中山醫學大學

委外管理程序書

機密等級：一般

文件編號：IS-B-010

版　　次：4.5

發行日期：115.05.06

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	97.11.04		梁憶芳	初版
1.1	102.07.02	1-2,6-7	梁憶芳	1.重新界定權責單位與資訊委外服務合約規範內容 2.修訂個資法法規異動名稱 3.增訂:要求委外廠商遵循並配合簽署遵循個人「保密切結書」
2.0	104.08.21	1-6	張巧蓉	修訂單位名稱及簡稱
2.1	105.07.07	7	趙慧婷	增訂異動採購或維護合約上述服務內容時，委外廠商需提出相關配套措施 機密等級修訂為「一般」
3.0	107.06.21		趙慧婷	新增 3.2
3.1	108.01.28	3	趙慧婷	新增 5.1.10
3.2	108.12.09		趙慧婷	為符合全校使用故修改如下: 新增 5.12、圖資處修改為本校或業務單位
3.3	109.08.18	封面	趙慧婷	校徽更換
3.4	110.11.09	8	趙慧婷	配合個資轉版 增訂 5.12.9　修訂 5.12.3
3.5	111.10.25	4	趙慧婷	因矯正單 111-005 增訂 5.1.11 之敘述
3.6	112.01.04	3,4,5,8	趙慧婷	配合個資 修訂 5.12.3、5.1.10 新增 IS-D-044 表單 刪除 5.1.5 合併至 5.1.4 新增 5.1.11
4.0	112.06.20	1 至 8	林翊樺	1.配合資通安全導入全校,進行改版。 2.修訂 3.1、5.2.1、5.2.2、5.2.2.2、5.2.2.3。 3.增訂 5.1.10、5.6.1。 4.5.2.2.1 增列 IS-D-036。 5.新訂文件： IS-C-010、IS-D-036
4.1	112.12.05	1、2、4、8	林翊樺	1.修訂適用範圍，納入個資。 2.定義資通訊委外系統、套裝軟

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
				體。 3.權責增加各單位權責之合約附件注意事項(資通訊系統注意事項與其他注意事項)、增加委外廠商應於合約終止後返還或刪除持有資料、委外廠商須配合本校其他相關安全規定。 4.新增委外作業評估,如為資通訊設備須填寫 IS-D-035 資通訊設備評估表 5.新增表單,資通訊設備自評表(IS-D-300)。
4.2	113.04.29	1、2、4、5、8、9、10	林翊樺	1.因應 ISO 27001:2022 版本更新修訂。 2.修訂 3.1.2、3.1.3.2、5.2.2 新訂文件「資通訊採購指引」(IS-C-011)。 3.修訂 3.1.5，單位應要求廠商須遵循本校資通安全管理政策、委外管理程序書、資安宣導單。 4.修訂4.2 套裝軟體依是否於本校架設伺服器予以分類定義。 5.新訂 5.4.2、5.4.3 選擇或新增安全需求之「資通訊系統等級異動申請表」、「資通訊系統清冊」作業說明。 6.新訂 5.13 雲端服務使用之管理。
4.3	113.11.05	1、2、8、10	林翊樺	1.修訂 3.16 新增表單「合約商資通安全管理作業查核表」 2.修訂 5.13.2 公有雲端服務供應商資安能力評估，刪除舉例的贅字。 3.修訂 6.17 IS-D-036 表單名稱

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
				從「資通訊系統委外評估表」變更為「資通訊系統、軟體、服務委外評估表」,以供系統以外之項目進行採購前評估。
4.4	114.02.27	1-6、9、11	林翊樺	1.修訂 3.1.3 原 3.1.4.2 資通訊系統、軟體、服務委外評估表項目調整次序納為委外共通事項。修訂 5.2.1、5.13.2 委外作業評估應記錄於「資通訊系統、軟體、服務委外評估表」。 2.修訂 3.1.4 委外【得檢附】改為【應檢附】「合約商個人資料保護自評表」、「個人資料委外監督合約補充條約」。新訂 3.2.6 委外廠商應配合填寫上述表單。 3.修訂 3..15、3.2.7 明定委外之產品類別，並將相關應備文件載明。 4.修訂 5.1.7 增列不得使用危害國家資安之服務，以及團隊成員不得為陸籍人士。 5.修訂 5.4.2、5.4.3、5.6.5、6.24 資通系統防護基準控制措施檢核表納入 ISMS 文件，文件編號 IS-D-448。 6.修訂 5.6.4 弱點掃描後應修正「嚴重」等級之風險。
4.5	115.05.06	1-7、 10、11	林翊樺	1.增列 2.2 適用範圍之例外，配合校內各項計畫之管理，得使用本程序書之相關文件，惟各計畫仍應依主管機關要求辦理。 2.修訂 3.1.3 表格名稱變更為「資通訊系統委外自評表」。

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
				3.修訂 3.1.5、3.2.7 應參照資通訊採購指引；委外雲端服務之要求列於 5.13.2。 4.修訂 3.1.8、3.2.5，要求委外廠商【應】返還資料。 5.新訂 4.5，依資通安全法(114/9/24)第三條之危害國家資通安全產品定義。 6.修訂 5.2.1，IS-D-036「資通訊系統、軟體、服務委外評估表」變更為「資通訊系統委外自評表」。僅第二類、第三類新申購時須填寫。 7.修訂 5.2.2，委外採購「應」參閱資通訊採購指引。 8.修訂 5.4.3 配合附表十修訂，已修訂本校資通系統防護基準控制措施檢核表(2.0)，故配合變更題項。 9.修訂 5.6.4 為 5.6.4.1、5.6.4.2 10.修訂 5.6.4.1 文字酌做修正，修訂為單位可定期申請弱點掃描，並於 5.6.4.2 詳述弱點掃描工具與參考之程序書。 11.修訂 5.13.2 考量各項服務已趨訂閱制度，無法要求廠商填寫評估表(例如 google、微軟等)，故予以刪除。增列 ISO 27017、27018 資安標準。

委外管理程序書					
文件編號	IS-B-010	機密等級	一般	版本	4.5

目錄

委外管理程序書					
文件編號	IS-B-010	機密等級	一般	版本	4.5

1 目的

本程序書制訂之目的在於確保中山醫學大學(以下簡稱本校)委外作業安全。

2 適用範圍

2.1 本校資訊軟硬體服務、業務資訊與個人資料蒐集處理利用及專業服務等委外作業均適用之。

2.2 適用範圍之例外

2.2.1 本校接受本校以外單位之委託案(如政府機關之委託案、專案計畫等)，應依據委託單位之規定落實相關資通安全管理作業。

2.2.2 委託案涉及資通系統建置、維護者，且具有複委託的作業時

2.2.2.1 如系統建置於校內，宜參考本程序書的相關規範，執行資通安全管理作業，本校得視狀況執行查核作業。

2.2.2.2 如系統建置於校外，且不使用本校 IP 位置與網域名稱者，宜參考本程序書的相關規範，執行資通安全管理作業。

3 權責

3.1 各單位權責

3.1.1 委外廠商之遴選暨監督委外廠商合約之履行。

3.1.2 依循「資通訊採購指引」執行採購事項。

3.1.3 應檢視並評估相關產品供應程序有無潛在風險，進而採取必要之防護機制，以降低潛在的資安威脅及弱點，如為新申購之第二類、第三類產品須將評估結果記錄於「資通訊系統委外自評表」。

3.1.4 如涉個人資料業務應檢附「合約商個人資料保護自評表」及「個人資料委外監督合約補充條約」。

3.1.5 擬定委外廠商服務相關合約內容，應依照「資通訊採購指引」各類別檢附「資通訊委外合約書附則」或相關文件。資通訊委外合約書附則中規範「應遵循本校資通安全管理政策與委外管理程序書」。

3.1.6 要求委外廠商遵循「資通安全管理政策」、「委外管理程序書」、「資安宣導單」並配合簽署「個人保密切結書」與「合約商保密切結書」。

3.1.7 必要時得稽核委外廠商安全管制措施，配合「合約商資通安全管理作業查檢表」查核作業。

3.1.8 委外關係終止或解除時，要求委外廠商應返還、移交、刪除或銷毀持有資料。

3.2 委外廠商

3.2.1 提供完整工作說明書或專案管理計畫書。

3.2.2 委外廠商應履行合約附件要求事項並配合填寫、簽訂合約附件相關表單，亦須提交工作報告或維護紀錄。

3.2.3 遵守資通安全管理法、資通安全管理法施行細則、個人資料保護相關法令及本校資通安全政策與規定，善盡保管、保密之責。

3.2.4 須遵守本校其他相關安全規定，並配合本校資通安全或個人資料管理稽核。

3.2.5 委外關係終止或解除時，委外廠商應返還、移交、刪除或銷毀持有資料。

3.2.6 如涉個人資料業務應配合填寫「合約商個人資料保護自評表」、簽署「個人資料委外監督合約補充條約」。

3.2.7 委外廠商應依本校委外管理程序及「資通訊採購指引」簽署或交付各產品類別資安文件，單位委外承辦人員應妥善保管。

4 名詞定義

4.1 資通訊系統：

4.1.1 指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

4.1.2 系統安裝於伺服器上，含虛擬主機及實體主機，伺服器裝有伺服器作業系統，如 Windows Server、Linux、Ubuntu Server、Debian Server、Fedora、OpenSUSE Leap、SUSE Linux Enterprise Server、Arch Linux 等。

4.2 套裝軟體：

4.2.1 安裝於個人電腦無須裝設於本校伺服器之套裝軟體：

軟體無使用者帳號建立及管理功能，且不具備網路資料傳輸及分享功能，如：Office 辦公室軟體、PDF、壓縮、防毒、繪圖等軟體。

4.2.2 安裝於本校伺服器之套裝軟體：

軟體具使用者帳號建立、管理、網路資料傳輸或分享等功能。

4.3 隱密通道：由惡意程式所建立，會將系統資訊暴露給未授權使用者之管道。

4.4 特洛伊木馬程式：藉由偽裝成其它種類應用程式來獲取未授權資訊之惡意程式。

4.5 危害國家資通安全產品：指經主管機關認定，對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統、服務或產品。

5 作業說明

5.1 一般條款

5.1.1 委外廠商應負責硬體設備(含虛擬主機)之作業系統及所有軟體之安裝、更新及維護，並提供聯絡窗口、電話詢答服務及解決軟硬體設備相關問題，配合本校「安全事件管理程序書」處理異常事件排除及通報事宜。

5.1.2 委外廠商處理個人資料應遵守「個人資料保護法」及本校之相關規定，並簽訂「個人保密切結書」與「合約商保密切結書」。

5.1.3 委外廠商安裝使用之軟體，須為合法授權軟體，不得違反智慧財產權之規定，如有違反事情發生，委外廠商須承擔所有法律責任。

5.1.4 委外廠商應留存使用之工具軟體、處理作業之執行紀錄及異常處理紀錄，本校有權進行稽核，廠商不得異議。

5.1.5 委外廠商所交付之標的物如侵害第三人合法權益時，應承擔一切法律責任。

5.1.6 委外廠商如因其員工執行業務之過失，造成本校損失或傷害，需負損害賠償責任。

5.1.7 廠商所提供的資訊與通訊技術之服務與產品，應符合合約書之規格需求，且保證無隱密通道、後門程式或其他非預期或不需要的功能。並依行政院政策要求，公務用之資通訊產品（含軟體、硬體及服務）不得使用危害國家資安之產品、服務（如大陸廠牌軟體、硬體及服務且團隊成員不得為陸籍人士）。

5.1.8 委外廠商發現或發生資安事件時應主動向委外單位窗口及本校緊急應變暨技術支援組進行通報及配合處理。

5.1.9 本校得對委外廠商其作業流程及安全控制措施進行書面或實地稽核。

5.1.10委外廠商對其產品供應鏈負有安全監督責任，並應評估其資安風險，不得造成資訊安全事件之發生。

5.2 委外作業之評估

5.2.1 各單位因業務需要若有新申購委外系統需求時，應評估委外廠商之公司規模、履約能力、售後服務、價格合理性、後續維護能力、維護合約費用上限及是否能持續編列維護費用等因素。將評估結果記錄於「資通訊系統委外自評表」。

5.2.2 各單位欲辦理委外採購時，應參閱「資通訊採購指引」辦理。

5.3 資產辨識與風險評鑑作業

5.3.1 各單位可參考本校「資訊資產管理程序書」及「風險評鑑與管理程序書」,依照委外標的之資訊資產價值、機密性、完整性及可用性，適當評估其可能之威脅及弱點。

5.4 選擇或新增安全需求

5.4.1 各單位可依據上述風險評鑑結果，進行風險管理作業，選擇適用之安全需求項目，明訂於合約之中。

5.4.2 資通系統應依據「資通安全責任等級分級辦法」附表九資通系統防護需求分級原則評定系統防護需求等級，並至少應符合附表十資通系統防護基準之各構面控制措施記錄於「資通系統防護基準控制措施檢核表」。新購、異動等級、停用、刪除皆須由單位窗口填寫「資通訊系統等級異動申請表」經資訊資產擁有單位主管同意，送交本校策略規劃組審核，經執行長、資通安全長核定後，資安專責人員協助將異動之系統列入本校「資通訊系統清冊」。

5.4.3 需安裝於伺服器之套裝軟體應落實本校「資通系統防護基準控制措施檢核表」第 1、2、4、6-10、17、18、20-23、43、44 項及其他合約要求之控制項規劃、設計及落實執行相關控制措施。

5.5 硬體採購與維護

5.5.1 廠商應提供與設備伺服器之架構、操作、管理、維護等相關之操作手冊、文件與技術支援，如必要亦應提供教育訓練課程。

5.6 系統開發及維護

5.6.1 系統若委由外部廠商開發，廠商應將系統安全需求列入考量，提供完整之系統架構說明、系統分析設計、資料庫欄位設計等相關文件。

5.6.2 委外廠商應確實控管程式與文件版本之一致性。

5.6.3 委外廠商進行系統開發與維護時，不得任意複製或攜出限閱(含)等

級以上之業務資料。

5.6.4 弱點掃描

5.6.4.1 上線前掃描

委外廠商需針對交付之系統，應保證系統內不含後門程式、隱密通道及特洛伊木馬程式。且系統通過使用者測試後，上線前須向圖書資訊處軟體系統組申請(EVS)網站弱點掃描，並至少須完成嚴重等級風險議題修正，始得上線，若經評估風險屬誤判或可接受之範圍風險則除外。各單位得依實際需求，定期申請 EVS 網站弱點掃描，以強化整體資通安全防護。

5.6.4.2 弱點掃描工具

校方弱點掃描工具為教育單位弱點檢測平台(EVS, Educational Institutions Vulnerability Scan Service)，若該平台失效或不再提供服務，由校方另尋其他公正第三方弱掃工具代替，各單位欲辦理弱點掃描時，應參閱「資通訊作業管理程序書」辦理。

5.6.5 若系統、軟體由委外廠商開發者，應由各單位測試及驗收上線之程式，確定符合相關需求後記錄於「資通系統防護基準控制措施檢核表」，可參照本校「系統開發與維護程序書」之程序進行上線作業。

5.6.6 程式修改與開發可參考本校「系統開發與維護程序書」之規定，若有例外，須經各單位主管同意以後，方可實施。

5.7 系統帳號管理

5.7.1 委外系統資料、軟體或作業系統最高權限帳號、資料庫最高權限帳號，應由系統負責人保管，不得直接授與委外廠商使用。

5.7.2 委外廠商之人員如因作業需求，需對業務單位系統進行存取，可參考本校「存取控制管理程序書」之相關管理規範，填寫「資通系統權限申請表」提出申請。

5.7.3 「資通系統權限申請表」中應載明作業需求內容、所需權限、帳號有效時間，經由各單位主管核准後，由系統管理者依照所需權限及帳號有效時間，建立獨立之帳號供委外廠商使用。

5.7.4 委外廠商對於系統帳號應善盡保管之責，系統帳號不得任意交由非作業相關人員使用。

5.7.5 委外廠商對於系統之操作，系統負責人應盡監督之責，委外廠商不得從事非工作範圍內之操作。系統負責人者並應於委外廠商人員完成工作後檢視系統紀錄。

5.8 緊急應變計畫

5.8.1 資訊作業委外時，得要求委外廠商配合定期進行業務永續經營計畫，針對委外標的建立緊急應變計畫，並定期進行測試；若該委外案件屬於整體委外者，應以委外系統及資料兩者中最高資訊資產價值衡量演練週期。

5.8.2 備援需求：依據不同資訊資產價值及可用性等級，考量其備援需求，必要時，得建立異地備援機制。

5.9 可攜式電腦及儲存媒體管理

5.9.1 委外廠商如需攜帶可攜式電腦或儲存媒體如磁片、光碟、隨身碟、外接式硬碟等進入本校安全區域使用，需經資訊資產權責單位或保管單位指派人員隨行並註記於「人員進出管制紀錄表」。

5.9.2 廠商維修人員，當進入安全區域並使用可攜式電腦或儲存媒體時，須有監控設備進行監控或資訊資產權責單位或保管單位指派人員全程陪同。

5.10 例外作業

各單位應遵循本程序書之規範，針對委外服務提出適當安全需求項目。但若因成本、時效、委外服務之特性、委外廠商之侷限性等相關因素之

考量，而致本程序書所規範之安全需求無法完全適用時，各單位得以簽呈方式，提出其他適切之安全需求與規劃，提報資通安全長簽核。

5.11 服務變更管理

委外廠商所提供之相關服務內容如有變更，需經由系統負責人請示單位主管，必要時需以簽呈方式通報資通安全長核示，並視需求附上相關風險評鑑之評估佐證資料，經資通安全長核可後，方能進行變更，其服務變更內容如下：

(1) 系統網路架構改變。

(2) 使用新的技術。

(3) 產品轉換至新版本。

(4) 新的開發工具及環境。

(5) 服務設備之搬遷。

(6) 更換服務提供廠商或服務人員。

異動採購或維護合約上述服務內容時，委外廠商需提出相關配套措施。

5.12 個人資料委外作業

若委外作業內含個人資料利用，應依個人資料保護法施行細則第八條規定對委外廠商為適當之監督，並明確約定相關監督事項及方式。內容應包含以下要求：

(1) 契約內應載明委外作業預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

(2) 委外廠商應簽訂前述合約附件，確保安全管理及負責安全事件責任。

(3) 本校宜對其作業流程及安全控制措施進行書面或實地稽核。本校得透過稽核或填寫「合約商個人資料保護自評表」、「個人資料委外監督合約補充條約」等方式監督委外廠商之個人資料管理作法，如個

資蒐集、處理、利用、傳輸與銷毀之管理情形。

(4) 委外廠商或其受僱人違反個人資料保護法、其他個人資料保護法律或其法規命令時，應向本校進行通報及採行補救措施。

(5) 本校如對委外廠商有保留指示者，其保留指示之事項。

(6) 委外關係終止或解除時，應將個人資料載體返還，並刪除持有之個人資料檔案。

(7) 遵循我國個人資料保護法律要求的要項。

(8) 對個人資料處理者，宜評估其經驗、依賴程度與個人資料防護要求的能力。

5.13 雲端服務使用之管理

5.13.1雲端服務之形式分為：

(1) 公有雲端硬碟：Google 雲端硬碟、OneDrive、Hicloud 等。

(2) 公有雲端伺服器服務：Google Cloud Platform、Microsoft Azure、Amazon AWS 等。

(3) 上級或主管機關所提供之具資料及檔案儲存或編輯功能之服務。

5.13.2使用公有雲端服務前，宜先對雲端服務供應商的資安能力進行評估，如透過網路查詢雲端服務供應商資安標準取得(如，ISO27017、ISO 27018)、相關法規遵守情況及服務可用性等資訊。

5.13.3針對公有雲端服務方面，各使用單位應注意以下事項：

(1) 宜有電子/書面化的協議（如合約、服務條款、訂單等）確保雲端服務供應商應盡責任及使用期限建立有效溝通管道。

(2) 定期維護雲端服務並進行安全管理機制，如：帳號權限清查、事件日誌紀錄檢視、系統更新維護、刪除不需保存之敏感個資或作遮蔽/加密保護機制。

(3) 如有使用上級或主管機關之雲端服務，應依其規範辦理相關作業。

5.13.4從雲端服務供應商撤出時應確保：

(1) 雲端服務內的資料及系統可正常移轉，如:移轉到新的雲端服務供應商或本校內的基礎設施。

(2) 雲端服務內的資料及系統可被完整刪除，以免系統或資料因未完整刪除造成外洩之資安事故。

6 相關文件

6.1 資通安全管理法

6.2 資通安全管理法施行細則

6.3 資通安全責任等級分級辦法

6.4 個人資料保護法

6.5 資通安全管理政策(IS-A-001)

6.6 資訊資產管理程序書(IS-B-003)

6.7 風險評鑑與管理程序書(IS-B-004)

6.8 資通訊作業管理程序書(IS-B-007)

6.9 存取控制管理程序書(IS-B-008)

6.10 系統開發與維護程序書(IS-B-009)

6.11 資通訊委外合約書附則(IS-C-010)

6.12 資通訊採購指引(IS-C-011)

6.13 外來文件、法規、法令一覽表（IS-D-007）

6.14 個人保密切結書(IS-D-013)

6.15 資安宣導單（IS-D-017）

6.16 合約商保密切結書(IS-D-034)

6.17 資通訊系統委外自評表(IS-D-036)

6.18 合約商個人資料保護自評表(IS-D-044)

6.19 合約商資通安全管理作業查核表(IS-D-045)

6.20 資通訊系統清冊(IS-D-070)

6.21 資通訊系統等級異動申請表(IS-D-071)

6.22 人員進出管制紀錄表(IS-D-201)

6.23 資通訊設備評估表(IS-D-300)

6.24 資通系統權限申請表(IS-D-401)

6.25 資通系統防護基準控制措施檢核表(IS-D-448)

6.26 個人資料委外監督合約補充條約(PIMS-C-007)