國立清華大學委外廠商資通安全檢核表

依據行政院「資通安全管理法」第九條及「資通安全管理法施行細則」第四條，本校各單位於委外辦理(資訊服務採購契約)資通系統之建置、維運或資通服務之提供，需依「國立清華大學資訊服務採購契約」第16條第17項辦理以下相關規定:

一、廠商於履約期間需同意本校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。

二、本校防護需求等級為「中級」以上資通系統之委外廠商需每年乙次以「國立清華大學委外廠商資通安全檢核表」完成自我檢核後，由本校業務單位(系統管理者或擁有者)進行複檢，以確認委外廠商落實資安相關要求。

三、本校將定期辦理廠商作業之檢查與稽核。經本校稽核抽查發現不符合資訊安全或個人資料保護規範，須於接獲本校通知期限內改善。受託者(委外廠商)如無法配合不符項目進行改善，本校將建議業務單位於下次續約時，重新審慎評估廠商合適性。

廠商名稱/單位		填表日	年　月　日
服務/系統名稱		IP	

檢核項目	檢核重點	檢核結果	勾符合請截圖佐證 勾不符合或不適用請說明理由
1.資安管理			
1.1是否通過資通安全相關 驗證 (如 ISO 27001/CNS 27001) 或訂定資安相關規範？	• 檢視 ISO 27001 / CNS 27001、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，定期審查報告，廠商是否仍維持導入或證書之有效性？ • 驗證範圍與專案作業範圍具有關聯性？ • 是否已建立資通安全管理文件與表單？	☐符合 ☐不符合 ☐不適用	
1.2是否能在發生資通安全事件時立刻通報機關並執行相關應變措施？	• 是否已建立資通安全事件通報及應變處理相關程序規範？ • 是否知道如發生資安事件應通報本校窗口人員之聯絡方式？	☐符合 ☐不符合 ☐不適用	
1.3人員是否接受資安相關訓練？	• 專案人員是否均曾接受過資安相關教育訓練？ • 如何確認教育訓練之有效性？	☐符合 ☐不符合 ☐不適用	
1.4員工是否了解本校資安相關規範？	• 專案人員是否取得本校資安相關規範？ • 專案人員作業時，是否依本校資安規定執行？	☐符合 ☐不符合 ☐不適用	

核項目	檢核重點	檢核結果	勾符合請截圖佐證 勾不符合或不適用請說明理由
2.資安防護			
2.1是否建置防毒機制並定期更新病毒碼(主機、個人電腦、筆記型電腦、電子郵件、行動載具)?	• 專案相關人員使用之電腦設備是否已安裝防毒軟體？ • 防毒軟體之病毒碼已更新到最新版本？ • 防毒軟體是否已設定定期執行全磁碟掃描？	☐符合 ☐不符合 ☐不適用	
2.2系統是否符合「資通安全責任等級分辦法」附表十系統防 護基準」?	☐普 ☐中 ☐高 級之控制措施	☐符合 ☐不符合 ☐不適用	
2.3專案相關設備是否建置系統監控機制?	• 專案相關伺服器是否已建立容量(如：CPU、RAM 或硬碟)監控機制？ • 專案相關伺服器如發生異常是否已建立處理機制？	☐符合 ☐不符合 ☐不適用	
2.4專案相關設備是否保留稽核軌跡(Log)?	• 專案相關伺服器是否已保存作業系統相關紀錄？ • 是否已訂定紀錄保存機制？	☐符合 ☐不符合 ☐不適用	
2.5專案相關設備是否安置於受管制之區域？	• 專案相關伺服器是否放置於機房並放置於機架中？ • 機房是否設有門禁管理措施？ • 門口是否設有監視設備？監視設備影像是否至少保存六個月以上？ • 機房內是否有溫溼度管理措施？ • 機房內是否有消防設施？是否設有氣體式(CO2、新海龍等)手提滅火器？	☐符合 ☐不符合 ☐不適用	

2.6專案相關設備是否定期進行弱點掃描並修補弱點?	• 是否定期執行弱點掃描？產出報告中是否包含專案相關設備？ • 是否已針對弱點進行評估或修補並留下紀錄？ • 是否於修補後執行複測？	☐符合 ☐不符合 ☐不適用	
檢核項目	檢核重點	檢核結果	勾符合請截圖佐證 勾不符合或不適用請說明理由
3.系統開發			
3.1是否制訂軟體開發生命週期之安全規範?	• 是否已制定程式開發相關管理程序規範？ • 是否已制定程式撰寫之安全原則規定(如：命名原則、程式撰寫格式、程式錯誤語法範例等)	☐符合 ☐不符合 ☐不適用	
3.2是否建置「源碼掃描」機制並執行?	• 是否已制定程式原始碼掃描機制？ • 程式原始碼掃描後，是否執行評估與程式修改並進行複測？	☐符合 ☐不符合 ☐不適用	
3.3是否建置「弱點掃描」機制並執行?	• 是否已制定程式弱點掃描機制？ • 程式弱點掃描後，是否執行評估與程式修改並進行複測？	☐符合 ☐不符合 ☐不適用	
3.4是否管理測試資料及環境?	• 是否設置測試環境並限制僅有本專案人員可以存取？ • 測試環境之測試資料是否為真實資料？如為真實資料是否有嚴格的存取管制措施？	☐符合 ☐不符合 ☐不適用	
3.5是否制訂軟體變更及組態管理之作業規範？	• 是否已建立程式、安裝軟體與組態變更管理機制？ • 執行變更前是否均先測試並經申請核准後才能執行變更？	☐符合 ☐不符合 ☐不適用	
3.6是否建立原始碼備份及版本管理機制?	• 是否已設置原始碼版本管控機制？ • 原始碼是否定期執行備份，並至少保存3代以上？	☐符合 ☐不符合 ☐不適用	
3.7是否定期執行軟體與資訊完整性檢查?	• 是否定期檢查軟體與客戶資料內容之完整性？ • 檢查如有異常，是否建立復原機制？	☐符合 ☐不符合 ☐不適用	

檢核項目	檢核重點	檢核結果	勾符合請截圖佐證 勾不符合或不適用請說明理由
4.資料保護			
4.1是否建立客戶資料保護機制(授權程序,存取管控,銷毀程序)?	• 是否建立客戶資料保護機制(如存取授權、存放位置規定等)? • 資料銷毀是否需要先申請核准並留下銷毀方式之紀錄？	☐符合 ☐不符合 ☐不適用	
4.2契約終止後取得之客戶資料是否返還、確實刪除或銷毀?	• 先前契約完成驗收後客戶資料之處理方式？ • 資料返還或銷毀方式是否留有紀錄？	☐符合 ☐不符合 ☐不適用	

廠商公司章		負責人簽章	

以下欄位由業務單位(系統管理者或擁有者)填寫					
不符項目之應進行改善					
檢查結果		檢查結果 ☐符合 ☐不符合			
系統管理者核章		二級主管核章		一級主管核章	
檢查日期		簽核日期		簽核日期	

備註:廠商如無法配合不符項目進行改善，本校會建議系統管理者於下次續約時，評估廠商合適性。

檢核不符合事項系統管理者請委外廠商提出改善方式、規劃時程、佐證資料表

不符合項目編號	規劃時程	改善方式	請截圖佐證

是否允以結案: □是 □否

未結案原因:

系統管理者核章		二級主管核章		一級主管核章	