1. 資訊安全管理政策

1.1 目的

南星醫院（以下簡稱本院）為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本院之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

1.2 適用範圍

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，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本院帶來各種可 能之風險及危害。管理事項如下：

1.2.1 資訊安全政策訂定與評估。

1.2.2 資訊安全組織。

1.2.3 資產管理。

1.2.4 人力資源安全。

1.2.5 實體與環境安全。

1.2.6 通訊與作業管理。

1.2.7 存取控制安全。

1.2.8 系統開發與維護之安全。

1.2.9 資訊安全事件之反應及處理。

1.2.10 業務永續運作管理。

1.2.11 相關法規與施行單位政策之符合性。 本院之內部人員、委外服務廠商與訪客皆應遵守本政策。

1.3 定義

1.3.1 資訊資產：係指為維持本院資訊業務正常運作之硬體、軟體、服務、文件及人員。

1.3.2 業務持續運作之資訊環境：係指為維持本院各項業務正常運作所需之電腦作業環境。

1.4 目標

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：

1.4.1 保護本院業務活動資訊，避免未經授權的存取。

1.4.2 保護本院業務活動資訊，避免未經授權的修改，確保其正確完整。

1.4.3 建立跨部門之資訊安全組織，制訂、推動、實施及評估改進資訊安全管理事項，確保本院具備可供業務持續運作之資訊環境。

1.4.4 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。

1.4.5 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。

1.4.6 實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。

1.4.7 本院之業務活動執行須符合相關法令或法規之要求。

1.5 責任

1.5.1 本院的管理階層建立及審查此政策。

1.5.2 資訊安全管理者透過適當的標準和程序以實施此政策。

1.5.3 所有人員和委外服務廠商均須依照相關安全管理程序以維護資訊安全政策。

1.5.4 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。

1.5.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本院之相關規定進行懲處。

1.6 審查

本政策應至少每年審查乙次,以反映政府法令、技術及業務等最新發展現況， 以確保本院永續運作及資訊安全實務作業能力。

1.7 實施

1.7.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

1.7.2 本政策經「資訊安全委員會」核定後實施，修訂時亦同。

2.資訊安全組織

2.1 建置目的

資訊安全組織之建立目的在資訊安全管理制度執行之有效性，期使本院制度達成既定之目標，以增進業務運作之安全。

2.2 資訊安全組織架構與工作執掌

2.2.1 資訊安全組織架構圖

資訊安全組織架構如下圖所示。

2.2.2 資訊安全組織架構說明

2.2.2.1 資訊安全委員會：由本院各單位主管組成，負責資訊安全管理制度相關事項決議。

l 每年定期或視需要召開會議，審查資訊安全管理相關事宜。

l 視需要召開跨部門之資源協調會議，負責協調資訊安全管理 制度執行所需之相關資源分配。

2.2.2.2 資訊安全秘書：由資訊安全委員會指派專人擔任。

l 協調資訊安全小組與緊急處理組執行資訊安全相關作業。

l 負責對資訊安全狀況進行預警、監控，並對資訊安全狀況與 事件進行處置。

l 對於資訊安全管理之改善提出建議，以及協助執行資訊安全 之自我檢核。

l 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢 核。

2.2.2.3 資訊安全小組：由資訊安全委員會指派人員組成，負責規劃及執行 各項資訊安全作業。

l 制定資訊安全管理相關規範。

l 推動資訊安全相關活動。

l 辦理資訊安全相關教育訓練。

l 建立風險管理制度，執行風險管理。

l 建立安全事件緊急應變暨復原措施。

l 執行稽核改善建議事項。

l 執行預防措施之改善。

l 研討新資訊安全產品或技術。

l 執行資訊安全委員會決議事項。

l 鑑別資訊安全相關之法規。

2.2.2.4 緊急處理組：緊急處理組為任務編組。成員相關權責及作業內容分述如下：

2.2.2.4.1 召集人：

l 當重大資安事件發生時，負責聯絡召集緊急處理組。

l 協調及督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

l 依據事故評估之結果，得依現況請資訊安全委員會召集人決議是否宣布災變及啟動業務持續計畫。

l 災變發生時，配合救災單位負責搶救人員、物資與設備等及現場指揮工作。

l 負責災後協調指揮清理災害現場。

l 負責規劃原營運場所之現場復原工作。

2.2.2.4.2 各關鍵業務流程負責人：

l 負責召集相關人員，發展、維護、更新修訂及執行各災害復原程序。

l 每年負責召集相關人員進行計劃之測試演練。

l 負責原營運場所或異地備援場所之應變、處理、復原及運轉測試工作。

l 負責災害現場證據收集俾利未來訴訟與損害求償事宜。

l 災害現場評估損害狀況及執行原營運場所之現場復原工作。

2.2.2.4.3 資訊安全稽核小組：由資訊安全委員會指派，負責查驗資訊安全管理制度之執行情形。

l 依據資訊安全查驗表執行資訊安全管理制度查驗作業。

l 追蹤不符合事項之改善執行情形。

2.3 資訊安全推動會議

2.3.1 資訊安全委員會每半年應召開一次資訊安全推動會議，必要時得召開臨時會議。

2.3.2 資訊安全推動會議審查內容建議包含如下：

l 資訊安全查驗項目執行結果及建議改善事項。

l 員工、上級指導單位及第三方單位等利害相關團體的建議。

l 新資訊安全產品或技術導入之審查。

l 矯正及預防措施檢討。

l 風險評鑑適切性審查。

l 前次審查會議決議執行狀況。

l 影響資訊安全制度之任何變更事項。

l 資訊安全組織成員所提出之改善建議。

2.3.3 資訊安全小組應每半年檢視「資訊安全查驗表」之量測 執行狀況。

3．資產管理

3.1 建立本院資產管理規範，訂定資訊資產分 類、分級、價值評估、標示及處理之遵循原則，並據以辦理各項資訊資產管 理及作業方法。用以保護各類資訊資產，避免因人為疏失、蓄意或自然災害等風險所造成之傷害。

3.2 權責人員

3.2.1 資訊安全執行秘書:負責定期審議資訊資產清單及價值評估結果,並督導相關活動之進行。

3.2.2 資訊資產權責單位：負責所管轄內資訊資產之存取授權，並評估與審核資訊資產分類分級及 其價值，指定資訊資產保管單位。

3.2.3 資訊資產保管單位：對於資訊資產權責單位所指定之資訊資產，具有落實保護管理責任。

3.2.4 資訊資產使用單位：對於資訊資產之使用，必須依據權責單位要求，並具有正確使用操作之責任。

3.3 資產鑑識

3.3.1 各資訊資產權責單位應鑑別所管轄之資訊資產，並建立「資訊資產清單」。

3.3.2 資訊資產權責單位應定期更新與維護所管轄之資訊資產清單。

3.4 資訊資產分類

3.4.1 資訊資產依其性質不同，分為 7 類：人員、文件、軟體、通訊、硬體、資料、環境。包括下列:

l 人員（People / PE）包含全體同仁及委外廠商。

l 文件（Document / DC）以紙本形式存在之文書資料、報表 等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。

l 軟體（Software / SW）作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。

l 通訊（Communication / CM）提供資訊傳輸、交換之線路或服務

l 硬體（Hardware / HW）網路設備、主機設備等相關硬體設施。

l 資料（Data / DA）儲存於硬碟、磁帶、光碟等儲存媒介之 數位資訊。

l 環境（Environment / EV）相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

3.5 資訊資產價值鑑識

3.5.1 資訊資產權責單位應鑑別其所管轄內所有資訊資產之價值。

3.5.2 資訊資產價值除考量資訊資產機密等級之外，尚需考量資訊資產之可用性及完整性，其評估標準如下：

3.5.3 機密性評估

評估標準	數值
一般：此資訊資產無特殊之機密性要求	1
限閱：此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位 使用	2
敏感：此資訊資產僅供內部相關業務承辦人員存取	3

機密:此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

3.5.4 完整性評估

評估標準	數值
資產本身完整性要求極低	1
資產本身具有完整性要求,但是完整性被破壞不會對 組織造成傷害	2
資產具有完整性要求,且完整性被破壞會對組織造成 傷害,但不至於太嚴重	3
資產具有完整性要求,且完整性被破壞會對組織造成 傷害,甚至會造成業務終止	4

3.5.5 可用性評估

評估標準	數值
資訊資產容許失效≧3 天	1
8 小時≦資訊資產容許失效＜3 天	2
4 小時≦資訊資產容許失效＜8 小時	3
資訊資產容許失效＜4 小時	4

3.5.6 資訊資產價值之決定，依據資訊資產之機密性、完整性及可用性評估後，取3者之最大值為資訊資產價值。

3.5.7 權責單位每年至少進行 1 次資產盤點與資訊資產清單覆核，以更新及確保資訊資產清單的正確性及完整性。

4.人力資源安全

4.1 其目的在於辦理本院全體同仁之安全管理及教育訓練，減少人員因資訊安全認知不足所引發之資訊安全事件。

4.2 新聘人員

4.2.1 資訊安全小組需針對本院新進人員辦理資通安全相關注意事項之說明

4.3 聘顧期間

4.3.1 為提升本單位人員之資訊安全意識與專業知識資訊安全小組每年應提供相關資安教育訓練課程,或派員接受外部單位辦理之專業資安課程以提升人員資訊安全知識及警覺意識,降低人為錯誤或故意誤用資訊之風險。

4.3.2 資訊安全小組應提供充足之資通安全教育訓練課程,並確保本院人員所受教育訓練時數: 每年主官至少 1 小時，主管至少 1 小時，技術人員至少 2 小時，一般人員至少 2 小時

4.4.聘雇終止或變更

4.4.1 離退人員之帳號應於人員離退後，進行相關帳號刪除

4.4.2 離退人員之資炫資產應於人員離退後，辦理相關資產轉移

4.5 教育訓練審查

4.5.1 教育訓練執行之成果，資訊安全小組應針對成果，進行必要檢討與後續改善作業

5. 實體與環境安全

5.1 確保資訊資產及周邊環境設施，減少環境安全問題所引發的危險，以便達成本單位安全控管之目的。

5.2 安全區域

5.2.1 本院之資訊機房為安全區域

5.2.2 為確保相關設施之安全，非權責單位指定之人員不得擅自進入安全區域或使用相關資訊設備。

5.2.3 若外部人員或本單位未具機房進出權限人員，因執行業務需求進入機房時，必須由資訊資產權責單位或保管單位指派人員隨行並 填寫「人員進出機房登記表」後方可進出機房，並遵守相關設備管理之規定。

5.3 設備安全

5.3.1 謹慎使用電源延長線，以免電力無法負荷而導致火災，於新增硬體設備時，應先評估電力負荷。

5.3.2 電力、網路、通信設備應予以保護，以防止遭有心人士截取或破壞。

5.3.3 電腦機房內應保持整齊清潔，並嚴禁吸煙、飲食或堆置易燃物。

5.3.4 電腦機房應設置專用空調設備以維持電腦主機正常運作。

5.3.5 經評估後,確定將資訊設備(如伺服器、防火牆等)委外維護時，應簽訂維護契約，並定期實施保養與維護，以確保設備完整性及可用性之持續使用。

5.3.6 重要電腦主機之資訊設備及警報系統等應定期檢修測試。

5.3.7 冷氣機、不斷電系統(UPS)等機電設備之使用，應依照設備說明書指示操作，並施行定期檢查作業。

5.3.8 相關核心系統之穩定可用率(主機、資料庫)，其穩定可用率應高於 95%。

6.通訊與作業管理

6.1 防止資訊在不安全之網路環 境下，遭致可能之破壞，或非預期及非經授權之修改，以確保資訊系統與資 料之安全性、可用性及完整性。

6.2 變更管理

6.2.1 新增設備及網路變動，應即時修改網路架構圖及設備資料。

6.2.2 架構調整：架構變動之影響性甚大者應經資訊安全執行秘書以上核准，並新增對外網路連線，需注意安全性考量，從嚴審核對外網路連線與內部之連接之方式

6.2.3 如有廠商參與安裝或設定，必須全程陪同參與並記錄。

6.2.4 為減少可能危害作業系統之風險應用程式之更新作業應限定只能由授權之管理人員才可執行，且應建立應用程式之更新稽核紀錄。

6.2.5 作業系統變更時，應審查與測試重要營運系統，以確保對組織作業或安全無不利之衝擊。

6.3 第三方服務交付管理

6.3.1 各系統、主機、機電或設備若有委外廠商執行維護時，相關委外維護作業記錄應予以保存

6.4. 系統規劃與驗收

6.4.1 系統及設備建置前，主辦單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。

6.4.2 主機及重要伺服器執行作業系統容量管理(包括: CPU, RAM 與硬碟使用)之數量，應予以定期審查，並檢討、追蹤後續可改善事項

6.5 備份

6.5.1 各項系統設定檔、網頁資料、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期，並依據週期執行系統排程或手動備份

6.5.2 應定期於測試主機上測試備份復原是否正確。

6.5.3 若備份回復失效，各資訊負責人應記錄其異常狀況，並予以檢討、追蹤後續可改善事項

6.6 網路安全管理

6.6.1 避免利用公共網路傳送敏感等級以上資訊，應保護資料在公共網路傳輸之完整性及機密性，並保護連線作業系統之安全性。

6.6.2 網路管理人員應利用網路管理工具，偵測及分析網路流量。

6.6.3 如果系統使用者為非合法授權之使用者時，應立即撤銷其系統使用權限；離（休）職人員應依資訊安全規定及程序，取 消其存取網路及系統之權限。網路管理人員除依相關法令或

規定，不得閱覽使用者之私人檔案；但如發現有可疑之網路 安全情事，網路系統管理人員得依授權規定，使用工具檢查 檔案。

6.6.4 網路管理人員除有緊急狀況外，未經使用者同意，不得增加、刪除及修改私人檔案。

6.6.5 網路管理人員應每日檢查所有網路設備並檢視是否有異常情形，並每月送主管簽核。

6.7 媒體處置

6.7.1 系統資料若需以各儲存媒體保存時該媒體應存放於安全設備或處所。

6.7.2 儲存媒體所使用之密碼或編碼技術不應透露予遞送人員或與業務無關之人員。

6.8 監視

6.8.1 每月應檢視一次各設備中系統時間是否一致並進行院正及同步作業。

6.8.2 大型主機之系統稽核應予以定期審查，並予以檢討、追蹤後續之改善事項。

7. 存取控制

7.1 為保護資訊資產，降低未經授權存取系統之風險，以達成本院資訊安全控管之目的。

7.1.2 資訊資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資訊資產。

7.1.3 非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安全控管措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。

7.1.4 被賦予系統管理最高權限之人員，掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

7.1.5 資料、資訊之存取，必須符合「電腦處理個人資料保護法」、「電子簽章法」及「智慧財產權」等相關法規、法令之規定，或契約對資 料保護及資料存取使用控管之規定。

7.2 使用者存取管理

7.2.1 各項系統資源使用權限之申請、註冊及註銷作業管理程序，並維護相關之申請、註冊、註銷資料與紀錄，以備查核。

7.2.2 使用者職務異動或離職時，部門主管應即時通知相關單位調整或終止使用者之存取權限。

7.2.3 各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）應有書面紀錄並妥善保管該項文件。

7.2.4 用者存取權限應定期審查，週期不得超過 1 年。

7.3 作業系統存取控制

7.3.1 系統設定應避免於終端機登入程序中以明碼方式顯示密碼相關資訊。

7.3.2 只有在完成所有的登入資料輸入後系統才開始查驗登入資訊的正 確性;如果登入發生錯誤,系統不應顯示那一部分資料是正確的， 那一部分資料是錯誤的。

7.3.3 系統管理人員結束系統維護作業後,應結束應用系統及網路連線，清除螢幕上的資訊，登出系統，並鎖定主控台螢幕。

7.3.4 作業系統登入失敗次數應予以限制，次數建議在 3 次。

7.4 帳號與密碼

7.4.1 使用者首次使用系統時,應立即更改密碼設定,並妥善保管帳號與維持密碼之機密性,保存帳號密碼之檔案應以加密方式處理。

7.4.2 系統管理者密碼設置，至少8 碼，且應符合密碼設置原則。

7.4.3 使用者密碼設置至少6碼，且應符合密碼設置原則。

7.4.4 密碼設置原則 應儘量避免使用易猜測或公開資訊為設定，例如：

A. 個人姓名、出生年月日、身分證字號

B. 機關、單位名稱或其他相關事項

C. 使用者 ID、其他系統 ID

D. 電腦主機名稱、作業系統名稱

E. 電話號碼

F. 空白

7.4.5 使用者遺忘密碼時，須填具「資訊服務申請表」經部門主管核准後，由帳號管理人員重新設定。

7.5 遠端存取之限制

7.5.1 所有資訊資源使用者,非經主管授權或允許,禁止執行遠端存取作業。

7.5.2 所有遠端存取需求須填具「資訊服務申請表」經部門主管核准後，由帳號管理人員設定。

8. 資訊系統獲取開發及維護

8.1 確保本院資訊中心資訊系統開發、測試與維護作業之安全管理。

8.1.2 應用系統之正確性處理應予以記錄，並避免因資訊系統不良導致不正常中斷。

8.1.3 應用程式原始碼,應集中存放,並指定專人管理程式之增修作業。

8.1.4 開發中之原始程式碼，應與線上程式碼分開放置與控管。

8.1.5 舊版的原始程式應妥慎保管，並詳細記錄使用的明確時間，以備新版失敗回復使用。

8.2 技術性脆弱管理

8.3 每年應定期查核一次技術符合性，進行弱點掃描，以確定資訊系統及網路環境符合安全實施標準。

9. 資訊安全事故管理

9.1 建立迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件所造成之損害。

9.1.1 應建立資訊安全事件之處理作業程序，並賦予相關人員必要責任，以便迅速有效處理資訊安全事件。

9.2 通報程序

9.2.1 疑似資訊安全事件發生時，發現人員應依事件歸屬通報權責單位， 並副本告知直屬主管。

9.2.2 權責單位於收到通知後，研判是否為資訊安全事件。若：

9.2.2.1.定為非資訊安全事件時，則將結果回覆予發現人員。

9.2.2.2 判定為資訊安全事件時，初估事件處理時間，並通知資訊安全執行秘書。

9.3 權責單位於發生資訊安全事件時，應立即填具「資訊安全事件報告單」

10.遵循性

10.1 資訊安全委員會須依據本院資訊安全管理系統，每半年定期執行資通安全制度管理內部稽核作業。

10.2 因應事件通報或內部稽核所引發之矯正與預防措施，權責單位應於預計時間內完成改善。

10.3 應定期查核技術符合性，進行弱點掃描或滲透測試，以確定資訊系統及網路環境符合安全實施標準。應定期查核技術符合性，進行弱點掃描或滲透測試，以確定資訊系統及網路環境符合安全實施標準。