教育部補助委辦採購維護伺服主機及應用系統網站資訊安全管理要點修正規定

第一章 總則

一、教育部（以下簡稱本部）為落實個人資料保護法、國家機密保護法、行政院及所屬各機關資訊安全管理要點及本部資訊安全管理規範等相關規定，特訂定本要點。

二、本部以補助或委辦方式，辦理採購、建置或維護之伺服主機及應用系統網站相關業務之機關（構）、學校及廠商（以下簡稱受補助或委辦單位），應以書面、電子傳輸或其他方式告知本要點研定義務，並規範其所屬員工及相關人員(包含分包或臨時人員)，依本要點辦理。

三、本部資訊業務委辦時，應於事前審慎評估可能之潛在安全風險（如資料或使用者通行碼被破解、系統被破壞或資料損失等風險），並與受補助或委辦單位簽訂適當之資訊安全協定，課予相關之安全管理責任，並納入契約條款。

四、補助或委辦之應用系統(網站)其營運涉及個人資料蒐集、處理、利用等事項者，受補助或委辦單位視同補助或委辦單位，並依個人資料保護法相關法規辦理。

第二章 綜合管理

五、受補助或委辦單位應配合本部資訊安全規定，執行相關工作。

前項本部資訊安全規定，由本部依相關法規訂定之，並公告於本部網站首頁。

六、受補助或委辦單位，應填寫資訊安全保密合約書。相關人員執行委託業務前，應填寫保密承諾書。保密合約書及相關人員之保密承諾書應簽署一式兩份，由本部補助或委辦單位及受補助或委辦單位留存。

七、受補助或委辦單位應配合本部進行資訊安全事件處理、演練及緊急應變措施等相關安全工作事項。受補助或委辦單位與本部簽訂之契約條款中，應包含營運持續管理(BCM, Business Continuity Management)計畫，並要求服務水準協議(SLA, Service Level Agreement)，並定義相關 RTO(Recover Time Objective)、RPO(Recover Point Objective)。

八、資安事件發生時，受補助或委辦單位及業務承辦人應配合本部資安事件通報應變流程，協助於時限內完成事件排除。

前項之處理時限，依行政院「國家資通安全通報應變、作業要綱」及本部資訊安全管理規範規定之時限。

九、本部應用系統(網站)委外開發時，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。

補助或委辦單位宜將安全性要求，或個人資料蒐集與利用之相關資料(資料類別、目的及法規依據)納入專案契約，並規劃適當經費執行。

十、應用系統(網站)委外之承辦單位，應每年定期維護應用系統(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，並告知資訊及科技教育司資訊安全業務承辦人。

十一、應用系統(網站)委外，其所申請之網域(domain)、網路位址(IP)之使用期間，以三年為限，期滿應用系統(網站)委外承辦單位應重新提出申請。

十二、下列資訊安全事項，應納入資訊業務委外之服務契約：

（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）受補助或委辦單位如何配合執行本部營運持續運作(BCM,Business Continuity Management)計畫。

（四）受補助或委辦單位應遵守之資訊安全規範及標準，以及評鑑受補助或委辦單位遵守資訊安全標準之衡量及評估作業程序。

（五）受補助或委辦單位處理及通報資訊安全(包括違反個人資料保護法)事件之責任及作業程序。

十三、應用系統(網站)開發，應預作下線或停止服務等退場機制，及保留所有原始契約和源碼(SOURCE CODE)，並於契約中詳述本部及受補助或委辦單位個別之權利與義務。

十四、本部應用系統(網站)業務補助或委辦單位應監督受補助或委辦單位，如未依本辦法落實應用系統(網站)資訊安全管理，致發生資安事件，依本部職員懲處要點相關規定議處。

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、所有伺服器應安裝防毒軟體，並隨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軟體更新及修補，並定期或不定期進行主機弱點掃描。

十八、主機、系統維護時，應於加密管道進行(如 SSH,SSL 等)，並限制維護來源 IP。

十九、受補助或委辦單位及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。但有警急狀況必須使用時，應於防火牆與伺服主機內限定維護來源之 IP，並設定時限。

二十、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、系統不得提供網路芳鄰功能，若單位建置完成系統、網路、主機等安控措施則不在此限。

二十二、主機系統每半年/不定期依人事組織進行實際使用權限之調整，變更使用者權限，協助本部業務負責人檢查各系統之使用者存取權限(利用應用系統存取權限清單)。

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、系統管理者應進行電腦系統作業容量之需求預測，以確保足夠之電腦處理及儲存容量。

二十五、業務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、系統管理人員應隨時注意及觀察分析系統資源使用狀況，包含處理器、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、管理人員應隨時注意前項設備之使用趨勢，尤應注意系統在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及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，以於災害發生或是儲存媒體失效時，得迅速回復正常作業。

三十、系統資料備份及備援作業，應符合機關業務永續運作之需求。

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、業務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、業務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）輸出及輸入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）確保輸入資料之真確性。

（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）應確保資訊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，業務單位應予適當保護，以防止不當利用。

三十七、業務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(如燒毀或是以碎紙機處理，或將資料從媒體中完全清除)。

三十九、資訊業務委辦處理之電腦文具、設備、媒體蒐集及委外處理資料，應慎選有足夠安全管理能力及經驗之機構作為委辦對象。

四十、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。

四十一、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

四十二、依本部資訊安全規定，網站及應用程式於上線前應定期完成弱點掃描並完成弱點修補，應用系統(網站)委外承辦單位並應於合約中明訂相關執行事宜及經費，以利承辦受補助或委辦單位執行。但未能預先規劃或現行已上線系統未規劃執行者，可由資訊及科技教育司執行，經費並由委外承辦單位自行吸收。

四十三、應用系統(網站)資安管理之執行作業，得參考下列規定：

（一）上線前:

1. 應用系統應即時進行相關程式、服務軟體、資料庫系統等軟體弱點掃描，並針對所有弱點、漏洞更新修補。受補助或委辦單位應提供原始碼以供檢查。
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）及資料庫注入攻擊(SQL-injection)。(相關防護可參考 OWASP Encoding Project)。
3. 針對應用系統程式、資料及資料庫應進行定期備份及配合本部執行業務持續運作（BCM）演練。

（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。受補助或委辦單位應提供原始碼以供檢查。
2. 系統程式變更應依本部資安規範填具版本更新表，並保留所有版本原始碼於系統負責人處。
3. 相關個人資料及機敏性資料提供填報或資料上載應提供加密機制(如 SSH, SSL, SFTP 等)。其因維護不當造成資料外洩者，依個人資料保護法負法律責任。

保　密　合　約　書

立 約 人：　　＜以下簡稱甲方＞
　　＜以下簡稱乙方＞

茲甲方因　　事宜，將交付相關機密資訊，爰訂立本契約，條款如下：

第一條：機密資訊

本合約所指之「機密資訊」，乃指甲方基於前開使用目的，直接或間接以口頭或書面告知予乙方之文件（包括但不限於：電子郵件、傳真、郵件等）、資料、物件、技術秘訣 Know How、儲存系統暨拓樸圖、相關解決方案暨架構、系統安全管理政策或其他與甲方營業秘密相關或本質上屬於機密之資料文件。

第二條：保密義務

一、 除為履行本契約或為法規命令之要求外，乙方不得洩露「機密資訊」予第三者。乙方應知「機密資訊」範圍，並應讓必須知道「機密資訊」之受僱人或其外包廠商，知其有保密之義務，且於向該受僱人透露「機密資訊」前，需先取得該受僱人簽署之同意受此保密義務條款拘束之書面文件或契約(附件二)，作為本約之附件，並視為本約之一部份。

二、 為切實有效執行本條第一款之規定，乙方應制定機密文件管理辦法，對上述「機密資訊」之使用、查閱、複印等，需有完善之控管及紀錄，並將公司對外對內之往返電子郵件紀錄，保存至少六個月以上。甲方對上述之紀錄有權於任何時間，至乙方處進行不定期之稽查。

三、 本合約規範之保密義務自該等「機密資訊」揭露後起算至該機密資訊合法揭露於公眾為止。

第三條：本契約到期或終止時，乙方應將所有「機密資訊」和其根據本約所製造之產品及其複製品返還予甲方。乙方同意於本契約到期或終止後，絕不使用該「機密資訊」，且使經由乙方而獲得「機密資訊」之受僱人、外包廠商(附件一)等，絕不再使用該「機密資訊」。

第四條：契約期限及終止

一、本契約自簽約日起生效，有效期限【三】年。

二、雙方得以書面方式終止本合約，其終止之效力應自收到書面通知後三十日起算。

三、本契約第二條所定之保密義務，不因本契約終止或屆滿而失效。

第五條：罰則

乙方如違反本保密承諾書之約定，甲方得就因此所生之實際損害數額，請求乙方賠償。甲方因此支出相關法律顧問、律師公費及訴訟、執行費用，由乙方全額負擔。乙方另應給付甲方新臺幣〇〇萬元作為懲罰性違約金，並保留法律追訴權，乙方不得異議。

第六條：準據法與管轄法院

本契約之解釋、效力、履行及其他未盡事宜，悉依中華民國法律為準。當事人間因本契約或違反本契約所致之任何糾紛或爭議，雙方同意以臺灣臺北地方法院為第一審管轄法院。

第七條：完整契約

甲乙雙方就本契約工作所做成之書面，如訂單、採購單等，為本契約之附件，並視為本契約之一部份。本契約之權利義務之免除、限制、轉讓、增刪、修正或修改，應由雙方合法授權之代表人以書面簽署之文件為之。

本契約壹式兩份，由甲乙雙方簽署後生效，雙方各執一份為憑。

立約人

甲　方：

代表人：

代理人：

地　址：

乙　方：

代表人：

代理人：　　**（無則免填）**

地　址：

中華民國 ____年____月____日

附件一

參與本契約相關工作之乙方員工及其他相關人員如下：

一、姓　名：
　　職　稱：
　　工作簡介：

二、姓　名：
　　職　稱：
　　工作簡介：

三、姓　名：
　　職　稱：
　　工作簡介：

附件二　　機密等級：機密

保　密　承　諾　書

緣____　（以下簡稱乙方）與____於民國____　年____　月____日簽訂保密合約書（以下簡稱主合約）。茲因乙方指定本人參與主合約書內所委任之工作，本人特此同意並承認前述主合約書內所訂之「機密資訊」係貴單位之機密資料，而該資料僅係為完成委任工作之目的而透露予本人。

本人並同意遵守且履行乙方在主合約書中有關本資料保密之責任與義務且本人及執行任務人員同意遵守下列各項保密約定：(閱讀完畢請勾選)

- □ 本人已詳讀「教育部本部資訊安全管理規範」(登載於教育部網站 http://www.edu.tw 下方)，並於執行任務時願配合相關安全規定。
- □ 不擅自使用或破壞未經甲方授權之資料、文件、設備。
- □ 不私自透過網路或任何媒體連接至未經甲方授權之資訊系統或網路設施，禁止使用本部(含學術)網路干擾、破壞、或影響網路上其他使用者或節點之軟硬體系統。散佈電腦病毒、嘗試侵入未經授權使用之電腦系統、以網路管理工具或軟體癱瘓網路、以電子郵件等方式大量傳送廣告信、或其它類似之情形者，皆在禁止範圍內。
- □ 執行任務期間所取得之資料僅係為完成委託工作之目的而使用，決不作其他用途且不會將任何資料洩漏予其他人員或單位。
- □ 任務完成或關係終止時，亦不洩漏任何資料予其他人員或單位。
- □ 如違反以上承諾，造成安全上之事件發生時，願負實質賠償損害之責任。

此致

立切結書人：____
姓　　名：____
職　　稱：____
住　　址：____
身分證字號：____