教育部主管目的事業之個人資料檔案

自我檢查表填表說明

壹、受檢單位基本資料

檢查事項	填表說明
1.受檢單位名稱	•私立幼兒園、私立國小、私立國中、私立高中、私立大專校院者，請參照教育部學校名錄(教育部統計處/網頁導覽/學校名錄及相關資訊)，請填報教育部核定之學校中文名稱。 •運動協會者請參照教育部體育署全國各運動協會(體育署首頁/體育團體/體育活動/全國各運動協會)。 •運動團體者請依向內政部登記之名稱為主。
2.填寫日期	•請依實際填寫日期填報。
3.經營業別	•參照各事業別轄管類別，如下分類： -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 •請依經營業別對應之代號填寫。
4. 具對外電子商務服務系統或具有特種個資之資通系統	•電子商務係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。 •若設有可識別為特種個資之欄位，視同具有特種個資。(例如有欄位為具有身障手冊)

5.個資保護要求強度等級

•如：保有個人資料筆數計算：將受檢機關所持有的各項個人資料檔案內個資筆數進行加總合計。

[範例]職員工個資檔案 300 筆、會員資料 600 筆、學生基本資料 30000 筆、人員進出管制個人資料檔 2000 筆，合計 32900 筆。

•如機關已辦理個資盤點清冊，可將盤點清冊內的保有個資筆數數量進行加總計算。

特種個資：資料性質較為特殊或具敏感性，如任意蒐集、處理或利用，恐會造成社會不安或對當事人造成難以彌補之傷害。特種資料包括病歷、醫療、基因、性生活、健康檢查及犯罪前科之6種個人資料。

外部利用：指將蒐集之個人資料為處理以外之使用。

國際傳輸：指將個人資料作跨國（境）之處理或利用。

「個資保護要求強度等級」區分目的是因各事業單位的規模不同致風險不一，以此讓不同風險事業適用不同強度的檢查項目暨佐證要求。

•依表 1 的各評估構面與構面權重，計算出各評估構面的要求強度分數並加總各構面分數。

要求強度總分=∑評估構面分數 x 構面權重。

表 1 個資保護要求強度構面分數表

評估構面	分數 / 權重	0	1	2	3
個資數量 A	1		1000 筆以下	一般個資 1001~50,000 筆 特種個資 1001~35,000 筆	一般個資 50,001 筆以上 特種個資 35,001 筆以上
外部利用 B	0.8	無外部利用情形	1000 筆內少量	一般個資 1001~50,000 筆 特種個資 1001~35,000 筆	一般個資 50,001 筆以上 特種個資 35,001 筆以上
國際傳輸 C	1.2	無國際傳輸	不涉及特殊類別敏感資訊 1000 筆內少量	一般個資 1001~50,000 筆 特種個資 1001~35,000 筆	一般個資 50,001 筆以上 特種個資 35,001 筆以上

[範例]某機構之個資數量構面評分數為 2 分、外部利用構面評分數為 2 分、國際傳輸構面評分數為評分 2 分

•受檢單位依照前述評定結果，在填寫檢查表時，僅需填寫對應個資保護要求強度

等級的檢查重點及其檢核細項項目。

表 2 個資保護要求強度等級評估表

要求強度等級	要求強度總分	說明
普	1~4	受檢單位擁有少量一般性個資及特種個資。
中	4.1~7	受檢單位擁有一定數量個資及特種個資，或有對外電子商務服務系統，或保有一定數量以上的特種個資之資通系統。
高	7.1~9	受檢單位擁有大量一般及特種個人資料(病歷、醫療、基因、性生活、健康檢查及犯罪前科)，有對外電子商務服務系統，或保有大量特種個資之資通系統。

貳、受檢單位自我填表項目

1. 個人資料檔案安全維護計畫

檢查細項	填表說明
1.1 訂定個人資料檔案安全維護計畫	• 請檢附所訂的***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)。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但有採行本項措施，亦可檢附相關佐證。

2. 組織及運作管理情形

檢查細項	填表說明
2.1 指定專人或建立專責組織負責管理	• 請填寫**專責單位名稱**或**專責(職)人員**名稱。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 **依經營業別提交所需之佐證資料：** **屬於私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園及海外臺灣學校或大陸地區臺商學校者，依個資保護要求強度等級檢附對應之佐證資料** • 等級 普：請檢附*受檢單位個資管理組織架構、或個資管理職務分配的說明文件。 • 等級 中：請檢附*指派專責(職)人員或專責單位的核准紀錄。 • 等級 高：請檢附*指派專責(職)人員或專責單位的核准紀錄或專責組織的設置法規。 **屬於私立兒童課後照顧服務中心、短期補習班或運動彩券，依個資保護要求強度等級檢附對應之佐證資料** • 等級 普：請檢附*受檢單位個資管理組織架構、或個資管理職務分配的說明文件。 • 等級 中：請檢附*指派專責(職)人員的核准紀錄。 • 等級 高：請檢附*指派專責(職)人員的核准紀錄或專責組織的設置法規。 • 本項佐證資料不以上述為限，建議本項可另外提供額外可參考佐證之文件，如單位個資管理組織圖或委員會組織圖、分工及相關辦法，或提出個資窗口所協助之各項個資保護工作事項(如：參與會議、盤點及風險評鑑工作、事件處理、個資管理審查相關會議紀錄等)。 相關名詞： • 專責單位：特定的組織或單位，其職責專門負責管理特定領域或特定任務。 • 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。 • 所訂定相關組織辦法：是指由受檢單位依據法律或法規所制定的組織運作規範或辦法。

3. 指定專人或建立專責組織負責管理

檢查細項	填表說明
3.1 規劃、訂定、修正與執行所訂安維計畫	**各經營業別需提交之佐證資料：** • 請檢附*同1.1項佐證資料，需有計畫管理人核准紀錄。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。
3.2 定期向管理人暨代表人或其他代表權人報告	• 報告對象含管理人、代表人或其他代表權人。 • 請勾選報告之形式，如核准紀錄、會議記錄，若選其他請寫出是何種形式。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 **依經營業別提交所需之佐證資料：** **屬於私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園或海外臺灣學校及大陸地區臺商學校者** • 請檢附*書面定期報告紀錄，核准紀錄及會議紀錄。 **屬於私立兒童課後照顧服務中心、短期補習班、運動彩券業者** • 請檢附*定期報告紀錄(不限形式)，需有報告對象簽核。 相關名詞： • 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。 • 代表人：在法律上有權代表公司的人，必須同時是負責人。 • 負責人：遵循法律掌管公司營運，並負責處理各種組織業務的人。 • 代表權人：被授予代表他人行使權力的人，其行動對被代表者具有法律效力。

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	• 請填寫稽核(查核)日期、並填寫改善報告提出日期(報告形式不限)。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 **依經營業別提交所需之佐證資料：** **屬於私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園、海外臺灣學校及大陸地區臺商學校、私立兒童課後照顧服務中心者** • 請檢附***稽核紀錄**、**稽核之不符合事項***追蹤改善紀錄**及***向管理人提出結果報告之紀錄**。 **屬於短期補習班、運動彩券業者** 注意事項：查核人員與指定之專責人員不得為同一人。 • 請檢附***個人資料檔案安全維護計畫執行之檢查紀錄**及***向負責人提出結果報告之紀錄**。 相關名詞： • 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。 • 代表人：在法律上有權代表公司的人，必須同時是負責人。 • 負責人：遵循法律掌管公司營運，並負責處理各種組織業務的人。 • 代表權人：被授予代表他人行使權力的人，其行動對被代表者具有法律效力。
3.4 訂定個人資料保護管理政策	• 本項僅針對個資保護要求強度等級高之受檢單位，若受檢單位已訂定個人資料保護政策，建議檢附**公開之紀錄**(如紙本或電子的公告紀錄)。 • 各事業別之安維辦法無具體規範，本項可勾選不適用之事業別無相關法規要求，但受檢單位有採行本項措施，亦可檢查相關佐證。
3.5 定期對所屬人員進行宣導或專業教育訓練	• 請填寫已執行之近期宣導、教育訓練次數及近期教育訓練日期。 • 請檢附人員定期*教育訓練紀錄或宣導紀錄，如：簽到紀錄 (教育訓練執行統計達成率)、教育訓練教材、課程時數認證證明、宣傳單等。 • 建議單位專責(職)人員具備專業證照或具有專業培訓紀錄。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 **注意事項：課程內容須與個人資料保護法相關。** 相關名詞： • 教育訓練：指通過線上或實體課程。 • 所屬人員：執行業務之過程必須接觸個人資料之人員，包括學校、機構之定期或不定期契約人員及派遣員工。 • 教育訓練執行統計達成率：指評估教育訓練計劃實施後所達到的目標或期望效果的比率

4. 個人資料盤點、管理與紀錄

檢查細項	填表說明
4.1 定期盤點所保有個人資料並確認應遵守之法令	• 請填寫近期個人資料檔案盤點日期。 • 請勾選*個人資料檔案盤點欄位內容項目。 **各經營業別提交所需之佐證資料：** • 請檢附*個人資料檔案盤點清冊紀錄。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 **•個人資料檔案盤點內容的選項說明：** 1、 個人資料之類別：一般個人資料、特殊種類個人資料。 2、 特種個資：含「病歷、醫療、基因、性生活、健康檢查及犯罪前科」之項目。 3、 蒐集方式：指以任何方式(如直接、間接、線上、紙本)取得個人資料。 4、 處理方式：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。 5、 利用方式：指將蒐集之個人資料為處理以外之使用。 6、 保存期限：保有個資之期間。 7、 銷毀方式：指個人資料辦理銷毀的頻率及銷毀的方式。 8、 控制措施：針對指個資實施的安全保護與控制項目。 9、 其他：若非以上複選項目，請勾選並補充說明。
4.2 風險分析及管控措施	• 是否已核定超出可接受風險值之風險處理計畫及核定時間(需有負責人、管理人之核可紀錄)。 • 請檢附經負責人、管理人核定之*風險評估文件資料。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關名詞： • 風險評估：為針對機構內所有單位、過程或步驟進行全面性評估，為使負責人、管理人確實了解機構所具備風險性，請確實評估。 • 可接受風險值：經由管理階層同意並授權，組織願意承擔的風險水平，通常取決於組織的風險容忍度和目標。 • 風險值：對個資發生損失或傷害的潛在威脅的量化評估。

4.3 依資料屬性訂定管理程序	**各經營業別提交所需之佐證資料：** • 請檢附*同1.1項佐證資料，內容須包含依資料屬性訂定不同管理程序之章節。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關名詞： • 資料屬性：係指一般個人資料及特殊種類個人資料。
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	• 請勾選告知形式，並檢附對應的佐證資料。 **各經營業別提交所需之佐證資料：** • 請檢附告知事項資料 相關法規/公告/其他： • 個人資料保護法第八條：公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項： 一、公務機關或非公務機關名。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、對象及方。 五、當事人依第三條規定得行使之權利及方。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影。 • 個人資料保護法第九條：公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。 • 本檢查細項是指在資料收集前或使用前提供必要訊息給當事人，以獲得其同意或選擇。 相關名詞： • 其他：若非以上複選項目，請勾選並補充說明。

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	• 請檢附如*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。 **注意事項：檢附資料須符合個人資料保護法第十九條之目的及要件。** 相關法規/公告/其他： • 個人資料保護法第十九條：非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。 三、當事人自行公開或其他已合法公開之個人資料。 四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 五、經當事人同意。 六、為增進公共利益所必要。 七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。 八、對當事人權益無侵害。 • 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。 • 本檢查項是指在資料已被收集並開始使用後，確保資料的使用符合法律法規的要求，並且對資料進行適當的管理和保護。 相關名詞： • 安全維護計畫執行之檢查報告：是指對組織所制定的安全維護計畫執行情況進行評估和檢查後所產生的報告。這份報告可自評或由專業第三方機構進行評估實施安全維護計畫方面的遵循程度和執行效果，並提供相應的改善建議。

4.6 委託他人進行資料蒐集、處理或利用，進行適當監督	• 如有委託他人進行資料蒐集、處理或利用個資時，請填寫近期對委外機構的檢核日期。 **各經營業別提交所需之佐證資料：** • 如有委外應檢附*委外監督紀錄**(監督項目應包含個資法施行細則第八條第2項規定)。** 相關法規/公告/其他： • 有關委託相關要求，請依循個資法施行細則第八條規定辦理。 • 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。 • 前項監督至少應包含下列事項： 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。 第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。 • 受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

4.7 首次利用個資行銷之當事人確認作業	**各經營業別提交所需之佐證資料：** • 若有首次利用個資行銷，請勾選形式，並檢附首次利用個資行銷進行告知紀錄，無則免附告知紀錄。 相關法規/公告/其他： • 有關首次利用個資行銷進行告知，請依循個人料保護法個資法第 20 條規定辦理。 • 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項： 一、公務機關或非公務機關名稱。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、對象及方式。 五、當事人依第三條規定得行使之權利及方式。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。 • 有下列情形之一者，得免為前項之告知： 一、一、依法律規定得免告知。 二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。 三、告知將妨害公務機關執行法定職務。 四、告知將妨害公共利益。 五、當事人明知應告知之內容。 六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。 相關名詞： • 首次：第一次利用個資進行行銷活動，即第一次向用戶或客戶發送行銷材料或開始進行行銷活動之前，需要進行的告知作業紀錄。 • 個資行銷：利用個人資料進行行銷活動，包括客戶分析、目標定位、廣告投放等方式推廣產品或服務。 • 其他：若非以上複選項目，請勾選並補充說明。
4.8 確認與維護保有個資之正確性	• 受檢單位個資異動(當事人請求更正或補充)受理窗口，請填寫個資受理窗口人員名稱及職稱。 **各經營業別提交所需之佐證資料：** • 請檢附*同 1.1 項佐證資料。 • 如有個資異動，請檢附紙本或電子紀錄。

4.9 針對所屬人員設定不同管理權限，並要求負保密義務	• 如有依人員性質不同而設定對應之權限者，請檢附*權限管控紀錄，若勾選無則免附。 • 如有委外，請檢附委外廠商/人員*簽訂保密切結書紀錄。 • 請檢附所屬人員所簽訂之*保密切結書紀錄。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關名詞： • 保密切結書：簽署文件承諾保護機密資訊，不得將其洩漏或違反保密協議。
4.10 對存有個資之系統設備、媒介物等採取安全管理措施	• 有勾選個資之系統設備、媒介物(含非電子類)採取必要之防護措施者。**依經營業別提交所需之佐證資料：** • **屬於私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園者** • 請檢附系統設備處理個人資料(含媒介物)之防護措施程序、與相對應之作業紀錄。 • 海外臺灣學校及大陸地區臺商學校建議可參考私立高級中等以下學校及幼兒園安維辦法辦理，但因所屬事業別之安維辦法並未規範，本項可勾選不適用。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 **屬於私立兒童課後照顧服務中心、短期補習班、運動彩券業者** • 請檢附所屬人員保管個人資料之儲存媒介物之紀錄，及保管及保密義務之紀錄。 相關名詞： • 系統設備：包括桌上型電腦、筆記型電腦、伺服器等。 • 媒介物：硬碟驅動器、固態硬碟、網路儲存裝置、USB、磁帶、磁碟、CD、DVD、藍光光碟等。 • 資料保存地點進出紀錄：記錄資料存儲地點的出入情況。 • 資料加密紀錄：記錄對資料進行加密的操作和方法。 • 災害恢復計畫：制定應對災害的恢復計劃，以保護資料安全。 • 監控設備的使用情況：記錄監控設備的使用情況和操作記錄。 • 及時檢測異常行為：監控系統，及時發現和應對異常行為，確保資料安全。 • 所屬人員保管個人資料之儲存媒介物之紀錄：是指紀錄所屬人員如何保存個人資料的存儲方式記錄。 • 保管及保密義務之紀錄：是指保存個人資料時有記錄所屬人員對個資的妥善保存和保密責任。

	• 若勾選系有採取系統設備、媒介物報廢或轉作他用時之防護措施紙本、電子資料及設備應訂有銷毀程序者，請檢附*個資紙本、*電子資料及設備之銷毀程序。 • 如有採取委託清除、處理者，請填寫清除、處理單位名稱。 • 海外臺灣學校及大陸地區臺商學校建議可參考私立高級中等以下學校及幼兒園安維辦法辦理，但因所屬事業別之安維辦法並未規範，本項可勾選不適用。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。
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	**各經營業別提交所需之佐證資料** • 請檢附*個資紙本、*電子資料及設備之銷毀作業紀錄、*硬體清除紀錄(如格式化或物理破壞等資料銷毀紀錄)。 相關名詞： • 委外：係指企業將特定功能與服務的執行工作和管理責任委由第三者來承擔，使得原本應由企業員工承擔的工作和責任轉由承包夥伴來承擔。 • 清除：將資料永久性地清除或銷毀，通常包括物理和數位的銷毀方法。 • 處理：除了資料銷毀外，包括資料的處理、分類、保密性檢查、合規性確認等。 • 紙本及電子個資資料清除作業紀錄：紀錄了清除個人資料的過程，包括何時、如何清除，清除的範圍和方式。 • 硬體清除紀錄：記錄了硬體設備（如電腦、硬碟等）中個人資料的清除過程，包括資料的刪除、格式化、或者是物理破壞等方式。
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	• 如有留存所有個資使用紀錄，請填寫受檢單位所訂個資使用、相關軌跡記錄保存期限，並依經營業別提交所需之佐證資料。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 **各經營業別提交所需之佐證資料**： • 請檢附留存之*留存個人資料使用紀錄、可供證明*系統主機或儲放個人資料之主機查軌跡紀錄檔設定畫面或其他相關資料。

5. 電子商務服務系統，或具有特種個資的資通系統之安全管理

補充說明：

- 若設有電子商務服務系統，或使用涉及特種個資之資通系統，或使用個人資料服務系統者，應訂定並落實相應之安全管理措施。
- 特種個資：病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。
- 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。
- 服務：指機構為提供或維持服務，對學生、家長或使用者進行聯繫、回覆或協助等互動行為。
- 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。

法規依據：

- 個人資料保護法第6條第1項
- 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12條之1
- 私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法第14條之1
- 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16條之1
- 私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法第17條
- 短期補習班個人資料檔案安全維護計畫實施辦法第15條
- 運動彩券業個人資料檔案安全維護計畫實施辦法第16條

檢查細項	填表說明
5.1 使用者身分確認及保護機制	有採取使用者身分確認及保護機制，請檢附*同 1.1 項佐證資料，若勾選無保護機制者請說明理由。 **各經營業別提交所需之佐證資料** • 請檢附紙本或電子*帳號申請及異動紀錄及*帳號定期盤點紀錄。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： • 個人資料保護法第 27 條第 1 項規定：非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 • 各事業別之安維辦法。

5.2 個人資料顯示之隱碼機制	• 請勾選系統輸出個資(如紙本列印、螢幕顯示)時所使用的隱碼遮罩處理形式。 **各經營業別提交所需之佐證資料** • 請檢附*螢幕截圖畫面或是*紙本輸出資料的隱碼作為。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： • 個人資料保護法第 27 條第 1 項規定：非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 • 各事業別之安維辦法。 相關名詞： • 隱碼機制：一種加密技術，用於將敏感資料轉換為不易識別的形式，以保護資料的隱私和安全。 • 隱碼遮罩：保護個人身份或其他敏感資訊的技術。通常涉及將真實資料替換為一系列無意義的符號或字元，從而隱藏原始資料的真實內容。(例如遮罩身份證後四碼，如 A223456789-今A22345****)

5.3 網際網路傳輸之安全加密機制	• 網路傳輸採取加密方式者，請勾選傳輸加密機制形式。 **各經營業別提交所需之佐證資料** • 請檢附*螢幕截圖畫面或產品購買或建置證明。 • 若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： •個人資料保護法第 27 條第 1 項規定：非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 •各事業別之安維辦法。 相關名詞： ·傳輸加密：一種資訊安全技術，用於保護數據在傳輸過程中的安全性。通過將數據轉換為加密形式，再透過安全的通訊通道（例如 TLS/SSL）傳輸。 1、 SSL/TLS：Secure Sockets Layer/Transport Layer Security，用於網路通信的加密協議。 2、 VPN：Virtual Private Network，通過加密隧道實現安全的遠程訪問。 3、 其他：若非以上複選項目，請勾選並補充說明。
5.4 個人資料檔案及資料庫之存取控制與保護監控措施	·若有存放個資之系統，請勾選資料庫存取控制與保護監控措施形式。 **各經營業別提交所需之佐證資料** •請檢附*資料檔案及資料存取控制與保護監控截圖畫面或作業紀錄。 ·若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： •個人資料保護法第 27 條第 1 項規定：非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 •各事業別之安維辦法。 相關名詞： 1、 強化身份驗證：實施身份驗證，確保僅授權用戶可以訪問資料庫。 2、 存取紀錄：記錄資料庫的存取記錄，追蹤用戶對資料的操作和變更。 3、 權限管理：設置資料庫用戶的權限，限制其對敏感資料的存取。 4、 安全訪問控制：實施訪問控制策略，限制訪問資料庫的 IP 地址範圍或時間段。 5、 系統日誌：定期審查系統日誌，監控資料庫的存取和活動，檢測異常行為。 6、 資料庫加密：對整個資料庫或特定欄位進行加密，以保護資料在儲存和傳輸時的安全性。 7、 定期漏洞掃描：定期對資料庫進行漏洞掃描，及時發現並修補安全漏洞。 8、 其他：若非以上複選項目，請勾選並補充說明。

5.5 防止外部網路入侵對策	‧請勾選*防止外部網路入侵對策形式，並請檢附受檢單位*網路架構(含設備資訊)。 ‧若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： ‧個人資料保護法第 27 條第 1 項規定：非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 ‧各事業別之安維辦法。 相關名詞： ‧防止外部網路入侵對策：保護系統免受未授權訪問的策略。 1、 防火牆：監控和控制網路流量，阻止未經授權的訪問。 2、 防毒：掃描、檢測和清除電腦系統中的惡意軟體和病毒。 3、 入侵防護 IPS / 入侵偵測 IDS：監控網路流量，檢測和防止潛在的入侵和攻擊。 4、 內外網路區隔：分隔內部網路和外部網路，限制內部資源的外部訪問，提高安全性。 5、 其他：若非以上複選項目，請勾選並補充說明。
5.6 非法或異常使用行為之監控與因應機制	‧請勾選監控作業形式，並請檢附相關佐證 **各經營業別提交所需之佐證資料** ‧等級 普：請檢附監控紀錄，若無此佐證資料，則應提供其他相關佐證。 ‧等級 中、高：請檢附*監控紀錄，或其他資料如行為監控分析紀錄。 ‧若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： ‧個人資料保護法第 27 條第 1 項規定：非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 ‧各事業別之安維辦法。 相關名詞： ‧監控作業形式：不同監控方式的操作方法和程序。 1、 LOG(日誌)：記錄作業系統或應用程序或防火牆/入侵偵測或 WEB 服務...等等運行時事件、錯誤和警告之檔案。 2、 自動警示機制：系統自動偵測異常情況，發出警示訊息以提醒操作者或管理者。 3、 存取控制：管理和限制使用者對資源或功能的存取權限，以確保資料安全。 4、 行為監控系統：追蹤使用者行為，監控系統內的活動，並檢測異常行為。 5、 行為分析：分析使用者行為模式，檢測異常或可疑活動，以提早發現安全風險。 6、 其他：若非以上複選項目，請勾選並補充說明。

5.7 定期演練及檢討改善	‧請填寫*定期演練日期、*檢討日期。 **各經營業別提交所需之佐證資料** ‧有演練者，請檢附如演練紀錄(如資料毀損、個資外洩、外部網路入侵、非法或異常使用行為、系統服務中斷、勒索軟體攻擊、垃圾郵件、釣魚攻擊、社交工程攻擊、自然災害等情況)、演練後檢討紀錄。 ‧若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： ・個人資料保護法第 27 條第 1 項規定：非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 ・各事業別之安維辦法。 相關名詞： ‧資料毀損：資料損壞或遺失，導致無法使用或無法正確解讀。 ‧個資外洩：個人資料被未經授權的方式洩露或泄露給第三方。 ‧外部網路入侵：未經授權的個人或組織通過網路進入系統或資料庫。 ‧非法或異常使用行為：未經授權或不正常的操作，可能導致安全風險或損害。 ‧系統服務中斷：系統或服務停止運作或無法提供服務，通常是由於故障、維護或攻擊引起。 ‧勒索軟體攻擊：使用惡意軟體加密或封鎖資料，然後要求贖金以解鎖或恢復資料。 ‧垃圾郵件：未經請求的大量電子郵件，通常包含廣告、詐騙或惡意連結。 ‧釣魚攻擊：偽裝成合法寄件人的電子郵件，試圖誘騙接收者提供敏感訊息或執行惡意操作。 ‧社交工程攻擊：利用心理手段誘騙人員提供機密訊息或執行操作，通常透過社交媒體或電話進行。 ‧自然災害：地震、颶風、洪水等自然事件導致的損害或中斷。

6. 環境管理措施

檢查細項	填表說明
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	‧本項僅針對個資保護要求強度等級中高之受檢單位，建議檢附同 1.1 項佐證資料。 ‧各事業別之安維辦法無具體規範，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 本項如**個人資料檔案安全維護計畫有所要求，除檢附個人資料檔案安全維護計畫外，再依個資保護要求強度等級檢附對應之佐證資料**： ‧等級 中：建議檢附如*存取記錄(重要區域人員進出紀錄等方式) 、*可攜式媒體申請管控紀錄、安全事件記錄、資料備份記錄。 ‧等級 高：除等級中檢附之資料外，併請檢附如合規性文件。 相關名詞： ‧存取媒介物：硬碟驅動器、固態硬碟、網路儲存裝置、USB、磁帶、磁碟、CD、DVD、藍光光碟等。 ‧存取記錄：記錄存取系統或場所的人員和時間。 ‧安全事件記錄：記錄發生的安全事件、日期和相關細節。 ‧資料備份記錄：記錄資料備份的時間、方式和存儲位置。 ‧設備維護記錄：記錄設備的維護歷史、維修情況和日期。 ‧可攜式媒體申請管控紀錄：記錄申請使用可攜式媒體的用途、審批和使用情況。 ‧合規性文件：確保組織符合相關法規的文件，如安全執照和標準遵循證書(資通環境安全相關第三方驗證證書)。

7. 業務終止之個資管理

檢查細項	填表說明
7.1 訂有業務終止之個資處置措施	**依經營業別提交所需之佐證資料及說明：** **屬於私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園、海外臺灣學校及大陸地區臺商學校者** ・請檢附*同 1.1 項佐證資料。 ・若非根據安維辦法所訂定的業務終止措施，則需提供其他內部規章規範作為佐證資料。 **屬於私立兒童課後照顧服務中心、短期補習班、運動彩券業者** ・請檢附*同 1.1 項佐證資料。 ・檢附定期向負責人報告之紙本或線上紀錄，若因無異動而未報告仍需提供前次報告紀錄。 ・若非根據安維辦法所訂定的業務終止措施，則需提供其他內部規章規範作為佐證資料。 ・若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。
7.2 留存相關紀錄	**依經營業別提交所需之佐證資料及注意事項：** ・**屬於私立專科以上學校及私立學術研究機構、海外臺灣學校及大陸地區臺商學校者** ・如有業務中止，請列舉*本年度業務中止之個資檔案清冊。 ・業務中止包括各種範疇，例如部門、系所、班級等。 ・**屬於私立高級中等以下學校及幼兒園、私立兒童課後照顧服務中心、短期補習班者** ・如有業務中止，請列舉*本年度業務中止之個資檔案清冊。 ・業務中止包括各種範疇，例如部門、系所、班級等。 ・紀錄至少留存五年。 ・若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： ・個人資料保護法第 27 條第 1 項規定：非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 ・各事業別之安維辦法。

8. 事故通報與應變程序

檢查細項	填表說明
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	**各經營業別提交所需之佐證資料及說明：** ・請檢附*同 1.1 項佐證資料。 ・檢查年度各經營業別個資洩漏情形 ・無個資洩漏事故者，請檢附空白事故通報紀錄表單，建議應進行單位模擬演練事故及通報模擬之作業。 ・有個資洩漏事故者，請填寫**近期事故通報日期、年度事故發生次數**並檢附事故通報紀錄。 ・若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： ・個人資料保護法施行細則第 12 條第 2 項規定：公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則： ・各事業別之安維辦法。
8.2 訂定對個資洩漏等事故採應變措施以控制損害	**各經營業別提交所需之佐證資料及說明：** ・請檢附*同 1.1 項佐證資料。 ・若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： ・個人資料保護法施行細則第 12 條第 2 項規定：公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則： ・各事業別之安維辦法。
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	**各經營業別提交所需之佐證資料及說明：** ・請檢附*同 1.1 項佐證資料。 相關法規/公告/其他： ・個人資料保護法施行細則第 12 條第 2 項規定：公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則： ・各事業別之安維辦法。

8.4 研議預防機制	**各經營業別提交所需之佐證資料及說明：** ・請檢附*同 1.1 項佐證資料。 ・組織如有發生事故 ・請填寫個資外洩事故案發日期。 ・請檢附矯正預防單。 ・請檢附預防機制說明。 ・若特定體育團體或體育運動團體及運動事業無相關法規要求，本項可勾選不適用，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關法規/公告/其他： ・個人資料保護法施行細則第 12 條第 2 項規定：公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則： ・各事業別之安維辦法。

9. 資安檢測

檢查細項	填表說明
9.1 系統弱點掃描	‧僅針對有處理個人資訊之資訊系統執行弱點掃描，請填寫日期及執行人員/機構名稱及弱點掃描後系統修補日期，若無修補則無須填寫。 ‧請檢附*弱點掃描紀錄、*修補紀錄。 ‧各事業別之安維辦法無具體規範，本項可勾選無，但受檢單位有採行本項措施，亦可檢附相關佐證。
9.2 滲透測試	‧僅針對有處理個人資訊之資訊系統執行滲透測試，若有請填寫日期及執行人員/機構名稱。 ‧請檢附*滲透測試紀錄。 ‧各事業別之安維辦法無具體規範，本項可勾選無，但受檢單位有採行本項措施，亦可檢附相關佐證。
9.3 資安健診	‧無論有無處理個人資料之資訊系統，皆需執行資安健診。 ‧如有自行執行資安健診，請填寫日期及執行人員/機構名稱，勾選健診項目，並檢附*資安健診紀錄。 ‧健診項目如網路架構檢視、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、資料庫安全檢視等。 ‧各事業別之安維辦法無具體規範，本項可勾選無，但受檢單位有採行本項措施，亦可檢附相關佐證。 相關名詞： ‧網路架構檢視：評估網路設計和結構，確保安全性和效率。 ‧網路惡意活動檢視(有線)：監控有線網路上的惡意活動，及時檢測並應對。 ‧使用者端電腦惡意活動檢視：監控使用者端電腦上的惡意活動，保護系統安全。 ‧伺服器主機惡意活動檢視：監控伺服器主機上的惡意活動，防範系統攻擊。 ‧目錄伺服器設定檢視：審查目錄伺服器的設定，確保合規和安全性。 ‧防火牆連線設定檢視：檢查防火牆的連線設定，保護網路免受未授權訪問。 ‧資料庫安全檢視：評估資料庫安全措施，防止敏感資料外洩或損害。

9.4 APP 檢測	‧如有處理個人資料 APP(自行開發或委外)，如有執行 APP 檢測，請填寫日期及執行人員/機構名稱。 ・請檢附*APP 檢測紀錄 ‧各事業別之安維辦法無具體規範，本項可勾選無，但受檢單位有採行本項措施，亦可檢附相關佐證。 ‧建議事項：各經營業別所挑選協助 APP 檢測之檢測實驗室，須符合數位發展部數位產業署推動行動應用 App 基本資安制度推動委員會所認可之「行動應用 App 資安認驗證制度認可實驗室」https://www.mas.org.tw/lab/successLabs。

10. 其他

檢查細項	填表說明
(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)