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修正規定

第一章 總則

一、教育部（以下簡稱本部）為落實資通安全管理法、個人資料保護法及國家機密保護法等相關規定，特訂定本要點。

二、本部各單位依政府採購法及本部採購程序辦理建置與維運伺服主機及應用系統網站相關業務之採購，應以書面、電子傳輸或其他適當方式，將本要點規範之義務告知向本部提供產品或服務之廠商。

本部各單位委請或補助機關（構）、學校辦理建置與維運伺服主機及應用系統網站相關業務，應以書面、電子傳輸或其他適當方式，將本要點規範之義務告知受委請或補助辦理之機關（構）、學校。

第一項之廠商及第二項之受委請或補助辦理之機關（構）、學校（以下合稱委外單位），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)，依本要點辦理。

三、本部各單位以委外單位辦理資訊業務時，應於事前審慎評估可能影響本部資產、流程、作業環境或對機關之特殊威脅等潛在安全風險，與委外單位簽訂適當之資通安全(以下簡稱資安)協議，課予相關安全管理責任，並納入契約、行政協議書或計畫書條款。

選任及監督委外單位時，除應依資通安全管理法施行細則第四條規定辦理外，並應限制使用危害國家資通安全產品；採購及使用之資通訊產品不得使用大陸廠牌，且於招標文件規定不允許大陸地區廠商及陸籍人士參與；大陸廠牌資通訊產品一律禁止處理公務事務或介接公務環境。

四、委外單位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及「教育部委外專案個人資料保護條款」(附件一)辦理。

第二章 綜合管理

五、委外單位應配合本部訂定之「資通安全與個人資料保護管理制度文件」（以下簡稱本部制度文件），執行相關工作。

六、委外單位應填寫「保密合約書」(附件二)。相關人員執行業務前，應填寫「保密同意書」(附件三)。「保密合約書」及相關人員之「保密同意書」應簽署一式三份，其中二份由本部各單位留存，另一份由委外單位留存。

七、委外單位應配合本部進行資安事件處理、演練及緊急應變措施等相關安全工作事項。

八、委外單位執行受委業務，違反資安相關法規或知悉資安事件時，委外單位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，依本部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，委外單位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，並配合本部資安人員進行相關作業。

九、本部各單位應用系統（網站）以委外單位開發者，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。

本部各單位應規劃適當經費執行資通系統之資安業務。

十、本部各單位應維護應用系統(網站)業務負責人、應用系統負責人及維護單位等相關通訊及聯絡資料，如有新增或異動時，應即時告知本部資訊及科技教育司(以下簡稱資科司)資安業務承辦人。

十一、本部各單位應用系統(網站)以委外單位辦理者，其申請之本部所屬網域(domain)、網際網路位址(以下簡稱IP)之使用最長期限為三年，期滿應重新提出申請。

十二、下列資安及個資保護事項，應納入委外之服務契約、行政協議書或計畫書：

（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）委外單位配合本部制度文件、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）委外單位應遵守之本部制度文件，以及評鑑委外單位遵守資通安全標準之衡量及評估作業程序。

（五）委外單位處理及通報資安(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」(附件四)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「教育部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」(附件五)。

（九）應遵循本部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。

十三、委外開發或維運應用系統(網站)，應預作下線或停止服務等退場機制，及保留所有原始契約、行政協議書或計畫書及最新版本源碼(SOURCE CODE)，並於契約、行政協議書或計畫書中詳列本部及委外單位個別之權利與義務。

十四、本部各單位應監督委外單位建立應用系統(網站)之資安防護，如未依本要點落實應用系統(網站)資安管理，致發生資安事件，依「教育部職員獎懲要點」及「教育部人員資通安全事項獎懲基準」相關規定議處。

本部得對於委外單位進行稽核，並得依需要，對委外單位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，委外單位應配合辦理，及於合理時間內配合提供本部相關書面資料，或協助約談相關人員，委外單位不得拒絕。

經稽核發現委外單位不符合資通安全管理法、個人資料保護法等相關法規、本要點、本部制度文件者，委外單位應於本部通知期限內改善。

第三章 作業系統管理

十五、伺服主機應安裝主機型防火牆，阻絕不使用之網路通訊埠，及定期檢視防火牆策略清單是否符合資安要求。

十六、伺服主機應安裝防毒軟體，並即時更新病毒碼及檢查運作是否正常。

十七、伺服主機應即時進行作業系統及相關應用軟體更新及修補，並定期或不定期進行主機弱點掃描。

十八、委外單位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，應經本部同意及授權，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。委外單位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。

十九、委外單位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。

二十、系統管理者不在場時，主控台（Console）應置於登出狀態，並設置密碼管理。

二十一、委外單位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。

二十二、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，由委外單位協助本部各單位業務負責人檢查各系統之使用者存取權限(例如利用本部制度文件規範之DBOS管理者存取權限清單、應用系統存取權限清單進行檢查)。

二十三、系統管理者應隨時注意及觀察分析系統之作業容量，以避免容量不足而導致主機當機或資料毀損。

二十四、系統管理者應進行系統作業容量之需求預測，以確保足夠之系統處理及儲存容量。

二十五、本部各單位應特別注意系統之作業容量，預留預算及採購行政作業之前置時間，以利進行前瞻性之規劃，並及時獲得必要之作業容量。

二十六、系統管理者應隨時注意及觀察分析系統資源使用狀況，包括處理器、主儲存裝置、檔案儲存、印表機及其他輸出設備及通信系統之使用狀況。

二十七、系統管理者應隨時注意前點相關設備之使用趨勢，尤應注意系統於業務處理及資訊管理上之應用情形。

二十八、系統管理者應隨時掌握與利用電腦及網路系統容量使用狀況之資訊，分析及找出可能危及系統安全之瓶頸，預作補救措施之規劃。

二十九、系統管理者應準備適當及足夠之備援設施，定期執行必要之資料與軟體備份及備援作業，以於災害發生或儲存媒體失效時，得迅速回復正常作業。

三十、系統資料備份及備援作業，應符合機關業務持續運作、系統或服務相關RTO、RPO及MTPD之需求。

三十一、電腦作業人員應忠實記錄系統啟動及結束作業時間、系統錯誤及更正作業等事項，並依實際需求保留所有紀錄檔。

三十二、電腦作業人員之系統作業紀錄，應定期交由客觀之第三者查驗並律訂保留期限，以確認其是否符合機關規定之作業程序。

第四章 機密性及敏感性資料(包括個人資料)之管理

三十三、本部各單位應建立機密性及敏感性資料(包括個人資料，以下同)之處理程序，防止洩漏或不法及不當之使用。

三十四、本部各單位應研訂處理機密性及敏感性資料之輸入及輸出媒體之安全作業程序(如文件、磁帶、磁片、書面報告及空白支票、空白收據等項目)。

三十五、機密性及敏感性資料之安全處理作業，應包括下列事項：

（一）輸入及輸出資料之處理程序及標示。

（二）依授權規定，建立收受機密性及敏感性資料之正式收文紀錄

（三）確保輸入資料之正確性。

（四）儘可能要求收受者提出傳送之媒體已送達之收訖證明。

（五）分發對象應以最低必要之人員為限。

（六）為提醒使用者注意安全保密，就機密資料應明確標示機密屬性、機密等級及保密期限。

（七）應定期評估機密性及敏感性資料之發文清單及檢討評估內容

（八）應確保資通系統內部資料與外部資料之一致性。

三十六、系統流程、作業流程、資料結構及授權程序等系統文件，本部各單位應予適當保護，以防止不當利用。

三十七、本部各單位及委外單位應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。

三十八、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)。

三十九、機關間進行資料或軟體交換，應訂定正式之協定，將機密性及敏感性資料之安全保護事項及有關人員之責任列入。

四十、機關間資料及軟體交換之安全協定內容，應考量下列事項：

（一）控制資料及軟體傳送、送達及收受之管理責任。

（二）控制資料及軟體傳送、送達及收受之作業程序。

（三）資料、軟體包裝及傳送之最基本之技術標準。

（四）識別資料及確定軟體傳送者身分之標準。

（五）資料遺失之責任及義務。

（六）資料及軟體之所有權、資料保護之責任、軟體之智慧財產權規定等。

（七）記錄及讀取資料及軟體之技術標準。

（八）保護機密或敏感性資料之安全措施（如使用加密技術）。

第五章 應用系統(網站)管理

四十一、本部各單位應於合約明定，網站及應用程式新開發或重大更新完成後，由委外單位實施弱點掃描，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。

四十二、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. 委外單位應提供資通系統安全等級評估表(附件四)及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. 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. 針對應用系統程式、資料及資料庫應進行定期備份、加密及配合本部執行業務持續運作演練。
4. 委外單位應於本部應用系統(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。

（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。委外單位應提供安全性檢測報告以供檢查。
2. 系統程式變更應依本部制度文件之系統獲取、開發與維護規範，填具教育部應用系統開發(變更)申請表、教育部應用系統維護紀錄表及教育部系統原始程式碼版本控制表，並保留所有版本源碼於應用系統負責人處。
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。