



伍、資訊安全自我檢核表

一、基層診所適用

資訊安全自我檢核表 - 基層診所

機密等級：

日期：

項次	檢核項目	檢核結果	簡述原因
A. 設備/醫務作業系統平台使用管理			
1	醫務/醫療作業所需使用之硬體設備(電腦、伺服器、筆電)或操作平台須區隔並為專屬使用。	☐ 符合 ☐ 不符合 ☐ 不適用	
2	落實醫療/醫務作業系統平台所使用之硬體設備之控管(電腦/筆電)，且於該列管之設備僅得以執行醫療作業相關之事務(包含電子郵件)。	☐ 符合 ☐ 不符合 ☐ 不適用	
B. 軟體安裝與更新			
3	醫務/醫療作業使用之電腦、筆電或伺服器皆已完成安裝防毒軟體。請檢視防毒軟體之病毒碼是否已更新至最新版本。建議避免使用網路上提供之免費使用防毒軟體以降低風險。	☐ 符合 ☐ 不符合 ☐ 不適用	防毒軟體： 最近更新日期：
4	確認最近一次作業系統安全性更新並將更新日期紀錄存查。每月更新一次為宜。如設備使用之作業系統版本較老舊且品牌原廠不再提供版本更新服務(EOS, End of Service)，則須改採符合軟體更新時效之應用軟體，或進行存取權限控管、增加資安防護設備(如防火牆)以及密碼應符合高複雜度以確保整體資訊安全機制之運行。	☐ 符合 ☐ 不符合 ☐ 不適用	版本更新日期：
C. 設備使用之安全性			
5	啟動螢幕保護並執行限制操作時間螢幕鎖定設定。建議螢幕鎖定之時間設定以不超過 15 分鐘為原則。	☐ 符合 ☐ 不符合 ☐ 不適用	
6	電腦密碼安全性設定 - 密碼長度、複雜性需求及有效期限建議如下： 「最小密碼長度」是否為 8〔含〕或以上； 「密碼必須符合複雜性需求」是否為開啟； 「密碼最長有效期」是否為 90 天〔含〕或以下，但如有密碼外洩之風險則應立即修改。	☐ 符合 ☐ 不符合 ☐ 不適用	



項次	檢核項目	檢核結果	簡述原因
7	密碼應妥善保管避免外洩，不得將密碼張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。	☐ 符合 ☐ 不符合 ☐ 不適用	
8	執行醫療/醫務作業使用之電腦/筆電請啟動本機防火牆設定，可啟動設置阻擋可疑連線或白名單建立之功能設定。	☐ 符合 ☐ 不符合 ☐ 不適用	
9	如業務需要安裝並開啟遠端連線軟體(如telnet)之設定使用，須檢視是否有限制連線時間/IP/Log 紀錄保存等管理機制。	☐ 符合 ☐ 不符合 ☐ 不適用	
10	如業務需要使用可攜式媒體儲存(USB、行動硬碟)傳遞含有機敏性個資或機密資料，須另採加密機制保護本機資料。	☐ 符合 ☐ 不符合 ☐ 不適用	
11	避免安裝或連結未經授權及來路不明之軟體。	☐ 符合 ☐ 不符合 ☐ 不適用	
12	啟用作業系統安全性設定之稽核原則設定。	☐ 符合 ☐ 不符合 ☐ 不適用	
13	定期執行重要資料之備份作業並加密處理。建議備份資料採異地(指非本機儲存空間)存放。	☐ 符合 ☐ 不符合 ☐ 不適用	
14	內部員工私接 MODEM、ADSL 及無線網路卡等網路通訊設備易造成病患個資外洩風險，對外連線須有適切的管制措施。	☐ 符合 ☐ 不符合 ☐ 不適用	
D. 設備資產保存或報廢處理			
15	醫療/醫務作業用電腦資產需造冊列管並設定專人保管並於安全場所存放，非授權作業人員不得操作使用。 可對設備使用/保存場所進行適當的監視錄影，監視錄影之影片建議存檔3個月以上。	☐ 符合 ☐ 不符合 ☐ 不適用	
16	任何儲存資訊之電子設備於報廢/丟棄之前，應將儲存資訊刪除，並徹底消磁或銷毀至無法解讀之程度。	☐ 符合 ☐ 不符合 ☐ 不適用	

本次資訊安全自我檢核結果，須改善項目紀錄/備註如下(可委由委外廠商協助檢核)：

檢核日期：

檢核人員：

受查代表：