文件名稱	委外管理作業	文件編號	IC-11420-008
所屬單位	圖書資訊處系統發展組	頁　　次	第 1 頁 共 5 頁

1.流程圖：

附件 1：委外管理作業流程圖

2.作業程序：

2.1 權責

2.1.1 主辦單位

a.負責依據本作業之規定，提出適當之安全需求及擬定與廠商服務相關契約內容。

b.辦理委外廠商招標作業應符合政府採購法與相關規定及本校採購執行作業手冊。

2.1.2 業務權責單位

a.負責審查主辦單位所擬定之契約，確認契約內容無違反本校應遵循之相關規定或傷害本校之權益。

2.2 名詞定義

a.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。

b.後門程式：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。

c.OWASP Top 10 威脅：由 OWASP 組織經過調查與彙整後，揭露常見的網站應用程式威脅與弱點，以供系統開發與管理人員參考。

2.3 作業程序

2.3.1 一般條款

2.3.1.1 委外廠商應遵守本校【資訊安全政策】及相關安全規範，若委外服務內容涉及資訊設備或系統，提供服務之人員均需簽署「委外廠商保密切結書」及「委外廠商資安監督查檢表」，若當日無法提供正本資料，則可先透過傳真提供資料，但仍應於 7 日內補上正本資料。

2.3.1.2 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。

2.3.1.3 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。

2.3.1.4 委外廠商履行契約應提供其使用之軟體，且均須為合法軟體，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。

2.3.1.5 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。

2.3.1.6 委外廠商應留存異常處理紀錄，本校得視需要查核。

2.3.1.7 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。

2.3.1.8 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。

2.3.1.9 委外廠商人員，於支援業務時所獲知「敏感」等級(含)以上資訊，非經本校授權，不得對不相干的第三方透露。

2.3.1.10 委外廠商存取組織資產之授權，需經過申請與評估程序方可取得，並需遵守所要求之資訊安全事項。

2.3.1.11 開放給廠商的存取權限，應以其最低資訊安全需求為考量，以避免過多的授權增加不必要的風險。

2.3.1.12 委外廠商有義務保護組織的重要資料，未經允許不可擅自帶走任何資料。

2.3.1.13 於委外合約中，宜說明廠商所提供的資訊與通訊技術之服務與產品，應符合組織預期的需求功能，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。

2.3.2 資訊系統委外服務提出

2.3.2.1 主辦單位因業務需求提出資訊委外服務，應適當評估資訊委外之必要性。

2.3.3 資產辨識與風險評鑑作業

2.3.3.1 主辦單位應依據【資產清查暨風險評鑑作業】，依照委外標的之資訊資產價值、機密性、可用性等級，適當評估其可能之威脅及弱點。

2.3.4 硬體採購與維護

2.3.4.1 廠商應視需求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，如必要應提供教育訓練課程。

2.3.5 系統開發及維護

2.3.5.1 系統若委由外部廠商開發，廠商應視需求提供完整之系統架構說明、系統分析設計、資料庫欄位設計等使用表單，經由本校相關人員確認後方能執行程式開發。

2.3.5.2 委外廠商應確實控管程式與文件版本之一致性。

2.3.5.3 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敏感(含)等級以上之業務資料。

2.3.5.4 委外廠商需針對交付之系統，應提供證明文件，確保系統未有 OWASP Top 10 威脅、後門程式及隱密通道。

2.3.5.5 若系統、軟體由委外廠商開發者，應由本校人員測試，確定符合相關需求後，方得依照【系統開發與維護作業】之程序進行上線。

2.3.5.6 程式修改與開發需遵守本校【系統開發與維護作業】之規定，若有例外，須經圖書資訊處(圖資處)圖資長同意以後，方可實施。

2.3.6 系統帳號管理

2.3.6.1 委外系統資料、軟體、資料庫或作業系統預設最高權限帳號，應由本校處理資訊單位人員保管，不得直接授與委外廠商使用。

2.3.6.2 委外廠商之人員如因作業需求，需對本校系統進行存取，應遵循相關管理規範。

2.3.6.3 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。

2.3.6.4 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。

2.3.7 營運持續運作

2.3.7.1 資訊作業委外若涉及本校之關鍵核心系統時，應要求委外廠商針對委外標的建立【營運持續計畫作業】，並配合本校定期進行【營運持續計畫作業】測試演練作業；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。

2.3.7.2 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。

2.3.8 可攜式電腦及儲存媒體管理

2.3.8.1 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機房使用，需經陪同之資訊單位承辦人員同意並註記於「電腦機房人員

及物品進出紀錄單」,「電腦機房人員及物品進出紀錄單」應定期由權責主管審閱。

2.3.8.2 廠商維修人員，當進入本校機房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本校人員全程陪同。

2.3.9 例外作業

2.3.9.1 資訊委外服務之主辦單位應遵循本作業之規範，提出適當安全需求項目。但若因成本、時效、委外服務之特性、委外廠商之局限性等相關因素之考量，而致本作業所規範之安全需求無法完全適用時，主辦單位得以簽呈方式，提出其他適切之安全需求與規劃，提報權責主管簽核。

2.3.10 服務變更管理

2.3.10.1 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鑑之佐證資料，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：

a.系統網路架構改變。

b.使用新的技術。

c.產品轉換至新版本。

d.新的開發工具及環境。

e.服務設備之搬遷。

f.更換服務提供廠商或服務人員。

2.3.11 服務監視與審查

2.3.11.1 組織針對委外廠商所提供之服務交付，宜進行監視與審查下列項目：

a.監視服務效能等級以查核契約的遵守程度。

b.按契約要求審查委外廠商產出的服務報告，或安排定期的進度報告會議。

c.解決並管理所有已識別出的問題。

2.13.12 業務終止

委外廠商在專案業務終止後，應簽署「個人資料銷毀切結書」保證將專案期間所接觸之資訊或個人資料銷毀，或交還本校之業務承辦單位，並保證絕不以任何形式對外洩漏、傳播、複製、告知、交付、移轉。

3.控制重點：

3.1委外服務內容涉及資訊設備或系統,提供服務之人員是否需簽署「委外廠商保密切結書」及「委外廠商資安監督查檢表」。

3.2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機房使用，是否註記於「電腦機房人員及物品進出紀錄單」,且「電腦機房人員及物品進出紀錄單」權責主管是否定期審閱。

4.使用表單：

4.1 委外廠商保密切結書(FM-11420-054)

4.2 電腦機房人員及物品進出紀錄單(FM-11420-001)

4.3 委外廠商資安監督查檢表(FM-11420-053)

4.4 個人資料銷毀切結書(FM-11420-045)

5.法源依據：

5.1 資通安全事件通報及應變辦法(110.08.23)

5.2 個人資料保護法(112.05.31)

5.3 個人資料保護法施行細則(105.03.02)

6.參考文件：

無

7.修訂記錄：

序號	修訂內容	發行日期
1	新制訂	103.06.26
2	修正表單編號	104.05.08
3	依據人事室 108.06.26 公告本校 107 學年度第二學期組織異動，修改「圖書資訊中心」為「圖書資訊處」。	108.07.31
4	依秘書處 110.06.24 公告弘光科技大學單位名稱之簡稱暨書寫說明，修改單位名稱呈現方式。	110.10.12
5.	修訂條文 2.3.1.1、3.1、4.1、附件一流程圖及新增條文 4.3、5.1、5.2、5.3 之內容。	112.08.08
6	因應 ISO 27001:2022 改版，配合新制修訂相關控制項目與檢視，修訂條文 2.3.12、4.4、5.1、5.2、5.3、附件 1。	112.11.29
7	依現行作業調整文件編號與所屬單位、表單編號 4.1、4.3、4.4 與修訂附表 1。	113.08.06

附件1：委外管理作業流程圖