|  |
| --- |
| 委外廠商資訊安全要求查核表 |
| 廠商名稱 |  | 統一編號 |  | 負 責 人 |  |
| 專案名稱 |  |
| 聯 絡 人 |  | 聯絡電話 |  | 查核日期 |  |
| 查核項目 | 查核內容 | 適用性 | 查核結果 | 查核紀錄 |
| 廠商自評 | 委託單位審核 |
| 1 | 得標廠商(含所有本專案成員及複委託之廠商)已明確了解並遵守政府相關資訊安全規定及本校資訊安全管理制度所有規範。 | 適用 | □符合□不符合 | □符合□限期改善 |  |
| 2 | 得標廠商之本專案成員應明確瞭解本專案需求規格書(RFP)中所列本校之各項需求。 | 適用 | □符合□不符合 | □符合□限期改善 |  |
| 3 | 得標廠商須於決標次日起\_\_\_日內提出「專案管理工作計畫書」(含光碟及書面文件)，內容應包括對本專案之執行敘述，包含專案管理、組織、參與人員名單、職掌、工作項目、作業時程、品質管制、維護移轉服務及服務水準約定(含違約罰則)等並交付本校審查。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 4 | 得標廠商須於決標次日起\_\_\_個工作天內簽署本校「委外廠商保密切結書」(含個人及公司)，若須提前參與本案，須於實際參與專案前完成簽署本校「委外廠商保密切結書」(含個人及公司)。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 5 | 配合本校實施之弱點掃瞄、滲透測試、資安健診、內部稽核、外部稽核等作業所提之檢測報告，得標廠商須依檢測報告提出系統資安問題分析與改善建議，如因特殊原因無法如期完成修正，廠商得敍明理由提交本校進行審查，本校得視情況酌予延長。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 6 | 本校原則禁止得標廠商透過Internet遠端維護系統。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 7 | 系統如發生資通安全事件(如資料外洩、被竊取、駭客入侵等情事)，須於\_\_\_個小時內到場協助本校辦理資通安全事件狀況處理相關作業程序及查明原因，並於\_\_\_小時內提供改善情形及建議報告書。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 8 | 程式變更需於本校測試環境測試無誤並保留變更前後差異之紀錄，並由本校程式管理人員確認後，於本校指定時間(含下班或例假日)安裝程式變更於正式作業，如程式變更後無法正常運作，則須立即恢復原狀。得標廠商應於更新完成後10個工作日內提供相關說明文件，如有必要需安排教育訓練。如程式變更涉及系統文件之修正，應於系統變更完成後1個月內修正完成送交本校。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 9 | 正式作業上線前應將作業系統及發展工具軟體等安裝至最新之修補程式，並針對程式做相關資訊安全檢測(例如SQL Injection、XSS、惡意程式碼檢測等)，並提交檢測報告。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 10 | 配合本校資訊安全風險評估及安全管理需求，對個人資料或機密資料，應妥善保護及加密處理，以確保資料之隱密性。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 11 | 得標廠商應遵循「個人資料保護法」之相關規定，保留個人資料存取紀錄與記錄分析管理報表，以利資安稽核。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 12 | 系統須將存於資料庫內之使用者密碼欄位以加密(不可逆)處理儲存，以防止使用者密碼為使用者以外人員知悉。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 13 | 系統應依使用者權限建立控制機制，以確保系統安全；若有儲存或傳輸具有機密性或高敏感性的資料，應使用加密技術。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 14 | 機敏系統須建立SSL機制以防止使用者透過Internet 作業時遭有心人士竊視。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 15 | 若應用ActiveX與Java applet，應採取相關防護措施(如：加註警語提醒使用者將下載之相關元件為何) 。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 16 | 得標廠商交付之系統，不得包含任何後門程式、隱密通道及特洛伊木馬程式等。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 17 | 系統須加強輸入檢核以防止SQL Injection、XSS、篡改輸入等攻擊，並配合本校要求，在必要時協助建立SQL Injection 與異常行為分析功能與報表。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 18 | 得標廠商應負責系統文件最新版本之建立與維護(含光碟及書面文件)，包含提供完整之系統架構說明、系統程式規格書、系統測試報告書、系統安裝手冊、原始程式碼及執行碼光碟、資料庫欄位及關連說明、系統維護手冊、系統使用手冊、教育訓練教材。有關原始程式碼及系統安裝建置，得標廠商須於本校建置所需環境供本校測試驗證原始程式碼與經編譯後之可執行檔版本是否相符，驗證通過本項工作才算完成。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 19 | 得標廠商應提供安全完整之系統備份與還原程序(含光碟及書面文件)，並負責設定。得標廠商得須於本校建置所需環境供本校測試驗證，驗證通過本項工作才算完成。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 20 | 系統測試計畫及測試報告(含光碟及書面文件)，各項測試報告應包含測試項目名稱、測試說明、測試條件、事先需成立之條件、測試預期結果、實際測試資料、測試時間、測試人員、測試結果。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 21 | 系統自動偵測密碼輸入錯誤次數超過3次即暫停或關閉用戶登入作業，並留下稽核紀錄。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 22 | 強化密碼品質，系統檢核使用者產生之密碼，確保其長度至少12位字元且為特殊符號與英數混合，系統要求使用者至少\_\_\_個月修改一次密碼，並於畫面上提示使用者如何產生強化密碼。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 23 | 符合資訊安全責任分散之權限控管機制(需區分申請、覆核、核准、稽核等角色，並加以控制)。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 24 | 系統須將使用者異動情形記錄於紀錄檔(Log File)，系統應提供查詢與列印使用者名冊、使用者授予權限功能及異動紀錄。得標廠商非經本校同意不得新增或刪除系統帳號及異動權限。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 25 | 系統應就涉及機敏資料部分建立資安稽核機制，並保留系統完整存取紀錄。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 26 | 應用系統伺服器上之應用程式不可以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。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 27 | 當系統異常無法正常運作，應配合做緊急處理，應於接獲通知\_\_\_個小時內進行處理，並於接獲本校通知後\_\_\_個小時內維修完畢。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 28 | 得標廠商應配合本校主機虛擬化作業時程，將系統原主機資料(包含應用系統、資料庫及檔案等)移轉至VM環境，並進行相關網路連線設定，於移機後須進行系統測試，以確保系統運作正常。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 29 | 維護期間內，得標廠商應配合本校要求，對於所維護之應用系統之系統運作環境(如：作業系統版本、資料庫系統版本或軟體版本…等) 之更動，協助進行事前評估及免費協助轉置，且於前述更動後，須進行系統測試，以確保系統運作正常及符合相容性。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 30 | 維護期間內，倘維護標的因故搬遷，得標廠商應免費協助本校辦理系統轉置或重新設定等相關事宜。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 31 | 維護期間內本校因軟硬體設備異動，因而涉及原系統環境變更時(如版本變更或安裝PATCH)，得標廠商應免費提供技術服務。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 32 | 維護期間內如因故終止服務，廠商應於本校規定期限內，將機關存在於委外廠商處的資料或設備移轉給機關或其他委外廠商。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 33 | 系統需符合IPV6協定。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 34 | 配合本校外部稽核作業之查核，廠商應配合接受本校或委託單位之稽核或查核等業務，其範圍包括本專案開發環境、設備、人員及系統之管理機制等。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 35 | 駐點人員使用之個人電腦，未安裝及使用來路不明或未經授權核准之軟體(符合智慧財產權)。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 36 | 專案範圍內之機敏文件不使用或長時間離開座位時，專案成員已收妥且存放於上鎖之儲櫃(確保實體安全)。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 37 | 駐點人員個人電腦未使用私人且未經授權之無線網路設備(如：AP無線基地台、行動通訊網卡)傳輸專案範圍內之機敏性資料。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 38 | 本專案成員使用電子郵件寄送相關機敏資料時，應加密或用密碼保護，但密碼不得寫於電子郵件內，應另外通知收件者。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 39 | 委外廠商人員至本校進行專案業務執行時，禁止使用大陸廠牌之資通訊產品，包含軟體、硬體及服務等。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 40 | 委外廠商需具備完善之資通安全管理措施或通過資通安全第三方驗證。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 41 | 委外廠商已指定專案管理人員，負責推動、協調及督導受託業務之資通安全管理事項。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 42 | 委外廠商應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。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 43 | 委外廠商依徵求建議書(RFP)相關採購文件中，落實執行資通系統防護基準需求。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 44 | 委外廠商如允許就委外業務項目分(轉)包，應明確界定分(轉) 包之範圍，以及分(轉)包之廠商需具備資通安全維護措施 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 45 | 委外廠商已提供資通系統之安全性檢測證明。 | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 46 | 委外廠商是否制訂資安事件通報機制？(如委外業務，違反資通安全相關法令或發生專案範圍內之資通安全事件時，須立即通知本校並採行相關補救措施並回報處理結果) | □適用□不適用 | □符合□不符合 | □符合□限期改善 |  |
| 審查結果 | □合格 □不合格 □待改善 | 審查意見 |  |
| 廠商代表 |  | 審查人員 |  | 權責主管 |  |