海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法第十五條、第十六條之一、第十六條之二修正總說明

海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法(以下簡稱本辦法)係於一百零五年九月一日訂定發布，歷經一次修正，最近一次係於一百零八年三月八日修正發布。依行政院一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」(第一次會議)有關非公務機關個資安全維護管理規劃與分級規範、強化資安標準規範之規劃、增訂非公務機關個資外洩事件通報(知)中央目的事業主管機關之規定決議，爰修正本辦法第十五條、第十六條之一及第十六條之二，其修正重點如次：

一、鑑於聯繫會議決議通報時點應為七十二小時內通報，爰修正為七十二小時內通報主管機關，並增訂應通報事項提供通報格式範本之附件，未依時限內通報者，應附理由說明及增列後續行政檢查，為適當之監督管理措施。(修正條文第十五條)

二、增訂境外臺校提供電子商務服務系統、特種個資或大量個資之連網資通系統時，應採取所列資訊安全措施，以加強管理。(修正條文第十六條之一)

三、增訂境外臺校進行跨境傳輸個人資料前，應確認是否有主管機關依本法第二十一條所定限制範圍，並告知學校學生及教職員其個人資料所欲跨境傳輸之區域，同時對資料接收方為相關事項監督。(修正條文第十六條之二)

海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法第十五條、第十六條之一、第十六條之二修正條文對照表

修正條文	現行條文	說明
第十五條　境外臺校應訂定應變機制，在發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理以保護當事人之權益。 前項應變機制，應包括下列事項： 一、採取適當之措施，控制事故對當事人造成之損害。 二、查明事故發生原因及損害狀況，並以適當方式通知當事人。 三、研議改進措施，避免事故再度發生。 境外臺校應自第一項事故發現時起七十二小時內，填具個人資料侵害事故通報與紀錄表（如附件），通報主管機關，未依時限內通報者，應附理由說明；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。 依規定通報後，主管機關得派員檢查，受檢者不得規避、妨礙或拒絕，主管機關並得依本法第二十二條至第二十五條規定為適當之監督管理措施。	第十五條　境外臺校應訂定應變機制，在發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理以保護當事人之權益。 前項應變機制，應包括下列事項： 一、採取適當之措施，控制事故對當事人造成之損害。 二、查明事故發生原因及損害狀況，並以適當方式通知當事人。 三、研議改進措施，避免事故再度發生。 境外臺校應自第一項事故發現之日起三日內，通報主管機關，並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。	一、第一項及第二項未修正。 二、修正第三項及增列第四項，說明如下： （一）為強化中央目的事業主管機關落實個人資料保護之監管，依行政院一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」決議略以，各中央目的事業主管機關所定個人資料檔案安全維護辦法，應至少明訂外洩通報對象、時點、應通報事項、後續行政檢查等事項；並參酌國家發展委員會一百十年六月二十五日發法字第一一〇二〇〇〇九四八號函，建議修正本條規定通報時限為自事故發現時起七十二小時，及參考該委員會訂定之「個人資料侵害事故通報與紀錄表」，爰修正本條之規範事項。 （二）第三項，修正個人資料侵害事件之通報

		時限為七十二小時，並明定應填具個人資料侵害事件通報與紀錄表，及未依時限通報者，應附理由說明。 (三) 第四項，依前項規定通報後，主管機關得派員進行行政檢查，受檢者不得規避、妨礙或拒絕；主管機關並得依個人資料保護法第二十二條至第二十五條規定，為適當之監督管理措施。
第十六條之一　境外臺校提供電子商務服務系統或本法第六條所定個人資料種類之資通系統時，應採取下列資訊安全措施: 一、使用者身分確認及保護機制。 二、個人資料顯示之隱碼機制。 三、網際網路傳輸之安全加密機制。 四、應用系統於開發、上線、維護等各階段軟體驗證及確認程序。 五、個人資料檔案與資料庫之存取控制與保護監控措施。 六、防止外部網路入侵對策。		一、本條新增。 二、依行政院一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」決議略以，有關非公務機關使用資通系統蒐集、處理或利用個資資料，若為甲級（保有消費者交易、使用商品或接受服務等過程之一般或特種個資，且該資料達一定之適用門檻，如：個資數量、該業者資本額達一定金額或其他中央目的事業主管機關指定之特定標準，或其他經中央目的事業主管機關指定)者，應增訂適當資安標準規範，以加強管理。目

七、非法或異常使用行為之監控與因應機制。 前項所稱電子商務，指透過網際網路進行有關商品或服務之廣告、行銷、供應或訂購等各項商業交易活動；資通系統，指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 第一項第六款及第七款所定措施，應定期演練及檢討改善。		前境外臺校保有大量師生個資連網資通系統，又學校保有學生健檢等資料，涉特種個資範圍，考量網際網路對於個人資料安全之潛在風險，需採行相關個人資料安全保護措施，包括系統使用者之身分確認、個人資料顯示之隱碼去識別化機制、網際網路傳輸之安全加密、系統中個人資料檔案及資料庫之存取控制與保護監控、防範外部網路入侵及其他非法或異常使用等，為境外臺校師生個人資料之安全維護，爰於第一項各款予以明定安全管理措施。 三、第二項，參考行政院所定電子商務消費者保護綱領，明定電子商務之定義，後段參考資通安全管理法所定資通系統之定義。 四、為使境外臺校之連網資通系統或電子商務系統遭遇各類資安事件時，得以儘速恢復正常並控制損害，爰於第三項明定境外臺校宜針對防範非法入侵或異常使用等應變措施定期進行演練及

		檢討改善。
第十六條之二　境外臺校進行個人資料國際傳輸前，應檢視有無主管機關依本法第二十一條規定為國際傳輸之限制，並且告知境外臺校學生及教職員其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督： 一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。 二、當事人行使本法第三條所定權利之相關事項。		一、本條新增。 二、考量目前本辦法並無針對境外臺校進行跨境傳輸個人資料有相關規範，爰參考製造業及技術服務業個人資料檔案安全維護管理辦法第九條及依本法第二十一條規定非公務機關為國際傳輸個人資料，有涉及國家重大利益、國際條約或協定有特別規定、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞、以迂迴方法向第三國（地區）傳輸個人資料規避本法之情形之一者，中央目的事業主管機關得限制之。明定境外臺校於跨境傳輸個人資料前應確認是否有主管機關依本法第二十一條所定限制範圍，並告知學校學生及教職員其個人資料所欲跨境傳輸之區域，同時對資料接收方為相關事項監督。

第十五條附件

<table>
<tr><th colspan="3">個人資料侵害事故通報與紀錄表</th></tr>
<tr><td>非公務機關名稱

通報機關</td><td colspan="2">通報時間：　　年　　月　　日　　時　　分
通報人：　　簽名（核章）
職稱：
電話：
E-mail：
地址：</td></tr>
<tr><td>事故發現時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事故發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個資侵害之總筆數（大約）</td></tr>
<tr><td>□一般個資＿＿＿＿筆
□特種個資＿＿＿＿筆</td></tr>
<tr><td>發生原因及事故摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩後 72 小時通報</td><td colspan="2">□是　　□否，理由：</td></tr>
</table>