儀器資安盤點項目表說明

1. **是否連線上網（有 IP 位址）：□是 □否（勾否者既未連線儀器以下免填）**
   說明：IP 位址（Internet Protocol Address） 是指分配給網路上設備的數字標識(例如：192.168.1.1)，用於在電腦網路中識別和定位設備，以便進行數據傳輸。其具備實體或無線網路模組，可透過通訊協定（如 TCP/IP）連接內部或外部網路，以實現資料交換、系統更新、遠端存取或雲端整合等功能。有接網路線但無使用也算連線。
   例如：A 台透過 RS232 傳資料給 B 台，B 台再透過網路線傳送到遠端資料庫，RS232 為點對點的本地連接，不具備網路協定功能，所以 A 台儀器不算是「有連線上網」的儀器，惟 A 和 B 倘共用 1 個儀器設備碼，就應合併來看，該儀器設備碼對應之裝置具備網路連線能力。
2. **IP 位址：□固定 □浮動 IP（DHCP）**
   承 2 若為固定 IP，請提供 IP 位址_____
   說明：寫 IPv4 位址
3. **資訊整合系統：□HIS（醫療資訊系統）□PACS（影像儲存系統）□其他：____**
   承第 3 題，其他資訊整合系統為_____
   說明：空格需填寫，不要空白，HIS 系統儲存信息，如生理監視器；PACS 系統儲存影像，如 X 光影像。本院還有其他系統如 NIS、LIS。
4. **是否可使用 USB 裝置：□是 □否**
5. **是否有安裝防毒軟體(註:windows 內建防毒軟體就算)：□是 □否**
   說明：例如 Windows 10 有內建防毒軟體，就選"是"）
6. **作業系統版本：_____ (例如 Windows 10)**
   說明：例如 Windows 10、Linux、Vendor OS、或"廠商專屬開發作業系統"
7. **MAC 位址：_____(例如: 0A: 1B: 2C: 3A: 44:5C)**
   說明：MAC 位址（Media Access Control Address，媒體存取控制位址）是一種用來識別網路裝置的唯一識別碼。若無法透過系統介面查詢 MAC 位址，請填寫『無法查得』，不要寫"無"。
8. **有無加裝硬體防護裝置：□有 □無**
   說明：例如邊界硬體防火牆、閘道器、TXOne Networks（EdgeIPS 系列）、Moxa（EDR 系列）、WatchGuard、Cisco – ASA 5506-X 或 Firepower 1010、Palo Alto Networks – PA-220
9. **是否含有個資？□含一般個資與特種個資 □僅有特種個資 □僅有一般個資 □無個資**
   說明：依個人資料保護法第 6 條：有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，為特種個資；能識別個人身份的資訊，如姓名、電話號碼、住址、身分證字號為一般個資。
10. **是否有設定對時機制(網路對時或手動對時皆算)：□是 □否**
    說明：可由網路對時或手動對時，選"是"
11. **二群五類儀器設備：□終端單機 □群組型儀器 □系統型儀器**
    說明：終端單機:指醫療儀器單機直接連結院內系統網路，如：超音波影像儀；群組型儀器:指多台功能相同醫療儀器，大多數有中央站主機，間接連結院內系統網路，如生理監視器；系統型儀器:指多台功能不相同模組單機組合而成一套醫療儀器,中控主機間接連結院內系統網路(Intranet)，如：放腫部之 CT、TOMO、電腦刀系統。
12. **是否允許遠端存取：□是 □否**
    承第 12 題，若有遠端存取，該處理方式為(如 VPN)_____
    承第 12 題，若有遠端存取，可遠端之人員（如廠商）_____

說明：常見遠端存取方式：VPN（虛擬私人網路）、遠端桌面(RDP)、第三方遠端控制工具

13. **該儀器使用者帳戶之命名原則：□是 □否，無命名原則**

    承第 13 題，使用者帳戶之命名原則_____

    說明: 若有命名原則，如卡號、部門代號、姓名縮寫、每個使用者個別提供或"出廠設置"

14. **該儀器管理者帳戶是否為共用帳號：□是 □否**

    說明:如使用者共用同一帳號選"是"，不同帳號選"否"

15. **制定該儀器使用者帳號類型與數量：□是 □否 □無帳號**

    承第 15 題，使用者帳號類型_____

    承第 15 題，使用者帳號數量_____

    說明：帳號類型: 使用者帳號、管理員帳號、廠商帳號、共用帳號

16. **制定該機使用者帳戶之密碼政策：□是 □否**

    承第 16 題，若有密碼政策，密碼更新週期_____

    說明：如果密碼無更新週期，就寫"無"

    承第 16 題，若有密碼政策，密碼複雜度規定（如長度、英文數字）：_____

    說明：如果密碼無特別規定，就寫"無規定，由使用者自訂"

17. **是否具備使用者帳戶鎖定機制：□是 □否**

    承第 17 題，若有鎖定機制，鎖碼次數（如登入幾次就鎖住）_____

18. **連線中斷後是否可用其他儲存方式上傳：□是 □否**

    承第 18 題，若有備用上傳機制，上傳方式為_____

    說明：例如資料先儲存在儀器本地儲存裝置（如 HDD/SSD/RAM）、SD 卡 / USB 隨身碟、光碟片備份、NAS 區域儲存或其他設備儲存後上傳

19. **儀器 Log 是否有備份：□是 □否**

    說明：Log（日誌） 是醫療儀器運行時自動產生的記錄檔，包含系統活動、開機、關機、運行狀態、系統錯誤等資訊錯、使用者操作等。

20. **Log 保存紀錄時間：□六個月或以上 □不足六個月**

    承第 20 題，若有其他 Log 保存紀錄，時間為_____

    說明：若無，就寫"無"或"依使用頻率而定"

21. **設備系統是否有還原機制：□是 □否**

    說明：當系統發生錯誤、異常或資安攻擊時，能夠恢復到正常運行狀態的機制，例如：作業系統內建還原、RAID 硬碟陣列備援

22. **儀器原始帳號密碼是否有更改過？□是 □否**

    說明：是否仍使用出廠時就設定的帳號密碼。

23. **儀器資產類別：□Physiologic monitors and systems □Defibrillators □Infusion pumps □Anesthesia units □Ventilators □Extracorporeal Assist □Vital sign monitors □Digital radiographic X-ray systems □CT and MRI scanners □Nuclear Machine □Fetal monitors □Laboratory analyzers □Diagnostic ultrasound □Electrocardiographs □Injectors, contrast media □Dialysis machine □Others**

    說明：□生理監測儀器與系統 □去顫器 □輸液泵 □麻醉機 □呼吸器 □體外輔助設備 □生命徵象監測儀 □數位 X 光影像系統 □電腦斷層掃描（CT）與磁共振影像（MRI）掃描儀 □核醫學設備 □胎兒監測儀 □實驗室分析儀器 □診斷性超聲波儀 □心電圖儀 □注射器（對比劑）□透析機 □其他

24. **儀器放置地點：□(1)手術室 □(2)檢查/治療室 □(3)一般病房 □(4) 加護病房 □(5)急診室**

□**(6) 門診。**

說明：此題依照 H-ISAC 提供的 6 種選項，選最接近的性質。

25. 儀器使用方式：□非侵襲性: 無侵入至人體亦對病人身體無危害之儀器 □侵襲性:有侵入至人體或對病人身體有危害之儀器。

說明：侵襲性 vs 非侵襲性的區別：

非侵襲性：不需要穿透皮膚或進入身體內部，例如放射線治療、超音波、MRI。

侵襲性：需要穿刺、切開、植入或其他形式進入體內，例如手術、內視鏡、導管等。

26. 以下各子題為了評估儀器資安風險等級，填完後系統會自動顯示風險等級：

承第 26 題，技能等級(就已知現狀醫院的評估威脅者的電腦技能選最高)：□1 級：無技術性技能或具一般電腦能力 □2 級：具備部分技術性技能或具備網路與程式撰寫能力 □3 級：具備資安滲透技能。

說明：評估醫療儀器在面對資訊安全威脅時，攻擊者可能具備的技術能力高低。1 級：如偶然誤觸者、社會工程被利用者；2 級：如內部威脅人員、有基礎駭客知識的個人；3 級：如能主動利用漏洞　進階駭客、有組織犯罪、國家級攻擊者。如果你認為醫療儀器可能成為進階持續性威脅攻擊（APT）或熟練駭客的目標，就應選擇 第 3 級技能等級。

承第 26 題，動機等級(資料有價值或量大可轉賣獲利/新上市高貴儀器可出名)：□1 級：低度或無獎勵或無誘因，如無個資為一般性設備 □2 級：可能有獎勵與誘因，如檢查量大設備且有醫療資訊 □3 級：高度獎勵與誘因，如尖端設備可成名,具價值的醫療資訊。

說明：指潛在攻擊者想要攻擊該儀器的誘因與潛在利益：1 級：沒有攻擊價值；2 級：可存取一定數量的醫療資訊或具資料轉賣價值；3 級：攻擊者可因破解此設備獲得名聲、資料或金錢報酬高。

承第 26 題，機會與資源等級(權限管理、實體環境/系統運作介面之控管)：□1 級: 門禁管制人員管理且有特殊權限，如專屬帳密 □2 級：僅有權限管理但無人員/角色管理，如共同帳密 □3 級：實體環境/系統運作介面有加以控管，但不需任何權限或資源可達成入侵目的

說明：攻擊者是否容易取得入侵該設備的機會與資源，1 級：有門禁、個人化帳密、可稽核操作；2 級：基本權限設定，但無人員識別控管，如多人共用帳號、未記錄使用紀錄；3 級：設備放置於無管制區，USB 隨插即用、系統未鎖定或防護。

承第 26 題，發現的難易度等級(視使用作業系統，若為主流設備或作業系統廠商較能支援)：□1 級：設備市佔高或設備之作業系統為大宗，廠商能支援程式修補 □2 級:使用的作業系統非大宗或較舊作業系統 但廠商仍支援程式修補 □3 級:舊作業系統之弱點廠商已不支援程式修補。

說明: 針對設備作業系統的市佔率與供應商支援性，3 級如 Windows XP、 Windows7

承第 26 題，可用性等級(視網路可找到的工具，若為主流作業系統,網路上可搜尋到較多的入侵工具)：□1 級：非大宗、 非主流作業系統或設備市佔低，網路入侵工具較少 □2 級：使用的作業系統非大宗或較舊作業系統，但網路入侵仍有工具 □3 級：設備市佔高、設備作業系統為大宗或主流，網路入侵工具較多。

說明：潛在攻擊者是否能輕易取得網路上現成的攻擊工具來入侵該設備或作業系統。1 級：廠商自製系統、特殊用途儀器；2 級：如 Windows 7；3 級如 Windows 10、Windows11

承第 26 題，入侵偵測等級(是否有安全偵測、有入侵日誌、能自動偵測)：□1 級：原廠有檢附防護機制或人員對入侵能即時偵測 □2 級：人員對入侵後知後覺 □3 級：人員對入侵不知不覺。

說明:駭客入侵時『後知後覺』即入侵當下無察覺，事後由人員手動比對日誌或異常才發現，典型情況包括：1. 日誌事後比對發現異常。2. 系統或設備出現異常行為後才懷疑被入侵。3. 使用

者通報異常後才回溯確認。4. 被第三方通報或外部稽核揭露。第 2 級『後知後覺』是指系統或人員未能即時察覺駭客入侵行為，但在事後透過某些跡象或檢查才發現系統已被入侵。第 3 級不知不覺指: 無任何監控或防護，也未察覺已遭入侵，駭客長期潛伏，直到資料外洩才發現。

承第 26 題，中斷對病人影響程度等級：□1 級：無損害或造成病人稍微不舒服 □2 級：間接傷害，指當下未造成病人直接傷害但病人有潛在傷害的風險 □3 級：直接傷害，當下即造成病人的損傷或傷害，嚴重者可能導致病人死亡。

說明：儀器因資安事件（如入侵、當機、勒索、病毒、惡意操控）而導致功能停止、異常、延遲或無法使用的情形。1 級：如血壓計故障，需改手動測量；2 級：如輸液幫浦中斷，但護理人員可手動替代或手術期間成像設備故障，需延後或改用其他方式；3 級：緊急應變，如呼吸器停止運作。

承第 26 題，發生可能性數值等級（如插槽可能成為感染風險來源）: □1 級：設備無插槽另提供外接或設備有插槽且有使用者管控措施 □2 級:設備有插槽但無使用者管控措施。

說明：本院訂有管控措施，資訊室訂有”資訊安全管理規定”，本部亦有訂” 醫療儀器資訊安全規範書”，使用單位必須遵照管控措施。

27. 備註:_____