移民業務機構個人資料檔案安全維護管理辦法部分條文修正條文對照表

修正名稱	現行名稱	說明
內政部指定移民業務機構個人資料檔案安全維護管理辦法	移民業務機構個人資料檔案安全維護管理辦法	配合個人資料保護法(以下簡稱本法)第二十七條第二項規範意旨，爰修正本辦法名稱。
修正條文	**現行條文**	**說明**
第五條　移民業務機構應配置適當管理人員及相當資源，負責規劃、訂定、修正及執行本計畫相關事項，並定期向負責人提出報告。	第五條　移民業務機構應配置適當人員及相當資源，負責規劃、訂定、修正與執行本計畫或業務終止後個人資料處理方法等相關事項。	一、本計畫內容已包含業務終止後之個人資料處理方法，無須重複規定，爰刪除相關文字。 二、參考內政部指定警政類非公務機關個人資料檔案安全維護管理辦法第五條第一項規定，增訂定期向負責人提出報告之規定，促使負責人能據以監督本計畫之執行，落實對個人資料保護之工作。
第六條　移民業務機構應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫之範圍。	第六條　移民業務機構應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。 移民業務機構經清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄。	一、參考內政部指定警政類非公務機關個人資料檔案安全維護管理辦法第六條規定，修正第一項規定。 二、現行條文第二項移列至第十八條，爰予刪除。

第十一條　內政部依本法第二十一條規定，對移民業務機構為限制國際傳輸個人資料之命令或處分時，移民業務機構應通知所屬人員遵循辦理。 移民業務機構將個人資料作國際傳輸者，應檢視是否受內政部限制，並告知當事人其個人資料所欲國際傳輸之區域，且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。	第十一條　移民業務機構進行個人資料國際傳輸前，應檢視有無內政部依本法第二十一條規定所為之限制。	一、本法第二十一條規定所為之命令或處分，移民業務機構應通知所屬人員知曉並遵照辦理，爰新增第一項。 二、現行條文移列為第二項，移民業務機構將個人資料作國際傳輸者，應檢視是否受內政部依本法第二十一條規定之命令或處分限制，並且告知個人資料所欲國際傳輸之區域，同時對資料接收方為相關之監督，以為強化移民業務機構進行消費者個人資料國際傳輸之具體措施，爰修正相關文字。
第十三條　移民業務機構應訂定應變機制，在發生個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害情形（以下簡稱事故）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、採取適當之措施以控制事故對當事人造成損害。	第十三條　移民業務機構應訂定應變機制，在發生個人資料被竊取、洩漏、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、採取適當之措施以控制事故對當事人造成損害。	一、配合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」第一次會議決議，修正第二項第四款，明定發生重大事故者，移民業務機構應於發現後七十二小時內填具書面通報內政部，內政部得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管

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事故事實、因應措施及諮詢服務專線等。 三、研議改進措施，避免類似事故再度發生。 四、發生重大事故者，應於發現後七十二小時內以書面通報內政部（書面通報格式如附件），內政部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。 前項第四款所稱重大事故，指個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害情形，達一百五十筆以上。	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事故事實、因應措施及諮詢服務專線等。 三、研議改進措施，避免類似事故再度發生。 四、發生重大個人資料事故者，應即以書面通報內政部。 前項第四款所稱重大個人資料事故，指個人資料被竊取、洩漏、竄改或其他侵害事故，致危及大量當事人權益之情形。	理措施。 二、依入出國及移民法第五十六條第六項規定，移民業務機構應每年陳報營業狀況，並保存相關資料五年。另考量每家移民業務機構經營規模不同，且實務上大多屬小公司，營運規模較小，人力成本有限，每年度所辦理之移民案件數相對較低。經綜合考量上開因素，爰將第三項所定重大事故，修正為達一百五十筆以上之情形，以臻明確。
第十四條之一　移民業務機構使用資通訊系統蒐集、處理或利用消費者個人資料達一千筆以上者，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。		一、本條新增。 二、依行政院一百十年二月三日會議決議，為強化資安標準規範，應建立個人資料管理分級制度。鑒於每家移民業務機構成立時間及營運規模不同，經統計成立十年以上且現仍存續中之移民業務機構，約佔三

三、網際網路傳輸之安全加密機制。 四、個人資料檔案與資料庫之存取控制及保護監控措施。 五、防止外部網路入侵對策。 六、非法或異常使用行為之監控及因應機制。 前項第五款及第六款所定措施，應定期演練及檢討改善。		十八家。相對蒐集、處理或利用之個人資料數亦累計增加，爰為能加強管理成立較久及較大規模之移民業務機構，於第一項明定移民業務機構使用資通訊系統蒐集、處理或利用個人資料達一千筆以上者，參照行政院資通安全處建議，至少應採取下列資訊安全措施，以落實保護個人資料：(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)個人資料檔案及資料庫之存取控制與保護監控措施；(五)防止外部網路入侵對策及(六)非法或異常使用行為之監控與因應機制。另參考資通安全責任等級分級辦法附表十資通系統防護基準，針對六項資訊安全措施之實作說明如下： (一)系統應建立帳號管理機制，包含帳號申請、建立、修改、啟用、停用及刪除程序，並執行身分驗證管理，如身分驗證資

		訊不以明文傳輸、密碼複雜度或帳號鎖定機制等。 （二）系統界面呈現個人資料時，應以適當且一致性之隱碼或遮罩處理，以避免過多且非必要之個人資料揭露，可參考 CNS 二九一九一「資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項」國家標準。 （三）個人資料傳輸時，應採用傳輸加密機制，如採用加密傳輸通道、使用公開、國際機構驗證且未遭破解之演算法。 （四）儲存於電子媒體及資料庫之個人資料，應適當加密保護，並提供使用者識別、鑑別及身分管理，並採用最小權限原則進行存取控制管理。 （五）針對外部入侵之防禦，應採用適當資安控制措施建立防禦縱深，包括防毒軟體、防火牆、入侵偵測與防禦系統，及應用程式防火牆等。

		（六）針對系統或個人資料檔案之存取，應確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件，且應留存系統相關日誌紀錄並定期檢視，或設置適當監控及異常行為預警機制。 三、隨網路科技之進步，個人資料遭外部網路入侵或非法或異常使用行為損害情形層出不窮，爰第二項明定針對第一項第五款及第六款所定措施，非公務機關應定期進行演練及檢討改善。
第十六條　移民業務機構應訂定個人資料檔案安全維護查核機制，並指定適當人員每年至少一次檢查本計畫之執行情形。 前項檢查結果應向負責人提出報告，並留存相關紀錄，其保存期限至少五年。 移民業務機構依第一項檢查結果發現本計畫不符法令或有不符法令之虞者，應即改善。	第十六條　移民業務機構應訂定個人資料檔案安全維護查核機制，定期或不定期檢查本計畫之執行情形。 前項定期檢查本計畫之執行，每二年至少一次，並作成書面紀錄，其保存期限至少五年。	為落實移民業務機構查核機制，並強化其對消費者之個人資料保護，應定期辦理執行情形之檢查，並由每二年至少一次增加為每年至少一次，爰修正第一項及第二項。另檢查結果不符法令或有不符之虞者，應即改善，爰新增第三項。
第十八條　移民業務機構執行本計畫所定各種個	第十八條　移民業務機構應採行適當措施，留存個人資料使用紀錄、自動化	一、參考內政部指定警政類非公務機關個人資料檔

人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。 移民業務機構依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄： 一、刪除、停止處理或利用之方法、時間或地點。 二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。 前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。	機器設備之軌跡資料或其他相關之證據資料，其保存期限至少五年。	案安全維護管理辦法第十八條第一項規定，修正第一項文字。 二、明定移民業務機構依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料時，亦應留存相關紀錄；且上述軌跡資料、相關證據及紀錄，除法令另有規定或契約另有約定者外，應至少留存五年，爰新增第二項及第三項。
第二十條之一　本辦法修正施行前，未訂定或已訂有本計畫之移民業務機構，應依本辦法規定訂定或修正，並於本辦法修正施行日起六個月內，將本計畫報請內政部備查。		一、本條新增。 二、增訂本辦法修正施行前之移民業務機構應依本辦法訂定或修正本計畫，並於一定期間內報送備查。

第十三條附件(新增)

附件

<table>
<tr><td colspan="3">個人資料事故通報及紀錄表</td></tr>
<tr><td>移民業務機構名稱
_____

通報機關
_____</td><td colspan="2">通報時間：　年　月　日　時　分
通報人：　　簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取
□竄改
□毀損
□滅失
□洩漏
□其他侵害情形</td><td>個人資料侵害之總筆數(大約)
_____</td></tr>
<tr><td>□一般個人資料 _____筆
□特種個人資料 _____筆</td></tr>
<tr><td>發生原因及摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</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>是否於發現個人資料外洩後七十二小時內通報</td><td colspan="2">□ 是　□否，理由：</td></tr>
</table>

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。

修正說明：

一、本附表新增。

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」第一次會議決議，定明移民業務機構遇個人資料事故發生後，應依本附件格式通報內政部。