輔仁大學資通服務委外合約書附則

版本 115 01

壹、 資通服務之提供

第一條　廠商應充分了解及確實遵守資通安全管理法及其相關子法、個人資料保護法及其施行細則、著作權法、專利法、營業秘密法等相關法令之規定及行政院所頒訂之各項資訊安全規範及標準。

第二條　廠商辦理委託業務之相關程序及環境，應具備完善之資通安全、個人資料保護管理措施或通過公正第三方驗證；並配置充足且經適當資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全、個人資料保護專業成員；廠商辦理本專案之相關資安管理作業措施應於簽約前經本校確認(如附件1)。

第三條　廠商承攬工作若涉及資訊或個人資料業務時，應遵守本校所制訂之各項資通安全、個人資料管理及保密相關規定，並簽訂相關保密協定，倘經發現因可歸責於廠商事由而洩密者，一切損害均由廠商負責，並依法追究其各項法律責任。

第四條　廠商知悉或取得本校公務秘密與業務秘密應限於其執行本專案所必需且僅限於本契約有效期間內，並僅提供、告知有需要知悉該秘密之廠商團隊成員，並應要求該等人員簽署合約商（如附件2）及個人保密切結書（如附件3）。若成員於受託業務執行期間有異動，應於成員異動前20天（可視個案要求訂定）通知本校，並重新簽署保密切結書。

第五條　本校保有對廠商檢查及稽核的權利，得依需要對專案相關工作之執行、資料處理及執行之紀錄，進行實地現場訪視或調閱資料，廠商應以合作態度及於合理時間內配合本校或委託之專業機構進行稽核作業，提供相關書面資料或協助約談相關人員，廠商不得有異議。廠商經檢查或稽核結果發現不符合資訊安全或個人資料保護規範者，應於本校通知期限內改善。

第六條　廠商專案成員至本校場所提供服務或維修，應在本校負責人員陪同下，使用指定之主機及帳號進行服務或維修工作。

第七條　廠商因執行本校專案所提供及使用之軟、硬體設備，應符合行政院「各機關對危害國家資通安全產品限制使用原則」，限制使用危害國家資通安全產品。

第八條　廠商提供服務，如違反資通安全相關法令或知悉本校或廠商發生資安事件時，均應於1小時內通報本校，執行緊急應變處置，並配合後續處理、提供相關紀錄或資料。

第九條　契約履約或終止後，廠商應刪除或銷毀執行服務所持有本專案相關資料，或依本校指示返還或移交之，並保留執行紀錄，本校認有必要時得為檢查及確認。

第十條　廠商得依本契約所需提供與本校之服務，分包由其他供應商（分包廠商）提供，惟對於分包廠商履約之部分，仍應負完全責任。但服務內容涉及個人資料之蒐集、處理或利用者，廠商應經本校事前書面同意，始得為之。

第十一條其餘涉及資通安全事項，由本校視個案實際需要，依國家資通安全研究院（網址：https://www.nics.nat.gov.tw）共通規範辦理，例如「政府資訊作業委外資安參考指引」或資通安全有關事項。

第十二條若廠商有違反法律規定或本契約之情事發生，致他人權利受有損害時，經查明後確定為廠商疏失，廠商應負相關責任與協助後續處理，若致本校受有損害時，廠商並應負損害賠償責任。若因此遭第三人請求損害賠償時，應由廠商負責處理並承擔一切法律責任（如於訴訟中，廠商應協助本校為必要之答辯及提供相關資料，並應負擔因此所生之訴訟費用、律師費用及其他相關費用，並負責清償本校因此對第三人所負之損害賠償責任）。

貳、 資通系統之建置、維運

第十三條　本契約所委託建置或維運之資通系統防護需求等級為□**普級**□**中級**□**高級**，廠商應依「資通安全責任等級分級辦法」附表十資通系統防護基準，規劃、設計及落實執行相關控制措施。

第十四條　涉及利用非自行開發之系統或資源者，廠商應標示非自行開發之內容與其來源及提供授權證明。

第十五條　廠商開發之資通系統應避免資訊安全組織公布已知易遭駭客攻擊之弱點，如 SANS Top20、OWASP Top 10，及未來發布之安全問題種類。

第十六條　廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）及隱密通道（covert channel），並提出安全性檢測證明；並應於上線前清除正式環境之測試資料與帳號。

第十七條　廠商於資通系統上線前，應通過資訊安全檢測，以降低遭受駭客攻擊之風險，不論新開發或功能增修之資通系統，廠商應交付：
□弱點掃描（Vulnerability Scan）檢測報告
□滲透測試（Penetration Test）檢測報告（可視個案要求）
□源碼檢測（Code Review）報告（可視個案要求）

第十八條　本專案所提供程式或元件如有安全漏洞者（來源包含但不限於安全性檢測報告、安全漏洞情資），廠商需針對高風險等級（含）以上的弱點進行修補，必要時需配合修改程式或使用元件；惟因作業系統、資料庫或開發工具（程式語言）老舊已無法更新者，應於報告中載明並經本校同意。

第十九條　本專案之資通系統原始程式碼，廠商應針對各版本程式進行版本管理，並依照資訊安全相關規範進行權限控管與存取紀錄保存。

第二十條　廠商應依需要配合執行資通系統業務永續運作演練、備份資料還原演練，協助完成系統災害復原手冊及演練報告。（可視個案要求）

第二十一條廠商完成本專案各項維護，應填具維護紀錄單，經本校承辦人確認後，列入驗收項目。（可視個案要求）

參、 個人資料保護

第二十二條廠商僅得於履行原契約目的之必要範圍及期間內，依雙方共同約定之內容及作業方式，蒐集、處理及利用基於本契約所取得之個人資料。

第二十三條本校若受理個人資料當事人依個人資料保護法第三條所定權利之請求，廠商應於本校指定期限內，配合提供必要資料或說明；個人資料當事人若逕向廠商及其受託人行使個人資料保護法第三條所定權利者，廠商及其受託人應依雙方約定表單或作業方式於期限內答覆，於有疑義時應通知本校協助處理，並留存所有紀錄以供本校查核。

第二十四條廠商、所屬人員及經本校同意之分包廠商應採行符合法令暨本校要求之安全維護事項及措施，以防止廠商於受託範圍內蒐集、處理及利用之個人資料遭未經授權、違法或逾越權限範圍之利用，並且防止個人資料遭到毀損、滅失或竄改。

第二十五條廠商經本校同意將服務分包時，應要求分包廠商遵守本校應遵循之法令、個人資料保護法暨相關法規、本契約之約定、及配合本校個人資料保護之稽核或指示，廠商並應對分包廠商進行監督且定期確認執行狀況及記錄之。

第二十六條廠商於執行受託業務時，若發現個人資料有遭到竊取、外洩、毀損、滅失、竄改或其他不利於當事人之情事時，應立即通知本校並採取必要措施以防止損害擴大。廠商應立即調查事故經過，並向本校報告事件狀況，若本校認有必要，亦得介入進行調查。廠商未經本校同意或授權之情況下，不得對外發言或透漏事件之任何訊息。

第二十七條若發生個人資料遭到竊取、外洩、毀損、滅失或竄改情事時，於事故經過經查明後，廠商得依本校同意之方式通知當事人。

第二十八條違約責任

本校若因廠商及其分包廠商違反本合約附則而受損害時，若事涉個人資料之蒐集、處理及利用，除前揭第十二條之規定外，本校並得請求下列懲罰性違約金(以金額較高者為準)：（1）依所涉個人資料筆數，以每筆新臺幣○○元整計算（視專案金額訂於新台幣500 元到 2 萬元間）作為懲罰性違約金；或（2）新臺幣○○○元整

之金額作為懲罰性違約金。