

實踐大學資通服務委外合約書附則

114 年 6 月 11 日 113 學年度第 2 學期資通安全暨個人資料保護委員會通過

114 年 12 月 31 日 114 學年度第 1 學期資通安全暨個人資料保護委員會修正通過

壹、一般條款

1. 委外廠商應提供負責系統維護、聯絡窗口及電話詢答服務，並解決系統相關事宜，並配合本校相關程序辦理異常排除及通報事宜，如必要應提供駐點服務。
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。
3. 委外廠商履行合約應提供其使用之軟體，且均需為合法軟體，並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。
4. 委外廠商使用之工具軟體及處理作業之執行紀錄，本校有權進行稽核，廠商不得異議。
5. 委外廠商應留存異常處理紀錄，本校得視需要查核。
6. 委外廠商所交付之標的物如侵害第三人合法權益時，應由承包廠商負責處理並承擔一切法律責任。
7. 委外廠商如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。
8. 委外廠商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及作業權限。
9. 委外廠商人員，於支援業務時所獲知限閱等級以上資訊，不得對外透露，為確保前述事項之落實，將要求廠商及其人員簽署「承包廠商保密同意書」及「承包廠商員工保密同意書」。
10. 委外廠商不得為大陸地區廠商，且委外廠商執行專案之團隊成員，其國籍不得為中國大陸，所提供之服務內容(含軟體、硬體及服務)亦不得使用大陸廠牌資通訊產品。如因特定業務有使用大陸廠牌資通訊產品之需求，原則禁止與公務環境交接，且需經本校評估同意。
11. 委外廠商人員必須完成資通安全相關教育訓練，並檢附相關受訓證明。

貳、硬體採購與維護

廠商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。

參、系統開發及維護

1. 系統若委由外部廠商開發，廠商應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，經由本校相關人員確認後方能執行。
2. 委外廠商應確實控管程式與文件版本之一致性。
3. 委外廠商進行系統開發與維護時，不得任意複製或攜出本校限閱等級以上之業務資料。
4. 委外廠商須針對交付之系統出具切結書，保證系統內不含後門程式及隱密通道。新購系統並出具弱點掃描報告（或依專案需求，提供滲透測試報告、源碼檢測報告...等），確保交付之系統無中高風險之弱點漏洞。既有維護系統由本校執行系統弱點掃描作業，提供弱點掃描報告，確保交付之系統無中高風險弱點漏洞。

5. 委外開發或維護之系統，於合約有效期間，若發現系統有安全漏洞，經委外廠商與校方以雙方可以接受並留存記錄的形式（包括電子郵件往來、系統通報紀錄、會議紀錄或其他足資證明之方式）予以確認後，該漏洞之修補作業應由委外廠商負責協助校方完成。
6. 若系統、軟體由委外廠商開發者，應由本校人員測試及驗收上線之程式，確定符合相關需求後，方得依照「系統開發與維護程序書」之程序進行上線。
7. 程式修改與開發需遵守本校「系統開發與維護程序書」之規定，若有例外，須經本校主管人員同意以後，方可實施。
8. 本案開發（含維護）系統依據資通系統分級結果，係為☐普級☐中級☐高級系統，相關資安防護控制措施請參考「資通安全責任等級分級辦法」附表十規定辦理，並自評實作內容，以確保符合防護基準要求。

肆、系統帳號管理

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，應由本校人員保管，儘可能避免直接授與委外廠商使用。
2. 委外廠商之人員如因作業需求，需對本校系統進行遠端存取，應填寫「資訊服務申請表」進行申請。
3. 「資訊服務申請表」中應載明作業需求內容、所需權限、帳號有效時間，經由本校主管核准後，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人員使用。
4. 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. 本校各系統管理者應盡監督之責，委外廠商人員不得從事非工作範圍內之操作，各系統管理者並應於委外廠商人員完成工作後檢視系統紀錄。

伍、緊急應變計畫

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處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。

陸、可攜式電腦及儲存媒體管理

1. 委外廠商如需攜帶可攜式電腦或儲存媒體如磁片、光碟、隨身碟等進入圖書暨資訊處機房使用，需記載於「資訊機房訪客進出登記表」後方可攜入。
2. 廠商維修人員，當進入機房並使用可攜式電腦或儲存媒體時，須有圖書暨資訊處人員全程陪同或由監視設備監控其活動。

柒、服務變更管理

委外廠商所提供之相關服務內容如有變更，需經由業務承辦人員以簽呈方式通報主辦單位主管，並視需求附上相關風險評估之佐證，經主辦單位主管核可後，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。

捌、委外關係終止及解除

本案若因期限屆滿、解除或其他原因而終止時，應確認委外廠商已返還、移交、刪除或銷毀履行契約而持有之專案資料與個人資料，委外廠商及其工作人員仍負有對本校相關業務資料之保密責任，倘有違反情形，本校得要求廠商應負賠償之責任。

玖、以上合約附則條款，遵請承包廠商配合辦理。

附件、廠商須交付文件

- 1. 委外廠商資訊安全自評表
- 2. 承包廠商保密同意書
- 3. 承包廠商員工保密同意書
- 4. 承包廠商資通安全相關教育訓練受訓證明
- 5. 承包廠商系統不含後門程式及隱密通道切結書，含無中高風險之系統弱點掃描報告