檔　　號：

保存年限：

教育部　函

機關地址：10051臺北市中山南路5號
傳　真：02-2737-7043
聯絡人：江宜倫
電　話：02-7712-9036

受文者：國立臺北科技大學

發文日期：中華民國110年6月18日
發文字號：臺教資(四)字第1100068264C號
速別：普通件
密等及解密條件或保密期限：
附件：發布令影本（含行政規則）(ATTCH14 A095N0000Q0000000_0068264CA0C_ATTCH14.pdf、ATTCH15 A095N0000Q0000000_0068264CA0C_ATTCH15.pdf、ATTCH16 A095N0000Q0000000_0068264CA0C_ATTCH16.pdf、ATTCH17 A095N0000Q0000000_0068264CA0C_ATTCH17.pdf、ATTCH18 A095N0000Q0000000_0068264CA0C_ATTCH18.pdf、ATTCH19 A095N0000Q0000000_0068264CA0C_ATTCH19.pdf、ATTCH21 A095N0000Q0000000_0068264CA0C_ATTCH21.odt、ATTCH24 A095N0000Q0000000_0068264CA0C_ATTCH24.pdf)

主旨：修正「教育部辦理或補助建置與維護伺服主機及應用系統網站資訊安全管理要點」，名稱並修正為「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」，業經本部於中華民國110年6月18日以臺資教（四）字第1100068264B號令修正發布，茲檢送發布令影本（含行政規則）1份，請查照。

說明：

一、本案電子檔得於本部主管法規查詢系統（http://edu.law.moe.gov.tw）下載。

二、若對本行政規則有任何疑問，請逕洽本部江宜倫小姐（電話：02-7712-9036）。

正本：各公私立大專校院、各公私立高級中學、各公私立高級職業學校、各直轄市及縣市政府教育局(處)、本部各單位、部屬機關(構)及國家運動訓練中心

副本：110/06/18 09:22:16

附件一

教育部委外專案個人資料保護條款（適用行政協助範本）

委外單位受機關委請蒐集、處理或利用個人資料及檔案時，雙方同意依個人資料保護法、個人資料保護法施行細則及教育部所訂定之規定訂定本條款，共同遵守，其條款如下：

第 1 條　蒐集、處理或利用時之義務

(1) 委外單位受機關委請蒐集、處理或利用個人資料及檔案（指個人資料保護法所規定之自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料）時，應符合個人資料保護法、個人資料保護法施行細則及教育部個人資料保護管理要點等相關規定。

(2) 委外單位僅得於機關指示及履行契約或協議之必要範圍內，蒐集、處理或利用個人資料（委外單位不得利用機關所提供或因執行本契約或協議專案所蒐集個人資料及檔案進行行銷或商業推銷等相關活動，或以任何方式或方法交付予履約無關之第三人，亦不得為本契約或協議專案以外之蒐集、處理或利用，包括但不限於結合委外單位原本所保有之個人資料及檔案，再為處理或利用）。

(3) 本契約或協議專案預定蒐集、處理或利用個人資料之

範圍：_____

類別：_____

特定目的：_____

期間：_____

機關保留指示之事項：_____

其他事項：_____

□上開範圍、類別、特定目的、期間、機關保留指示之事項和其他事項詳計畫、需求書。

第 2 條　安全維護措施

(1) 委外單位在執行本契約或協議專案委請業務所必要之範圍內，應依個人資料保護法施行細則第 12 條之規定採取適當安全維護措施，並指定專人辦理安全維護事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

(2) 前款安全維護措施以與所欲達成之個人資料保護目的間，應符合適當比例，並由委外單位依個人資料保護法施行細則第 12 條第 2 項所列事項，逐一確認並說明，以書面方式呈現前開事項之確認及說明，並提出予機關。

第 3 條　複委託

□雙方約定禁止複委託。

□雙方約定複委託時，委外單位義務如下：

(1) 委外單位執行業務若有複委託之需求，就涉及個人資料之蒐集、處理或利用之行為應事前取得機關之書面同意及該複委託單位對於個人資料保密之書面承諾，並以書面通知機關複委託單位之名稱、地址及個人資料之蒐集、處理、利用之範圍。

附件一

(2) 委外單位應依本條款第 1 條規定限定複委託單位蒐集、處理、利用個人資料之範圍，並對該複委託單位依個人資料保護法、個人資料保護法施行細則及教育部個人資料保護管理要點等相關規定進行適當之監督。

(3) 委外單位應於複委託合約中載明複委託單位所應遵循之個人資料保護條款，其條款包括但不限於本條款之所有義務及應盡責任。

第 4 條　當事人權利行使時之義務

委外單位執行本契約或協議之業務，接獲個人資料當事人行使權利之通知或申請時，應依相關規定予以回覆，並做成紀錄，供機關備查。

第 5 條　資料提供與受監督之義務

(1) 機關要求委外單位提供所蒐集之個人資料檔案、個人資料檔案保有之依據及特定目的、個人資料之類別等相關資訊及其蒐集、處理、利用之相關資料時，委外單位不得拒絕，並應於機關指定期限內提供。依本條款第 3 條規定經機關事前書面同意之複委託單位亦具有提供前開資料之義務。

(2) 機關定期針對委外單位之個人資料安全維護措施執行狀況進行確認，並將確認結果記錄之；必要時，得派員進行實地訪查或委託專業人員進行查核，查核項目得參照「教育部專案受託單位個人資料保護檢查表」，委外單位應予配合。查核後，認有缺失，應以書面敘明理由請委外單位限期改善。

第 6 條　通知義務

(1) 委外單位或其受僱人違反個人資料保護法、其他個人資料保護法律或其他法規命令時，應立即通知委請機關，並查明前開事項及採取因應及補救措施。

(2) 委外單位因履行契約或協議，致個人資料被竊取、洩漏、竄改或其他侵害之情形時，應立即通知機關並採取因應及補救措施；若機關認為有必要時，得介入進行調查，委外單位應予配合。委外單位於查明前開情形後，應將其違反情形(包括個人資料被侵害之事實)、涉及個資範圍、已採取及預定採取之因應及補救措施，經機關同意後，依個人資料保護法之規定以適當方式通知當事人。因調查、採取因應及補救措施、通知當事人而衍生之相關費用，由委外單位支付。

(3) 委外單位未經機關同意，應嚴守保密義務，不得對外發言或透露事故之任何訊息。

(4) 委外單位認機關之指示有違反個人資料保護法、其他個人資料保護法律或其法規命令者，應立即通知機關。

第 7 條　個人資料之刪除或返還義務

(1) 於履約期間，機關得隨時要求委外單位將執行契約或協議業務而蒐集、處理、利用之個人資料返還機關或予以刪除，且不得留存任何備份。

(2) 契約或協議終止或解除時，委外單位應刪除或銷毀因履行契約或協議而保有之個人資料，且應返還個人資料之載體及移除存取資料之權限；並提供刪除、銷毀、返還個人資料之時間、方式、地點等紀錄。

(3) 前款刪除、銷毀作業，機關於必要時，得實地查訪，委外單位應予配合。前款返還，委外單位得以交付機關指定之第三人為之。

(4) 契約或協議終止或解除時，若機關要求委外單位移轉因執行受委業務所保有之個人資料，應留存移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項

附件一

個人資料之合法依據等紀錄。

(5) 委外單位應簽署「教育部委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書正本交由機關收執。

(6) 委外專案所涉個人資料之重要性或機密性程度較高時，機關得要求委外單位執行契約或協議之執行任務人員簽署「教育部委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書正本交由機關收執。若嗣後委外單位專案人員異動，委外單位需主動要求異動人員簽署「教育部委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書交由機關收執。

第 8 條　損害賠償責任

(1) 委外單位因履行契約或協議而違反個人資料保護法、個人資料保護法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。

(2) 機關如因委外單位或其所屬人員違反個人資料保護法、個人資料保護法施行細則，而遭受損害時，得向委外單位請求損害賠償。因此遭第三人請求損害賠償時，應依照「個人資料保護法」、「國家賠償法」及其他相關法令辦理。對上述條款有疑義時，委外單位應行文機關請求解釋。

(3) 委外單位違反本條款第 1 條至第 7 條之規定，機關得依委外單位違反本條款之情節輕重，要求減少部分或全部價金；或以書面通知委外單位終止或解除契約之部分或全部；機關受有損害者，並得請求損害賠償。

第 9 條　違約金

(1) 委外單位違反本條款第 1 條至第 4 條及第 6 條至第 7 條之規定，委外單位除應負損害賠償責任外，需支付機關懲罰性違約金；懲罰性違約金金額，視委外單位違反上開規定之情節輕重，以契約或協議價金總額之 10%為上限。

(2) 委外單位違反本條款第 5 條之規定，逾期未提供資料或未限期改善，委外單位除應負損害賠償責任外，按日處以契約或協議總價千分之一作為逾期違約金，逾期違約金之總額以契約或協議價金總額之 20%為上限。

第 10 條　準據法與管轄法院

若因契約或協議所衍生之爭議與訴訟，雙方均同意以中華民國法律為準據法且以臺灣臺北地方法院為第一審管轄法院。

附件一

教育部委外專案個人資料保護條款（範本）

委外單位受機關委請蒐集、處理或利用個人資料及檔案時，雙方同意依個人資料保護法、個人資料保護法施行細則及教育部所訂定之規定訂定本條款，共同遵守，其條款如下：

第 1 條　蒐集、處理或利用時之義務

(1) 委外單位受機關委請蒐集、處理或利用個人資料及檔案（指個人資料保護法所規定之自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料）時，應符合個人資料保護法、個人資料保護法施行細則及教育部個人資料保護管理要點等相關規定。

(2) 委外單位僅得於機關指示及履行契約或協議之必要範圍內，蒐集、處理或利用個人資料（委外單位不得利用機關所提供或因執行本契約或協議專案所蒐集個人資料及檔案進行行銷或商業推銷等相關活動，或以任何方式或方法交付予履約無關之第三人，亦不得為本契約或協議專案以外之蒐集、處理或利用，包括但不限於結合委外單位原本所保有之個人資料及檔案，再為處理或利用）。

(3) 本契約或協議專案預定蒐集、處理或利用個人資料之

範圍：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

類別：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

特定目的：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

期間：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

機關保留指示之事項：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

其他事項：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

□上開範圍、類別、特定目的、期間、機關保留指示之事項和其他事項詳計畫、需求書。

第 2 條　安全維護措施

(1) 委外單位在執行本契約或協議專案委請業務所必要之範圍內，應依個人資料保護法施行細則第 12 條之規定採取適當安全維護措施，並指定專人辦理安全維護事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

(2) 前款安全維護措施以與所欲達成之個人資料保護目的間，應符合適當比例，並由委外單位依個人資料保護法施行細則第 12 條第 2 項所列事項，逐一確認並說明，以書面方式呈現前開事項之確認及說明，並提出予機關。

第 3 條　複委託

□雙方約定禁止複委託。

□雙方約定複委託時，委外單位義務如下：

(1) 委外單位執行業務若有複委託之需求，就涉及個人資料之蒐集、處理或利用之行為應事前取得機關之書面同意及該複委託單位對於個人資料保密之書面承諾，並以書面通知機關複委託單位之名稱、地址及個人資料之蒐集、處理、利用之範圍。

附件一

(2) 委外單位應依本條款第 1 條規定限定複委託單位蒐集、處理、利用個人資料之範圍，並對該複委託單位依個人資料保護法、個人資料保護法施行細則及教育部個人資料保護管理要點等相關規定進行適當之監督。

(3) 委外單位應於複委託合約中載明複委託單位所應遵循之個人資料保護條款，其條款包括但不限於本條款之所有義務。

(4) 委外單位對於複委託單位蒐集、處理、利用個人資料之行為應負完全責任。

第 4 條 當事人權利行使時之義務

委外單位執行本契約或協議之業務，接獲個人資料當事人行使權利之通知或申請時，應依相關規定予以回覆，並做成紀錄，供機關備查。

第 5 條 資料提供與受監督之義務

(1) 機關要求委外單位提供所蒐集之個人資料檔案、個人資料檔案保有之依據及特定目的、個人資料之類別等相關資訊及其蒐集、處理、利用之相關資料時，委外單位不得拒絕，並應於機關指定期限內提供。依本條款第 3 條規定經機關事前書面同意之複委託單位亦具有提供前開資料之義務。

(2) 機關定期針對委外單位之個人資料安全維護措施執行狀況進行確認，並將確認結果記錄之；必要時，得派員進行實地訪查或委託專業人員進行查核，查核項目得參照「教育部專案受託單位個人資料保護檢查表」，委外單位應予配合。查核後，認有缺失，應以書面敘明理由請委外單位限期改善。

第 6 條 通知義務

(1) 委外單位或其受僱人違反個人資料保護法、其他個人資料保護法律或其他法規命令時，應立即通知委請機關，並查明前開事項及採取因應及補救措施。

(2) 委外單位因履行契約或協議，致個人資料被竊取、洩漏、竄改或其他侵害之情形時，應立即通知機關並採取因應及補救措施；若機關認為有必要時，得介入進行調查，委外單位應予配合。委外單位於查明前開情形後，應將其違反情形(包括個人資料被侵害之事實)、涉及個資範圍、已採取及預定採取之因應及補救措施，經機關同意後，依個人資料保護法之規定以適當方式通知當事人。因調查、採取因應及補救措施、通知當事人而衍生之相關費用，由委外單位支付。

(3) 委外單位未經機關同意，應嚴守保密義務，不得對外發言或透露事故之任何訊息。

(4) 委外單位認機關之指示有違反個人資料保護法、其他個人資料保護法律或其法規命令者，應立即通知機關。

第 7 條 個人資料之刪除或返還義務

(1) 於履約期間，機關得隨時要求委外單位將執行契約或協議業務而蒐集、處理、利用之個人資料返還機關或予以刪除，且不得留存任何備份。

(2) 契約或協議終止或解除時，委外單位應刪除或銷毀因履行契約或協議而保有之個人資料，且應返還個人資料之載體及移除存取資料之權限；並提供刪除、銷毀、返還個人資料之時間、方式、地點等紀錄。

(3) 前款刪除、銷毀作業，機關於必要時，得實地查訪，委外單位應予配合。前款返還，委外單位得以交付機關指定之第三人為之。

(4) 契約或協議終止或解除時，若機關要求委外單位移轉因執行受委業務所保有之個

附件一

人資料，應留存移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據等紀錄。

(5) 委外單位應簽署「教育部委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書正本交由機關收執。

(6) 委外專案所涉個人資料之重要性或機密性程度較高時，機關得要求委外單位執行契約或協議之執行任務人員簽署「教育部委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書正本交由機關收執。若嗣後委外單位專案人員異動，委外單位需主動要求異動人員簽署「教育部委外專案契約終止或解除個人資料確認刪除、銷毀及載體返還、移轉切結書」，並將前開切結書交由機關收執。

第 8 條　損害賠償責任

(1) 委外單位因履行契約或協議而違反個人資料保護法、個人資料保護法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。

(2) 機關如因委外單位履行契約或協議而違反個人資料保護法、個人資料保護法施行細則，而遭受損害時，得向委外單位請求損害賠償。因此遭第三人請求損害賠償時，應由委外單位負責處理並承擔一切法律責任（如於訴訟中，委外單位應協助機關為必要之答辯及提供相關資料，並應負擔因此所生之訴訟費用、律師費用及其他相關費用，並負責清償機關因此對第三人所負之損害賠償責任）。

(3) 委外單位違反本條款第 1 條至第 7 條之規定，機關得依委外單位違反本條款之情節輕重，要求減少部分或全部價金；或以書面通知委外單位終止或解除契約之部分或全部；機關受有損害者，並得請求損害賠償。

第 9 條　違約金

(1) 委外單位違反本條款第 1 條至第 4 條及第 6 條至第 7 條之規定，委外單位除應負損害賠償責任外，需支付機關懲罰性違約金；懲罰性違約金金額，視委外單位違反上開規定之情節輕重，以契約或協議價金總額之 10%為上限。

(2) 委外單位違反本條款第 5 條之規定，逾期未提供資料或未限期改善，委外單位除應負損害賠償責任外，按日處以契約或協議總價千分之一作為逾期違約金，逾期違約金之總額以契約或協議價金總額之 20%為上限。

第 10 條　準據法與管轄法院

若因契約或協議所衍生之爭議與訴訟，雙方均同意以中華民國法律為準據法且以臺灣臺北地方法院為第一審管轄法院。

附件二

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，爰訂立本合約書，條款如下：

第一條：「機密資訊」定義

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、個人資料或其他與甲方公務機密相關或本質上屬於機密之資料文件。

第二條：保密義務

一、除為履行本合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等參與人員，知其有保密之義務，且向該參與人員透露「機密資訊」前，應先取得該參與人員簽署之保密同意書（附件三），並要求其負擔與乙方相同之保密義務及連帶責任。

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，應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、本合約之保密義務自該等「機密資訊」合法揭露於公眾為止。

第三條：本合約到期或終止時，乙方應將所有「機密資訊」和其根據本合約所製造之產品及其複製品返還予甲方。乙方同意於本合約到期或終止後，絕不使用或洩漏該「機密資訊」，且經由乙方而獲得「機密資訊」之受僱人、外包廠商等參與人員，絕不再使用或洩漏該「機密資訊」。

第四條：合約期限及終止

一、本合約自簽約日起生效，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、本合約第二條、第三條所定之保密義務，不因本契約終止或屆滿而失效。

第五條：賠償責任

乙方如違反本保密合約書之約定或有任何可歸責於乙方之事由，致使

甲方機密資訊公開或洩漏者，乙方願負一切賠償責任，除負擔一切法律上責任外，並對因此造成甲方一切損害（包括人格權、名譽權之侵害）負連帶賠償責任。

第六條：準據法與管轄法院

本合約之解釋、效力、履行及其他未盡事宜，悉依中華民國法律為準。當事人間因本契合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：完整合約

甲乙雙方就本合約工作所做成之書面，如訂單、採購單等，為本合約之附件，並視為本合約之一部分。本合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。

本保密合約壹式三份，由甲乙雙方簽署後生效，甲方收執二份，乙方收執一份為憑。

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

附件三

保密同意書

茲緣於簽署人 .....（簽署人姓名，以下稱簽署人）參與.....（乙方名稱，以下稱乙方）之教育部（以下稱本部）.....（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條 簽署人已詳讀

□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

□教育部委外專案個人資料保護條款

第二條 簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切本部未標示得對外公開之公務秘密，以及本部依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於本部指定之處所內使用之。非經本部事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至本部或本部所指定處所以外之處所。

第三條 簽署人知悉或取得本部公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約乙方團隊成員人員。

第四條 簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由本部提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約本部業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第五條 簽署人若違反本同意書之規定，本部得請求簽署人及其任職之乙方賠償本部因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之乙方亦應負賠償責任。

第六條 簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第七條 本同意書一式叁份，本部、簽署人及.....（乙方）各執存一份。

簽署人姓名及簽章：

簽署人身分證字號：■-■■■■■ _ _ _ _

簽署人聯絡電話：

乙方名稱及蓋章：

乙方負責人或代理人姓名及簽章：

中 華 民 國 年 月 日

附件四

「　　（系統名稱）」資通系統安全等級評估表

紀錄編號：YYYMMDD	填表日期：　　年　　月　　日

功能說明：

影響構面				資通系統安全等級
1.機密性	2.完整性	3.可用性	4.法律遵循性	

設定影響構面等級

影響構面	安全等級		原因說明
1.機密性	初估		
	異動		
2.完整性	初估		
	異動		
3.可用性	初估		
	異動		
4.法律遵循性	初估		
	異動		
備註			

承辦單位	資訊單位

註：請各機關依本身實際陳核流程調整簽核欄位。

附件五

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

（委外單位）

立切結書人（委外單位）於中華民國　年　月　日起至　年　月　日止，執行教育部專案＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（以下簡稱本案）。並切結下列事項：

一、委外單位對於本案所蒐集、處理、利用之個人資料及履行契約(含行政協議書)而持有之資料，應善盡保管義務，未得教育部書面同意，不得洩露、幫助、告知、交付、複製、節錄或以其他任何方式移轉與第三人，即使中途解約亦同。委外單位對其人員之行為應負連帶責任，並於本案契約或行政協議終止、解除或履行完畢時，將所持有之個人資料及履行契約(含行政協議書)而持有之資料進行刪除、銷毀及載體返還、移轉。

二、委外單位確認已詳細閱讀

□教育部委外專案個人資料保護條款

□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

及契約(含行政協議書)等相關規定，如有不當使用個人資料或侵害個人隱私，除應依相關規定追究行政責任外，應負法律責任，並賠償教育部之損害。

三、若因此契約或協議所衍生之爭議及訴訟，委外單位與教育部均同意以中華民國法律為準據法，且以臺灣臺北地方法院為第一審管轄法院。

四、本切結書正本由教育部收執，影本由立切結書人收執。

此致

教育部

委外單位：

代表人：

統一編號：

地　　址：

電　　話：

中　華　民　國　　年　　月　　日

附件五

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

（執行任務人員）

立切結書人（執行任務人員）於中華民國　年　月　日起至　年　月　日止，執行教育部專案＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（以下簡稱本案）。並切結下列事項：

一、本人對於本案所蒐集、處理、利用之個人資料及履行契約(含行政協議書)而持有之資料，應善盡保管義務，未得教育部書面同意，不得洩露、幫助、告知、交付、複製、節錄或以其他任何方式移轉與第三人，即使中途因故離職亦同。並於本案契約或行政協議終止、解除或履行完畢時，將所持有之個人資料及履行契約(含行政協議書)而持有之資料進行刪除、銷毀及載體返還、移轉。

二、本人確認已詳細閱讀

□教育部委外專案個人資料保護條款

□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

及契約(含行政協議書)等相關規定，如有不當使用個人資料或侵害個人隱私，除應依相關規定追究行政責任外，應負法律責任，並賠償教育部之損害。

三、若因此契約或協議所衍生之爭議及訴訟，本人與教育部均同意以中華民國法律為準據法，且以臺灣臺北地方法院為第一審管轄法院。

四、本切結書正本由教育部收執，影本由立切結書人收執。

此致

教育部

執行任務人員(本人簽章)：

所屬單位：

電　　話：

地　　址：

中　華　民　國　　年　　月　　日

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。

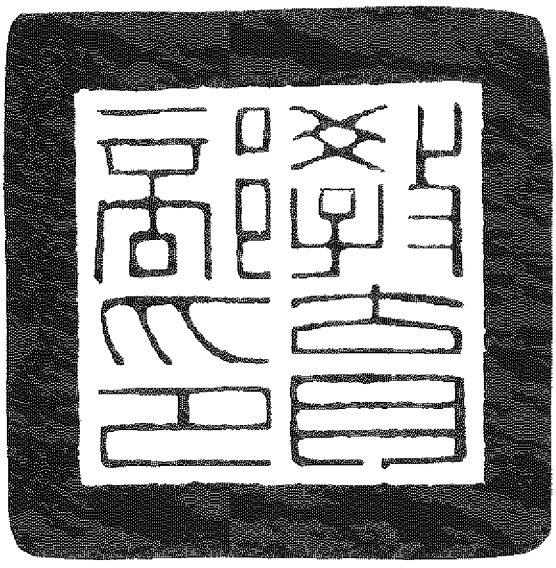
（二）上線後：

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。

檔　　號：
保存年限：

教育部　令

發文日期：中華民國110年6月18日
發文字號：臺教資(四)字第1100068264B號



裝

修正「教育部辦理或補助建置與維護伺服主機及應用系統網站資訊安全管理要點」，名稱並修正為「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」，並自即日生效。

訂

附修正「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」

部長潘文忠

線