMS-3-03_資訊備份管理作業說明書
	16. 通訊管理	資通安全資安組	ISMS-3-01_實體與環境安全工作說明書
	17. 系統獲取、開發及維護	資通安全資安組	ISMS-2-12_資訊系統獲取、開發與維護管理程序書
	18. 供應者關係	資通安全資安組	ISMS-2-11_委外管理作業說明書
	19. 資通安全事故管理	資通安全管理委員會、資通安全資安組	ISMS-2-07_資通安全事件通報、處理及緊急應變程序書
	20. 營運持續管理之資通安全層面	資通安全資安組	ISMS-2-08_營運持續管理程序書 ISMS-3-04_營運持續管理作業說明書
	21. 遵循性	資通安全資安組	ISMS-2-02_資通安全實施程序書 ISMS-2-03_資通安全管理文件管理程序書
檢查(C)	22. 內部稽核	資通安全管理委員會、資通安全稽核組	ISMS-2-09_資通安全內部稽核程序書

階段	作業步驟	執行單位	主要參考資料
稽　核(A)	23. 矯正與改善	資通安全管理委員會、資通安全資安組、通安全稽核組	ISMS-2-10_矯正措施管理程序書

4　政策

4.1 行動裝置政策

本院個人行動裝置在登記管制後可登入內部網路。

4.2 存取控制政策

資訊機房門禁、資訊系統帳號、網路規則等作業存取權限，均須有正式的存取授權紀錄。

4.3 使用密碼控制措施的政策

為確保資料的安全防護，涉及民眾權益、公務機密…等機敏性資訊於公眾網路傳輸時應採用加密技術，例如：VPN、HTTPS、SSH…等，如透過 Email 傳輸時應使用密碼加密。

4.4 桌面淨空與螢幕淨空政策

暫時離開座位時應將桌面上敏感性資料收到辦公抽屜中，避免被非法人士不當瀏覽，且將電腦螢幕畫面鎖定。

4.5 資訊傳送政策與程序

4.5.1 應避免含有公務資料之電子文件於網路上傳送，需使用載體，以公文方式交付。

4.5.2 使用共同系統，須依循共同系統主管機關規範作業。

4.5.3 紙本資料傳送，以公文方式或依循業務相關主管機關規範交付。

4.6 軟體與系統安全發展政策

4.6.1 軟體與系統發展的規則應建立與應用，需考量機密性、完整性、可用性及適法性，規劃設計符合業務所需之軟體與系統。

4.6.2 資通系統應依「資通安全責任等級分級辦法」，附表九「資通系統防護需求分級原則」，完成普、中、高系統分級，後依附表十「資通系統防護基準」各構面對應控制措施，完成防護基準。

4.7 供應者安全之資通安全政策

對與廠商合約，需載明本院對於資通安全與個人資料保護的要求。

4.8 安全政策與標準之遵循性

每年至少一次審查資通安全政策、標準與任何其它安全要求事項，做為處理及程序的遵循性。

5 變更管理：

5.1 組織或業務流程變更時，應評估對資通安全的影響，並留下適當的評估紀錄，除例行性變更(windows update 等)外，將變更過程紀錄於「ISMS-2-02-1_變更管理紀錄表」如有顯著的影響時，應經正式核備授權（至少取得部門主管同意），採取適當的因應措施。

5.2 變更評估方式

5.2.1 重大變更。

於資訊系統分類分級與鑑別機制作業，被判定為關鍵性業務系統或衝擊高系統，執行相關變更時應經正式核備授權並取得單位主管同意，採取適當的因應措施。

5.2.2 一般變更

於資訊系統分類分級與鑑別機制作業，非判定為關鍵性業務系統或衝擊高系統，執行相關變更實應經正式核備授權並取得部門主管同意，採取適當的因應措施。

5.2.3 緊急變更

若發生緊急狀況，系統須及時採取變更時，無法完成正式核備授權時，會同業務承辦同仁或機房管理同仁，進行變更，相關變更紀錄須確實記錄於「ISMS-2-02-1_變更管理紀錄表」內，並說明原因及過程，參與人員需簽名。

6 溝通

6.1 與內部同仁、資訊相關供應廠商每年至少一次進行溝通作業。

6.2 與內部同仁溝通部分，以教育訓練、公告（Email、通訊軟體等）、會議方式進行，並以抽查、實施稽核方式確認其有效性。

6.3 與供應廠商溝通部分於專案需求討論期間進行會議討論，並將要求載明合約中及留存

會議紀錄，內部稽核（供應商稽核）時確認其有效性。

6.4 與民眾溝通部分，使用網頁、Email、通訊軟體等方式進行。

6.5 上述溝通項目至少包含影響範圍、需配合事項及確認有效性方式，相關執行計畫與執行紀錄，執行溝通人員由該項業務負責同仁規劃執行，並留存相關紀錄。

7 管制考核

7.1 資訊安全管理系統(ISMS)文件架構，參考「ISMS-2-03_資通安全管理文件管理程序書」。

7.2 文件管制

所有資通安全管理相關文件（含執行紀錄）均需管制，依「ISMS-2-03_資通安全管理文件管理程序書」辦理。

7.3 考核

由各主管負責監督所負責之資通安全程序是否依規定進行,若有不符合之處應予以糾正,若發現程序和控制措施的瑕疵,應規劃預防及改善措施,經權責單位核定後實施,同時留下紀錄。管理審查會議召開時，除「資通安全管理委員會」成員應出席外，並通知相關人員列席。

7.4 資通安全管理目標及有效性量測

參考「ISMS-2-13_資訊服務管理程序書」辦理。

7.5 管理階層審查

資訊安全管理系統(ISMS)的執行結果，視需要陳報「資通安全管理委員會」。每年至少實施一次管制考核，以確保資訊安全管理系統(ISMS)的適用性和有效性，並持續改善，同時評估改進資訊安全管理系統(ISMS)的機會。

7.5.1 管理審查之輸入輸出項目，須符合 ISO27001(CNS 27001)規範。

7.5.2 管理審查之項目

7.5.2.1. 來自先前管理審查的狀態與行動

7.5.2.2. 與資訊安全管理系統有關的內部與外部議題之變更

7.5.2.3. 與資訊安全管理系統相關關注方之需要及期望的變更。

7.5.2.4. 資訊安全管理系統的回饋，包括下列：

7.5.2.4.1不符合項目與矯正措施

7.5.2.4.2監督與測量結果

7.5.2.4.3稽核結果

7.5.2.4.4實現資訊安全目標

7.5.2.5. 關注方的回饋

7.5.2.6. 風險評鑑結果與風險處理計畫之狀態

7.5.2.7. 持續改進的機會

7.5.3 管理審查之輸出

應包括與持續改進機會有關之決策與任何對資訊安全管理系統變更之需求。

8 稽核

8.1 依據資通安全法規定本院每一年至少實施二次資訊安全內部稽核。

8.2 內部稽核依「ISMS-2-09_資通安全內部稽核程序書」，由資安稽核組規劃執行。

8.3 辦理稽核前，應於稽核計畫中審慎規劃稽核活動中運作系統與稽核工具保護措施，俟稽核計畫核定後方可著手稽核。

8.4 稽核的結果及協助執行稽核之設備(工具)應有適當保護措施。

8.5 稽核過程應量測風險管理措施的有效性，並發掘潛在性的風險，以利進行矯正措施，防止資訊安全危機事件的發生。

9 其他

資訊安全管理系統實施範圍中，若中央機關另有相關規範，需依相關規範執行作業。

10 實施與修訂

本程序書奉　資通安全委員會副主任委員核定後實施，修正時亦同。

11 輸出文件/紀錄

ISMS-2-02-1_變更管理紀錄表