委外資訊系統契約參考

發布日期：108.04.09

以下條款內容可於委外資訊系統簽約、採購或編寫需求規格書時，依系統特性及需求參酌加入及修改內文說明，其中甲方代表本校（國立臺北科技大學），乙方代表委外廠商，紅色字體可視情況填入日期或數字，並請搭配「委外資訊系統建置需求標準作業流程」進行採購前審核，請各單位配合辦理，以落實本校資訊安全政策。

第一條、 履約標的

（一）、標的名稱：XXXXXX

（二）、功能規格需求說明：系統所有功能敘述或產品應達到我方相關需求條列說明。經三家以上廠商訪談及報價分析，請廠商提供需求建議書，匯整功能規格需求…。

（三）、付款方式：依建置或維護進度分期付款，需附上相關建置進度或維護紀錄。

（四）、違約及服務績效罰則：未達所定服務水準及績效時，計算違約點數，履約期間內乙方未達甲方所定服務水準及績效，依評估項目、評斷方式要求基準訂定處罰規則。

（五）、使用者操作功能：

1. 支援主流瀏覽器（需完整支援 Internet Explorer、Edge、Chrome、Firefox、Safari 等主流瀏覽器最新穩定版本。）。
2. 支援多(雙)語系(支援正體中文、英文語系)。
3. 響應式網頁設計：應符合不同主流裝置瀏覽需求。
4. 符合無障礙網頁規範：依各系統需求，應配合國發會網站無障礙規範最新版本。
5. 認證機制：介接單一帳密登入，應配合本校認證機制介接及更新。
6. 系統需介接其他資料庫，應配合本校資料庫介接及更新。
7. 資料備援及移置：
   （1）廠商應協助定期備份資料庫、電子檔案、系統程式碼、系統設定、log 等資料，並明列各項機制說明及執行週期。
   （2）若因資料量增加或其它因素，需更換設備或升級作業系統，廠商應無條件協助移轉系統及資料庫。
8. 版本更新：
   （1）廠商應修正系統錯誤，進行本系統版本更新。
   （2）廠商應協助更新因法規或作業方式修改，進行本系統版本更新。
   （3）廠商得以本校提供設備後，協助本校建置測試機。
   （4）系統重大更新前應於測試機測試驗收，再於正式機進行版本更新。
   （5）當版本更新出錯，導致系統中斷無法運行，應復原至前一版，待錯誤修正後再進行版本更新。
   （6）系統應於作業系統進行版本更新後，仍可正常運行作業。
   （7）應於甲乙雙方討論同意後，再執行版本更新作業。
9. 系統效能：
   （1）各項操作功能回應時間，系統回應不可超過幾秒。
   （2）同時連線人數，至少能承載幾位使用者同時連線並正常使用。
   （3）安全穩定的架構，可配合學校之網路架構及系統負載需求，調整安全穩定的

系統架構。

10. 資訊安全管理：

（1）乙方需落實甲方資訊帳號管理原則，且必需配合甲方之「資訊安全管理系統ISMS)」制度以及資通安全管理法等最新相關資訊安全管理及保密規定。

（2）乙方相關人員應據實簽署「國立臺北科技大學計算機與網路中心保密承諾書」。

（3）甲方提供一切機敏性資料、文件等均屬甲方之資產，約定期間或雙方無法合作、或技術移轉時，乙方應依甲方要求，無條件將所持有之原本交還，複製之機敏文件、資料、媒體應予銷毀。

（4）乙方因執行本契約業務而違反個資法，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。

（5）配合甲方資安相關措施發現需改善之系統漏洞，應配合改正，甲方可定期進行資訊安全演練、入侵偵測、弱點掃瞄、應用程式防火牆 WAF、SSL 等資安相關措施，如發現需改善之系統漏洞，乙方應配合改正。

（6）提供相關資安文件確保系統可使用性，乙方需提供弱點掃瞄、滲透測試及網站效能檢測等資安文件，確保系統可使用性。

（7）乙方應配合甲方指定流程，協助進行業務持續運作演練，確保系統緊急中斷、災害發生時之應對處理。

（8）災難還原機制，當系統發生中大事故、中斷、錯誤無法運行，或系統無法復原之情境，乙方應協助將備援資料還原至設備並再度啟用系統，令甲方業務持續進行。

（9）乙方應提供程式原始碼及系統相關操作、說明文件，日後若系統升級或新增功能，乙方需主動提供系統變化的文件說明。

（10）乙方需提供資料庫的存取權限、資料綱要的文件說明，甲方需擁有系統及資料庫存取之最高權限。

（11）乙方維修人員不得輸入任何干擾程式或探取、損壞、消除、竊閱、洩漏甲方輸入電腦資料，如有上列情形，願負一切法律上之責任。

（12）開發設計之原始碼若引(使)用開源程式碼(Open Source)須符合 GNU 與 GPL 規範。

（13）必須完整符合資通安全管理法施行細則第四條之委外系統所需事項。

（14）伺服器與使用者平台系統得在政府組態基準(GCB)套用之環境下運作。

11. 教育訓練及輔導上線：

（1）規畫系統管理人員及系統使用人員教育訓練幾次以上，每次幾小時。

（2）上線時乙方是否到場支援或以其他方式支援。

12. 權利及責任：

（1）乙方所提供之軟體需合法並提供使用授權，不得違反智慧財產權行為，如有違反智慧財產權者，乙方應承擔所有法律責任。

（2）乙方履約結果涉及智慧財產權者，著作財產權歸甲方所有，乙方對甲方不行使著作人格權。

13. SSL 憑證敘明安裝權責及費用歸屬。

14. 行動化應用程式(APP)：

（1）敘明 APP 上架評估及費用歸屬，並需配合教育部規範，上架逾一年下載次數未達一萬次以上需下架。

（2）敘明 APP 檢測規範及費用歸屬，並需配合「行政院及所屬各機關行動化服務發展作業原則」，並通過經濟部訂定行動化應用軟體之檢測項目。

15. 物聯網設備：行政院國家通訊傳播委員會(NCC)規範之物聯網設備，配合 NCC 之要求，公務單位必須優先採購已取得經濟部物聯網資安驗證標章之產品。

（六）、系統環境建置：

1. 乙方應依據功能面及業務面之需求，提出專案系統架構規劃，內容至少應包括：置於 VM 環境下之新系統之架構及網路圖、作業平台、伺服器設備規格(CPU、記憶體、空間等)。
2. 作業系統版本、應用程式伺服器及資料庫伺服器、核心開發程式、其他開發技術等皆需為最新穩定版本，且具有二年以上之產品更新生命週期，同時需能配合伺服器作業系統升級。
3. 應含 SSL 傳輸協定憑證，且購買(至少二年期且費用需含於此案中)、安裝，且必須採用 TLS1.2 以上最新協定。
4. 使用帳號密碼登入時，需介接甲方單一帳密登入認證機制，如遇該機制更新時，乙方應配合更新與升級作業。
5. 主機防火牆設定：關閉不必要連接埠，並拒絕所有連線，只開放必要之通訊埠連線及管理者 IP 連線。
6. 主機校時：排程每日向校時國家時間與頻率標準實驗室進行校時。

第二條、 驗收及文件交付

（一）、乙方須確實交付測試與驗收報告，應至少包含下列項目：

1. 系統功能需求規格書。
2. 軟體授權證明書：註明產品授權數、授權使用時間。
3. 保固保證書：註明保固期間，免費修復及維護方式。
4. 系統架構圖：伺服器硬體等級與系統組成及相關運作流向說明。
5. 系統建置及管理手冊：包含相關系統安裝、版本，系統服務啟動與停止、系統備份與還原、系統 log 等路徑及指令說明。
6. 管理者操作手冊：管理者相關功能手冊。
7. 使用者操作手冊：使用者相關功能手冊。
8. 程式原始碼：提供最新版本，須確保原始程式碼可運行、第三方套件需一併提供原始碼。
9. 資料庫 Schema：提供最新版本，包含資料表名稱、欄位名稱、欄位描述、欄位類型、長度、允許空值等。密碼欄位均不得採用明碼或可還原之編碼或加密演算法儲存，雜湊(Hash)函數使用必須使用 SHA2 以上版本。

（二）、乙方須確實交付資訊安全相關文件，應至少包含下列項目：

1. 保密承諾書(可由乙方乙公司名義或所有相關參與人員填寫)
2. 需檢附自行或第三方驗證之效能檢測報告，符合甲方同時連線多少人數及回應幾

秒之正常使用需求。

3. 需檢附自行或第三方驗證源碼檢測報告，無中等級(含)以上風險。

4. 需檢附自行或第三方驗證弱點掃瞄報告，無中等級(含)以上風險。必須符合行政院-政府機關弱點掃描服務委外服務案建議書徵求文件最新版。

5. 需檢附自行或第三方驗證滲透測試報告，無中等級(含)以上風險。必須符合行政院-政府機關滲透測試服務委外服務案建議書徵求文件最新版。

第三條、 維護保固

(一)、服務範圍：

1. 維護保固項目：維持本案所含相關系統功能正常運作。

2. 維護保固期間：提供維護保固服務起迄日期。

3. 功能增修需求：可配合甲方有功能增修需求，依雙方討論同意後執行。

(二)、維護內容：

1. 諮詢服務：提供單一諮詢窗口、系統的操作問題與說明、e-mail 及客服電話諮詢。

2. 作業系統維護：作業系統調校與升級及漏洞修補。

3. 伺服器維護：相關伺服器調校與升級及漏洞修補。

4. 應用系統維護：

（1）平台相關維護。

（2）log 檔清除整理。

（3）平台效能調校(tuning)。

（4）除錯、更新及漏洞修補。

（5）硬碟空間檢查與整理。

（6）系統稽核。

5. 維護方式：

（1）當維護標的系統發生問題時，乙方在接到甲方通知後，應負責與系統相關問題之診斷及排除，進行系統相關資料、程式之救援與回復。

（2）於服務時間內依以下方式處理：

A. 緊急狀況：屬系統無法運作之情況，於幾小時內電話回覆並處理，乙方應於通報後幾工作小時內恢復運作。

B. 其他狀況：於幾個工作小時內回覆或透過遠端連線完成維護服務， 如線上無法解決，甲方得視狀況決定乙方是否需到達系統所在地進行檢修，幾工作小時內完修。

（3）服務時間：星期一至星期五 AM8:00-PM18:00，不含國定假日。

（4）連線方式：遠端連線或到場維護，遠端連線需要維護時才開放之模式。

6. 交付文件：

（1）定期維護報告：每月或每季至少提供一次的系統維護報告，並以電子郵件方式提供相關系統現況之資訊。例如系統是否有不正常紀錄，如使用者登入登出紀錄、使用者帳號與群組之異動、特殊權限帳號之異動與存取紀錄、系統參數之異動、重要資料存取成功與失敗紀錄、系統錯誤事件等系統稽核、硬碟空間、記憶體使用容量、備份清冊等報告。

（2）相關文件應隨時提供系統更新後最新版本之文件及檔案，包含管理者操作手冊、使用者操作手冊、程式原始碼與資料庫 Schema。

7. 資訊安全：

（1）業務持續運作計畫演練報告：一年乙次業務持續運作演練。

（2）弱點掃瞄報告：半年乙次自行或第三方驗證弱點掃瞄報告。

（3）滲透測試報告：半年乙次自行或第三方驗證滲透測試報告

第四條、 違約及服務績效違約金

（一）、 履約期間內廠商未達機關所定服務水準及績效，除有不可抗力或不可歸責於廠商事由外，依本款約定計算違約金。

（二）、 服務水準及績效，列舉如下(同一評估項目具有二種（含）以上之評斷方式者，如廠商同時違反二種（含）以上時，其違約金係採罰責較重者)：

評估項目	評斷方式	要求基準	處罰規則
機關資訊資產遭不當取得、刪除或變更	乙方因故意或過失導致發生狀況	每次統計	每次計罰◯點
資安管制措施相關規定	乙方如有違反管制措施，一經發現追溯自行為日起	每次統計	每◯◯日（或小時）計罰◯點
系統發生資訊安全事件時	發生資訊安全事件時應即通報甲方，並按甲方之「業務持續運作管理程序」處理	每次統計	每次計罰◯點
入侵之事故或發生之資安事故已見諸於媒體影響機關名譽	重大新聞事件經確定屬實且可歸責乙方者	每次統計	每次計罰◯點
定期維護	未依契約規定維護	每次統計	每次計罰◯點
故障排除、系統修復	經機關通知（不限形式）後，未依契約規定，修復或提供相同系統供機關暫時使用	每次統計	每次計罰◯點
系統可用率	系統各項功能，可正常提供使用者 之時間百分比，不得低於◯◯%	每季統計	每不足◯◯%計罰◯點
	單日累計故障時數（不滿 1 小時，以 1 小時計）	每日不得超過◯◯小時	每日不得超過◯◯小時，每逾◯◯小時計罰◯點

評估項目	評斷方式	要求基準	處罰規則
資安指標	對於所維護之系統，未於規定期限取得認證日數	每次認證超過期限	每逾○○日計罰○點
派駐機關服務人員	累計遲到及早退之總時數（不滿 1 小時，以 1 小時計）	每季統計	每季不得超過○小時，每逾○○小時計罰○點
服務團隊成員	服務團隊成員未依工作計畫（或建議書）滿編，依未滿編之日數計算	每季統計	每日計罰○點
	服務團隊成員離任人數（扣除機關要求離任）除以全體成員之異動率，不得高於○○%	每季統計	每逾○○%計罰○點
會議決議	累計未依會議決議執行之次數	每季不得超過○次	按未依會議紀錄執行，超過之次數計算，每次計罰○點
	累計未依會議決議應完成期限天數	每季不得超過○○天	按超過之天數計算，每天計罰○點
節能減碳	按招標文件規定及乙方投標文件承諾事項，未達成之成效認定	招標或投標文件載明之項目	按未達項目，每項計罰○點
其他	違反契約與服務建議書約定廠商應履行之項目	不得違反契約與服務建議書文件所列事項	每乙次計罰○點
……	……	……	……

本案每點違約金金額為新臺幣○○○元（由機關於招標時載明；未載明者依契約價金總額 1 ‰計算，未達新臺幣伍仟元者，以新臺幣伍仟元計）。（以上內容與乙方協調後增刪）