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

資通安全組織章程

－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：資通安全組織章程

文 件 編 號：ISMS-1-02

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
98.09.01	初版		1.0
100.06.20	資訊安全與資訊治理推動小組成員由總務部改為工務部	9	1.1
108.12.09	加入資訊治理組織	全	1.2
111.01.25	依組織現行編制進行修訂	全	1.3
111.07.19	組織架構調整，增加資安專責人員職務	全	1.4
112.04.22	依組織名稱、架構及職責修訂相關內容	全	1.5
114.05.26	因應 ISO27001:2022 轉版，相關內容改版	全	3.0

新光醫療財團法人新光吳火獅醫院

文件編號	ISMS-1-02	文件名稱	機密等級	版本	3.0
制訂單位	資訊部	資通安全組織章程	內部使用	頁數	1/11

1. 目的

為有效推動與辦理新光吳火獅紀念醫院（以下簡稱本院）資通安全之各項工作，特成立資通安全管理委員會，以擬定本院資通安全發展之方向、策略及步驟，促使資通安全管理制度能持續穩健運作。

2. 資通安全管理委員會

2.1. 成員

本委員會設主任委員一名、副主任委員一名、委員若干名、執行秘書一名。

2.1.0. 主任委員：由行政副院長（資安長）親自擔任。

2.1.1. 副主任委員：由資訊部主任擔任。

2.1.2. 執行秘書：由資訊部硬體架構課主管擔任。

2.1.3. 委員：由主任委員聘任院內資訊、稽核、企劃、工務、醫工、總務、採購等各領域委員擔任。任期二年，每任期由主任委員重新推薦原額二分之一之新任委員。委員中途出缺時，繼任人員之任期至原任期屆滿之日止。

2.1.4. 資安緊急應變小組：由資安長召集全院相關部門成立。

2.2. 職責

2.2.0. 本院資通訊發展暨安全管理階層的決策組織。

2.2.1. 審查與頒布資通安全政策。

2.2.2. 規劃並決定資通安全管理系統目標的需求。

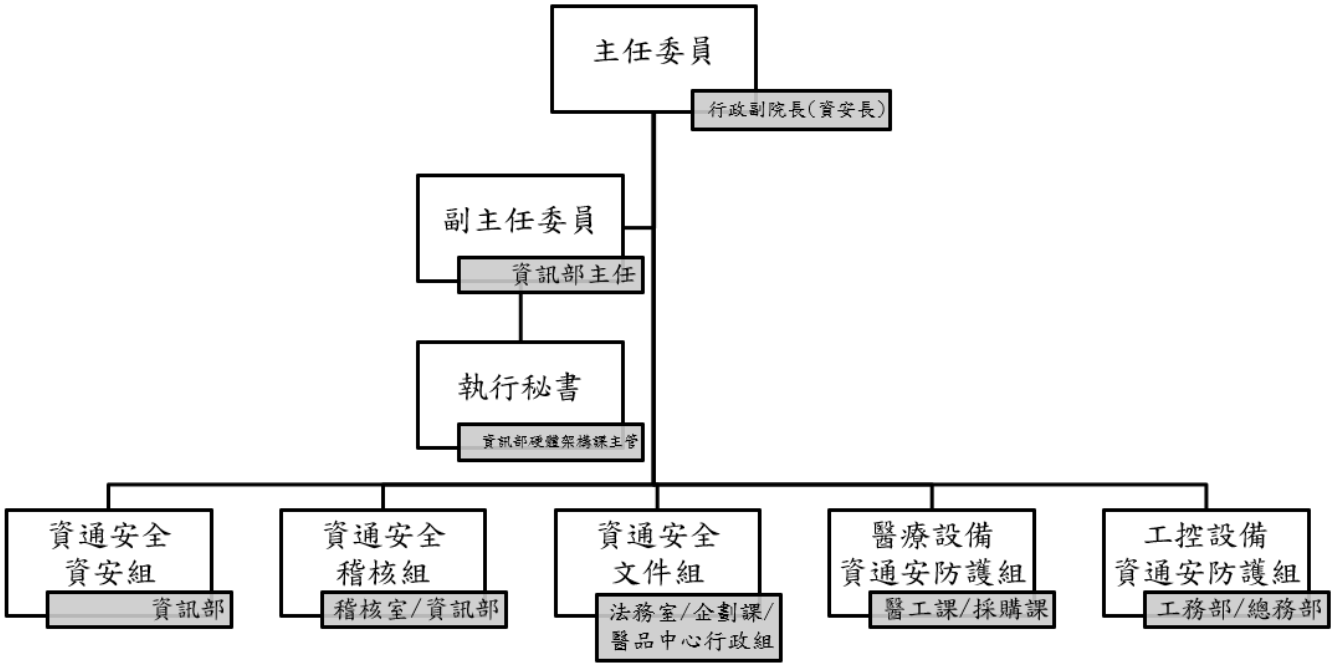
2.2.3. 制定資通安全事件應變機制。

2.2.4. 制定資通安全維護計畫。

2.2.5. 指導通過 ISO 27001 等資訊安全管理相關認證。

2.2.6. 每年至少召開管理審查會議 1 次，必要時得召開臨時會議。

3. 組織架構


主任委員
行政副院長(資安長)
副主任委員
資訊部主任
執行秘書
資訊部硬體架構課主管
資通安全
資安組
資訊部
資通安全
稽核組
稽核室/資訊部
資通安全
文件組
法務室/企劃課/
醫品中心行政組
醫療設備
資通安防護組
醫工課/採購課
工控設備
資通安防護組
工務部/總務部

4. 職掌與分工

4.1. 主任委員

4.1.0. 由行政副院長（資安長）擔任。

4.1.1. 職責

4.1.1.1. 領導本院推動有關資通安全維護之各項業務。

4.1.1.2. 領導本會策劃、推動有關資通安全事項之工作。

4.1.1.3. 針對資通安全管理委員會會議之各項討論議題進行裁決。

4.1.1.4. 指派同仁擔任資通安全稽核組、資通安全資安組、資通安全文件組、醫療設備資通安防護組、工控設備資通安防護組之組長(代表)一職，各組成員由各組組長(代表)指派。

4.1.1.5. 協調及督導各關鍵業務流程負責人執行作業，提供資通安全所需的資源，並協調資源之調派使用。

4.1.1.6. 依據資通安事件評估之結果，得依現況決議是否宣布災變或是否啟動營運持續計畫。

4.1.1.7. 負責規劃原營運場所之現場復原工作。

4.2. 副主任委員

4.2.0. 由資訊部主任兼任。

4.2.1. 職責

4.2.1.1. 協助主任委員推動資通安全相關應辦事項之業務。

4.2.1.2. 協助資通安全相關事務的推動、計畫、設計與推行。

4.2.1.3. 協助制訂本院之資通安全應變機制，執行各項資通安全之維護。

4.2.1.4. 協助制定及落實執行各項資通安全維護計畫，取得 ISO 27001(CNS 27001)認

證。

4.2.1.5. 即時反應院內有關資通安全之問題，避免資安事件的發生與問題解決。

4.2.1.6. 為本院資通安全管理代表。

4.2.1.7. 協助主任委員統籌資通安全管理委員會運作相關事項。

4.2.1.8. 資通安全特定角色職責指派。

4.2.1.9. 負責合訂本院資通安全相關管理文件紀錄，並為本院資通安全風險管理人。

4.2.1.10. 當重大資通安事件發生時，負責聯絡召集資通安全資安組人員。

4.3. 執行秘書

4.3.0. 由資訊部硬體架構課主管擔任。

4.3.1. 職責

4.3.1.1. 協助主任委員及副主任委員執行各項業務。

4.3.1.2. 負責會議召開、記錄、有關議案之蒐集、決議案件之執行、追蹤以及會務處

理等事務。

4.3.1.3. 配合資通安全計畫研擬之機制，執行委員會所負責指標項目之監控與改善。

4.3.1.4. 審查資通安全政策與目標與確認控制措施的有效性。

4.3.1.5. 資訊資產之安全需求研議、使用管理及保護等事項。

4.3.1.6. 對資通安全狀況進行預警、防禦、監控等規劃。

4.3.1.7. 規劃本院資通安全認知所需資源，如教育訓練資源。

4.3.1.8. 規劃及處理資通安全與資訊管理事件處理與通報。

4.3.1.9. 確認資通安全風險及實施風險處理。

4.3.1.10. 持續改善資訊安全管理制度。

4.4. 資通安全資安組

4.4.0. 成員： 由資訊部委員擔任代表。

4.4.1. 職責

4.4.1.1. 執行資通安全管理委員會的決議事項。

4.4.1.2. 制定、定期檢視資通安全政策。

4.4.1.3. 擬定並執行資訊風險評鑑作業。

4.4.1.4. 審查資通安全管理制度的矯正措施。

4.4.1.5. 依據資訊安全稽核報告執行改善行動。

4.4.1.6. 提報資通安全工作執行狀況。

4.4.1.7. 執行資通安全教育訓練規劃與推動，並維護相關紀錄。

4.4.1.8. 執行各項資通安全例行作業檢查。

4.4.1.9. 蒐集資通安全相關資訊（如修補程式、防毒及防駭措施）並發布公告。

4.4.1.10. 協調及支援應用系統的安全措施，確保系統的可用性、機密性與完整性。

4.4.1.11. 確保應用系統管理及開發符合相關程序規範。

4.4.1.12. 確保帳號管理符合存取控管規範，並適當控管網域使用者的存取權限。

4.4.1.13. 確保作業系統及各項服務的更新與修補。

4.4.1.14. 使用適當工具或方法確保主機、資料庫及相關設備正常運作。

4.4.1.15. 維護防火牆、IPS/IDS 等資通安設備，監控異常行為，確保設定與規則的適切性。

4.4.1.16. 確保網路設備與通訊系統的安全性與穩定性。

4.4.1.17. 確保電腦機房與辦公區域的實體安全機制正常運作，符合相關安全規範。

4.4.1.18. 規劃危機處理程序，清查事件原因、影響範圍及損失評估，執行應變措施與

資訊安全通報。

4.4.1.19. 評估監控資訊，審查資訊安全事故並建議適當措施，必要時尋求專家建議。

4.4.1.20. 依據相關程序書執行資通安全事件通報與營運持續管理。

4.5. 資通安全文件組

4.5.0. 成員：由法務室、企劃課、精實醫療品質管理中心-行政組委員擔任代表。

4.5.1. 職責

4.5.1.1. 資訊安全管理系統四階文件發行、回收、保管、借閱與銷毀及版本管理。

4.5.1.2. 資訊安全管理系統四階文件、電子文件公告及更新管理。

4.5.1.3. 蒐集並分析相關資安法律與規定，研擬相關規範對策。

4.6. 稽核組

4.6.0. 成員：由稽核室委員及資訊部稽核員擔任代表。

4.6.1. 職責

4.6.1.1. 稽核組組長：監督稽核的公正性及客觀性，並確保發現事項的改善追蹤。

4.6.1.2. 負責評估資通安全管理制度之落實與遵行情形

4.6.1.3. 訂定相關之稽核計畫、執行稽核作業。

4.6.1.4. 稽核資通安全管理制度之落實與遵行情形。

4.6.1.5. 撰寫資通安全管理系統稽核報告及提出建議。

4.6.1.6. 追蹤缺失事項之執行情形。

4.7. 資通安全專責人員

4.7.0. 成員

資通安全專責人員，由資安長指定取得證書同仁擔任。

4.7.1. 職責

策略面：

4.7.1.1. 本院資通安全政策、資源分配及整體防護策略之規劃。

4.7.1.2. 資通安全維護計畫實施情形之績效評估與檢討。

管理面：

4.7.1.3. 訂定、修正及實施資通安全維護計畫並提出實施情形。

4.7.1.4. 訂定及建立資通安全事件通報及應變機制。

4.7.1.5. 辦理本院資通安全責任等級之應辦事項：資訊安全管理系統(ISMS)之導入及通過公正第三方之驗證、業務持續運作演練、辦理資通安全教育訓練等。

4.7.1.6. 委外廠商管理與稽核。

技術面：

4.7.1.7. 整合、分析與分享資通安全情資。

4.7.1.8. 配合主管機關辦理機關資通安全演練作業。

4.7.1.9. 辦理本院資通安全責任等級之應辦事項：安全性檢測、資通安全健診、資通安全威脅偵測管理機制、弱點通報機制、資通安全防護等。

4.8. 醫療設備資通安防護組

4.8.0. 成員：由醫工課及採購課委員擔任代表。

4.8.1. 職責

4.8.1.1. 負責醫療儀器設備之資通安防護及相關作為。

4.8.1.2. 由醫工課及採購課委員擔任代表。

4.8.1.3. 執行主管機關及本院對醫療儀器設備之資通安全管理規定，以符合相關法規要求。

4.9. 工控設備資通安防護組

4.9.0. 成員：由工務課及總務部委員擔任代表。

4.9.1. 職責

4.9.1.1. 負責工務安控等相關設備之資通安防護及相關作為。

4.9.1.2. 由工務課及總務部委員擔任代表。

4.9.1.3. 執行主管機關及本院對工控設備之資通安全管理規定，以符合相關法規要求

5. 成員能力需求

資通安全管理審查管理會各組成員能力需求說明如下表：

角色	人員能力需求
資通安全管理審查管理會成員	無
資通安全稽核組	稽核組長：需完成3小時資安通識課程。 組員： 依成員角色需求通過 ISO 27001主導稽核員(Lead Autidor) 或 ISO 29100主導稽核員(Lead Autidor) 或 BS10012主導稽核員(Lead Autidor)課程訓練 或執行稽核、觀察員之經驗
資通安全文件組	曾接受資訊安全相關教育訓練者
資通安全資安組	依成員角色需求不同，熟悉領域知識， EX： 1. ISO 27001主導稽核員(Lead Autidor) 2. 網路管理能力，如：防火牆、路由器、交換器、防毒及防駭能力
資通安全專責人員	依據「資通安全責任等級 A 級之特定非公務機關應辦事項」，需具有資安專業證照及職能證書。
醫療設備資通安防護組	宜具備 ISO 27001主導稽核員證照。
工控設備資通安防護組	宜具備 ISO 27001主導稽核員證照。

6. 內部組織資訊安全管理

6.1. 資通安全管理委員會為資通安全管理制度之管理權責單位，資通安全管理委員會所轄各分組統籌辦理資通安全管理制度相關事宜，並委任資通安全資安組依據「ISMS-1-01_資通安全政策」，規劃與制定相關安全作業流程及程序，由資通安全管理委員會核准後實施。

6.2. 資通安全管理委員會為達成資通安全政策目標，應識別與明確定義相關資通安全工作

角色與職掌，以執行資通安全作業流程及程序，維護資通資產安全。

6.3. 各項資通資產應依據「ISMS-2-05_資通資產管理程序書」，由權責單位指派專人負責，建立資通資產管理與使用授權程序，並依據風險評鑑結果實施必要控制措施。

6.4. 資訊機房管理維運相關人員，應依據「ISMS-2-06_人員管理及教育訓練程序書」，簽署保密切結。

6.5. 資通安全管理委員會為持續改善資通安全管理制度、獲取資通安全技術、產品資訊與知識及處理資通安全事件或事故或執行系統修補等資訊，應隨時與相關技術廠商、各種專家安全性論壇、專業協會及政府機關維持聯繫，以取得各方資通安全建議。相關權責單位與利害團體之聯繫關係及權責應詳列於「ISMS-1-02-2_外部單位聯絡清單」。

6.6. 資通安全管理制度應依據「ISMS-2-09_資通安全內部稽核程序書」進行獨立審查，確認資通安全管理制度落實情形，並且持續改善。

6.7. 資通安全管理委員會應依據「ISMS-2-07_資通安全事件通報、處理及緊急應變程序書」與相關權責單位建立通報管道並執行通報作業。

7. 外部組織資訊安全管理

7.1. 外部組織存取組織內之資通處理設施或資訊前，應評估其風險，並遵循相關資通安全管理制度或依循標準之要求，採取適當控制措施。

7.2. 委外合約中，應制定可滿足資通安全需求之合約條款，並與委外廠商簽訂、遵循保密切結書並執行保密作業。

7.3. 委外服務內容變更，應審查是否影響相關資通安全管理制度或依循標準之要求，評估其風險，採取適當控制措施。

7.4. 委外作業規格書或徵求建議書說明文件，應包含資通安全需求，並依資通安全法相關規範謹慎評估委外廠商資格。

7.5. 委外廠商須依合約執行相關工作，應提交工作報告或維護紀錄，以監督委外作業契約履行情形及執行績效，必要時應稽核委外廠商安全控管措施，評鑑時機可參考專案

交付驗收點進行。

7.6. 委外廠商須遵守本院內之相關資通安全規定並配合資通安全稽核活動。

7.7. 委外人員執行業務時，應遵守本院資通安全相關規定，若違反時應依相關法令、本院相關規定及契約懲處。

7.8. 外部組織因應業務需要需存取組織內之資通處理設施或資訊，應遵守本院資通安全相關規定，資訊資產管理權責單位應依據本院資通安全相關規定進行安全管制，並告知使用者所須遵循之權責義務，妥善使用資通處理設施或資訊，涉及資通資產完整性與機密性之資通安全管理範圍者，應簽署保密協議書，使其瞭解未遵循本院資通安全相關規定或有行使任何危及本院資通安全之行為，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。

8. 實施與修正

本程序書奉　資安長核定後實施，修正時亦同。

9. 相關文件

ISMS-1-01_資通安全政策

ISMS-2-05_資通資產管理程序書

ISMS-2-07_資通安全事件通報、處理及緊急應變程序書

ISMS-2-09_資通安全內部稽核程序書

10. 輸出文件/紀錄

ISMS-1-02-1_資通安全組織成員表

ISMS-1-02-2_外部單位聯絡清單