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

資通安全內部稽核程序書

－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：資通安全內部稽核程序書

文 件 編 號：ISMS-2-09

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
98.10.05	5.2.2 修正內部稽核分組員擔任資格	2	1.1
109. 04. 10	整併資訊服務管理制度		1.3
109.04.29	與 ISO20000 文件整併為:資通安全與資訊管理稽核程序書 (原 27001 文件名稱: E000－2010 資通安全稽核程序書)		1.4
111.04.25	修訂資通安全管理制度之內部稽核頻率為每年至少二次	3	1.5
111.07.19	修訂稽核員資格	2	1.6
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	1.7
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-2-09	文件名稱	機密等級	版本	3.0
制訂單位	資訊部	資通安全內部稽核程序書	內部使用	頁數	1/4

1 目的：

建立資訊安全管理系統（以下簡稱 ISMS）獨立稽核之規範，以判斷各項作業的控制目標、措施、流程及程序是否符合法規、ISO27001(CNS 27001)標準及組織之資通安全要求。

2 範圍：

本院 ISMS 各項作業流程之稽核作業。

3 權責

3.1 資通安全管理委員會

3.1.1 指派資通安全稽核組組長。

3.1.2 負責督導資通安全稽核作業。

3.2 資通安全稽核組

3.2.1 辦理稽核作業相關事宜。

3.2.2 稽核缺失定期追蹤改善情形並加以記錄。

3.3 資通安全稽核組組長

3.3.1 指派資通安全稽核組組員。

3.3.2 確保稽核業務依本程序書確實執行。

3.3.3 協調提供稽核所需資源。

3.3.4 編製資通安全稽核計畫自行查核計畫。

3.3.5 召開資通安全稽核組準備會議。

3.3.6 召開稽核啟始及結束會議。

3.3.7 負責報告稽核執行情形及成果。

3.3.8 列管「資通安全稽核報告」及所附相關查核資料。

3.4 資通安全稽核組組員：配合資通安全稽核組組長指示執行稽核作業、完成各項紀錄及查證矯正措施執行情形。

3.5 受稽部門：受稽部門之主管於稽核期間應指派人員接受稽核，並協助調閱有關紀錄、報告或文件。對於稽核發現缺失應提出並執行矯正措施。

4 定義

4.1 資通安全稽核：一種有系統且獨立的資通安全檢查，以決定各項活動及相關結果是否與所計畫的安排相符，此等安排是否有效執行及達成目標。

4.2 稽核類別：

4.2.1 內部稽核：由資通安全稽核組針對作業程序之安全控制、風險評估、營運持續計畫…等程序的運作情況，進行定期查核，以確保其成效。

4.2.2 外部稽核：由本院以外單位所進行的資通安全稽核。

4.2.3 專案稽核：針對資通安全事件、資訊系統的重大變更申訴案件，特定目的的稽核。專案稽核得視稽核之特定目的需求，以不定期專案方式進行。

5 作業內容

5.1 稽核頻率

5.1.1 每年應至少辦理二次資通安全管理制度內部稽核作業。

5.1.2 視需要不定期執行專案稽核。

5.2 稽核人員之要求

資通安全稽核組組長由資通安全管理委員會指派，資通安全稽核組組員由資通安全稽核組組長指派。為確保稽核過程的客觀性與獨立性，稽核之執行應由非受稽單位擔任稽核員。稽核人員資格要求如下之一：

5.2.1 具有 ISO 27001 主導稽核員認證。

5.2.2 接受至少 6 小時以上之資訊安全管理系統(ISMS)相關稽核專業訓練。

5.2.3 至少參加 1 次之資安稽核見習。

5.2.4 接受資安相關教育訓練 3 小時以上。

5.2.5 由資通安全管理委員會指定適合人員。

5.3 ISMS 稽核作業

5.3.1 稽核計畫

為達稽核之有效性，資通安全稽核組組長應事前規劃並編製「ISMS-2-09-1_資訊安全管理制度內部稽核計畫」，以作為執行稽核指導綱要，內容應包括：稽核範圍、項目、人員、時程、程序等，並經資通安全管理委員會核准後執行。

5.3.2 稽核準備

5.3.2.1 資通安全稽核組組長應研擬規劃「ISMS-2-09-2_資訊安全內部稽核查核表」，並召開準備會議，提示稽核要點、協調分工及排定時程。

5.3.2.2 資通安全稽核組組長需於查核前通知受稽部門。

5.3.2.3 受稽部門於接獲稽核通知後，應配合準備稽核所需相關資料。

5.4 稽核執行

5.4.1 資通安全稽核組組長應於稽核前，召集資通安全稽核組、受稽單位召開啟動會議，說明稽核範圍、時程、配合事項等。

5.4.2 資通安全稽核組組員於稽核時，應依抽樣之原理收集足夠之客觀證據，以研判該稽核項目是否符合相關規範以及稽核時應保存適當的稽核軌跡。

5.4.3 資通安全稽核組組員依「ISMS-2-09-2_資訊安全內部稽核查核表」執行稽核，逐項填寫稽核結果。ISMS-2-09-2_資訊安全內部稽核查核表」若須增修時，需經資通安全稽核組組長同意。

5.4.4 受稽部門應尊重及支持資通安全稽核組組員，誠實答覆稽核員所提問題，並接受調閱有關紀錄、報告及文件。

5.5 稽核報告

5.5.1 各資通安全稽核組組員應將稽核結果透過資通安全稽核組會議討論、彙整後由資通安全稽核組組長提出稽核報告。

5.5.2 資通安全稽核組組長應於稽核完成後召開稽核結束會議，由資通安全稽核組組長報告稽核結果及發現，並對疑義進行澄清後，產製稽核報告。

5.5.3 受稽部門於接獲稽核報告後，應依據「ISMS-2-10_矯正措施管理程序書」之規定，分析缺失原因及擬採行之矯正措施填列於「ISMS-2-10-1_矯正措施單」內，且主管核定後回覆資通安全稽核組。

5.6 矯正措施

稽核缺失之後續追蹤應依據「ISMS-2-10_矯正措施管理程序書」辦理。

5.7 稽核技巧與工具保護

5.7.1 系統稽核工具（例如弱點掃描等）之存取應由授權的人員於授權範圍內操作，並留有存取、操作紀錄，以防止任何可能的誤用或破解。

5.7.2 系統稽核工具應存放於獨立系統及安全的地點內，防止不當操作造成其他系統之損害。

5.8 相關法令之要求

資通安全稽核組亦應於每次進行資安稽核時檢視其符合性。

6　實施與修訂

本程序書奉　資訊安全委員會副主任委員核定後實施，修正時亦同。

7　相關文件

ISMS-2-10_矯正措施管理程序書

ISMS-2-06_人員管理及教育訓練程序書

8　使用表單

ISMS-2-09-1_資訊安全管理制度內部稽核計畫

ISMS-2-09-2_資訊安全內部稽核查核表

ISMS-2-10-1_矯正措施單