管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-018	
文件名稱	委外作業管理程序書	
發行單位	文件管制小組	
發行日期	104年07月06日	
版　　次	A	
訂修廢單位	審　　查	核　　准
資通安全處理小組	資訊網路中心 中心主任 陳君毓	行政 副校長 翁順祥

（原版簽名頁保存於文件管制小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
A	104/07/06	初版發行

1. 目的

為促使本校委外廠商及委外廠商人員在本校進行各項委託業務作業及存取資訊時，有一明確的安全規範，以確保本校資料的機密性，維護資訊委外作業之安全，特制定本程序書。

2. 適用範圍

凡本校各項業務委外處理作業，以及委外服務廠商透過遠端方式進行系統維護、外部單位駐點人員與外單位訪客使用本校內部網路或作業過程中與外單位交換資料之委外作業，均適用本程序書。

3. 參考文件

3.1. ISMS-P-011 實體與環境安全管理程序書。

3.2. ISMS-P-003 資訊資產管理程序書。

3.3. ISMS-P-013 帳號密碼及存取控制管理程序書。

3.4. ISMS-P-009 資訊安全事件管理程序書。

3.5. ISMS-P-008 矯正及預防管理程序書。

4. 名詞定義

4.1. 委外

依據契約協議，將某項服務的持續管理責任轉嫁第三者執行，本校負有監督管理責任。

5. 作業內容

5.1. 委外作業管理流程圖

作業流程	權責單位	相關表單
提出服務需求	需求單位	
評估及審核（No）	權責單位	
Yes		
遴選委外服務廠商	需求單位	評選標準
委外服務執行管理	資通安全處理小組	委外廠商保密協議書 委外廠商人員保密切結書 委外廠商資安規範查核表
進行存取作業	委外廠商 專案相關外部人員	管制區域進出管制登記表
問題檢討與改善（No）	委外廠商 資通安全處理小組	會議紀錄單
驗收	權責單位	驗收相關文件
Yes		
付款核銷	權責單位	
紀錄保存	相關業務承辦人員	

5.2. 提出委外服務需求

5.2.1. 本校因業務需求提出資訊委外服務時，若發生下列之情事者，即可進行適當之評估及考量將業務委外辦理。

5.2.1.1. 限於專業技術或人力無法自行辦理。

5.2.1.2. 自行辦理難以滿足時效要求。

5.2.1.3. 自行辦理不符經濟成本效益。

5.2.1.4. 其他相關環境條件無法配合。

5.2.2. 經需求單位評估後需提出業務委外時，應擬妥簽呈並檢附需求規格，詳載業務委外各項之服務需求後提出申請。

5.3. 評估及審核

需求單位將委外需求簽呈及相關附件會相關權責單位審核，若審核通過則移由事務組依本校採購相關規定辦理採購。

5.4. 遴選委外服務廠商

辦理業務委外時，由需求單位參考政府採購法及本校相關廠商評選辦法遴選合格的供應廠商。

5.5. 委外服務執行管理

5.5.1. 一般條款

5.5.1.1. 應要求委外廠商遵循本校資安政策與資安目標，恪守本校資訊安全管理制度（ISMS）各項作業規範及相關法規之要求。

5.5.1.2. 委外廠商執行業務上若有複委託之需求，應事前取得本校之同意，委外廠商應對複委託廠商依本校資訊安全管理制度（ISMS）相關規定進行適當之監督與管理。

5.5.1.3. 委外廠商及其複委託廠商於執行本校資通訊技術服務與產品業務時，應對所承接之業務所涉及之資訊資產或服務，進行風險評鑑並提出相關紀錄，本校須針對風險評鑑結果進行審查，必要時得派員進行實地查核，廠商應予配合。機關於查核後若有缺失，得以書面敘明理由請廠商限期改善。

5.5.1.4. 委外廠商因執行委外業務，須接觸「密」等級（含）以上資訊，除應遵守相關法令法規及本校資訊安全規範外，尚須簽署「ISMS-P-018-01 委外廠商保密切結書」，委外廠商人員需簽署「ISMS-P-018-02 委外廠商人員保密切結書」。

5.5.1.5. 委外廠商應提供負責委外業務的聯絡窗口及電話，協助解決相關問題，並配合本校業務執行及異常狀況排除。

5.5.1.6. 委外廠商於履行合約期間所使用之軟體，均需為合法軟體，並不得違反智慧財產權之規定，如有違法情事發生，委外廠商須承擔應負之法律責任。

5.5.1.7. 委外廠商所使用之工具軟體以及處理作業之執行紀錄，本校有權進行稽核審查，廠商不得異議。

5.5.1.8. 委外廠商應留存異常處理紀錄，本校得視需要進行查核。

5.5.1.9. 委外廠商所交付之標的物如侵害第三人合法權益時，應由委外廠商負責處理並承擔一切法律責任。

5.5.1.10. 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，委外廠商需負損害賠償責任。

5.5.1.11. 負責執行委外業務之廠商人員離職時，應由承辦單位要求廠商人員繳回其所借用之設備、軟體及註銷其存取權限。

5.5.1.12. 委外廠商人員，於支援業務時所獲知「密」等級（含）以上資訊，不得對外透露，為確保前述事項之落實，將要求其人員簽署「ISMS-P-018-02 委外廠商人員保密切結書」。

5.5.1.13. 委外廠商應依據契約中所詳載之委外需求，提供委外服務並完全滿足服務需求。

5.5.1.14. 委外廠商需保證與委外作業有關的各方（包括分包商）都應遵守資訊安全法令規定。

5.5.2. 委外服務管理

5.5.2.1. 委外廠商人員於本校執行委外業務時，所需使用之相關資源，應依相關之申請規定辦理。

5.5.2.2. 委外廠商人員於執行委託業務期間，若違反本校資安政策或安全管理規範，應依合約條款發函告知所屬企業或組織處理，或依相關法令訴諸法律行動。

5.5.2.3. 委外廠商人員進出本校辦公室及管制區域時，應確實遵守「ISMS-P-011 實體與環境安全管理程序書」之規定，落實實體與環境安全之控制。

5.5.2.4. 服務變更管理
委外廠商所提供之相關服務內容如有重大變更，由業務承辦單位視需要附上相關風險評鑑之佐證資料，經一級主管決行後方能進行變更。

5.5.3. 委外存取作業管理

5.5.3.1. 服務廠商及其相關人員，於完成簽署保密協議及獲得資訊存取權限後，由業務承辦人員向廠商詳細說明本校資訊安全管理制度之各項安全規定後，始得進行資訊的存取作業。

5.5.3.2. 本校僅提供必要之網路服務項目，所有行為不得與本校網路安全相關規定抵觸。若有特殊需求，則須經專案審查、評估核准後，方可建立連線與開放存取權。

5.5.3.3. 對外提供或交換本校員工、客戶或廠商之相關資料時，如為電子檔案、電子郵件形式，應依「ISMS-P-003 資訊資產管理程序書」之規定，按其機密等級採適當保護措施後傳送。

5.5.3.4. 對外提供或交換本校員工或民眾之資料時，如為書面或以其它儲存媒體型式傳送，應依「ISMS-P-003 資訊資產管理程序書」之規定辦理。

5.5.3.4.1. 如為書面型式的資料，應使用信封妥善封存及簽署，並密封交寄。

5.5.3.4.2. 如為存放於實體儲存媒體的數位資料，應完整包覆儲存媒體，並密封交寄以確保媒體之機密性與完整性。

5.5.3.5. 委外系統之資料、軟體、作業系統及資料庫等最高權限帳號，應由本校各業務承辦人員保管，除經授權不得直接授與

委外廠商使用。

5.5.3.6. 委外廠商人員如因作業需求，需取得帳號及存取權限對本校系統進行存取，應依「ISMS-P-013 帳號密碼及存取控制管理程序書」之相關規定提出申請，經核可後方可開放存取權限。

5.5.3.7. 委外廠商人員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。

5.5.3.8. 委外廠商人員對於系統之操作，本校各系統管理者應盡監督之責，委外廠商人員不得任意從事非工作範圍內之操作，且各系統管理者應視需要於委外廠商人員完成工作後檢視系統紀錄。

5.5.4. 委外專案之安全要求

5.5.4.1. 對於委託給委外廠商提供服務之任何專案，應在合約或任何安全條款或協議中，明確陳述專案過程中應遵循之各項安全規範，也可委請委外廠商針對所承接之專案內容，進行風險評鑑作業，並根據風險評鑑結果用以決定各項資訊安全要求與規定。

5.5.4.2. 本校業務承辦人員應依據與委外廠商所簽訂合約或任何安全協議中所陳述之資安規範，製作「ISMS-P-018-03 委外廠商資安規範查核表」，並委請廠商依查核表之內容進行自評，廠商完成自評後再由本校進行複查，若發生不符合項目時則通報廠商限期改善。

5.5.5. 可攜式電腦及儲存媒體管理

5.5.5.1. 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管制區域使用，須經權責單位同意後，註記於「ISMS-P-011-02 管制區域進出管制登記表」中，並遵守相關設備管理之規定。

5.5.5.2. 委外廠商維修人員，進入管制區域並使用經本校授權之可攜式電腦或儲存媒體時，須有本校員工陪同或適當監視。

5.5.6. 緊急應變計畫

5.5.6.1. 資訊作業委外若涉及本校之關鍵業務時，應要求委外廠商配合本校定期進行業務持續計畫測試及演練，針對委外標的建立緊急應變計畫，並定期進行測試及衡量其演練週期。

5.5.6.2. 備援需求
依據不同資訊資產之價值及可用性等級，考量其備援需求，必要時得建立異地備援機制。

5.5.7. 硬體採購與維護
委外廠商應提供所交付設備之架構、操作、管理、維護等相關之操作手冊、文件與技術支援服務，如有必要應請委外廠商提供訓練課程。

5.6. 問題檢討與異常處理

5.6.1. 委外廠商於進行委外服務時，若無法滿足委外契約之要求時，應由承辦單位與委外廠商，就雙方爭議之部分舉行會議協商，進行問題之檢討與改善，直至雙方達成共識為止，並將會議之結果記錄於「ISMS-P-002-03 會議紀錄單」備查。

5.6.2. 委外廠商人員以遠端方式進行系統維護時，系統管理者必須隨時掌握系統維護狀況，如發生資訊安全事件時，應依據「ISMS-P-009 資訊安全事件管理程序書」之相關規定進行通報。

5.6.3. 若發生異常狀況時，由業務承辦人員即時處理，異常狀況無法解決時，則依據「ISMS-P-008 矯正及預防管理程序書」之相關規定執行矯正與預防措施，進行問題矯正及風險預防的作業。

5.7. 驗收
委外廠商完成委外契約所載之各項服務需求時，由權責單位依據契約之驗收標準進行驗收作業。

5.8. 付款核銷
委外廠商完成所有驗收程序時，由權責單位依本校相關規定辦理付款核銷作業。

5.9. 紀錄保存
相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	委外廠商保密切結書	資網中心	永久保存
2	委外廠商人員保密切結書	資網中心	永久保存
3	委外廠商資安規範查核表	資網中心	至少一年

6. 附件

6.1. ISMS-P-018-01 委外廠商保密切結書。

6.2. ISMS-P-018-02 委外廠商人員保密切結書。

6.3. ISMS-P-018-03 委外廠商資安規範查核表。

6.4. ISMS-P-011-02 管制區域進出管制登記表。

6.5. ISMS-P-002-03 會議紀錄單。