

新光吳火獅紀念醫院

矯正措施管理程序書

[illegible]

新光醫療財團法人新光吳火獅醫院

文件編號	ISMS-2-10	文件名稱	機密等級	版本	3.0
制訂單位	資訊部	矯正措施管理程序書	內部使用	頁數	1/2

1 目的：

針對資通安全管理系統（ISMS）運作過程中發生之缺失及潛在之風險，採取相關的矯正措施，以防止類似事件發生，進而達成持續改善之目標。

2 依據

2.1 ISMS-1-01_資通安全政策

2.2 ISMS-2-02_資通安全實施程序書

3 範圍：

本院 ISMS 各項作業流程發生之缺失、資訊安全事件及潛在之風險處理事項。

4 權責

4.1 資通安全管理委員會：負責矯正措施之管理審查。

4.2 缺失權責單位：負責稽核所發現缺失、資通安全事件（含重大異常事件）、資通安全管理運行缺失或自行發現缺失之原因分析，決定優先順序與處理時限，提出矯正措施並實施。

5 定義

5.1 矯正措施：為防止不符合 ISMS 實施、操作及使用之事項重複發生，所採取之措施。

5.2 缺失：

5.2.1 主要缺失：未執行 ISMS 之要求，或多個次要缺失集中於同一控制措施者。

5.2.2 次要缺失：未能完全遵循 ISMS 之要求，但為單一事件者。

5.3 觀察：發現可能對 ISMS 造成影響的事實及事件，但未有足夠證據顯示會影響資通安全政策及目標的達成，卻因未來可能成為缺失而需要再覆核。

5.4 建議：發現可能對 ISMS 造成影響的潛在問題，可提出建議之改善措施。

5.5 缺失權責單位：矯正措施之實際執行單位。

6 作業內容

6.1 執行時機

6.1.1 內部及外部稽核發現缺失或潛在不符合時，缺失權責單位之資安專責人員需提出矯正措施，並填寫於「ISMS-2-10-1_矯正措施單」。

6.1.2 資通安全事件 3、4 級、自行發現缺失，或潛在不符合時，缺失權責單位之資安專責人員需提出矯正措施，並填寫於「ISMS-2-10-1_矯正措施單」。

新光醫療財團法人新光吳火獅醫院

文件編號	ISMS-2-10	文件名稱	機密等級	版本	3.0
制訂單位	資訊部	矯正措施管理程序書	內部使用	頁數	2/2

6.2 原因分析

防制缺失權責單位應分析問題發生之原因及影響程度，決定優先順序與處理時限。

6.3 矯正措施評估

6.3.1 缺失權責單位應提出矯正措施，以防止類似事件發生。

6.3.2 評估措施時須考慮成本效益及可行性。

6.4 追蹤執行狀況

6.4.1 矯正措施之執行狀況，應由缺失權責單位依據「ISMS-2-10-1_矯正措施單」確實執行。

6.4.2 有關執行狀況之追蹤，由資通安全稽核組員、組長或相關權責人員負責。

6.5 管理審查

缺失權責單位應彙整相關矯正措施之執行狀況，於資通安全管理委員會會議提出報告。

7 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。

8 相關文件

無

9 使用表單

ISMS-2-10-1 矯正措施單