國立高雄餐旅大學

NATIONAL KAOHSIUNG UNIVERSITY
OF HOSPITALITY AND TOURISM

「資訊安全管理系統」
委外管理程序書

機密等級：一般

編　　號：**IS-02-010**

版本編號：2.3

修定日期：113.09.12

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說　　明	核准者
1.0	100.04.01	資訊安全執行小組	初稿修訂	圖資館 副館長
1.0	100.07.26	資訊安全執行小組	首次發行	圖資館 副館長
1.1	101.08.27	資訊安全執行小組	修訂 5.1.2 及 6.1	圖資館 副館長
2.0	104.08.17	資訊安全執行小組	新增 4.3、5.1 及 5.12 之規範	圖資館 副館長
2.1	110.06.10	資訊安全執行小組	修訂增列要求委外作業要求事項。	資訊安全管理代表
2.2	110.09.24	資訊安全執行小組	刪除 5.1.2…並依「資通安全責任等級分級辦法」之「限制使用危害國家資通安全產品」規定，不得採購或使用危害國家資通安全產品，….	資訊安全管理代表
2.3	113.09.12	資訊安全執行小組	新增 5.19 程序	資訊安全管理代表

本程序書由資訊安全執行小組負責維護。

目錄：

1 目的

1.1 本程序書制訂之目的在於確保國立高雄餐旅大學（以下簡稱本校）資訊委外作業之安全。

2 適用範圍

2.1 適用於本校各項資訊業務委外處理作業。

3 權責

3.1 主辦單位：負責依據本程序書之規定，提出適當之安全需求及擬定與供應商服務相關合約內容，並確實在合約中訂定「保密條款」。

3.2 業務權責單位：

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

3.2.2 對於服務提供供應商之遴選，應符合主辦單位所提出之安全需求及採購辦法之規範。

4 名詞定義

4.1 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。

4.2 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。

4.3 PMBOK：專案管理知識體系（Project Management the Body of

Knowledge,簡稱 PMBOK），由美國專案管理協會（PMI）總結了專案管理實踐中成熟的理論、方法、工具和技術所提出。

5 作業說明

5.1 供應商關係之資訊安全政策

5.1.1 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，並依「資通安全管理法施行細則」第四條規定所應注意事項，選任適當之受託者，並監督其資通安全維護情形。

5.1.2 各資訊系統於建置、調整及停用前，應將安全需求納入規劃，且將系統發展生命週期各階段依等級將安全需求納入委外契約，辦理資通安全分析及研訂規格，確保符合相關資訊系統之安全要求。

5.1.3 已開發及開發前之資通系統，應由機關評估其資通系統安全等級，並依據資通安全責任等級分級辦法之附表十「資通系統防護基準」執行控制措施應辦事項，委外廠商應依契約要求填寫「資通系統防護基準控制措施查檢表」

5.2 委外契約資安條款注意事項

5.2.1 廠商未經機關同意，不得將契約內容洩漏予履約無關之第三人。

5.2.2 廠商專案人員於執行專案期間所知悉機關任何不公開之文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片等訊息，均應保密，不得洩漏。

5.2.3 廠商專案人員於執行專案期間所知悉、持有有關之資料、程式、檔案、媒體或電磁紀錄等內容，應遵守如「個人資料保護法」、「國家機密保護法」等相關法令及契約之規定，善盡保密之責。

5.2.4 凡未經機關書面同意或授權，不得以任何形式對外洩漏或交付他人。如有違反應負民事及刑事責任，廠商並負連帶責任。

5.2.5 廠商及專案人員均應簽署保密切結/同意書。

5.3 資通安全事項檢視

5.3.1 廠商應遵守行政院所頒訂之各項資通安全規範及標準，並遵守本校資通安全管理及保密相關規定，此外本校保有對廠商執行稽核的權利。

5.3.2 契約履約或終止後，廠商應刪除或銷毀執行服務所持有本校之相關資料，或依本校之指示返還之，並保留執行紀錄。

5.3.3 廠商提供服務，如發生資安事件時，必須通報本校，提出緊急應變處置，並配合本校做後續處理。

5.4 委外廠商服務的管理

應對委外廠商提供的服務進行適當的管理，無正式協議之外部單位，不得使用其所提供的服務(公共服務除外)。對於使用委外廠商服務，應確認以下事項：

5.4.1 服務內容安全性審查。

5.4.2 服務人員的資格審查。

5.4.3 服務人員的保密切結。

5.4.4 服務成效審查，得經由會議紀錄、彙整資料審查或現場實地訪查。

5.4.5 委外廠商提供之服務如須變更時，應正式函文通知並經雙方同意後始得進行變更。

5.4.6 委外廠商應依本校需求進行資通安全自主查核，並填寫「委外廠商查核表」予本校。

5.5 保密需求

5.5.1 廠商與專案參與人員需簽署行政院公共工程委員會訂定之「資訊服務採購契約範本」相關資通安全保密同意與切結書。

5.5.2 專案採購文件另有訂定者，從其約定，不在此限。

5.6 資通安全管理

應對委外廠商執行計畫人員，說明本機關之資通安全管理相關規範，得要求其參與機關資通安全教育訓練並遵循資通安全管理規定。

5.7 資料使用完畢之處理

委外關係終止或解除，委外廠商應刪除或銷毀因履行與本校委外契約或服務而持有之資料，將委外服務資料返還或提供銷毀紀錄，如有非委外關係提供之資料應比照辦理。

5.8 資訊系統委外服務提出

5.8.1 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。

5.8.2 若為主機系統之委外採購，主辦單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。

5.9 資產辨識與風險評鑑作業

5.9.1 主辦單位應依據「資訊資產管理程序書」、「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、可用性等級，適當評估其可能之威脅及弱點。

5.10 選擇或新增安全需求

5.10.1 主辦單位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。

5.11 硬體採購與維護

5.11.1 供應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。

5.12 系統開發及維護

5.12.1 系統若委由外部供應商開發，供應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。

5.12.2 委外供應商應確實控管程式與文件版本之一致性。

5.12.3 委外供應商進行系統開發與維護時，不得任意複製或攜出本校限閱(含)等級以上之業務資料。

5.12.4 委外供應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。

5.12.5 若系統、軟體由委外供應商開發者，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。

5.12.6 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，須經資訊單位主管人員同意以後，方可實施。

5.13 系統帳號管理

5.13.1 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，應由各系統管理者保管，不得直接授與委外供應商使用。

5.13.2 委外供應商之人員如因作業需求，需對本校系統進行存取，應

參考「存取控制管理程序書」之相關管理規範。

5.13.3 委外供應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。

5.13.4 委外供應商人員對於系統之操作，本校各系統管理者應盡監督之責，委外供應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供應商人員完成工作後檢視系統紀錄。

5.14 緊急應變計畫

5.14.1 資訊作業委外若涉及本校之關鍵業務時，應要求委外供應商配合本校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。

5.14.2 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。

5.15 可攜式電腦及儲存媒體管理

5.15.1 委外供應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人員進出機房登記表，人員進出機房登記表應定期由權責主管審閱。

5.15.2 供應商維修人員，當進入機房重地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。

5.16 例外作業

5.16.1 資訊委外服務之主辦單位應遵循本程序書之規範，提出適當安全需求項目。但若因成本、時效、委外服務之特性、委外供應商之局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，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。

5.17 服務變更管理

5.17.1 委外供應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：

5.17.1.1 系統網路架構改變。

5.17.1.2 使用新的技術。

5.17.1.3 產品轉換至新版本。

5.17.1.4 新的開發工具及環境。

5.17.1.5 服務設備之搬遷。

5.17.1.6 更換服務提供供應商或服務人員。

5.18 專案管理

5.18.1 本校各項資訊作業專案管理，依據 PMBOK 規範，分別考量下列五個程序中的資訊安全要求：

5.18.1.1 起始程序 (Initiating Processes)：專案啟動前，須遵循本校「風險評鑑與管理程序書」評估專案運作過程對於現有資訊流程的風險。

5.18.1.2 規劃程序 (Planning Processes)；在定義專案目標及選擇最佳方案時，須考量資訊安全需求為何，並將其納入規劃中。

5.18.1.3 執行程序 (Executing Processes)：執行專案時，須考量各項資訊流程的存取控制以及資訊傳遞的安全要求，並留下相關紀錄備查。

5.18.1.4 控制程序 (Controlling Processes)：專案監督過程須注意所規劃之安全事項，是否皆已實作，並確認其符合性。

5.18.1.5 結案程序 (Closing Processes)：結案所牽涉的資訊移轉或專案中止後之資料銷毀與歸還，皆須納入考量，並確保存取控制已被規劃與實作。

5.19 使用雲端服務安全管理

5.19.1 獲取階段

5.19.1.1 應識別欲採用雲端服務之利害關係人，並蒐集與考量來自各利害關係人的期待與建議。

5.19.1.1.1不得使用中國大陸等不安全之雲端服務平台，如百度、騰訊等。

5.19.1.1.2雲端服務供應商應取得國際資訊安全相關認證，並確認其認證有效性。

5.19.1.2 依「資訊安全組織程序書」及「文件管理程序書」執行適用法規與利害關係人盤點，對其變更進行評估。

5.19.1.3 依組織相關政策與程序識別雲端資訊資產及其風險，並實施帳號權限管理、運作與通訊安全管理、系統開發或系統獲取之相關風險管理。

5.19.1.4 評估使用雲端服務前使用之雲端服務層級（如 SaaS、PaaS、IaaS 等）、雲端服務之目的與範圍、雲端服務使用期限、雲端服務的服務水準協議(SLA)。

5.19.1.5 宜訂定資料遷移至雲端及資料退出雲端之管理計畫。

5.19.1.6 宜訂定雲端資料保留、備份與刪除計畫。

5.19.1.7 如相關服務使用公有雲，即認定為本公司雲端服務專案，應建立「雲服務使用管理表」。

5.19.2 使用及管理階段

5.19.2.1 應與雲端服務提供者建立正式服務契約或服務水平協議，並依合約執行資訊安全管理。

5.19.2.2 應建立與雲端服務提供者專責聯繫窗口，確保相關服務期間諮詢及申請支援等情事可被順利且即時的執行。

5.19.2.3 使用 IaaS 或 PaaS 服務時應考量：

5.19.2.3.1 宜定期相關產出雲端服務報告或使用紀錄，如主機容量監控、CPU 負載、記憶體使用量、儲存使用空間、網路使用頻寬等項目。

5.19.2.3.2 雲端服務使用範圍所需的資料和配置資訊需備份，應遵循「備份管理說明書」執行備份作業。

5.19.2.4 使用 SaaS 服務時應考量：

5.19.2.4.1 確認關閉不必要之通訊埠與共用資料夾。

5.19.2.4.2 確認雲端服務有相關網路入侵防護、實體入侵防護、監測活動管理或防毒機制。

5.19.2.4.3 宜建立加密機制，如網際網路資料傳輸加密、資料儲存加密等。

5.19.2.5 宜定期執行雲端服務中斷之營運持續演練。

5.19.3 變更及退出階段

5.19.3.1 雲端服務組態變更，記錄相關變更軌跡。

5.19.3.2 組織想要退出雲端服務時，服務提供者應在適當的時間範圍內提供支持和服務的可用性；應視雲端服務架構大小、

複雜度、資料量大小，提供相關服務移轉或退出的作業時間，宜依資料退出雲端之管理計畫執行。

5.19.3.3 當在服務提供期間或服務終止時被請求時，提供並返回雲端服務客戶擁有的資訊，例如設定檔、原始程式碼和資料。有關資產歸還之管理應遵循相關之雲端資料保留、備份與刪除計畫。

6 相關文件

6.1 保密切結書。

6.2 雲服務使用管理表。