管理系統文件

文件類別	第二階文件	
文件編號	IMS-P-018	
文件名稱	資通業務委外作業管理程序書	
發行單位	國立虎尾科技大學	
發行日期	112 年 05 月 05 日	
版　　次	2.5	
適用單位/範圍	全校	
訂修廢單位	審　　查	核　　准

（原版簽名頁保存於 IMS 推動小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
1.0	106/01/11	初版發行
2.0	108/08/21	因應資通安全管理法施行修訂相關用詞及規範。(5.5 遴選委外服務廠商、5.7.3 委外專案之安全要求)
2.1	109/06/12	增訂 5.6.2.5 資通系統驗收作業，以符合資通安全責任等級分級辦法之 B 級單位應辦事項。
2.2	109/08/12	將 5.10 紀錄保存表單的保存地點由「電子計算機中心」改為「各單位」。
2.3	110/03/29	1.修訂「3.1 附錄 A 資通安全管理規範」為:「3.1 國際標準資訊安全管理系統(ISO27001：2013)」。 2.刪除原「3.2 教育體系資通安全暨個人資料管理規範」。
2.4	111/07/02	修訂條文 5.7.1.3
2.5	112/05/05	1. 5.1 委外作業管理流程圖修正 2. 條文 5.4 新增

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，維護資通業務委外作業管理之安全。

2. 適用範圍

本校各項資通業務委外處理作業，以及委外廠商透過遠端方式進行系統維護、委外廠商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資通業務委外作業管理。

3. 參考文件

3.1　資通安全管理法。

3.2　資通安全管理法施行細則。

3.3　資通安全責任等級分級辦法。

3.4　國際標準資訊安全管理系統(ISO27001：2013)。

3.5　教育體系資通安全暨個人資料管理規範。

3.6　IMS-P-003 資通資產管理程序書。

3.7　IMS-P-004 資通安全風險管理程序書。

3.8　IMS-P-006 業務持續管理程序書。

3.9　IMS-P-008 矯正預防及持續改善管理程序書。

3.10　IMS-P-013 帳號密碼及存取控制管理程序書。

3.11　IMS-P-014 系統發展與維護管理程序書。

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。

4.2　可攜式設備與儲存媒體

泛指重量輕盈、體積大小合宜及便於攜帶使用的電子資料處理或儲

存設備。

4.2.1 可攜式資通設備

包含筆記型電腦、平板電腦、智慧型手機、個人數位助理(PDA)、數位播放器、數位相機、錄音筆、燒錄設備或其他具存取數位資料功能之可攜式資通設備及其周邊設備等。

4.2.2 可攜式儲存媒體

可供使用者透過資通設備之通信埠，如 Ethernet、USB 埠、1394 埠等進行大量資料存取之媒體，包含 USB 隨身碟、可攜式硬碟、磁帶、光碟片、Compact Flash（CF 卡）、Secure Digital card（SD 卡）等數位相機記憶卡或其他具存取數位資料功能之媒體。

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
提出委外服務需求	需求單位	本校各單位推動業務委託民間辦理申請單
委外業務風險評估	需求單位 IMS 推動小組	
委外廠商風險自評	委外廠商 需求單位	委外廠商資通安全要求查核表
評估及審核（未通過）	需求單位 IMS 推動小組	委外廠商資通安全要求查核表
通過		
執行委外業務	委外廠商	
委外服務執行管理	委外需求單位	委外廠商保密切結書 委外廠商人員保密切結書 人員機房進出紀錄表
問題檢討與改善	委外廠商 委外需求單位	
Yes		
委外監督與管理	委外需求單位	委外廠商資通安全要求查核表
紀錄保存	IMS 推動小組	

5.2　提出委外服務需求

5.2.1　本校因業務需求提出資通委外服務時，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　需求單位因業務需求提出資通委外服務，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。

5.2.3　需求單位辦理委外作業時，應針對各項資安及個資保護需求，於規劃前徵詢廠商提供相對應之建議措施，以符合資安及個資保護安全要求。

5.3　委外業務風險評估

5.3.1　委外需求單位應依據「IMS-P-004 資通安全風險管理程序書」之規定，對委外業務中的資通資產依機密性、完整性及可用性進行價值鑑別，並適當評估其可能之威脅及弱點。

5.3.2　委外需求單位依據風險評鑑結果，進行風險管理作業，選擇適用之防護措施，以降低風險到可接受等級。

5.4　委外廠商風險自評

廠商辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。委外廠商應填寫「 IMS-P-018-03 委外廠商資通安全要求查核表」，以供識別專案管理中所相關之風險，防範發生危害系統安全之情況 。

5.5　評估及審核

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

5.6　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、資通安全管理法及

本校相關廠商評選辦法遴選合格的供應廠商。

5.7　執行委外業務

5.7.1　硬體採購與維護

委外廠商於保固期限內應提供與設備主機之架構、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。在保固期滿後，若需要時為維持原硬體之功能及正常運作，廠商應提供硬體定期維護合約工作。

5.7.2　系統開發與維護

5.7.2.1　資通系統若委由外部廠商開發，廠商應對系統分析、系統設計、程式設計與系統測試等階段提供相關報告書。

5.7.2.2　委外廠商應確實控管程式與文件版本之一致性。資通系統程式原始碼版本控制，並只准許授權人員執行變更。

5.7.2.3　委外廠商進行系統開發與維護時，除獲得授權外不得任意複製或攜出本校機密等級屬「機敏」之業務資料。

5.7.2.4　委外廠商所交付之資通系統應於安裝前進行測試，確保系統內不含惡意程式、隱密通道及特洛伊木馬程式。

5.7.2.5　資通系統驗收時，應由權責單位確認如下事項：

5.7.2.5.1　應由本校人員測試上線之程式，並依規格需求確認資通系統是否符合並確實核對契約規範之系統相關文件。

5.7.2.5.2　系統經由本校權責單位依據「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」鑑定之等級，須完成「資通安全責任等級分級辦法附表十-資通系統防護基準」所對應等級之各項防護措施使得進行驗收作業。

5.7.2.6　程式開發與維護需遵守本校「IMS-P-014 系統發展與維護管理程序書」之規定，若有新增功能或修改之需求時，應檢附相關文件填寫「IMS-P-014-01 資通系統軟體及資料庫異動申請單」提出申請。

5.8　委外服務執行管理

5.8.1　一般條款

5.8.1.1　本校委託單位應要求委外廠商遵循本校資安及個資保護政策與目標，恪守本校資安及個資保護管理制度（IMS）各項作業規範及相關法規之要求。

5.8.1.2　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委外廠商依本校資安及個資保護管理制度（IMS）相關規定進行適當之監督與管理。

5.8.1.3　委外廠商及其複委託委外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通資產或服務，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，委外廠商應予配合。本校於查核後若有發現缺失，得以書面敘明並請委外廠商限期改善。

5.8.1.4　委外廠商處理個人資料應遵守「個人資料保護法」，委外合約中應包含保密條款並簽署「IMS-P-018-01 委外廠商保密切結書」，委外廠商人員若須接觸本校機敏資訊時，應簽署「IMS-P-018-02 委外廠商人員保密切結書」，並遵守相關法令法規及本校資安及個資保護安全規範。

5.8.1.5　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。

5.8.1.6　委外廠商於履行契約期間所使用之軟體，均需為合法授權軟體，並不得違反智慧財產權及本校之規定，如有違法情事發生，委外廠商須承擔應負之法律責任。

5.8.1.7　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，委外廠商不得異議。

5.8.1.8　委外廠商於執行本校委託之業務時，應留存異常處理紀錄，本校得視需要進行查核。

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

5.8.1.10 負責執行委外業務之委外廠商人員離職時，應由承辦單位要求委外廠商人員繳回所借用之設備及軟體並註銷存取權限。

5.8.1.11 委外廠商人員於執行委託業務期間，若違反本校資安及個資保護安全政策或資安及個資保護管理規範，應依契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。

5.8.2 委外存取作業管理

5.8.2.1 委外廠商及其相關人員，於完成簽署保密協議及獲得資訊存取權限後，由業務承辦人員向委外廠商詳細說明本校資安及個資保護管理制度之各項安全規定後，始得進行資訊的存取作業。

5.8.2.2 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。

5.8.2.3 對外提供或交換本校利害關係人的資料時，如為電子檔案、電子郵件形式，應依「IMS-P-003 資通資產管理程序書」之規定，按其機密等級採適當保護措施後傳送。

5.8.2.4 對外提供或交換本校利害關係人之資料時，如為書面或以其它儲存媒體型式傳送，應依「IMS-P-003 資通資產管理程序書」之規定辦理。

5.8.2.4.1 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。

5.8.2.4.2 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。

5.8.2.5 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。

5.8.2.6 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。

5.8.3　委外專案之安全要求

5.8.3.1　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通安全要求與規定。

5.8.3.2　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「IMS-P-018-03 委外廠商資通安全要求查核表」，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。

5.8.3.3　委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。相關細節應依資通安全管理法施行細則第四條辦理。

5.8.3.4

5.8.4　系統帳號管理

5.8.4.1　委外廠商人員如因作業需求，需對系統資料、軟體、作業系統及資料庫進行存取，應依照「IMS-P-013 帳號密碼及存取控制管理程序書」之規定辦理，其中資料庫之存取，應填寫「IMS-P-014-01 資通系統軟體及資料庫異動申請單」向管理人員提出申請，經核准後始得啟用。

5.8.4.2　委外廠商人員系統帳號及存取權限，應僅限於從事本身資通系統範圍之操作，而其系統帳號不得任意交由非作業相關人員使用。

5.8.4.3　為有效控管資料及系統存取，系統管理員至少每年審查、檢討及評估使用者之存取權限。

5.8.5　系統備援

5.8.5.1 委外資通系統必須依據其提供及處理資料可容許的中斷，建立適當的備援方案，以確保服務的可持續運作，必要時得建立異地備援機制。

5.8.5.2 為確保備援方案的正常運作，系統管理人員應依據「IMS-P-006 業務持續管理程序書」之規定進行演練或測試，並根據測試結果進行改善。

5.8.5.3 資通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。

5.8.6 變更管理

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

5.8.6.2 委外資通系統應於作業系統、應用系統、資料庫系統等變更前，評估資通系統安全控制措施和系統的完整性，並確保不受系統變更操作影響。

5.8.6.3 資通系統如於上線後需執行變更或維護作業，應由系統管理人員公告變更或維護作業時程，以便相關人員配合進行下線或停機作業；系統變更後，應主動公告異動範圍、時間及可能的影響。

5.8.6.4 作業系統在升級、進行重大更新或系統程式變更，應評估其對應用系統之影響，須經適當的授權核准，並留存紀錄備查。

5.8.6.5 系統變更前應進行備份並記錄備份位置，且備份位置不得與線上資料同一目錄，以避免變更失敗、資料毀損或影響其他系統之正常運作。

5.8.7 可攜式電腦及儲存媒體管理

委外廠商非經許可，不得攜帶可攜式電腦或儲存媒體進入本校管制區域使用。只有在特定目的與被授權情形下才能進入，並須由內部人員陪同且註記於「IMS-P-011-01 人員機房進出紀錄表」。

5.9　問題檢討與異常處理

5.9.1　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，應由委外需求單位與委外廠商，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。

5.9.2　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「IMS-P-008 矯正預防及持續改善管理程序」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。

5.10　委外監督與管理

5.10.1　委外專案之安全要求

對於委託給委外廠商提供服務之任何專案，應在契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。

5.10.2　委外監督與稽核

本校委外需求單位應依據與委外廠商所簽訂契約或任何安全協議中所陳述之資通安全規範，製作「IMS-P-018-03 委外廠商資通安全要求查核表」，並委請委外廠商依查核表之內容進行自評，委外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委外廠商限期改善。

5.10.3　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。

5.10.4　委外廠商需保證與委外作業有關的各方（包括分包商）都應遵守資安及個資保護法令規定。

5.11　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	各單位	契約終止後3年
2	委外廠商人員保密切結書	各單位	契約終止後3年
3	委外廠商資通安全要求查核表	各單位	至少 3 年

6.　附件

6.1　IMS-P-014-01 資通系統軟體及資料庫異動申請單。

6.2　IMS-P-018-01 委外廠商保密切結書。

6.3　IMS-P-018-02 委外廠商人員保密切結書。

6.4　IMS-P-011-01 人員機房進出紀錄表。

6.5　IMS-P-018-03 委外廠商資通安全要求查核表。