文件類別	適用性聲明書(三階)		文件編號	W-A4100-009	版次3.0
文件名稱	資訊安全適用性聲明書		機密等級	一般	
制定單位	資訊中心				
項次	發行/修訂日期	修訂內容摘要	修訂頁次	撰寫單位簽章	
1	102.8.15	新訂	無	承辦人	韓睿
				審核	吳彥璋
				核定	楊明正
2	104.7.15	修改成ISO 27001:2013	P1-P8	承辦人	韓睿
				審核	吳彥璋
				核定	楊明正
3	104.9.2	增加A9.3及A9.4	P2、P3	承辦人	韓睿
				審核	吳彥璋
				核定	楊明正
4	108.8.1	增加A.6.2.2、A.9.4.5、A.10.1.1、A.10.1.2、A.12.1.4、A.14.1.2、A.14.1.3、A.14.2.2、A.14.2.3、A.14.2.5、A.14.3.1、A.18.1.5等12項控制措施	全部	承辦人	韓睿
				審核	吳彥璋
				核定	楊明正
5	109.4.30	修訂 1.審核 2.18.1.5勘誤	P7	承辦人	韓睿
				審核	林紫晴
				核定	楊明正
6	113.2.29	依ISO 27001:2022版項目修正相關內容	ALL	承辦人	廖元馳
				審核	鍾維哲
				核定	林冠宏

資訊安全適用性聲明書					
文件編號	W-A4100-009	機密等級	一般	版次	3.0

目錄

資訊安全適用性聲明書					
文件編號	W-A4100-009	機密等級	一般	版次	3.0

1 目的

為明確說明馬偕醫學院資訊中心電腦機房之 ISO/IEC 27001:2013 安全控制措施適用情況，以強化本校資訊中心電腦機房之資訊安全管理，特制訂本文件。

2 範圍

馬偕醫學院(新北市三芝區中正路三段 46 號)之資訊機房，網路維運及資訊中心實體環境之安全管理。

3 定義

無。

4 權責

無。

5 內容

5.1 適用聲明

編號	控制措施	適用性	適用/不適用理由	相關參考文件
5_組織控制措施				
5.1	資訊安全政策	適用	資訊安全政策及主題特定政策應予以定義、由管理階層核 可、發布、傳達予相關人員及相關關注方，且其係知悉， 並依規劃期間及發生重大變更時審查。	資通安全政策
5.2	資訊安全之角色及責任	適用	應依組織需要，定義並配置資訊安全之角色及責任。	資通安全組織管理程序書
5.3	職務區隔	適用	衝突之職務及衝突的責任範圍應予以區隔。	資通安全組織管理程序書
5.4	管理階層責任	適用	管理階層應要求所有人員，依組織所建立資訊安全政策、主題特定政策及程序，實施資訊安全。	資通安全組織管理程序書
5.5	與權責機關之聯繫	適用	組織應建立並維持與相關權責機關之聯繫。	資通安全組織管理程序書
5.6	與特殊關注群組之聯繫	適用	組織應建立並維持與各特殊關注群組或其他各專家安全論壇及專業協會之聯繫。	資通安全組織管理程序書 委外管理程序書

				系統開發與維護程序書
5.7	威脅情資	適用	應蒐集並分析與資訊安全威脅相關之資訊，以產生威脅情資。	資通安全事件管理程序書
5.8	專案管理之資訊安全	適用	資訊安全應整合入專案管理中。	資通安全組織管理程序書 委外管理程序書
5.9	資訊及其他相關聯資產之清冊	適用	應製作並維護資訊及其他相關聯資產(包括擁有者)之清冊。	資訊資產管理程序書
5.10	可接受使用資訊及其他相關聯資產	適用	應識別、書面記錄及實作對處置資訊及其他相關聯資產之可接受使用的規則及程序。	資訊資產管理程序書
5.11	資產之歸還	適用	適切時，人員及其他關注方於其聘用、契約或協議變更或終止時，應歸還其持有之所有組織資產。	資訊資產管理程序書
5.12	資訊之分類分級	適用	資訊應依組織之資訊安全需要，依機密性、完整性、可用性及相關關注方要求事項分類分級。	資訊資產管理程序書
5.13	資訊之標示	適用	應依組織所採用之資訊分類分級方案，發展及實作一套適切的資訊標示程序。	資訊資產管理程序書
5.14	資訊傳送	適用	應備妥資訊傳送規則、程序或協議，用於組織內及組織與其他各方間之所有型式的傳送設施。	存取控制管理程序書 通訊安全管理程序書
5.15	存取控制	適用	應依營運及資訊安全要求事項，建立並實作對資訊及其他相關聯資產之實體及邏輯存取控制的規則。	存取控制管理程序書 通訊安全管理程序書
5.16	身分管理	適用	應管理身分之整個生命週期。	存取控制管理程序書
5.17	鑑別資訊	適用	鑑別資訊之配置及管理應由管理過程控制，包括告知人員關於鑑別資訊的適切處理。	存取控制管理程序書
5.18	存取權限	適用	應依組織之存取控制的主題特定政策及規則，提供、審查、修改及刪除對資訊及其他相關聯資產之存取權	存取控制管理程序書

			限。	
5.19	供應者關係中之資訊安全	適用	應定義並實作過程及程序，管理與供應者產品或服務之使用相關聯的資訊安全風險。	委外管理程序書
5.20	於供應者協議中闡明資訊安全	適用	應依供應者關係之型式，建立相關的資訊安全要求事項，並與各供應者議定。	委外管理程序書
5.21	管理 ICT 供應鏈之資訊安全	適用	應定義並實作過程及程序，管理與 ICT 產品及服務供應鏈相關聯之資訊安全風險。	委外管理程序書
5.22	供應者服務之監視、審查及變更管理	適用	組織應定期監視、審查、評估及管理供應者資訊安全實務作法及服務交付之變更。	委外管理程序書
5.23	使用雲端服務之資訊安全	適用	應依組織之資訊安全要求事項，建立獲取、使用、管理及退出雲端服務的過程。	網路管理作業說明書
5.24	資訊安全事故管理規劃及準備	適用	組織應藉由定義、建立並溝通或傳達資訊安全事故管理過程、角色及責任，規劃並準備管理資訊安全事故。	資通安全事件管理程序書 人員管理與教育訓練程序書
5.25	資訊之評鑑及決策	適用	組織應評鑑資訊安全事件，並判定是否將其歸類為資訊安全事故。	資通安全事件管理程序書
5.26	對資訊安全事故之回應	適用	應依書面記錄程序，回應資訊安全事故。	資通安全事件管理程序書
5.27	由資訊安全事故中學習	適用	應使用由資訊安全事故中所獲得之知識，強化及改善資訊安全控制措施。	資通安全事件管理程序書
5.28	證據之蒐集	適用	組織應建立並實作程序，用以識別、蒐集、獲取及保存與資訊安全事件相關之證據。	資通安全事件管理程序書
5.29	中斷期間之資訊安全	適用	組織應規劃，如何於中斷期間維持資訊安全於適切等級。	營運持續運作管理程序書

5.30	營運持續之 ICT 備妥性	適用	應依營運持續目標及 ICT 持續之要求事項，規劃、實作、維護及測試 ICT 備妥性。	營運持續運作管理程序書
5.31	法律、法令、法規及契約要求事項	適用	應識別、書面記錄及保持更新資訊安全相關法律、法令、法規及契約之要求事項，以及組織為符合此等要求事項的作法。	資通安全組織管理程序書 資通安全文件管理程序書
5.32	智慧財產權	適用	組織應實作適切程序，以保護智慧財產權。	人員管理與教育訓練程序書 作業安全管理程序書
5.33	紀錄之保護	適用	應保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。	資通安全文件管理程序書
5.34	隱私及 PII 保護	適用	組織應依適用之法律、法規及契約的要求事項，識別並符合關於隱私保護及 PII 保護之要求事項。	資通安全組織管理程序書
5.35	資訊安全之獨立審查	適用	應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全的作法及其實作(包括人員、過程及技術)。	資通安全組織管理程序書 資通安全稽核管理作業程序書
5.36	資訊安全政策、規則及標準之遵循性	適用	應定期審查組織資訊安全政策、主題特定政策、規則及標準之遵循性。	資通安全政策 資通安全稽核管理作業程序書 矯正及預防管理程序書 作業安全管理程序書
5.37	書面記錄之運作程序	適用	應書面記錄資訊處理設施之運作程序，並使所有需要的人員均可取得。	資通安全文件管理程序書
6_人員控制措施				
6.1	篩選	適用	對所有成為員工之候選者，應於其加入組織前，進行背景查證調查，且持續進行，同時將適用的法律、法規及倫理納入考量，並宜相稱於營運要求事項，其將存取之資訊的分類分級及所察覺之風險。	人員管理與教育訓練程序書

6.2	聘用條款及條件	適用	聘用契約協議應敘明人員及組織對資訊安全之責任。	人員管理與教育訓練程序書
6.3	資訊安全認知及教育訓練	適用	組織及相關關注方之人員，均應接受與其工作職能相關的組織資訊安全政策、主題特定政策及程序之適切資訊安全認知及教育訓練，並定期更新。	人員管理與教育訓練程序書
6.4	獎懲過程	適用	應明確訂定並傳達獎懲過程，以對違反資訊安全政策之人員及其他相關關注方採取行動。	人員管理與教育訓練程序書
6.5	聘用終止或變更後之責任	適用	應對相關人員及其他關注方定義、施行並傳達於聘用終止或變更後，仍保持有效之資訊安全責任及義務。	人員管理與教育訓練程序書
6.6	機密性或保密協議	適用	反映組織對資訊保護之需要的機密性或保密協議，應由人員及其他相關關注方，識別、書面記錄、定期審查及簽署。	人員管理與教育訓練程序書 委外管理程序書
6.7	遠端工作	適用	應實作安全措施，當人員於遠端工作時，保護於組織場所外存取、處理或儲存之資訊。	存取控制管理程序書 作業安全管理程序書 通訊安全管理程序書
6.8	資訊安全事件通報	適用	組織應提供機制，供人員透過適切之管道，及時通報所觀察到或可疑的資訊安全事件。	資通安全事件管理程序書 人員管理與教育訓練程序書
7_實體控制措施				
7.1	實體安全周界	適用	應定義及使用安全周界，以保護收容資訊及其他相關聯資產之區域。	實體安全管理程序書
7.2	實體進入	適用	保全區域應藉由適切之進入控制措施及進出點加以保護。	實體安全管理程序書
7.3	保全辦公室、房間及設施	適用	應設計辦公室、房間及設施之實體安全並實作之。	實體安全管理程序書
7.4	實體安全監視	適用	應持續監視場所，防止未經授權之實體進出。	實體安全管理程序書

7.5	防範實體及環境威脅	適用	應設計並實作防範實體及環境威脅(諸如天然災害及其他對基礎設施之蓄意或非蓄意的實體威脅)之措施。	實體安全管理程序書
7.6	於安全區域內工作	適用	應設計並實作於安全區域內工作之安全措施。	實體安全管理程序書
7.7	桌面淨空及螢幕淨空	適用	應定義對紙本及可移除式儲存媒體之桌面淨空規則，以及對資訊處理設施的螢幕淨空規則，並適切實施之。	存取控制管理程序書 實體安全管理程序書 作業安全管理程序書
7.8	設備安置及保護	適用	設備應安全安置並受保護。	實體安全管理程序書
7.9	場所外資產之安全	適用	應保護場域外資產。	實體安全管理程序書 作業安全管理程序書
7.10	儲存媒體	適用	儲存媒體應依組織之分類分級方案及處置要求事項，於其獲取、使用、運送及汰除的整個生命週期內進行管理。	實體安全管理程序書 作業安全管理程序書
7.11	支援之公用服務事業	適用	應保護資訊處理設施免於電源失效，以及因支援之公用服務事業失效，所導致的其他中斷。	實體安全管理程序書 營運
7.12	佈纜安全	適用	應保護傳送電源、資料或支援資訊服務之纜線，以防範竊聽、干擾或破壞。	實體安全管理程序書
7.13	設備維護	適用	應正確維護設備，以確保資訊之可用性、完整性及機密性。	實體安全管理程序書
7.14	設備汰除或重新使用之保全	適用	應查證包含儲存媒體之設備項目，以確保於汰除或重新使用前，所有敏感性資料及具使用授權的軟體已移除或安全覆寫。	資訊資產管理程序書
8_技術控制措施				
8.1	使用者端點裝置	適用	應保護儲存於使用者端點裝置、由使用者端點裝置處理或經由使用者端點裝置可存取之資訊。	作業安全管理程序書
8.2	特殊存取權限	適用	應限制並管理特殊存取權限之配置及使用。	作業安全管理程序書 存取控制管理程序書

8.3	資訊存取限制	適用	應依已建立之關於存取控制的主題特定政策，限制對資訊及其他相關聯資產之存取。	存取控制管理程序書 作業安全管理程序書
8.4	對原始碼之存取	適用	應適切管理對原始碼、開發工具及軟體函式庫之讀寫存取。	存取控制管理程序書 作業安全管理程序書 系統開發與維護程序書
8.5	安全鑑別	適用	安全鑑別技術及程序應依資訊存取限制及關於存取控制之主題特定政策實作。	存取控制管理程序書 作業安全管理程序書
8.6	容量管理	適用	資源之使用應受監視及調整，以符合目前容量要求及預期容量要求。	作業安全管理程序書 系統開發與維護程序書
8.7	防範惡意軟體	適用	應實作防範惡意軟體之措施，並由適切的使用者認知支援之。	作業安全管理程序書 系統開發與維護程序書
8.8	技術脆弱性管理	適用	應取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適切措施。	作業安全管理程序書 系統開發與維護程序書
8.9	組態管理	適用	應建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全組態)。	資訊資產管理程序書
8.10	資訊刪除	適用	當於資訊系統、裝置或所有其他儲存媒體中之資訊不再屬必要時，應刪除之。	資通安全文件管裡程序書
8.11	資料遮蔽	適用	應使用資料遮蔽，依組織關於存取控制之主題特定政策及其他相關的主題特定政策，以及營運要求事項，並將適用法令納入考量。	系統開發與維護程序書
8.12	資料洩漏預防	適用	應將資料洩露預防措施，套用至處理、儲存或傳輸敏感性資訊之系統、網路及所有其他裝置。	作業安全管理程序書
8.13	資訊備份	適用	應依議定之關於備份的主題特定政策，維護資訊、軟體及系統之備份複	作業安全管理程序書

			本，並定期測試之。	
8.14	資訊處理設施之多備	適用	資訊處理設施之實作應具充分多備(redundancy)，以符合可用性之要求事項。	營運持續運作管理程序書
8.15	存錄	適用	記錄活動、異常、錯誤及其他相關事件之日誌，應產生、儲存、保護及分析之。	資通安全稽核管理作業程序書 作業安全管理程序書 系統開發與維護程序書
8.16	監視活動	適用	應監視網路、系統及應用之異常行為，並採取適切措施，以評估潛在資訊安全事故。	作業安全管理程序書
8.17	鐘訊同步	適用	組織所使用資訊處理系統之鐘訊，應與經認可的時間源同步。	作業安全管理程序書
8.18	具特殊權限公用程式之使用	適用	應限制並嚴密控制可能篡越系統及應用程式之控制措施的公用程式之使用。	存取控制管理程序書 作業安全管理程序書
8.19	運作中系統之軟體安裝	適用	應實作各項程序及措施，以安全管理對運作中系統安裝軟體。	作業安全管理程序書 系統開發與維護程序書
8.20	網路安全	適用	應受保全、管理及控制網路與網路裝置，以保護系統及應用程式中之資訊。	存取控制管理程序書 通訊安全管理程序書
8.21	網路服務之安全	適用	應識別、實作及監視網路服務之安全機制、服務等級及服務要求事項。	存取控制管理程序書 通訊安全管理程序書
8.22	網路區隔	適用	應區隔組織網路中各群組之資訊服務、使用者及資訊系統。	存取控制管理程序書 通訊安全管理程序書
8.23	網頁過濾	適用	應管理對外部網站之存取，以降低暴露於惡意內容。	通訊安全管理程序書
8.24	密碼技術之使用	適用	應定義並實作有效使用密碼技術之規則(包括密碼金鑰管理)。	存取控制管理程序書 系統開發與維護程序書
8.25	安全開發生命週	適用	應建立並施行安全開發軟體及系統	系統開發與維護程序

	期		之規則。	書
8.26	應用系統安全要求事項	適用	開發或獲取應用系統時，應識別、規定並核可資訊安全要求事項。	系統開發與維護程序書
8.27	安全系統架構及工程原則	適用	應建立、書面記錄及維護工程化安全系統之原則，並套用於所有資訊系統開發活動。	系統開發與維護程序書
8.28	安全程式設計	適用	軟體開發應施行安全程式設計原則。	系統開發與維護程序書
8.29	開發及驗收中之安全測試	適用	應於開發生命週期中定義並實作安全測試過程。	系統開發與維護程序書
8.30	委外開發	適用	組織應指引、監視及審查與委外系統開發相關之活動。	系統開發與維護程序書
8.31	開發、測試與運作環境之區隔	適用	應區隔開發環境、測試環境與生產環境，並保全之。	系統開發與維護程序書
8.32	變更管理	適用	資訊處理設施及資訊系統之變更，應遵循變更管理程序。	系統開發與維護程序書 作業安全管理程序書
8.33	測試資訊	適用	應適切選擇、保護及管理測試資訊。	系統開發與維護程序書
8.34	稽核測試期間資訊系統之保護	適用	涉及運作中系統之評鑑的稽核測試及其他保證活動，應於測試者與適切管理階層間規劃並議定。	資通安全稽核管理作業程序書 作業安全管理程序書 系統開發與維護程序書

6 相關文件

6.1 資訊安全政策。

6.2 資訊安全組織暨管理審查程序書。

6.3 文件管理程序書。

6.4 資訊資產暨風險評鑑管理程序書。

6.5 人員安全與教育訓練程序書。

6.6 實體安全管理程序書。

6.7 通信與作業管理程序書。

6.8 存取控制管理程序書。

6.9 系統開發與維護程序書。

6.10 委外管理程序書。

6.11 安全事件管理程序書。

6.12 業務永續運作管理程序書。

6.13 資訊安全稽核作業程序書。

6.14 矯正管理程序書。

7 相關表單

略。