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

資通安全組織全景管理程序書

－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：資通安全組織全景管理程序書

文 件 編 號：ISMS-2-01

制 定 單 位：資訊部

制 定 日 期：114 年 07 月 01 日			
修訂日期	修訂內容摘要	頁次	版本
111.06.14	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	新增表單編號	2	1.2
114.05.26	因應 ISO27001:2022 轉版，相關內容改版		3.0
114.07.01	修訂 4.4 資訊安全管理系統實施及驗證範圍	5	3.1

新光醫療財團法人新光吳火獅醫院

文件編號	ISMS-2-01	文件名稱	機密等級	版本	3.1
制訂單位	資訊部	資通安全組織全景管理程序書	內部使用	頁數	1/4

1. 目的

為推動新光吳火獅紀念醫院（以下簡稱本院）資通安全政策，藉由全面性了解影響本院核心營運業務之資通安全內、外部議題，及與本院往來之關注方對本院資通安全期望與要求，訂定評估方法，以界定本院資通安全管理的策略方針與實施範圍。

2. 依據

ISO 27001。

3. 權責

3.1. 管理階層

3.1.1. 負責審查組織全景評鑑過程紀錄，以及本程序書適當性。

3.1.2. 擔任組織面風險的管理者。

3.1.3. 決定風險因應對策的實施，及對風險的接受。

3.2. 資通安全資安組

3.2.1 鑑別組織的宗旨與營運目標

3.2.2 鑑別外部關注方及其需要與期望

3.2.3 鑑別內部關注方及其需要與期望

3.2.4 界定資訊安全管理系統實施範圍

3.2.5 評估資訊安全管理系統實施範圍與組織宗旨及關注方需要與期望的差異風險

3.2.6 評估當鑑別的風險發生時，其潛在的衝擊影響

3.2.7 參與風險因應對策之討論與決策

3.2.8 定期與不定期重新進行組織全景評鑑，以鑑別風險之變化與新風險的產生。

4. 程序

4.1. 組織營運宗旨與目標及關注方需要與期望的鑑別

在鑑別組織全景時，首先須取得管理階層對組織營運宗旨與目標的看法與共識。其次，鑑別涉及本院主要核心營運作業與服務之資通安全相關的外部關注方及其需要與期望，以及內部關注方及其需要與期望。

資通安全相關之內部與外部議題及關注方之期望與要求來源：

1. 內部議題：

1.1 本院之資通安全願景。

1.2 本院各項會議或公文決議之重大資安決策事項。

1.3 本院發生重大資安事件相對應之矯正措施因應對策。

2. 外部議題：

2.1 涉及本院應遵循之資通安全相關法律的頒布或變更。

2.2 新興資訊科技所帶來之資安風險議題(如雲端應用、行動裝置、巨量資料、人工智慧及物聯網…等)。

2.3 近期外部及醫療單位發生之重大資安事件。

3. 關注方之期望與要求：

3.1 主管機關發布之資通安全相關命令或規定。

3.2 與業務合作夥伴或承攬醫療相關業務(如健診)訂定合約、協議與資通安全相關之要求事項。

3.3 來自內部員工資安相關重大提案。

3.4 集團管理單位對資通安全的期望與要求事項。

綜整組織營運宗旨與目標及各關注方需要與期望的內容，記載於「ISMS-2-01-2_資通安全組織全景評鑑表」、「ISMS-2-01-3_資通安全內外部議題清單」、「ISMS-2-01-4_資通安全利害相關人列表」，或以其他方式補充。

4.2. 評估組織全景的風險

針對「ISMS-2-01-2_資通安全組織全景評鑑表」所鑑別出的每一項需要與目標，無論其是否納入 ISMS 實施或驗證範圍，進行分析當未符合時可能的衝擊情境，以及該威脅可能對組織造成的衝擊程度等級，依據「表格 1：組織全景風險鑑別等級表」的判定條件，判斷威脅衝擊的等級，衝擊等級 4 屬本院核心系統或資訊作業必須納入 ISMS 導入實施範圍。

表格 1：組織全景風險鑑別等級表

衝擊等級	威脅衝擊程度
1	未能達成需要與目標對本院無傷害： 1). 對本院業務營運無任何影響。 2). 涉及資通系統資料屬一般可公開性資料無需特別保護。 3). 不存在任何法令/法規/契約的要求，或違反相關的處罰規定。 4). 不影響本院資安管理制度。
2	未能達成需要與目標對本院產生輕微傷害： 1). 對本院業務營運造成輕微的影響，威脅造成的衝擊可接受。 2). 涉及資通系統資料屬本院內部使用資料，資料外洩未涉及法律層面，致多涉及內部行政懲處，對本院影響輕微。

衝擊等級	威脅衝擊程度
	3). 可能違反本院內部的行政規範或契約的要求。 4). 不影響本院資安管理制度但須個案處理。
3	未能達成需要與目標對本院產生中度傷害： 1). 對本院業務營運造成一定的影響（造成部分非主要核心業務中斷），威脅造成的衝擊產生一定的損害。 2). 資通系統資料屬密等資料或含有一般性個資，資料外洩涉及法律層面，對本院有一定程度影響。 3). 可能違反法令/法規的要求，引起主管機關關注，但不致引起媒體關注。 4). 影響資安管理制度，但僅適用本院部分資訊作業(屬例外管理部分)。
4	未能達成需要與目標對本院產生嚴重傷害： 1). 對本院業務營運造成嚴重的影響（造成主要核心業務中斷），威脅對本院的衝擊產生重大的損害。 2). 資通系統資料內含密等內醫院營業機資料或病人醫療資料，資料外洩涉及法律層面，對本院有嚴重影響，須嚴密保護。 3). 可能違反法令/法規的要求，並引起主管機關及媒體關注。 4). 影響本院資安管理制度，且適用本院所有相關之資訊作業。

4.3. 控制目標，控制措施和因應對策的鑑別

對「ISMS-2-01-2 組織全景評鑑表」所有層面的需要與目標進行討論，決定是否採取適當的因應對策或接受風險，將計畫採取的因應對策敘述於「ISMS-2-01-2_資通安全組織全景評鑑表」，並確認所採取的因應對策與 ISO 27001 控制條款間之關係，彙整到「ISMS-2-15_適用性聲明書」(SOA)。

部分無法對應 ISO 27001 控制條款的風險處理對策，亦應妥善分析處置，確實對每一項「ISMS-2-01-2_資通安全組織全景評鑑表」鑑別出的需要與目標進行風險管理。

4.4. 資訊安全管理系統實施及驗證範圍

資訊安全管理系統實施範圍為全院，驗證範圍依據主管機關要求、資通安全維護計畫及「ISMS-2-01-2_資通安全組織全景評鑑表」各方面的需要與目標討論結果，由最高管理階層決定納入 ISMS 驗證範圍，並將明確的 ISMS 驗證範圍描述載明於適當之文件或會

議記錄。

4.5. 組織全景評鑑紀錄

針對上述流程執行過程與結論(亦即「ISMS-2-01-2_資通安全組織全景評鑑表」)，應呈報「管理階層」,使得「管理階層」可以清楚地了解本院營運要求以及民眾的期望，與驗證單位實施 ISMS 範圍的差異，以及可能存在的風險，以期給予最高的注意力及保證程度的等級，提供相關關注方信心。並將相關風險，選擇其重要關注項目列入「ISMS-2-13-1_資通安全量化指標有效性量測表」定期量測。

5. 監控和審查

組織全景評鑑應至少每年審查一次，並在有任何關於營運流程的改變、組織結構變更，或關注方產生新需要或期望時，應修訂「ISMS-2-01-2_資通安全組織全景評鑑表」。

當變更較為明顯且必要時，應一併修訂「ISMS-2-15_適用性聲明書」(SOA)。

6. 實施與修正

本程序書經 資通安全委員會副主任委員核定後頒布實施，修正時亦同。

7. 輸出文件／紀錄

ISMS-2-01-1_資通安全組織全景表

ISMS-2-01-2_資通安全組織全景評鑑表

ISMS-2-01-3_資通安全內外部議題清單

ISMS-2-01-4_資通安全利害相關人列表