# 資訊系統委外綜合需求規範書

## 第一條：總則與適用範圍

（一）優先順序：本文各項規定如與本案中其他文件規定有牴觸者，以本文為準。

（二）條文標記：各條文如有方框（□或■）標記者，空心方框標記之項目及其下層項目應予忽略。

（三）用詞定義：

1. 本規範所稱「廠商」，係指本案(「_____」系統，系統等級為「__」)承作廠商；若為招標階段，則指得標廠商。
2. 依據「資通安全管理法」,「廠商」亦包含受託辦理資通系統開發、建置、擴充、遷移、運作管理及維護業務之受託者。

（四）法規遵循：廠商辦理受託業務應遵守「資通安全管理法」及其子法、個人資料保護法及本校資通安全維護計畫等相關法令與規範。

（五）專案類型(擇一勾選)：

□ 本案包含資通系統開發(適用全條文)。

□ 本案僅含資通系統維護(適用本規範條文，但第四條(一)「安全開發管理要求」除外)。

## 第二條：廠商資通安全管理與人員保密要求

（一）管理措施：廠商辦理受託業務之相關人員、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。相關要求如下：(擇一勾選，廠商應提供佐證資料備查)

1. □完善之資通安全管理措施：
   - 1.1. 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。
   - 1.2. 每二年辦理一次內部資通安全稽核。
   - 1.3. 無使用危害國家資通安全產品：依「危害國家資通安全產品審查辦法」，嚴禁使用大陸廠牌之硬體、軟體及資通服務。
   - 1.4. 受託環境應具備防毒軟體、網路防火牆。
   - 1.5. 具有郵件伺服器者，應備電子郵件過濾機制。
   - 1.6. 每人每年接受三小時以上之資通安全通識教育訓練。
2. □通過第三方驗證：廠商應提供有效期限內之第三方驗證證書(如 ISO/IEC 27001 等)，且其驗證範圍應涵蓋本案受託服務之領域。

（一）保密切結與查核：

1. 廠商及其參與人員應簽署「保密切結書」及「委外廠商保密切結書」(或保密同意書)。

2. 適任性查核：
   2.1. 基本要求：廠商應確保參與人員具備專業能力、不具備大陸地區人民身分且無資通安全相關犯罪紀錄。本校得要求檢附「受託辦理資通安全業務人員適任性切結書」。
   2.2. 國家機密特殊規範：受託業務涉及國家機密者，相關人員應接受適任性查核，並依「國家機密保護法」管制其出境。
3. 廠商辦理受託業務得否複委託：(擇一勾選)
   3.1. ■本案不得轉包。
   3.2. □本案得轉包。
      3.2.1. □轉包之範圍與對象：
      3.2.3. □轉包之廠商應具備之資通安全維護措施：

**第三條：技術需求與環境規範**

(一) 軟體授權規範：

1. 合法授權與費用：廠商應確保其所提供之軟體皆包含正確足夠的授權。如須建置作業系統或資料庫系統，應由廠商提供，費用內含於本案價金。
2. 授權計算標準：計算授權數時，本校虛擬平台之實體主機以 16 核計算。
3. 使用者端限制：除作業系統、瀏覽器、PDF/ODF 等常備軟體、漸進式網頁應用(PWA)之離線入口網頁外，使用者設備上不須安裝其他軟體或檔案。
4. 第三方組件：涉及利用非自行開發之系統或資源者，應標示內容與來源並提供授權證明。

(二) 系統運行環境要求：(註：若屬維護案，則以記錄現有環境版本為主，廠商須確保系統與本校現行平台之相容性。)

1. 作業系統：須與本校現行虛擬化平台(vSphere 8.0)相容，且為原廠支援中(Non-EOL)之版本，由廠商提報並經本校資訊組核可(僅限 Windows Server 及 Ubuntu Server LTS 版)。擬採用/現有版本：_____。
2. 資料庫系統：須為原廠支援中(Non-EOL)之版本，由廠商提報並經本校資訊組核可。擬採用/現有版本：_____。
3. 本校得於伺服端主機安裝防毒軟體，廠商須確保不影響功能。
4. 網頁架構：(擇一勾選)
   4.1. □本案不使用 Web 架構。
   4.2. □本案使用 Web 架構，且須符合以下規範。
      4.2.1. 支援主流瀏覽器(Chrome/FireFox/Safari/ Edge)、免安裝外掛程式。
      4.2.2. 導入網站流量統計分析技術(如 Google Analytics)，其管理(分析)權限需設定為本校人員。
      4.2.3. 本校得於該系統或其前端佈署網頁應用防火牆(WAF)，廠商須確

保不影響功能。

4.2.4.□導入本校 SAML 單一登入架構，本校資訊組負責安裝設定 Service Provider(SP)，廠商負責應用系統整合。

4.2.5.響應式網頁設計(RWD)：系統須符合 RWD。(□後台管理介面可不符合 RWD。)

4.2.6.網頁無障礙標章：(擇一勾選)

4.2.6.1.□本案非屬公開網頁系統。

4.2.6.2.□本案須由廠商通過無障礙檢測並取得第一次 AA 級標章，通過的期限為(如驗收前、驗收後幾日等)，未符合之罰則為(如每延遲一日罰尾款或保固保證金幾‰)。廠商應提供文件說明編輯時或維護時的注意事項，以確保系統內容持續符合標章標準。

5.檔案格式規範：

5.1.系統如有匯入或匯出檔案的功能，其檔案格式須符合政府 ODF 政策要求，亦即：若檔案為可編輯者，應包含 ODF 格式；若為不可編輯者，應包含 ODF 格式或 PDF 格式。

5.2.CSV 檔、純文字檔或圖檔不在此限。

5.3.使用者上傳不符合規定的檔案時，應予以禁止，並提示原因。

**第四條：開發與維護作業安全**

(一)安全開發管理要求【依開發類型適用，維護案免填】:

1.□【客製化開發案適用】SSDLC 流程與檢核：應納入 SSDLC 流程，並確實填寫提交「SSDLC 檢核表」與佐證資料。

2.□【非客製化/套裝軟體適用】安全性證明：應提供產品之安全性聲明或已知漏洞修補紀錄。

(二)原始碼交付：廠商(含開發、建置及維護)須提供完整原始碼於系統主機，並確保主機內原始碼版本與執行環境一致，以作為本校資安驗證、備份及後續維護使用。

(三)弱點檢測與持續維護要求：廠商(含開發、建置及維護)交付系統或進行重大變更前應進行弱點檢測並交付報告；系統上線後，本校得不定期進行掃描檢測。如存有中高風險漏洞，廠商應於合約履約或維護期間內無償完成修補。

(四)資通系統防護基準遵循與自評：廠商辦理受託業務(含開發、建置及維護)，應依本案資通系統分級，採取相對應之防護基準；並依據資通安全管理法之附表十「資通系統防護基準」確實執行各項控制措施，填寫提交「資通系統防護基準自評表」及其佐證資料，經本校資訊組核可。若屬維護案，廠商應重新更新自評表，以確保系統持續符合法規要求。

(五)遠端維護管制：原則禁止遠端連線。如有需求須依本校規範填寫「資訊服務申

請表」，經本校核准並開通防火牆後方得連線。

**第五條：資安稽核、演練與事故通報**

(一)稽核權利：

1. 本校得使用「委外廠商查核項目表」進行定期或不定期稽核，廠商應予配合提供相關佐證資料。
2. 稽核發現之缺失，廠商應於本校要求之期限內完成改善；逾期未改善者，視同違約。

(二)事故通報與緊急應變：

1. 廠商知悉資安事件或違反資安相關法令時，應於 1 小時內通知本校及採行補救措施。
2. 應於事故發生後 24 小時內提交初步書面處理報告(含事件起因、影響範圍及初步補救措施)，並於事故結案後提交完整原因分析與改善建議。
3. 如因廠商過失導致之資安事件，廠商應無償負擔損害控管及復原工作。

(三)攻防演練：廠商應配合教育部資安網路攻防演練計畫，並於發現系統弱點時，在時限內完成修補。

**第六條：契約終止與資料處理**

(一)資料處置：契約關係終止或解除時，廠商應返還、移交、刪除或銷毀履行委託契約而持有之資料。

(二)銷毀證明：廠商應提供資料銷毀證明文件，並確保無私自保留本校任何公務資料。

**廠商確認簽署：(本公司已充分瞭解本規範書之內容，並同意於合約期間嚴格遵守)**

廠商名稱：　　統一編號：

負責人：

公司印鑑：　　負責人印鑑：

日期：中華民國　　年　　月　　日