OOOO 公司

業務委外管理作業程序

ISMS-B-010

版本 1.0

中華民國 105 年 MM 月 DD 日

文件編號	ISMS-B-010	業務委外管理作業程序	文件類別	限閱
版　　次	V1.0		發布日期	105/MM/DD

1. 目的

為維護 OO 公司（以下簡稱本公司）為辦理本公司相關資訊作業委外服務有所參照或依循，特訂定本程序。

2. 範圍

適用於本公司資訊安全管理制度所涵蓋範圍內之作業流程，所辦理之資訊服務委外作業，如服務提供、硬體建置與維護、軟體建置與維護等之資訊系統相關的變更及維護活動。。

3. 權責

3.1 主辦單位

3.1.1 編列專案預算。

3.1.2 負責提出明確需求內容、數量與作業時程等。

3.1.3 簽請資訊作業准予委外服務。

3.1.4 草擬委外需求規格書及合約，並提出適當之安全需求及擬定與廠商服務相關合約內容，並確實在合約中訂定委外廠商保密協議書或保密條款。

3.1.5 負責制訂投標須知內容。

3.1.6 依需求規格書評估廠商資格及保密作業情形。

3.1.7 與委外廠商簽定保密切結書，要求委外廠商遵循保密切結書內容。

3.1.8 管理及督導委外廠商及人員之作業，以符合資安相關規定及合約要求。

3.1.9 辦理驗收作業。

3.2 採購單位

3.2.1 委外採購案之簽核作業。

3.2.2 負責委外開標或議價，簽約、驗收等行政業務。

3.3 委外廠商、供應商(者)

3.3.1 依契約內容要求，執行本公司委託之業務作業、設備或服務之提供者，均為委外廠商。

3.3.2 依需求規格書要求，提供完整的工作說明書或專案管理計畫書並依限完成。

3.3.3 按照合約要求及雙方協議規定執行保密作業。

3.3.4 配合本公司資訊安全政策及資訊安全相關規定辦理。

3.4 資訊安全工作分組及專員

協助進行相關資訊安全、個人資料保護管理之需求諮詢、審查與提供建議。

4. 定義

4.1 委外廠商、供應商(者)
依契約內容要求，執行本公司委託之業務作業、設備或服務之提供者，統稱為委外廠商。

4.2 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。

4.3 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。

5. 作業內容

5.1 委外或供應服務之提出

5.1.1 主辦單位因業務需求提出資訊委外服務或供應服務時，應適當評估服務之必要性。

5.1.2 若為實體設備或軟體之採購案，主辦單位應對系統需求做適當規劃，以確保足夠的資訊處理能力及儲存容量。

5.2 資產辨識與風險管理作業

5.2.1 主辦單位應依據【資訊安全管理作業程序】、【資訊資產管理作業程序】，依照標的之資訊資產價值的機密性、完整性、可用性及個人資料等級，適當評估其可能威脅及弱點之風險評估。

5.2.2 依據上述風險評估結果，應識別及規定特別處理委外廠商或供應商存取資訊系統之安全控制措施，並進行風險管理作業，選擇適用之安全控制措施，並明訂於合約或安全事項要求之中。

5.2.3 控制措施之考量選擇包括但不限於下列作業：

5.2.3.1. 識別及紀錄，本公司將允許存取相關資訊的委外廠商或供應商之型式，例如 IT 服務、後勤公用設施、財務服務、IT 基礎建設組件等。

5.2.3.2. 界定不同委外廠商或供應商之資訊存取型式與授權，並監視及控制其存取過程及程序。

5.2.3.3. 以基於營運需求之最低資訊安全要求和風險狀況與個別委外廠商或供應商協議，其所需資訊與資訊存取型式。

5.2.3.4. 實施確保資訊或各方提供資訊處理之完整性之控制措施。

5.2.3.5. 明訂發生事故或應變時，委外廠商或供應商與公司之雙方責任；必要時，安排回復及應變，以確保資訊或各方提供資訊處理之可用性。

5.2.3.6. 委外廠商或供應商之人員，接受必要之資訊安全認知訓練。

5.2.3.7. 資訊安全要求及控制措施之情況將由雙方簽署書面協議。

5.2.3.8. 管理必要之資訊、資訊處理設施及物品的傳送，並確保整段傳送期間之資訊安全。

5.2.4 與委外廠商或供應商之協議， 應包含因應與資訊、通訊技術服務及產品供應鏈關聯之資訊安全風險責任承擔，例如：

5.2.4.1. 獲取資訊及通訊技術產品或服務的資訊安全要求。

5.2.4.2. 對資訊及通訊技術產品，若上述產品包括採購自其他供應商之組件，則要求委外廠商或供應商應負責對整個供應鏈傳遞適切的安全實務。

5.2.4.3. 管理委外廠商或供應商不再營運，與因技術進展而不再提供相關組件之風險責任。

5.2.5 上述作業之安全需求項目，由資訊安全推動組協助進行相關資訊安全、個人資料保護之諮詢、審查與提供建議。

5.3 委外廠商、供應者之評估

5.3.1 有委外需求時，應依據招標或採購相關作業管理辦法辦理，篩選合格廠商。

5.3.2 主辦單位於招標規格相關文件，應載明保密要求，必要時要求廠商，提供資安認證之相關佐證資料。

5.3.3 主辦單位於進行委外廠商資格評估時，可自行擬定評估方式及格式，惟應於執行後留下紀錄備查。

5.3.4 主辦單位及相關單位根據委外業務性質依「資訊作業委外合約檢核表」進行檢核合約內容對委外廠商規範之完備性，並將此檢核表簽核後留存備查。

5.4 委外廠商、供應者管理規定

5.4.1 委外廠商須依專案規模，提供完整之工作說明書或專案管理計畫書，需針對專案目標、範圍、時程、組織(雙方)、配合事項、管理機制、服務水準、變更要求等作一完整、實際具體之陳述。

5.4.2 委外廠商應依本公司之相關規範，簽署委外廠商保密協議書或保密切結書或於合約中明訂保密協議，並視需求另行要求委外廠商人員，簽署資訊業務外部人員保密切結書。

5.4.3 委外廠商若有違反相關規定或表現不佳，於接獲通知後須配合改進或人員撤換。

5.4.4 本公司發生資安事故時或委外廠商發生資訊安全事件時，應立即通報本公司專案窗口人員，依【資訊安全事故管理作業

程序】處理。

5.4.5 本公司舉辦災害復原演練時，須配合執行演練計畫。

5.5 一般安全要求

5.5.1 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，並配合本公司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。

5.5.2 委外廠商人員，於執行或支援業務時所獲知限閱級(含)以上之資訊，不得對外透露或以任何型式散播。

5.5.3 委外廠商處理個人資料及機敏性資料時應遵守個人資料保護、資訊安全之相關法令及法規以及本公司相關規定辦理。

5.5.4 委外廠商履行合約所提供之軟體或交付之標的物，需具備合法性，不得違反智慧財產權之規定或侵害第三人合法權益，如有違反事情發生，應由承包廠商負責處理並承擔所有一切法律責任。

5.5.5 委外廠商使用之工具軟體、處理作業、維護或異常處理之執行紀錄，本公司得視需要查檢或稽核，廠商不得異議。

5.5.6 委外廠商如因其員工執行業務之過失，而造成本公司損失或傷害，委外廠商需負損害賠償責任。

5.5.7 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。

5.5.8 合約完成或終止時，本公司所提供機敏性之資訊、資產，委外廠商應依合約要求，歸還本公司或銷毀，相關歸還與銷毀之作業紀錄應留存備查。

5.5.9 於合約期間出入本公司辦公場所時，需依相關規劃換證或申請臨時出入證，除工作場所外，勿隨意於其它辦公場所走動，若需於非上班時間加班作業時，應事先提出申請，以利管控人員出入。

5.5.10 委外廠商之人員不得存取未經授權之資訊資產，如因作業需求，需對本公司系統或資料進行存取，應依據【存取控制管理作業程序】之相關管理規範辦理。

5.5.11 攜帶筆記型電腦、行動裝置設備至本公司，應依據【通訊與作業管理作業程序】辦理。

5.5.12 若因維護或其它需求須使用特定之資訊環境設定或網路 IP 時，應依據【通訊與作業管理作業程序】辦理，提出申請並由本公司權責單位負責配置。

5.5.13 委外協議或合約內應明訂作業、使用或服務範圍、雙方之權利義務、維護與管理之作業權責、發生服務中斷或障礙時雙方之作業權責及責任歸屬和緊急應變時雙方之作業權

責、作業程序及所應提供之資源、時效，同時本公司應定期及不定期查核委外廠商是否確實執行,並留存查核紀錄。

5.6 硬體採購與維護要求

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。

5.7 系統開發及維護要求

5.7.1 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，經由本公司相關人員確認後方能執行。

5.7.2 委外廠商應確實控管程式與文件版本之一致性。

5.7.3 委外廠商進行系統開發與維護時,不得任意複製或攜出限閱級(含)以上之資料。

5.7.4 委外廠商需針對交付之應用系統軟體,應保證系統內不含後門程式、隱密通道及特洛伊木馬程式等惡意程式。

5.7.5 委外廠商交付之系統軟體，應由本公司人員測試，以確定符合相關需求後，方得依照【資訊系統獲取、開發及維護管理作業程序】之程序進行上線及驗收。

5.7.6 系統開發與修改需遵守本公司【資訊系統獲取、開發及維護管理作業程序】之規定，若有例外者，需經資訊單位主管人員同意以後，方可實施。

5.8 系統帳號管理要求

5.8.1 委外之系統軟體或作業系統最高權限帳號、資料庫最高權限帳號，應由本公司處理並由作業管理人員保管，不得直接授與委外廠商使用。

5.8.2 委外廠商人員對於本公司系統之帳號密碼應善盡保管之責，帳號密碼不得任意交由非作業相關人員使用。

5.8.3 委外廠商人員不得從事非工作範圍內之系統,同時對於系統之各項操作，本公司各系統管理者應盡監督之責，並應於委外廠商人員完成工作後檢視各系統紀錄。

5.9 緊急應變計畫

5.9.1 資訊作業委外若涉及本公司之關鍵業務時,應要求委外廠商建立並交代緊急應變計畫，並配合本公司定期進行測試。

5.9.2 主辦單位可依據不同資訊資產價值及可用性等級要求,考量其備援需求，必要時，得建立異地備援機制。

5.10 可攜式電腦及儲存媒體管理

5.10.1 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公司機房使用，需經機房管理人員及陪同之單位承辦人員同意並註記於人員進出機房

登記表；於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公司人員全程陪同。

5.11 服務變更管理

5.11.1 委外服務內容若有重大變更時，主辦單位應審查是否影響相關資訊安全管理制度或依循標準之要求，評估其風險，採取適當控制措施，並經主辦單位主管核可後，方能進行變更。

5.11.2 重大服務內容變更如下：

5.11.2.1. 使用新的技術。

5.11.2.2. 產品轉換至新版本。

5.11.2.3. 新的開發工具及環境。

5.11.2.4. 服務設備之搬遷。

5.11.2.5. 更換服務提供廠商或服務人員。

5.12 委外合約之資訊安全條款內容要求要點如下：

5.12.1 乙方須配合本公司資訊安全政策、資訊安全相關規定及本公司主管機關相關規範辦理，甲方得定期及不定期查核乙方須是否確實執行。

5.12.2 乙方因處理委託案，需存取甲方之資訊資產時須經甲方之同意，並簽署委外廠商保密協議書或資訊業務外部人員保密切結書並遵守本公司資訊安全規範後始得為之，同時僅可存取經甲方授權之資訊資產。

5.12.3 乙方派駐本公司人員或派至本公司服務人員，應接受本公司之資訊安全教育訓練。

5.12.4 乙方及其工作人員因履行本契約而取得之甲方業務資料，未經甲方同意，不得揭露與本契約履行無關之第三人；本契約因期限屆滿、解除或其他原因而終止時，乙方及其工作人員仍負有前款之保密責任。

5.12.5 乙方如發生資訊安全事件時應即通報甲方，並按甲方之【資訊安全事故管理作業程序】處理；甲方舉辦災害復原演練時，須配合執行演練計畫。

5.12.6 得標委外廠商簽訂委外合約時，若需再委外於其他協力廠商合作時，須於委外合約中列示，同時由本公司與委外廠商事前協定，得標委外廠商與再委外協力廠商之業務分工事項，並於合約內載明，否則不可有再委外之作業。

5.12.7 再委外之協力廠商其權利義務視同得標委外廠商，需簽署委外廠商保密協議書或資訊業務外部人員保密切結書並遵守本公司資訊安全規範，同時得標委外廠商需對委外之協力廠商負連帶責任。

5.12.8 乙方處理委託案時應考量並承擔，包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險與責任。

5.13 例外作業

資訊系統委外服務之主辦單位應遵循本程序之規範，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，而致本程序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。

6. 相關資料

6.1【資訊安全事故管理作業程序】

6.2【存取控制管理作業程序】

6.3【通訊與作業管理作業程序】

6.4【資訊系統獲取、開發及維護管理作業程序】

6.5【資訊安全管理作業程序】

6.6【資訊資產管理作業程序】。

7. 附件

7.1 資訊作業委外合約檢核表