國立金門高級中學
委外業務資安條款契約範本

學校單位：＿＿＿＿＿＿＿＿＿＿（以下稱甲方）

廠　　商：＿＿＿＿＿＿＿＿＿＿（以下稱乙方）

第一章 總則

一、乙方應規範其所屬員工及相關人員(包括複委託單位或臨時人員)，依法令及本契約辦理資通安全相關事宜。

二、乙方為履行本契約，不得使用危害國家資通安全產品；為履行本契約所提供及使用之資通訊產品亦不得使用大陸廠牌，且不得有大陸地區廠商及陸籍人士參與履約；大陸廠牌資通訊產品一律禁止處理甲方公務事務或介接甲方公務環境。

三、乙方履行本契約之標的，應符合我國資通安全相關法令之規定，以及本校資通安全相關章則之要求。若有違反致生損害，應負賠償責任。

四、乙方辦理建置或維運事項涉及個人資料(以下簡稱個資)蒐集、處理、利用者，應依個人資料保護法相關規定辦理。

第二章 綜合管理

五、乙方應配合甲方訂定之資通安全維護計畫，執行相關工作。

六、乙方相關人員執行業務前，應填寫「保密同意書」及「保密切結書」。「保密同意書」及「保密切結書」各簽署一式三份，其中二份由甲方各單位留存，另一份由乙方留存。乙方並應對本案人員保密義務負連帶保證責任，甲方得於契約期間對乙方實施之保密作業進行稽核。

七、乙方應配合甲方進行資安事件處理、演練及緊急應變措施等相關安全工作事項。

八、甲方所提供之一切機密資料、文件，均屬甲方所有之資產。於約定期間內或雙方無法成立合作事宜或技術移轉時，乙方應依甲方要求，立即無條件將其所持有(及員工所持有)之原本交還予甲方或其指定人，其他複製或記錄有該等機密資料之文件、媒體則應予銷毀。

九、乙方執行受委業務，違反資安相關法規或知悉資安事件時，乙方相關人員應配合協助於時限內完成損害控制或復原作業；事件通報及應變之方式、對象等應遵循事項，依甲方制度文件之事件管理程序及相關規範辦理。

資安事件發生時，乙方應協助相關證據之保全，如維護現場完整，避免改變數位證據原始狀態，確保非業務承辦人員或未取得權責主管授權之人員不得進出資安事件現場，並配合甲方資安人員進行相關作業。

十、乙方開發之資通系統，應通過安全性檢測（弱點掃描、滲透測試）並持續維護，降低遭受入侵、竄改或刪除之風險。

十一、甲方及乙方於訂定本契約前，應先行確認以下事項：

（一）涉及機密性、敏感性或關鍵性之應用系統項目。

（二）應經核准始得執行之事項。

（三）乙方配合甲方制度文件、業務持續運作管理(BCM, Business Continuity Management) 及其演練計畫、服務水準協議(SLA, Service Level Agreement)要求，並定義系統或服務相關復原時間目標(RTO, Recover Time Objective)、可容忍資料損失時間 (RPO, Recover Point Objective)及最大可容忍中斷時間(MTPD, Maximum Tolerable Period of Disruption)。

（四）乙方應遵守之甲方制度文件，以及評鑑乙方遵守資通安全標準之衡量及評估作業程序。

（五）乙方處理及通報資安(包括違反個人資料保護法)事件之責任及作業程序。

（六）依資通安全責任等級分級辦法之規定，使用「資通系統安全等級評估表」評估資通系統之防護需求等級，逐項檢視並實作該等級所要求之防護基準控制措施。

（七）資通系統安全性要求及個資蒐集、處理與利用之相關資料(資料類別、目的、範圍及法規依據)。

（八）簽署「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」。

（九）應遵循甲方通行密碼原則之規範：

1. 通行密碼長度應至少八碼。
2. 使用者每一百八十天應更換通行密碼，密碼最短使用期限應至少一天。
3. 通行密碼應避免重複使用前三次變更之通行密碼。
4. 禁止使用者共用帳號及通行密碼。
5. 禁止使用身分證字號、學校代碼、易猜測之弱密碼或其他公開資訊等作為帳號及密碼。

（十）應用系統(網站)下線或停止服務等退場機制，及保留所有原始契約、最新版本源碼(SOURCE CODE)，並於契約中詳列甲方及乙方個別之權利與義務。

十二、乙方應建立應用系統(網站)之資安防護。

十三、甲方得對於乙方進行稽核，並得依需要，對乙方專案相關工作之執行、資料之處理及執行之紀錄，進行實地現場訪視或調閱資料，乙方應配合辦理，及於合理時間內配合提供甲方相關書面資料，或協助約談相關人員，乙方不得拒絕。

十四、甲方經稽核發現乙方不符合資通安全管理法、個人資料保護法等相關法規、甲方制度文件者，乙方應於甲方通知期限內改善，並不得請求甲方支付任何費用，或由甲方提供任何補償。

第三章 作業系統管理

十五、乙方原則禁止遠端維護資通系統，如因緊急狀況等特殊原因須例外開放，應經甲方同意及授權，並依資通安全管理法施行細

則第四條規定及資通安全責任等級分級辦法附表十之遠端存取措施內容規定辦理。

遠端存取開放期間以短天期為原則，並應建立異常行為管理機制。乙方於結束遠端存取期間後，應確實關閉網路連線，並每次更新遠端存取通道登入密碼。

主機、系統遠端維護時，應於加密通道進行及限制來源 IP，並建立監控機制。

十六、乙方之系統維護人員不得使用任何遠端遙控軟體進行系統管理、維護或更新。但有緊急狀況必須使用時，應於防火牆與伺服主機內限定維護來源之 IP，並設定使用時限。

十七、乙方建置之系統如需提供網路芳鄰功能，應先建立網路及主機之安全控制措施。

十八、伺服主機、資料庫系統、應用系統應定期依人事及業務異動情形進行使用權限之調整，由乙方協助甲方各單位業務負責人檢查各系統之使用者存取權限(例如利用甲方制度文件規範之 DBOS 管理者存取權限清單、應用系統存取權限清單進行檢查)。

第四章 機密性及敏感性資料(包括個人資料)之管理

十九、乙方應共同保護重要之資料檔案，以防止遺失、毀壞、被偽造或竄改。重要之資料檔案應依相關規定，以安全之方式保存。

二十、乙方儲存機密性及敏感性資料之電腦媒體，當不再繼續使用時，應以安全之方式處理(如以用重物敲碎搗毀或以碎紙機處理，或將資料從媒體中完全清除)。

第五章 應用系統(網站)管理

二十一、網站及應用程式新開發或重大更新完成後，由乙方實施弱點掃描，及完成中、高風險弱點修補，並驗證修補情形，完成後始得正式上線啟用。

二十二、應用系統或網站資安管理之執行作業，規定如下：

（一）上線前:

1. 乙方應提供安全性檢測報告以供檢查。資通系統開發階段應避免常見漏洞(如 OWASP Top 10等)，且針對核心資通系統，應執行源碼掃描安全檢測。
2. 乙方應用程式所有輸入及輸出欄位應完成過濾及編碼（encode）排除特殊字元(如’ "!$%^&*_|->;等)或跳脫字元，以避免被進行跨網站（XSS）及注入攻擊(Injection)，對於使用者輸入欄位資料，採用正規表示式(Regular Expression)進行檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法，並應於伺服器端進行檢查。
3. 乙方應針對應用系統程式、資料及資料庫應進行定期備份、加密及配合甲方執行業務持續運作演練。
4. 乙方應於甲方應用系統(網站)業務負責人確認安全性檢測與功能性檢測結果後，經單位主管審核同意始可進行相關上線之作業。
5. 應用系統應就涉及機敏資料部分建立稽核日誌，並確保資通系統有稽核特定事件(至少包括更改密碼、登入成功及失敗、資通系統存取成功及失敗)之功能，採用單一日誌記錄機制，確保輸出格式之一致性，且僅限特定授權之使用者能存取稽核日誌。
6. 應用系統具備直接蒐集個人資料之功能時，應依個人資料保護法之規定，於蒐集前設計應告知事項之頁面，明確告知當事人應告知之事項。
7. 應用系統具備上傳計畫或成果報告等含個人資料檔案之功能時，應於蒐集前明確告知當事人，並將其個人資料部分進行遮罩或去識別化後再上傳。
8. 移除任何測試性服務、資料、功能、模組、埠口、帳號等影響正式上線安全性之項目，並關閉有關作業系統、應用程式、開發套件及軟硬體版本資訊等相關錯誤訊息頁面，並確保已更新至最新版本。

9. 乙方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)及隱密通過(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

（二）上線後:

1. 應用系統應定期進行相關程式、服務軟體、資料庫系統等軟體弱點掃描並依掃描報告要求完成弱點、漏洞更新修補。乙方應提供安全性檢測報告以供檢查。
2. 系統程式變更應依甲方制度文件之系統獲取、開發與維護規範。
3. 相關個人資料及機敏性資料提供填報或資料上載應採用加密機制(如 SSH, TLS, SFTP 等)。其因維護不當造成資料外洩者，應負相關法律責任。
4. 應用系統伺服器上之應用程式不得賦予資料庫及作業系統最高權限帳號，應給予最小需用權限，以免惡意人員透過資料庫管理系統破壞內部資訊作業。
5. 乙方應定期更新伺服器主機系統資訊安全修正程式，並依甲方資訊安全規定每月提供資安報告。
6. 乙方可採電話、傳真、電子郵件等方式，適時提供資訊安全警訊通報服務，通過內容以中文為主，包括：資訊安全威脅類型、說明、可能造成之影響。
   (1) 各大原廠發布的最新修正檔。
   (2) 新發現資訊安全漏洞與補救措施。
   (3) 資訊安全事故紀錄與報導。
   (4) 漏洞分析、修補建議或對策。
7. 甲方舉辦災害復原演練時，乙方須配合執行演練計畫。
8. 如甲方發生資安事故時，乙方須配合甲方辦理災害復原程序。

9.如甲方資安事故發生時，甲方除依乙方通報內容之應變措施處置外，得要求乙方派員至甲方協助事故處理，乙方應於接到通知後6小時內派員到場協助，乙方不得拒絕。

第六章 驗收

二十三、乙方須確實交付測試與驗收報告，應至少包含下列項目：

（一）系統功能需求規格及資安需求文件。

（二）相關系統文件之提供。

（三）智慧財產權之歸屬。

（四）相關保密契約與處罰條款。

（五）系統後續保固責任與方式。

二十四、基於資訊安全，本案所有系統及應用軟體於驗收時須檢附第三方資訊安全檢測報告，內容需含 WEB AP 弱點掃描、滲透測試相關措施報告，並於保固期間內每年半至少提供乙次弱點掃描、滲透測試及修補等相關報告。

（一）WEB AP 弱點掃描(Application Level Vulnerability Assessment)：針對 Web AP 進行弱點掃描，例如 SQL injection、Cross-Site 等。

（二）滲透測試(Penetration Test)：針對 Web 網站進行模擬駭客攻擊測試，例如網站漏洞、後門等。

第六章 其他

二十五、乙方於履約期間，應無償提供下列服務：

（一）提供甲方或其教育行政主管機關所需資通安全相關之書面佐證資料。

（二）出席甲方或其教育行政主管機關辦理之資通安全稽核會議，並配合甲方之教育行政主管機關，辦理 1 次資料備份還原業務持續運作演練，並就演練發現之缺失完成改善。

（三）提供甲方或其教育行政主管機關原始程式碼，並依甲方或其教育行政主管機關辦理弱點掃描、滲透測 試、資通安全健診及源碼檢測之結果，完成中、高風險修補。

（四）協助甲方將本契約建置之資通系統移入甲方之教育行政主管機關指定之機房，移入以 1 次為限。

（五）配合甲方或其教育行政主管機關，執行「資通安全管理法」、「資通安全責任等級分級辦法」、「資通安全事件通報及應變辦法」、「教育部委外辦理或補助建置維運伺服主機及應用系統網站資通安全及個人資料保護管理要點」等相關資安規定。

二十六、本契約建置之資通系統於移入甲方之教育行政主管機關指定之機房前，乙方應執行「異機備份」；並協助甲方進行「異地備份」，所需經費由甲方支應。

二十七、乙方提供甲方與資通系統相連或相關之資通訊產品，不得使用大陸廠牌（含硬體、軟體及服務）。

第七章 罰則

二十八、乙方辦理本案如有洩密、疏失、管理不善等情事，致甲方遭致損失，乙方應負全責並賠償甲方之損失。

二十九、乙方因故意或過失，致機關資訊資產遭不當取得、刪除或變更等情事，按次以契約價款之◯%計算違約金。

三十、乙方需遵守甲方資安管制措施之相關規定，如果違反一經發現追溯自行為日起按日以契約價款◯%計罰。

三十一、乙方如引起甲方發生資訊安全事件時應即通報甲方，所造成損失由乙方賠償，並依本契約規定及實際損害計算違約金。

三十二、本契約有效期間，若甲方遭受外來駭客攻擊入侵事故或政府機關攻防演練被入侵之事故或發生資安事故已見諸於媒體影響機關名譽，經確定屬實且可歸責乙方者，甲方按次以契約價款之◯%計算違約金。

三十三、若有違反上述規定之情事發生，甲方得隨時以書面終止或解除契約，且乙方應就甲方所受損害負賠償之責，如致他人權利受有損害時，乙方亦應負責。