教育部主管目的事業之個人資料檔案

自我檢查表

說明：

1. 依個人資料保護法第27條及第48條第1項及第3項之規定，各受檢查單位(即教育部所轄之非公務機關)應依個人資料保護法及受檢查單位(非公務機關)所自行制定之個人資料檔案安全維護計畫（以下簡稱安全維護計畫），落實個資保護機制，故不限於本表所列項目。
2. 經營業別(代碼)： A：私立專科以上學校；B：私立兒童課後照顧服務中心；C：短期補習班；D：私立高級中學；E：私立國民中學；F：私立國民小學；G：私立幼兒園；H：運動彩券業；I：特定體育團體；J：體育運動團體；K：運動事業；L：海外臺灣學校；M：大陸地區臺商學校；N：其他；
3. **受檢單位若因所屬之事業別尚未有個人資料檔案安全維護計畫實施辦法，針對該事業別每個未有法規規範的檢查項，如所提供的佐證已經達符合條件，則可勾選符合；若無相關項目業務，則可勾選“不適用”之” 無此項業務”。若無相關法規要求，則可勾選“不適用”之”無明確法規要求”，但業者有採行本項措施，亦可檢附相關佐證。**
4. **請檢附自我檢查項目之相關佐證文件與簡要說明，佐證文件以112年度成果為主，若112年度尚未完整執行，亦可提供本(113)年度之成果資料加強說明。**
5. **「○」選項代表單選，「□」選項代表複選，檢查重點說明請參照「填表說明」，「*」選項代表必須繳交之佐證資料。**
6. 請依照各事業別主管司署，要求提供相應的紙本或電子佐證資料檔。
7. **提供的佐證檔案請適當去識別化，避免衍生個資爭議。**
8. 所提供之佐證資料如過多者，請以標籤紙標註檢查項目要求之條文位置，以利檢查委員審查。
9. **每個檢查項如未達符合條件，均為不符合。**
10. **名詞解釋**
    1. 特定目的：參考法務部101年10月01日修正之「個人資料保護法之特定目的及個人資料之類別」法規。
    2. 專人：指由各受檢查單位(非公務機關)所指定，負責規劃、訂定、修正及執行安全維護計畫，及業務終止後個人資料處理方法與其他相關事項，並應定期向組織提出報告之人員。
    3. 管理人：由負責人擔任或指定人選，負責督導安全維護計畫訂定及執行。
    4. 稽核人員：由負責人指定，負責定期或不定期檢核專人或專責組織是否落實執行安全維護計畫之相關事項。
    5. 電子商務服務系統：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。
    6. 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。

壹、 受檢查單位基本資料

		填表說明對應頁數
1.受檢查單位名稱	(非學校單位，請填報立案全名稱)	
2.填寫日期	_____年_____月_____日	1
3.經營業別	○ A ○ B ○ C ○ D ○ E ○ F ○ G ○ H ○ I ○ J ○ K ○ L ○ M ○ N	1
4.具對外電子商務服務系統或具有特種個資之資通系統	○是○否	1
5.個資保護要求強度等級	個資數量分級：○ 1○ 2○ 3	2
	外部利用分級：○ 0○ 1○ 2○ 3	2
	國際傳輸分級：○ 0○ 1○ 2○ 3	2
	等級：○普 ○中 ○高	2-3

貳、 受檢單位自我檢查項目

檢查事項	檢核細項	個資保護要求強度等級	檢查內容	填表說明對應頁數
1、個人資料檔案安全維護計畫	1.1 訂定「個人資料檔案安全維護計畫」	普中高	訂定個人資料檔案安全維護計畫(含業務終止後個人資料處理方法) ○是 ○否 ○不適用(無明確法規要求)	4
2、組織及運作管理情形	2.1 指定專人或建立專責組織負責管理	普中高	個資保護專人或專責組織 ○無 ○有，專責單位名稱或專責(職)人員_____ ○不適用(無明確法規要求)	5
3、專責人員或專責組織任務	3.1 規劃、訂定、修正與執行所訂安維計畫	普中高	規劃、訂定、修正與執行個人資料檔案安全維護計畫 ○有，檢附相關佐證資料 ○無 ○不適用(無明確法規要求)	6
	3.2 定期向管理人暨代表人或其他代表權人報告	普中高	專責人員定期向管理人暨代表人或其他代表權人報告個人資料檔案安全維護計畫執行情況 ○無 ○有，報告形式 □核准紀錄 □會議紀錄 □其他，_____	6

檢查事項	檢核細項	個資保護要求強度等級	檢查內容	填表說明對應頁數
			◯不適用(無明確法規要求)	
	3.3 依稽核人員評核結果檢討改進，並向管理人與稽核人員提出書面報告	普中高	個人資料檔案安全維護計畫執行情形，定期或不定期稽核 ◯無 ◯有，檢附相關佐證資料 1、 稽核/查核日期:＿＿年 月 日＿＿ 2、 專責人員或專責組織改善報告提出日期： ＿＿年 月 日＿ ◯不適用(無明確法規要求)	7
	3.4 訂定個人資料保護管理政策	高	訂定個人資料保護管理政策 ◯無 ◯有，檢附個人資料保護管理之政策公開紀錄 ◯不適用(無明確法規要求)	7
	3.5 定期對所屬人員進行宣導或專業教育訓練	普中高	提升個資保護意識護宣導或其他教育訓練執行情形 1、 近期宣導、教育訓練次數：＿＿＿＿＿ 2、 近期教育訓練日期：＿年 月 日＿＿ ◯不適用(無明確法規要求)	7
4、個人資料盤點、管理與紀錄	4.1 定期盤點所保有個人資料並確認應遵守之法令	普中高	個人資料檔案盤點情形 近期個人資料檔案盤點日期：＿年 月 日＿ 個人資料檔案盤點欄位包含以下哪些內容(可複選)： □個人資料之類別 □特種個資 □蒐集方式 □保存期限 □銷毀方式 □處理方式 □利用方式 □控制措施 □其他，＿＿＿＿ ◯不適用(無明確法規要求)	8
	4.2 風險分析及管控措施	普中高	分析評估風險，訂定適當之管控措施評估 1、 已核定可接受之風險值：◯是◯否 2、 負責人或管理人核定風險值時間： ＿年 月 日 ◯不適用(無明確法規要求)	8
	4.3 依資料屬性訂定管理程序	普中高	資料蒐集、處理及利用管理程序規範 ◯無 ◯有，檢附相關佐證資料 ◯不適用(無明確法規要求)	9

檢查事項	檢核細項	個資保護要求強度等級	檢查內容	填表說明對應頁數
	4.4 向當事人蒐集個資，或於利用非由當事人提供之個資前，盡告知義務	普中高	利用非由當事人提供之個資前告知形式(可複選) □書面通知 □口頭告知 □網站公告 □個資收集表單 □隱私政策聲明 □簡訊通知 □其他，____	9
	4.5 檢視蒐集、處理個人資料是否符合個人資料保護法第十九條規定之目的及要件	普中高	適用個人資料保護法第十九條規定之目的及要件 ○無 ○有，檢附以下相關佐證資料(可複選) □安全維護計畫執行之檢查報告 □個資蒐集紙本表單 □個資蒐集系統畫面截圖	10
	4.6 委託他人進行資料蒐集、處理或利用，進行適當監督	普中高	委託他人進行資料蒐集、處理或利用 ○無個資委外 ○有個資委外 1、 委外進行資料蒐集、處理或利用之監督情形近期對委外機構的檢核日期: 年 月 日 2、 委外監督事項應包含個資法施行細則第八條第2項規定： 一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 二、受託者就個資法施行細則第十二條第二項採取之措施。 三、有複委託者，其約定之受託者。 四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。 五、委託機關如對受託者有保留指示者，其保留指示之事項。 六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。	11
	4.7 首次利用個資行銷之當事人確認作業	普中高	○無首次利用 ○有首次利用(可複選) □電子郵件 □書面通知 □簡訊	12

檢查事項	檢核細項	個資保護要求強度等級	檢查內容	填表說明對應頁數
			□電話 □網站公告 □其他，_____	
	4.8 確認與維護保有個資之正確性	普中高	為維護保有個資正確性的機制，應主動或依當事人之請求更正或補充之： 受檢單位個資受理窗口： 姓名：_____職稱：_____	12
	4.9 針對所屬人員設定不同管理權限，並要求負保密義務	普中高	建立管理機制，設定所屬人員不同之權限 ○無（免附權限管控紀錄） ○有（請檢附權限管控紀錄） 是否有委外廠商/人員 ○無（請檢附所屬人員之保密切結書紀錄） ○有（請檢附所屬人員及委外廠商/人員之保密切結書紀錄） ○不適用(無明確法規要求)	13
	4.10 對存有個資之系統設備、媒介物等採取安全管理措施	普中高	系統設備、媒介物(含非電子類)及採取必要之防護措施 ○無 ○有，檢附相關防護措施佐證 ○不適用(無明確法規要求)	13
	4.11 存有個資之系統設備、媒介物報廢或轉作他用時，採取適當防護措施	普中高	系統設備、媒介物報廢或轉作他用時之防護措施 1. 紙本、電子資料及設備應訂有銷毀程序 ○無 ○有 ○自行清除、處理 ○由委外方清除、處理 清除單位：_____處理單位：_____ ○不適用(無明確法規要求)	14
	4.12 留存所有個資使用紀錄、機關設備軌跡紀錄、相關證據紀錄	普中高	安全維護計畫各項程序及措施執行紀錄 ○無執行 ○有，檢附相關保留佐證 受檢單位目前個資保存期限：_____ ○不適用(無明確法規要求)	14
5、保有個資達一百筆，或具對外電子商務服務系	5.1 使用者身分確認及保護機制	普中高	使用者身分確認及保護機制 ○無，請說明理由_____ ○有，檢附相關佐證資料 ○不適用(無明確法規要求) ○不適用(不符合本項條件)	15
	5.2 個人資料顯示之隱碼機制	普中高	系統輸出個資(如紙本列印、螢幕顯示)時，以適當隱碼遮罩處理)	15

檢查事項	檢核細項	個資保護要求強度等級	檢查內容	填表說明對應頁數
統，或具有特種個資之資通系統之安全管理			○無 ○有，隱碼遮罩項目 □身份證字號 □姓名 □其他，_____ ○不適用(無明確法規要求) ○不適用(不符合本項條件)	
	5.3 網際網路傳輸之安全加密機制	普中高	網路傳輸加密機制 ○無傳輸加密 ○有傳輸加密，傳輸加密機制形式(可複選) □ SSL/TLS □ VPN □其他，_____ ○不適用(無明確法規要求) ○不適用(不符合本項條件)	16
	5.4 個人資料檔案及資料庫之存取控制與保護監控措施	普中高	○存放個資之系統，資料庫存取控制與保護監控措施形式(可複選) □強化身份驗證 □存取紀錄 □權限管理 □安全訪問控制 □系統日誌 □資料庫加密 □定期漏洞掃描 □其他，_____ ○不適用(無明確法規要求) ○不適用(不符合本項條件)	16
	5.5 防止外部網路入侵對策	普中高	○有系統，防止外部網路入侵對策形式(可複選) □防火牆 □防毒 □入侵防護IPS / 入侵偵測IDS □內外網路區隔 □其他，_____ ○不適用(無明確法規要求) ○不適用(不符合本項條件)	17
	5.6 非法或異常使用行為之監控與因應機制	普中高	○有系統，監控作業形式(複選) □LOG(日誌) □自動警示機制 □存取控制 □行為監控系統 □行為分析	17

檢查事項	檢核細項	個資保護要求強度等級	檢查內容	填表說明對應頁數
			□其他，_____ ○不適用(無明確法規要求) ○不適用(不符合本項條件)	
	5.7 定期演練及檢討改善	普中高	定期演練情形 ○無 ○有，演練日期：　年　月　日 檢討日期：　年　月　日 ○不適用(無明確法規要求) ○不適用(不符合本項條件)	18
6、環境管理措施	6.1 對個資存取媒介物及環境(如機房、雲端)，採取環境管理措施	中高	個資存取媒介物及環境(如機房、雲端、媒介物保存櫃)管理措施 ○無 ○有，檢附相關資料 ○不適用(無明確法規要求)	19
7、業務終止之個資管理	7.1 訂有業務終止之個資處置措施	普中高	業務終止之個資處置措施程序 ○無 ○有，檢附相關資料 ○不適用(無明確法規要求)	20
	7.2 留存相關紀錄	普中高	○無業務中止 ○有，請列舉本年度業務中止之個資檔案清冊： _____	20
8、事故通報與應變程序	8.1 訂定個資洩漏等事故發生或知悉起72小時內通報流程	普中高	1.訂定個人資料事故通報作業規範/應變機制 ○無 ○有，檢附相關資料 ○不適用(無明確法規要求) 2.截至填報日期前本年度事故 ○無事故發生 ○曾有事故者，事故發生次數_____，最近一次事故通報日期:_____，檢附相關資料	21
	8.2 訂定對個資洩漏等事故採應變措施以控制損害	普中高	訂定個資洩漏等事故應變措施 ○無 ○有，檢附相關資料 ○不適用(無明確法規要求)	21
	8.3 訂定查明事故後以適當方式通知當事人之程序並告知已採取因應措施	普中高	訂定事故應變機制對通知當事人之程序及規範 ○無 ○有，檢附相關資料	21

檢查事項	檢核細項	個資保護要求強度等級	檢查內容	填表說明對應頁數
	8.4 研議預防機制	普中高	應變機制之矯正預防程序 ◯無事故發生 ◯有事故者，事故案發日期：_____ 矯正預防紀錄最近日期：_____ ◯不適用(無明確法規要求)	22
9、資安檢測	9.1 系統弱點掃描	普中高	如有自行開發或委外之資訊系統，若屬於服務型系統，請依下列事項： ◯無 ◯有處理個人資料之資訊系統 ◯未執行弱點掃描 ◯弱掃日期：_____ 弱掃執行人員/機構名:_____ 修補日期：_____	23
	9.2 滲透測試	普中高	◯無 ◯有處理個人資料之資訊系統， ◯未執行滲透測試 ◯滲透測試日期：_____ 執行人員/機構名稱:_____	23
	9.3 資安健診	普中高	◯無 ◯資安健診日期：_____ 執行人員/機構名稱:_____ 資安健診項目(可複選) ☐網路架構檢視 ☐網路惡意活動檢視(有線) ☐使用者端電腦惡意活動檢視 ☐伺服器主機惡意活動檢視 ☐目錄伺服器設定檢視 ☐防火牆連線設定檢視 ☐資料庫安全檢視 ☐其他，_____	23
	9.4 APP檢測	普中高	如有自行開發或委外之APP，若為服務型使用，請依下列事項填寫： ◯無 ◯有APP，檢測紀錄日期：_____ 執行人員/機構名稱:_____	24
10、其他	(由各事業別主管司署自行增列)		(由各事業別主管司署自行增列所需檢查細項，並提供填表說明)	24

代表人(負責人/管理人，如個資長)： 填表人 (如專責人員)：