



委外管理程序書

文件編號：NDHU-I-B-11

機密等級：限閱

單位：國立東華大學

版次：1.1

發行日期：113 年 12 月 30 日

[illegible]

目錄

1 目的 1

2 適用範圍 1

3 權責 1

4 名詞定義 1

5 作業說明 1

6 相關文件 9

1 目的

本程序書制訂之目的在於確保國立東華大學（以下簡稱「本校」）資通委外作業安全管理有所依循，以符合資通安全規範。

2 適用範圍

2.1 適用於本校委外資通作業項目，包括：

- 2.1.1 主機系統採購與維護。
- 2.1.2 網路相關硬體設備採購與維護。
- 2.1.3 網路相關線路服務租用。
- 2.1.4 應用系統委外開發及維護。
- 2.1.5 應用系統套裝軟體客製化及維護。
- 2.1.6 專業顧問服務。

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委外服務相關契約內容，並確實在契約中訂定保密條款。

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。
- 3.2.2 對於服務提供廠商之遴選，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以竊取未授權資訊之惡意程式。
- 4.3 後門程式：會竊取電腦內的資料(如：帳號、密碼、檔案等)與操控對方的電腦(被控端)的程式。
- 4.4 服務水準協議(Service Level Agreement, SLA)：指服務提供者與使用客戶之間，應就服務品質、水準以及性能等方面達成協議或訂定契約。

5 作業說明

5.1 委外管理通則

- 5.1.1 業務需求單位應依業務需求規劃專案，撰寫建議書徵求文件（Request For Proposal, RFP），其內容應明確表達專案需求、管理需求、執行專案過程之安全需求及交付項目之要求，如：架構、功能、時程、交付項目、安全、測試、驗收、技術移轉、教育訓練及保固需求等。
- 5.1.2 委外相關安全要求，應遵循「資通安全管理法」及其子法，先判定該資通系統之防護需求等級，依據「資通系統籌獲各階段資安強化措施」，於需求、建置及維運各階段，結合安全系統發展生命週期(SSDLC)，評估及執行各項要求，以確保程式開發安全，從而減少軟體中潛在安全漏洞與風險，並依循本程序書各項委外服務安全要求辦理。
- 5.1.3 委外廠商應提供作業維護聯絡窗口以及專線電話諮詢服務，以解決資通作業相關事宜，並配合本校作業辦理異常排除及事件通報事宜，如必要得提供駐點服務。
- 5.1.4 應與涉及存取、處理、儲存、溝通或管理本校資通系統的委外廠商簽訂契約，並將資通安全要求事項(例如保密條款等)納於契約中。
- 5.1.5 委外廠商於履行契約期間所使用之軟體，須為合法，並不得違反智慧財產權之規定，如有違法情事發生，委外廠商須承擔應負之法律責任。
- 5.1.6 委外廠商所使用之工具軟體以及處理作業之執行紀錄，本校有權進行稽核審查，廠商須配合提供相關資訊，不得異議。
- 5.1.7 委外廠商須留存本校作業異常處理紀錄，本校得視需要進行查核。
- 5.1.8 委外廠商所交付之標的物如侵害第三人合法權益時，委外廠商須負責處理並承擔一切法律責任。
- 5.1.9 委外廠商如其員工執行業務之過失，造成本校損失或傷害，委外廠商須負損害賠償責任。
- 5.1.10 委外廠商相關人員離、調職或專案完成時，系統管理人員應刪除其相關作業權限，如有借用設備、軟體，應繳回或移除。
- 5.1.11 委外廠商人員(或廠商由合作夥伴所調派之支援人員，例如原廠工程師)，於支援業務時所獲知敏感等級以上資訊，不得對外透露，為確保前述事項之落實，得要求其人員簽署「NDHU-I-B-11-03 保密切結書(受託單位)」及

「NDHU-I-B-11-04 保密切結書(受託者)」。

5.1.12 請購單位承辦人員須依契約類型填寫「NDHU-I-B-11-01 資通安全委外契約檢核表」，連同契約稿陳報單位主管審核確認其適用性。

5.2 委外資通作業服務需求

5.2.1 承辦單位因業務需求提出資通委外服務時，應適當評估資通委外之必要性。

5.2.2 依專案需求訂定廠商履約服務水準協議(SLA)。

5.2.3 業務需求單位應評估委外需求對機關資通安全風險之影響，並參考國家資通安全研究院頒訂之「資通系統委外開發範本」，擬定資通安全相關規範事項，若資通系統須納入主管機關機房共構統籌管理，委外服務廠商應配合主管機關資通安全要求辦理。

5.2.4 委外廠商違反上級機關或本校資通安全規範，造成有形或無形之損害時，本校有權要求廠商負損害賠償之責。

5.2.5 委外廠商應於專案開始時提出專案執行或維護服務計畫，且應於每階段工作完成後提供相關紀錄備查。

5.2.6 訂定委外作業終止時，廠商應配合辦理之移交事項。

5.2.7 針對本校風險評鑑後所提之風險處理(改善)計畫，業務需求單位應於契約中明定委外廠商須配合辦理各項風險改善建議措施。

5.3 硬體資通安全要求

5.3.1 若為主機系統之採購，承辦單位應對系統需求做適當規劃，以確保足夠之電腦處理及儲存容量(預估此電腦之資料處理與未來資料之成長量)。

5.3.2 資通訊硬體設備價值昂貴或取得不易(採購至出貨需超過3個月以上)者，需持續簽訂設備維護契約，必要時於契約中要求廠商提供緊急替代品，以備不時之需。

5.3.3 採購或維護硬體設備時，應要求廠商提供定期維護、技術支援、保固期限或維修更換等事項。

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

5.4 應用系統委外資通安全要求

5.4.1 委外廠商應依據委外服務需求或建議書徵求文件，設計及執行相關安全控制

措施，以達應用系統安全要求。

5.4.2 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、資料庫說明表等系統規格文件，經由本校相關人員確認後方能執行。

5.4.3 委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

5.4.3.1 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

5.4.3.2 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

5.4.3.3 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

5.4.3.4 受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

5.4.3.5 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

5.4.3.6 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知本校及採行之補救措施。

5.4.3.7 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

5.4.3.8 受託者應採取之其他資通安全相關維護措施。

5.4.3.9 委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

5.4.3.10 各機關自行或委外開發之資通系統應依「資通安全責任等級分級辦法」附表九所定「資通系統防護需求分級原則」完成資通系統分級，並依附表十所定「資通系統防護基準」執行控制措施。

5.4.4 委外廠商應確實控管程式與文件版本之一致性。

- 5.4.5 委外廠商進行系統開發與維護時，未經本校業務承辦單位主管授權，不得任意複製或攜出本校限閱等級以上之資料。
- 5.4.6 委外廠商應提供測試計畫，並備妥測試環境後，由專案承辦人員及業務需求單位等進行系統測試。
- 5.4.7 測試與正式系統所使用之環境及資料應獨立分開。
- 5.4.8 具機敏性之測試資料，應僅由系統管理人員進行存取，若須提供委外廠商測試資料，應將機敏性之資料內容移除或轉換為虛擬資料，或測試時由本校同仁陪同，測試結束後，應將資料刪除，如有特殊情況需使用實際資料，應請廠商至現場(到點)作業，由業務負責人員全程陪同；本校業務負責單位應提供測試環境與資料，測試完後應將資料立即刪除/銷毀。
- 5.4.9 應用系統上線前在資源允許的情形下，應進行原始碼檢測、弱點掃描，並提供相關檢測報告，以確保系統安全。
- 5.4.10 應用系統上線前，委外廠商應提供系統上線作業程序，並產出系統相關文件及交付程式原始碼、執行碼光碟。
- 5.4.11 委外廠商針對交付之系統，應出具切結書確保系統內不含後門程式、隱密通道及特洛伊木馬程式。
- 5.4.12 委外廠商須針對所交付之系統進行技術安全稽核，以確保系統之安全，並提供相關稽核報告(如：弱點掃描報告、滲透測試報告、Active 簽章認證或相關安全性檢測報告等)。
- 5.4.13 委外開發或維護之系統，於契約有效期間，若發現系統有安全漏洞，委外廠商須無償修改，惟修改方式及交付時間須經本校同意。
- 5.4.14 委外開發之系統，須經由本校業務承辦人員或需求單位測試及確認符合契約相關要求後，依據「NDHU-I-B-10 系統開發與維護程序書」之程序進行系統上線作業。
- 5.4.15 委外廠商對於系統開發之程式修改與作業需求，應遵守本校「NDHU-I-B-10 系統開發與維護程序書」之規定，如有例外，須經權責單位主管同意後，方可實施。

5.5 資料委外服務

- 5.5.1 代表本校處理資料之委外廠商應遵守本校契約及相關安全要求，未經本校許

可，不得將資料處理再行分包委外。經本校許可之再分包委外廠商亦應遵守本校相關安全要求。

5.6 系統帳號管理

- 5.6.1 委外開發之應用系統及相關之作業系統、資料庫系統等最高權限帳號，應由本校系統管理人員保管，除經授權，不得授予委外廠商使用。
- 5.6.2 委外廠商之人員如因作業需求，需對本校系統進行存取，應參考「NDHU-I-B-09 存取控制管理程序書」之相關管理規範，並依據「NDHU-I-C-04 網路管理作業說明書」填寫「NDHU-I-B-07-03 資訊服務申請單」提出申請，經權責單位主管核可後，方可開啟遠端服務。
- 5.6.3 「NDHU-I-B-07-03 資訊服務申請單」中應載明作業需求內容、所需權限、帳號有效時間，經由權責單位主管核准後，由系統管理者依照所需權限及帳號有效時間，開放必要之帳號供委外廠商人員使用。
- 5.6.4 委外廠商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。
- 5.6.5 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，委外廠商人員不得任意從事非工作範圍內之操作。各系統管理者應視需要於委外廠商人員完成工作後檢視系統紀錄。

5.7 可攜式電腦及儲存媒體管理

- 5.7.1 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時，須經權責單位同意，遵守相關設備管理之規定並註記於「NDHU-I-B-06-01 人員進出機房登記表」。
- 5.7.2 委外廠商維修人員進入機房時，須由本校業務承辦人員陪同或輔以錄影監視。

5.8 資產辨識與風險評鑑作業

- 5.8.1 承辦單位應依據「NDHU-I-B-03 資訊資產管理程序書」、「NDHU-I-B-04 資通安全風險評鑑與管理程序書」之規定，依照委外標的之資訊資產價值、機密性、完整性及可用性等級，適當評估其可能面臨之風險。
- 5.8.2 承辦單位依據上述風險評鑑結果，進行風險管理作業，並選擇適用之安全需求項目，明訂於契約中。

5.9 緊急應變計畫

5.9.1 資通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校定期進行業務永續計畫，並針對委外標的建立緊急應變計畫，定期進行演練；若該委外案件屬於整體委外者，應就委外系統及資料兩者中資訊資產價值取其高者，衡量演練週期。

5.9.2 備援需求

依據不同資訊資產之價值及可用性等級，考量其備援需求，必要時，得建立異地備援機制。

5.10 例外作業

資通委外服務之承辦單位應遵循本程序書之規範，提出適當之安全需求項目。若因成本、時效、委外服務之特性、委外廠商之侷限性等相關因素考量，而致本程序書所規範之安全需求無法適用時，承辦單位得以簽呈方式，提出其他適切之安全需求與規劃，提報權責主管批核。

5.11 委外服務監視審查

業務承辦人應定期監視、審查與稽核委外廠商的服務交付情形，必要時於專案驗收過程中詳細核對。

5.11.1 如涉及個資委外，委外廠商提供所蒐集之個人資料檔案、個人資料檔案保有之依據及特定目的、個人資料之類別等相關資訊及其蒐集、處理、利用之相關資料時，委外廠商不得拒絕，並應於機關指定期限內提供。經本校事前書面同意之複委託單位亦具有提供前開資料之義務。

5.11.2 如涉及個資委外，本校得針對委外廠商之個人資料安全維護措施執行狀況進行確認，並將確認結果記錄之；必要時，得派員進行實地訪查或委託專業人員進行查核，查核項目得參照「教育部主管目的事業之個人資料檔案自我檢查表」，委外廠商應予配合。查核後，認有缺失，應以書面敘明理由請委外廠商限期改善。

5.12 資料之刪除或返還義務

5.12.1 如涉及個資委外，於履約期間，本校得隨時要求委外廠商將執行契約或協議業務而蒐集、處理、利用之個人資料返還機關或予以刪除，且不得留存任何

備份。

5.12.2 如涉及個資委外，契約或協議終止或解除時，委外廠商應刪除或銷毀因履行契約或協議而保有之個人資料，且應返還個人資料之載體及移除存取資料之權限；並提供刪除、銷毀、返還個人資料之時間、方式、地點等紀錄。刪除、銷毀作業，本校於必要時，得實地查訪，委外廠商應予配合。

5.12.3 如涉及個資委外，契約或協議終止或解除時，得要求委外廠商移轉因執行受委業務所保有之個人資料，應留存移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據等紀錄。

5.12.4 如涉及個資委外，委外廠商應簽署「國立東華大學委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書正本交由本校收執。

5.12.5 委外專案所涉個人資料之重要性或機密性程度較高時，本校得要求委外廠商執行契約或協議之執行業務人員簽署「國立東華大學委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書正本交由本校收執。若專案人員異動，委外廠商需主動要求異動人員簽署「國立東華大學委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書交由本校收執。

5.13 委外服務變更管理

委外廠商所提供之相關服務內容如有重大變更應先行評估其風險，並留有相關紀錄，經由業務承辦人員呈單位權責主管核可後，方能進行變更，其服務變更內容提供參酌包括但不限於下列項目：

5.13.1 系統網路架構改變。

5.13.2 使用新的技術。

5.13.3 產品轉換至新版本。

5.13.4 新的開發工具及環境。

5.13.5 服務設備之搬遷。

5.13.6 更換服務提供廠商或服務人員。

5.14 委外廠商績效評鑑

5.14.1 為建立合格廠商資料庫，需求單位得進行委外廠商績效評鑑。

5.14.2 績效評鑑應填寫「NDHU-I-B-11-02 廠商績效評鑑表」，評鑑執行時可視需要自行新增評鑑標準，並留存紀錄。

6 相關文件

- 6.1 資通安全管理法及其子法。
- 6.2 資通系統籌獲各階段資安強化措施。
- 6.3 NDHU-I-B-03 資訊資產管理程序書。
- 6.4 NDHU-I-B-04 資通安全風險評鑑與管理程序書。
- 6.5 NDHU-I-B-08 通訊安全管理程序書。
- 6.6 NDHU-I-B-09 存取控制管理程序書。
- 6.7 NDHU-I-B-10 系統開發與維護程序書。
- 6.8 NDHU-I-C-04 網路管理作業說明書。
- 6.9 NDHU-P-C-02 個人資料委外監督控管作業說明書。
- 6.10 NDHU-I-B-11-01 資通安全委外契約檢核表。
- 6.11 NDHU-I-B-11-02 廠商績效評鑑表。
- 6.12 NDHU-I-B-11-03 保密切結書(受託單位)。
- 6.13 NDHU-I-B-11-04 保密切結書(受託者)。
- 6.14 NDHU-I-B-06-01 人員進出機房登記表。
- 6.15 NDHU-I-B-07-03 資訊服務申請單。
- 6.16 國立東華大學委外專案契約終止或解除資料確認刪除、銷毀及載體返還、移轉切結書