<table>
<tr><td>文件類別</td><td colspan="2">適用性聲明書(三階)</td><td>文件編號</td><td colspan="2">W-A4100-009</td><td>版次2.3</td></tr>
<tr><td>文件名稱</td><td colspan="2">資訊安全適用性聲明書</td><td>機密等級</td><td colspan="3">一般</td></tr>
<tr><td>制定單位</td><td colspan="6">資訊中心</td></tr>
<tr><td>項次</td><td>發行/修訂日期</td><td>修訂內容摘要</td><td>修訂頁次</td><td colspan="3">撰寫單位簽章</td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">102.8.15</td><td rowspan="3">新訂</td><td rowspan="3">無</td><td>承辦人</td><td colspan="2">韓睿</td></tr>
<tr><td>審核</td><td colspan="2">吳彥璋</td></tr>
<tr><td>核定</td><td colspan="2">楊明正</td></tr>
<tr><td rowspan="3">2</td><td rowspan="3">104.7.15</td><td rowspan="3">修改成ISO 27001:2013</td><td rowspan="3">P1-P8</td><td>承辦人</td><td colspan="2">韓睿</td></tr>
<tr><td>審核</td><td colspan="2">吳彥璋</td></tr>
<tr><td>核定</td><td colspan="2">楊明正</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">104.9.2</td><td rowspan="3">增加A9.3及A9.4</td><td rowspan="3">P2、P3</td><td>承辦人</td><td colspan="2">韓睿</td></tr>
<tr><td>審核</td><td colspan="2">吳彥璋</td></tr>
<tr><td>核定</td><td colspan="2">楊明正</td></tr>
<tr><td rowspan="3">4</td><td rowspan="3">108.8.1</td><td rowspan="3">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</td><td rowspan="3">全部</td><td>承辦人</td><td colspan="2">韓睿</td></tr>
<tr><td>審核</td><td colspan="2">吳彥璋</td></tr>
<tr><td>核定</td><td colspan="2">楊明正</td></tr>
</table>

		措施			
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				承辦人	
				審核	
				核定	

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	2.3

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	2.3

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)之資訊中心電腦機房實體環境及預算會計系統開發與維護流程之安全管理。

3 定義

無。

4 權責

無。

5 內容

5.1 適用聲明

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.5		安全政策(2)				
A.5.1		資訊安全政策				
A.5.1.1		資訊安全之管理指導方針	資訊安全政策	V		1
A.5.1.2		資訊安全政策之審查	資訊安全政策 資訊安全組織暨管理審查程序書	V		1

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.6		資訊安全組織(7)				
A.6.1		內部組織				
A.6.1.1		資訊安全之角色及責任	資訊安全政策 資訊安全組織暨管理審查程序書 業務永續運作管理程序書 人員安全與教育訓練程序書	V		1
A.6.1.2		職務區隔	實體安全管理程序書書	V		1
A.6.1.3		與權責機關之連繫	業務永續運作管理程序書 資訊安全組織暨管理審查程序書	V		1
A.6.1.4		與特殊關注方之連繫	接收資安組織如中華電信 教育部之資安訊息並保持合作	V		1
A.6.1.5		專案管理之資訊安全	實體安全管理程序書 系統開發與維護程序書	V		1
A.6.2		行動裝置及遠距工作				
A.6.2.1		行動裝置政策	通信與作業管理程序書 實體安全管理程序書	V		1

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.6.2.2		遠距工作	通信與作業管理程序書	V		1
A.7		人力資源安全(5)				
A.7.1		聘用前				
A.7.1.1		篩選	人員安全與教育訓練程序書	V		1
A.7.1.2		聘用條款及條件	人員安全與教育訓練程序書	V		1
A.7.2		聘用期間				
A.7.2.1		管理階層責任	資訊安全政策 資訊安全組織暨管理審查程序書	V		1
A.7.2.2		資訊安全認知、教育及訓練	人員安全與教育訓練程序書	V		1
A.7.2.3		懲處過程	人員安全與教育訓練程序書	V		1
A.8		資產管理(10)				
A.8.1		資產責任				
A.8.1.1		資產清冊	資訊資產暨風險評鑑管理程序書	V		1
A.8.1.2		資產擁有權	資訊資產暨風險評鑑管理程序書	V		1
A.8.1.3		資產之可被接受使用	資訊資產暨風險評鑑管理程序書 實體安全管理程序書	V		1

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
			人員安全與教育訓練程序書 通信與作業管理程序書			
A.8.1.4		資產之歸還	通信與作業管理程序書 人員安全與教育訓練程序書 資訊資產暨風險評鑑管理程序書	V		1,2
A.8.2		資訊分級				
A.8.2.1		資訊之分級	資訊資產暨風險評鑑管理程序書	V		1
A.8.2.2		資訊之標示	資訊資產暨風險評鑑管理程序書	V		1
A.8.2.3		資產之處置	資訊資產暨風險評鑑管理程序書	V		1
A.8.3		媒體處置				
A.8.3.1		可移除式媒體之管理	資訊資產暨風險評鑑管理程序書 通信與作業管理程序書	V		1
A.8.3.2		媒體之汰除	資訊資產暨風險評鑑管理程序書 實體安全管理程序書	V		1
A.8.3.3		實體媒體傳送	資訊資產暨風險評鑑管理程序書	V		1
A.9		存取控制(14)				

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.9.1		存取控制之營運要求事項				
A.9.1.1		存取控制政策	資訊安全政策 存取控制管理程序書	V		1
A.9.1.2		對網路及網路服務之存取	資訊安全政策	V		1
A.9.2		使用者存取管理				
A.9.2.1		使用者註冊及註銷	存取控制管理程序書	V		1,2
A.9.2.2		使用者存取權限之配置	存取控制管理程序書	V		1,2
A.9.2.3		具特殊存取權限之管理	實體安全管理程序書 存取控制管理程序書	V		1
A.9.2.4		使用者之秘密鑑別資訊的管理	存取控制管理程序書	V		1,2
A.9.2.5		使用者存取權限之審查	存取控制管理程序書 實體安全管理程序書	V		1
A.9.2.6		存取權限之移除或調整	人員安全與教育訓練程序書 通信與作業管理程序書	V		1,2
A.9.3		使用者責任				

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.9.3.1		秘密鑑別資訊之使用	存取控制管理程序書	V		1,2
A.9.4		系統及應用存取控制				
A.9.4.1		資訊存取限制	存取控制管理程序書	V		1
A.9.4.2		保全登入程序	存取控制管理程序書	V		1
A.9.4.3		通行碼管理系統	存取控制管理程序書	V		1
A.9.4.4		具特殊權限公用程式之使用	存取控制管理程序書	V		1
A.9.4.5		對程式源碼之存取控制	系統開發與維護程序書	V		1
A.10		密碼學(2)				
A.10.1		密碼式控制措施				
A.10.1.1		使用密碼式控制措施之政策	通信與作業管理程序書	V		1
A.10.1.2		金鑰管理	通信與作業管理程序書	V		1
A.11		實體及環境安全(15)				
A.11.1		保全區域				
A.11.1.1		實體安全周界	實體安全管理程序書	V		1,2
A.11.1.2		實體進入控制措施	實體安全管理程序書	V		1,2
A.11.1.3		保全之辦公室、房間及設施	實體安全管理程序書	V		1,2

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.11.1.4		防範外部及環境威脅	實體安全管理程序書	V		1,2
A.11.1.5		於保全區域內工作	實體安全管理程序書	V		1
A.11.1.6		交付及裝卸區	實體安全管理程序書	V		1,2
A.11.2		設備				
A.11.2.1		設備安置及保護	實體安全管理程序書	V		1,2
A.11.2.2		支援之公用服務事業	實體安全管理程序書	V		1,2
A.11.2.3		佈纜安全	實體安全管理程序書	V		1
A.11.2.4		設備維護	實體安全管理程序書	V		1
A.11.2.5		資產之攜出	實體安全管理程序書 通信與作業管理程序書	V		1,2
A.11.2.6		場所外設備及資產之安全	實體安全管理程序書	V		1,2
A.11.2.7		設備汰除或再使用之保全	實體安全管理程序書 資訊資產暨風險評鑑管理程序書 通信與作業管理程序書	V		1
A.11.2.8		無人看管之使用者設備	存取控制管理程序書 實體安全管理程序書	V		1

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.11.2.9		桌面淨空及螢幕淨空政策	存取控制管理程序書	V		1
A.12		運作安全(14)				
A.12.1		運作程序及責任				
A.12.1.1		文件化運作程序	隨機或隨設備附的操作手冊	V		1
A.12.1.2		變更管理	通信與作業管理程序書	V		1
A.12.1.3		容量管理	實體安全管理程序書	V		1
A.12.1.4		開發、測試及運作環境之區隔	系統開發與維護程序書	V		1
A.12.2		防範惡意軟體				
A.12.2.1		防範惡意軟體之控制措施	通信與作業管理程序書	V		1,2
A.12.3		備份				
A.12.3.1		資訊備份	通信與作業管理程序書	V		1
A.12.4		存錄及監視				
A.12.4.1		事件存錄	實體安全管理程序書	V		1,2
A.12.4.2		日誌資訊之保護	實體安全管理程序書	V		1
A.12.4.3		管理者及操作者日誌	實體安全管理程序書	V		1

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.12.4.4		鐘訊同步	實體安全管理程序書	V		1
A.12.5		運作中軟體之控制				
A.12.5.1		對運作中系統之軟體安裝	系統開發與維護程序書 通信與作業管理程序書	V		1
A.12.6		技術脆弱性管理				
A.12.6.1		技術脆弱性管理	通信與作業管理程序書 系統開發與維護程序書	V		1
A.12.6.2		對軟體安裝之限制	系統開發與維護程序書 通信與作業管理程序書	V		1
A.12.7		資訊系統稽核考量				
A.12.7.1		資訊系統稽核控制措施	資訊安全作業稽核程序書	V		1
A.13		通訊安全(7)				
A.13.1		網路安全管理				
A.13.1.1		網路控制措施	通信與作業管理程序書	V		1
A.13.1.2		網路服務之安全	通信與作業管理程序書	V		1
A.13.1.3		網路之區隔	通信與作業管理程序書	V		1

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.13.2		資訊傳送				
A.13.2.1		資訊傳送政策及程序	通信與作業管理程序書	V		1
A.13.2.2		資訊傳送協議	通信與作業管理程序書	V		1
A.13.2.3		電子傳訊	通信與作業管理程序書	V		1
A.13.2.4		機密性或保密協議	人員安全與教育訓練程序書 通信與作業管理程序書	V		1
A.14		系統獲取、開發及維護(13)				
A.14.1		資訊系統之安全要求事項				
A.14.1.1		資訊安全要求事項分析及規格	系統開發與維護程序書	V		1
A.14.1.2		保全公共網路之應用服務	系統開發與維護程序書	V		1
A.14.1.3		保護應用服務交易	系統開發與維護程序書	V		1
A.14.2		資訊系統之安全要求事項				
A.14.2.1		保全開發政策	系統開發與維護程序書	V		1
A.14.2.2		系統變更控制程序	系統開發與維護程序書	V		1

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.14.2.3		作業系統變更後應用系統的技術審查	系統開發與維護程序書	V		1
A.14.2.4		套裝軟體變更之限制	系統開發與維護程序書	V		1
A.14.2.5		保全系統工程原則	系統開發與維護程序書	V		1
A.14.2.6		保全開發環境	系統開發與維護程序書	V		1
A.14.2.7		委外開發	系統開發與維護程序書 委外管理程序書	V		1
A.14.2.8		系統安全測試	系統開發與維護程序書	V		1
A.14.2.9		系統驗收測試	系統開發與維護程序書	V		1
A.14.3		測試資料				
A.14.3.1		測試資料之保護	系統開發與維護程序書	V		1
A.15		供應者關係(5)				
A.15.1		供應者關係中之資訊安全				
A.15.1.1		供應者關係之資訊安全政策	資訊安全政策 委外管理程序書	V		1
A.15.1.2		於供應者協議中闡明安全性	資訊安全政策	V		1

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
			委外管理程序書			
A.15.1.3		資訊及通訊技術供應鏈	委外管理程序書	V		1,2
A.15.2		供應者服務交付管理				
A.15.2.1		供應者服務之監視及審查	實體安全管理程序書 委外管理程序書	V		1
A.15.2.2		管理供應者服務之變更	實體安全管理程序書 委外管理程序書	V		1
A.16		資訊安全事故管理(7)				
A.16.1		資訊安全事故及改善之管理				
A.16.1.1		責任及程序	安全事件管理程序書 矯正管理程序書 業務永續運作管理程序書	V		1,2
A.16.1.2		通報資訊安全事件	安全事件管理程序書	V		1,2
A.16.1.3		通報資訊安全弱點	安全事件管理程序書	V		1,2
A.16.1.4		對資訊安全事件之評鑑及決策	安全事件管理程序書	V		1

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
A.16.1.5		對資訊安全事故之回應	安全事件管理程序書	V		1
A.16.1.6		由資訊安全事故中學習	安全事件管理程序書 矯正管理程序書 業務永續運作管理程序書	V		1
A.16.1.7		證據之收集	安全事件管理程序書 矯正管理程序書 業務永續運作管理程序書	V		1,2
A.17		營運持續管理之資訊安全層面(4)				
A.17.1		資訊安全持續				
A.17.1.1		規劃資訊安全持續	業務永續運作管理程序書	V		1
A.17.1.2		實作資訊安全持續	業務永續運作管理程序書	V		1,2
A.17.1.3		查證、審查並評估資訊安全持續	業務永續運作管理程序書	V		1
A.17.2		多重備援				
A.17.2.1		資訊處理設施之可用性	實體安全管理程序書	V		1

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	2.3

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
			業務永續運作管理程序書			
A.18		遵循性(8)				
A.18.1		對法律及契約要求事項之遵循				
A.18.1.1		適用之法規及契約的要求事項之識別	資安相關法令規章	V		1
A.18.1.2		智慧財產權	人員安全與教育訓練程序書 通信與作業管理程序書	V		1
A.18.1.3		紀錄之保護	文件管理程序書 資訊資產暨風險評鑑管理程序書	V		1
A.18.1.4		個人可識別資訊之隱私及保護	資安相關法令規章 資訊資產暨風險評鑑管理程序書	V		1
A.18.1.5		密碼式控制措施之監管		V		1
A.18.2		資訊安全審查				
A.18.2.1		資訊安全之獨立審查	資訊安全組織暨管理審查程序書	V		1
A.18.2.2		安全政策及標準之遵循性	資訊安全作業稽核程序書	V		1

ISO/IEC 27001 要求			對應文件	適用性		理由
				適用	不適用	(註)
			資訊安全組織暨管理審查程序書			
A.18.2.3		技術遵循性審查	資訊安全作業稽核程序書 資訊安全組織暨管理審查程序書	V		1

適用理由	理由說明
1	標準要求
2	管理階層要求
3	風險評鑑結果
不適用理由	
1	驗證範圍內不提供此服務，不使用此資源、方法、作法
2	國內法令法規並無相關使用限制, 驗證範圍內亦無與使用者或合約相關之使用協議
3	風險評鑑結果

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。