私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法第八條、第十二條之一、第十二條之二修正總說明

現行私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法（以下簡稱本辦法）係於一百零三年八月二十一日訂定發布。鑒於行政應落實個人資料保護執行，強化資安標準規範之規劃，及非公務機關個人資料外洩事件通報中央目的事業主管機關之規定，爰修正本辦法第八條、第十二條之一、第十二條之二，其修正要點如下：

一、學校、機構應自資安事故發現時起七十二小時內，通報主管機關，及未依時限內通報者，應附理由說明，並明定通報內容及後續行政檢查。（修正條文第八條）

二、學校、機構提供電子商務服務系統或個人資料保護法第六條所定個資種類之資通系統時，應採取相關之資訊安全措施。（修正條文第十二條之一）

三、學校、機構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。（修正條文第十二條之二）

私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法第八條、第十二條之一、第十二條之二修正條文對照表

修正條文	現行條文	說明
第八條　學校、機構應訂定應變機制，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。 學校、機構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，為適當之監督管理機制。	第八條　學校、機構應訂定應變機制，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。	一、第一項及第二項未修正。 二、增列第三項及第四項，說明如下： (一)依行政院一百十年三月四日院授發協字第一一〇二〇〇〇三四三號函，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」決議相關事項，及教育部「行政機關落實個資保護執行聯繫會議之本部應辦事項」「未依時限內通報者，應附延遲理由」之相關文字；並參酌一百十年七月七日教育部「有關行政機關落實個資保護執行聯繫會議決議本部相關辦法修正建議」修正通報時限為發現時起「七十二小時」，並增列「應通報之內容及後續行政檢查事項」。 (二)第三項，增列個人資料侵害事件之通報時限，並明定應填具個人資料侵害事故通報與紀錄表及未依時限內通報者，應附理由

		說明。 (三)第四項,依第三項規定通報後，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。
第十二條之一　學校、機構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及保護監控措施。 六、防止外部網路入侵對策。 七、非法或異常使用行為之監控及因應機制。 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		一、本條新增。 二、為強化資安標準規範，增加分級原則及資安標準規範,第一項增列「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管制措施」之相關文字。 三、第二項，前段參考行政院所定「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、第三項，為使學校、機構提供之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，爰明定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。

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。		
第十二條之二　學校、機構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、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、以迂迴方式向第三國（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。考量本辦法並無針對境外學校、機構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，明定學校、機構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個人資料所欲跨境傳輸之區域，同時對資料接收為相關事項監

		督。

第八條附件

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></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>