國立空中大學資訊委外服務資訊安全管理事項

經98.11.10國立空中大學98學年度第1次資訊環境規劃委員會通過
經100.11.22國立空中大學100學年度第1次資訊環境規劃委員會修正通過

壹、資訊安全組織

本校資訊委外服務之承包廠商(含分包廠商)以下統稱為委外廠商，配合本校資訊安全管理，應指定專案管理人員，負責督導業務相關人員並推動下列資訊安全管理事項：

一、資訊安全政策之核定、核轉及督導。

二、資訊安全責任之分配及協調。

三、資訊資產保護事項之監督。

四、資訊安全事件之檢討及監督。

貳、委外廠商需遵守之資訊安全控制措施說明

委外廠商必須認知遵守本校資訊安全控制措施之義務，並接受涉及存取、處理、通信或管理機關資訊與資訊處理設施的各項基本責任與強制責任並配合達到本校資訊安全要求：

一、本校資訊安全政策。

二、資產保護的控制措施，包括：

（一） 保護機關資產(包括資訊、軟體及硬體)。

（二） 遵守任何所需的實體保護控制措施與機制。

（三） 確保不受惡意軟體攻擊的控制措施。

（四） 遵守任何資產損害發生(如資料、軟體及硬體的遺失或被修改)之處理程序。

（五） 遵守契約終了或議定某一時間點，資訊和資產歸還或銷毀之控制措施。

（六） 確保機關資產的機密性、完整性、可用性與任何其他相關特性。

(七) 遵守對複製和揭露資訊，以及使用機密協議的各項限制條件。

（八） 必須參與使用者與行政管理人員在方法、程序與安全上的教育訓練。

（九） 委外廠商管理階層及委外人員必須對其配合之資訊安全責任與事宜有明確認知，同時並遵守「個人資料保護法」及本資訊安全

管理事項之相關規定，並應分別簽訂「委外廠商保密協議書」及「委外廠商人員保密切結書」。

（十） 遵守本校對於委外人員調任之規定。

(十一)遵守本校軟硬體安裝與維護的相關責任。

(十二)明確的通報結構和議定的通報格式。

(十三)變更管理的明確且已規定之過程。

(十四)存取控制政策，涵蓋：

1. 委外廠商配合委外業務執行之存取需求必須先申請，核准授權後在授權範圍內及有效時間內方可進行存取。
2. 必須使用核准識別符(如使用者ID 和通行碼)，並善盡保管之責。
3. 禁止所有未明確授權之存取。
4. 必須即時通報、通知資訊安全事故及安全違例事項，並配合事故與事件之相關調查。
5. 委外廠商及其委外人員必須遵守智慧財產權及保護著作權轉讓本校之共同著作。
6. 委外廠商均應遵守本存取控制政策。

參、委外人力資源安全

委外廠商必須篩選委外人員以降低竊盜、詐欺或設施誤用的風險，並遵守契約條款闡明廠商應負之安全責任。

一、人員派駐前

（一） 承包廠商(含分包廠商)依相關法律、法規及倫理篩選合格人員。

（二） 委外廠商派駐人員之學經歷必須遞交本校檢核並確認派駐人員之學歷與專業資格。

（三） 本校保有對於委外廠商之派駐人員提出獨立身份檢核（護照或類似文件）及進行銀行信用核對或犯罪紀錄檢核。

（四） 遇資訊安全事故及發生安全違例事項，本校授權人員得進行獨立身份檢核及進行銀行信用核對或犯罪紀錄檢核，委外廠商不得拒絕。

二、派駐期間

（一） 派駐人員須接受本校資訊安全政策與程序相關之教育訓練

（二） 派駐人員須接受包括安全要求、法律責任和營運控制措施，及資訊處理設施的正確使用訓練。

（三） 派駐人員必須即時通報資訊安全事故及安全違例事項，不得隱瞞。

三、懲處罰則

（一） 派駐人員發生嚴重不當行為違反相關資安政策，須立即暫停職務、存取權限與特權，必要時立即將其護送出該場域。

（二） 派駐人員違反相關資安政策，依契約相關罰則進行處置，如情節造成重大資安事件達「國家資通安全通報應變作業綱要」等級3以上，本校將立即終止及解除契約，並自負違反法律之責。

（三） 本校保有本校及與第三方稽核單位或人員至委外廠商進行契約內資訊安全相關作業稽核之權利，廠商不得拒絕。

四、派駐終止或變更

（一） 委外專案完成、契約或協議終止後，委外廠商及其派駐人員仍須遵守契約中機密性協議之責任。

（二） 委外作業完成、契約或協議終止，委外廠商及其派駐人員須歸還擁有本校之所有資產，包括借用及刻正使用之軟體、文件、設備，存取卡、軟體手冊及儲存於電子媒體之資訊等需一併歸還。有關歸還方式如下：

1. 若委外作業由廠商提供或使用設備，廠商需將所有相關的資訊移轉回本校並安全地自設備上清除歸還本校，如為廠商擁有之設備化電子媒體，廠商需在本校見證下安全地自設備上清除。本校保有至廠商檢核設備之權利。

2. 若承商擁有對進行中之運作重要的知識，宜將該資訊文件化並移轉回本校。

（三） 委外作業完成、契約或協議終止，委外廠商及其派駐人員對資訊及資訊處理設施的存取權限本校將立即移除，並移除資訊系統及服務相關之資產的存取權限。

五、委外實體與環境安全

（一） 委外廠商及其派駐人員未經授權，不得進入本校關鍵或敏感的資

訊處理安全區域，防止未經授權的實體存取、損害及干擾。

（二） 本校安全區域均設門禁管制系統，並依業務權限給予不同門禁之授權，委外廠商及其派駐人員經授權核准持通行卡進出安全區域，不得交換門禁通行卡，以確保安全區域之機密性、完整性及可用性。

（三） 委外廠商及其派駐人員因業務所需，必須攜入資訊設備，包括個人電腦、個人數位助理、行動電話、智慧卡等，必須先經本校單位管理階層授權核准，方能使用，必要時本校資訊安全管理人員得檢視廠商及派駐人員攜入資訊設備。

六、委外之作業管理

（一） 委外人員必須遵循本校各式開機與關機程序、備份、設備維護、媒體處置、電腦機房與郵件處置管理文件之作業程序，不可隨意變更或違反程序。

（二） 委外人員於執行業務所產生對資訊處理設施與系統之變更須先經核准授權後方可進行變更。進行變更前，須填寫變更計畫書及復原程序，包括不成功的變更和意料之外事件的中止和復原之程序，變更完成後記錄含所有相關資訊的稽核日誌。

（三） 委外人員須依循業務掌管領域進行各項業務之委辦，禁止未經授權或非意圖的修改或誤用及未經授權或未受偵測的存取、修改或使用資產。

（四） 委外廠商執行委外開發、測試及運作專案時，須分隔開發、測試及運作之設施，以降低對運作系統未經授權存取或變更的風險，必須採取以下控制措施：

1. 將軟體由開發移轉到運作狀態的規則，須加以定義及文件化。
2. 開發和運作之軟體必須於不同的系統或電腦處理器上運轉，且位於不同的網域或目錄。
3. 未經授權前，不得自運作之系統存取編譯器(Compiler)、編輯器(Editor)和其他開發工具或系統公用程式。
4. 測試系統環境應模擬實際運作系統環境。
5. 運作測試系統，須使用不同使用者測試帳號，功能選單並顯示適

切的識別訊息以降低錯誤的風險。

6. 敏感資料不得複製至測試系統環境。
7. 預先規劃與準備，確保足夠容量與資源達成規範要求之系統效能，並對未來的容量要求預作規劃，降低系統超載風險。
8. 降低委外開發或維護資訊系統失效之風險，新系統驗收與使用前，委外廠商須配合進行下列審查措施：

(1) 硬體採購與維護

- 委外廠商應提供所交付設備之架構、操作、管理、維護等相關操作手冊、文件與技術支援服務，如必要應提供教育訓練課程。

(2) 軟體委外開發相關事項

- 新系統授權作業、程式碼所有權及智慧財產權等之移轉至本校。
- 委外廠商須確保品質驗證和工作執行的準確性。
- 預防委外廠商因故無法執行契約，廠商須定期交付系統各式文件及程式碼，作為日後託管作業之依據。
- 委外廠商於委外工作完成時，須提供為稽核品質和正確性所需的存取權限。
- 委外廠商之程式碼品質須符契約規範要求。
- 委外廠商須依契約交由第三方於安裝前進行測試，檢查是否有惡意程式和特洛伊木馬程式、SQL Injection及Cross Site Scripting。

(3) 訂定新系統被認可及納入正式作業的標準，並在新系統上線作業前，執行適當的測試。

(4) 委外開發產製新系統被認可及納入正式作業，委外廠商須執行以下事項：

- 評估系統作業效能及電腦容量是否滿足本校需求。
- 檢查發生錯誤後之回復作業及系統重新啟動程序的準備作業，以及資訊安全事件之緊急應變作業是否已經完備。
- 進行新系統正式納入例行作業程序之準備及測試。

- 選定經評估過的安全控制措施並提出相關文件。
- 制訂有效的手動作業程序並製作為標準程序書。
- 符合本校營運持續管理要求。
- 評估新系統的建置不致影響現有系統作業及對系統尖峰作業時段之影響。
- 辦理新系統作業及使用者教育訓練。
- 新系統作業應為容易使用，且不影響使用者工作並避免產生錯誤。

(5) 在開發系統時，應確定系統功能及系統效能符合契約規範，在系統開發每一階段，充分諮詢相關人員意見。新系統上線作業前，應執行適當測試作業，以驗證系統功能符合既定的標準。如係委由第三者執行查核與驗證事宜，則應舉行專案聯席會議，確定專案進行程序與作業紀錄之表單等，確保專案順利進行。

（五） 廠商服務交付管理

1. 本校定期檢視及審查委外廠商提供之服務、報告與紀錄，並定期執行稽核，確保委外廠商遵守協議中的資訊安全條款與條件，且資訊安全事故和問題均受到妥適管理，定期檢視及審查委外廠商目的為：

(1) 檢視服務效能等級以查核協議的遵守程度。

(2) 依協議審查廠商產出的服務報告，並安排定期的進度會議。

(3) 依協議與任何支援指導綱要與程序之要求，提供關於資訊安全事故的資訊，並由廠商與本校審查該資訊。

(4) 審查與所交付服務相關的安全事件、運作之問題、失效、失誤追蹤及中斷等的廠商稽核存底與紀錄。

(5) 解決並管理所有已識別出的問題。

2. 本校基於維持與改進現有的資訊安全政策、程序及控制措施，對於廠商委外之所提供服務之變更列入管理，並對於變更所衍生引發之風險重新評鑑，委外廠商服務變更列入管理項目如下：

(1) 網路的變更與加強。

(2) 新技術的使用。

(3) 新產品或較新版本發行的採用。

(4) 新開發工具和環境。

(5) 服務設施實體位置的變更。

（六） 委外廠商於委外作業中不得安裝非授權軟、硬體（含各式資訊、通訊設備載體及可攜式媒體），並依規定安裝各式防護軟體及遵守各項管制措施，防止及偵測惡意碼與未經授權行動碼的植入，保護軟體與資訊的完整性，本校資訊安全管理者保有將檢核委外廠商使用之資訊設備之權利，防止、偵測及移除惡意碼與控制行動碼。

（七） 委外廠商對於委外作業有關之媒體之使用、存取、移除與報廢，必須經過授權方能遂行後續作業，防止資產被未經授權的揭露、修改、移除或破壞及營運活動的中斷，並防止文件、電腦媒體(例如：磁帶、磁碟)、輸入、輸出資料及系統文件被未經授權的揭露、修改、移除及破壞。

1. 本校可攜式媒體包括磁帶、磁碟、快閃磁碟、抽取式硬碟、光碟(*CD*)、數位視訊影碟(*DVD*)及印出之媒體，委外作業人員使用之可移除式媒體必須經過授權核准，避免資訊外洩或惡意碼入侵，並遵守下列原則：

(1) 若不再需要，任何從本校移除之可再利用媒體的內容，應使其無法復原(如備份之磁帶、可覆寫光碟片)。

(2) 若需要及實際可行時，從本校移除媒體宜需要授權，並保存該筆移除紀錄，維持稽核存底。

(3) 委外廠商攜帶可攜式媒體進入本校應受程序管制或限制。

(4) 委外廠商須遵守本校書面記載所有程序與授權等級。

2. 委外廠商經委外作業產製之系統文件須進行保護，禁止未經授權之存取，並遵守下列管控措施：

(1) 須於相關文件規定與載明資訊安全控制措施，以利使用者及電腦支援人員明瞭電腦系統內建之安控系統功能。

(2) 系統文件在每次完成變更作業後，應立即更新，舊版的系統

文件亦應妥善保管及處理。

(3) 確保操作文件和使用者程序根據需要作適切變更。如資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支援程序、營運持續管理計畫、預備作業計畫等。

(4) 委外作業人員辦公桌面必須淨空，減少文件及儲存媒體等於正常的辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

(5) 委外作業人員離職必須繳回機關資產，包括所發給的軟體、文件及設備，例如行動式電腦設備、憑證、手冊及其他必須繳回之電子媒體。

(6) 電腦及網路之日常管理作業，例如開關機程序、資料備援、設備維護、電腦機房之安全管理之作業程序應視為正式文件，作業程序的更改必須經權責單位核准。

(7) 保全委外作業系統文件須符合下列規定：

- 系統文件宜安全地存放。
- 系統文件之存取清單須維持最簡短且經應用系統擁有者授權。
- 放在公眾網路上或透過公眾網路提供的系統文件宜加以妥善保護。
- 系統文件可包含一系列的敏感資訊，例如：對應用過程、程序、資料結構及授權過程等之說明。

七、委外使用者存取管理

為確保未經授權委外作業人員對資訊系統的存取，委外廠商必須遵守下列存取控制規定：

（一） 委外作業人員必須經過系統擁有者授權使用資訊系統或服務。

（二） 委外作業人員所授予之存取權限等級，不得交換權限、違反資訊安全政策及違反職務區隔。

（三） 委外作業人員必須遵守委外作業人員存取權限書面聲明。

（四） 委外廠商及委外作業人員均應簽署聲明，表示瞭解其存取的限制及保密義務。

（五） 委外作業人員於完成授權程序前不得存取及開放所提供服務。

（六） 委外作業人員必須維護所有註冊使用該委外服務使用者之正式紀錄。

（七） 委外作業人員必須使用本校所核發之「唯一」帳號進行委外作業，不得交換及私自設定授權以外之帳號。

（八） 委外作業人員因變更角色或調職或離職後，本校立即移除並封鎖其存取權限。

八、委外資訊安全事故管理

委外廠商必須配合本校相關教育訓練，確保委外作業相關之資訊安全事件與弱點，採取及時矯正措施的方式傳達，認知及熟悉資產安全造成衝擊之不同型式事件與弱點之通報程序，並立即向指定的聯絡點通報任何資訊安全事件與弱點，通報程序包括：

（一） 記錄資安事件的作業處理程序，確保資安事件回報處理或撰寫資安事件檢討(或結果)報告。

（二） 資訊安全事件報告須支援回報行為，及協助回報人員記錄在資訊安全事件所有必要的行為狀況。

（三） 發生資訊安全事件狀況後的正確行動

1. 記錄所有重要細節(例如：螢幕上出現的錯誤訊息及奇怪的現象)。
2. 除規定的處理程序外(例如：中毒時，應先行拔掉網路線以防止擴散)，應立即通知相關人員處置，不得隨意執行任何動作。

（四） 資訊安全弱點之反映

1. 委外人員須隨時注意資訊系統或資訊服務施設內部安全弱點、可能面臨之威脅，並立即向本校業務承辦人或主管報告。
2. 系統安全之弱點，須回報專業人員處理，不得由系統使用者自行修改。

（五） 軟體功能不正常之反映

委外作業人員發現軟體功能出現異常時，應迅速告知本校業務承辦人或向主管報告並要求資訊單位支援。

九、遵循適法性要求

委外作業含括資訊系統設計、運作、使用及管理都須受法律、法令、法

規或契約之安全要求所規範，本校明確界定、文件化委外作業所參照之規範並維持最新狀態。