個資安全維護計畫撰寫工作坊 (北部場)

115.06.16 13:00-17:00

資料來源：教育體系個資安維行政檢查計畫PDSAI
https://sites.google.com/ntub.edu.tw/personaldata/

大綱

核心重點：個人資料盤點與風險評估、個資行政檢查作業準備與因應

個人資料盤點與風險評估

自我檢查表各項檢查內容之填寫

檢附之佐證資料範例與準備原則

檢查依據及目的

檢查依據

1 個人資料保護法第27條及個人資料保護法施行細則第12條

2 行政院及所屬各機關落實個人資料保護聯繫作業要點

非公務機關應遵循之安全維護義務

依「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。

- **第27條**（個資法第27條於114年11月11日修正公布-刪除-尚未生效，施行日期由行政院定之）

個人資料保護委員會籌備處公告：預告訂定「檢查非公務機關落實個人資料保護法情形作業辦法」草案

個資法第27條：
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。
中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫 或業務終止後個人資料處理方法。
前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

檢查目的

依個人資料保護法第~~27條第2項~~、第3項及個人資料保護法施行細則第12條規定，非公務機關保有個人資料檔案者，應採行適當安全維護措施，防止個人資料外洩，而中央目的事業主管機關亦得指定其所轄管之非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

- **第27條**（個資法第27條於114年11月11日修正公布-刪除-尚未生效，施行日期由行政院定之）

個人資料保護委員會籌備處公告：預告訂定「檢查非公務機關落實個人資料保護法情形作業辦法」草案

個資法第27條：
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。
中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫 或業務終止後個人資料處理方法。
前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

- 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
- 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
- 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
- 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
- 短期補習班個人資料檔案安全維護計畫實施辦法
- 運動彩券業個人資料檔案安全維護計畫實施辦法

檢查對象

私立大專校院事業分組 (由高教司及技職司主辦)

1. 私立大專校院(依私立學校法核准設立之私立專科以上學校)
2. 依學術研究機構設立辦法核准設立之私立學術研究機構

私立高中以下學校及學前事業分組 (由國教署主辦)

1. 私立高中以下學校及學前教育
2. 國教署轄管之其他非公務機關或事業

境外臺校事業分組 (由國際司主辦)

1. 海外臺灣學校及大陸地區臺商學校
2. 國際司轄管之其他非公務機關或事業

終身學習事業分組 (由終身司主辦)

1. 短期補習
2. 課後照顧中心

體育事業分組 (由體育署主辦)

體育署轄管之其他非公務機關或事業

資料來源：PDASI簡報：0606受檢業者說明會v202406061910

- 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
- 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
- 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
- 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
- 短期補習班個人資料檔案安全維護計畫實施辦法
- 運動彩券業個人資料檔案安全維護計畫實施辦法

法令規章

個人資料保護法及相關實施辦法

遵循個資法

- 第8、9條
- 第11條 第1項
- 第12條
- 第19條
- 第20條 第2、3項
- ~~第27條 第2項~~（個資法第27條於114年11月11日修正公布-刪除-尚未生效，施行日期由行政院定之）

個人資料保護法施行細則

遵循個資法個資法施行細則

- 第8條

個人資料保護委員會籌備處公告：預告訂定「檢查非公務機關落實個人資料保護法情形作業辦法」草案

個資法第27條：
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。
中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫 或業務終止後個人資料處理方法。
前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關 定之。

個資法https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050021

個資施行細則 https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050022

資料來源：PDASI簡報：0606受檢業者說明會v202406061910

資訊總覽
關於我們
最新消息
法令及執行措施
為民服務
資訊專區
國際資訊

首頁 › 最新消息

https://www.pdpc.gov.tw/

最新消息

關鍵字： 請輸入關鍵字 送出

全部 公告 新聞稿 會議及活動

上版日期	主題
115-05-14	系統維護公告
115-03-09	個人資料保護委員會籌備處公告：預告訂定「公務機關個人資料保護管理事項實施情形稽核辦法」草案
115-02-11	個人資料保護委員會籌備處公告：預告訂定「檢查非公務機關落實個人資料保護法情形作業辦法」草案
115-02-06	個人資料保護委員會籌備處公告：預告訂定「個人資料保護政策推進會議運作辦法」草案
115-02-06	個人資料保護委員會籌備處公告：預告訂定「個人資料保護法第五十一條之一第一項所稱由中央目的事業主管機關或直轄市、縣（市）政府管轄之非公務機關列表」草案
115-01-22	個人資料保護委員會籌備處公告：預告修正「個人資料保護法施行細則」部分條文
115-01-22	個人資料保護委員會籌備處公告：預告訂定「個人資料保護長及相關人員執掌職能條件及訓練辦法」草案
115-01-22	個人資料保護委員會籌備處公告：預告訂定「個人資料檔案安全維護管理辦法」草案
115-01-22	個人資料保護委員會籌備處公告：預告訂定「個人資料事故通知通報及應變辦法」草案
114-12-26	個人資料保護法修法問答集
114-11-20	個人資料保護法部分條文修正對照表
114-11-11	個人資料保護法部分條文修正案，業於今(114年11月11日)日經總統公布，本次修正條文施行日期將另由行政院定之

教育體系各事業別個人資料檔案安全維護計畫實施辦法

- 私立專科以上學校及私立學術研究機構(103年施行)
- 私立高級中等以下學校及幼兒園(106年施行)
- 海外臺灣學校及大陸地區臺商學校(105年施行)
- 私立兒童課後照顧服務中心(107年施行)
- 短期補習班(103年施行)
- 運動彩券業(104年施行)

資料來源：PDASI簡報：0606受檢業者說明會v202406061910

個人資料盤點與風險評估

個人資料檔案盤點：流程與重點作業

準備與計畫

1

確定目標與範圍
成立盤點小組
制定盤點標準與工具

資料蒐集

2

各單位填寫盤點表
工具掃描檔案
訪談各業務單位

檔案分類與識別

3

辨識個人資料類型
(e.g., contact, financial)
定義敏感度等級
確認個資項目

生命週期分析

4

分析資料流向與來源
確認蒐集目的與依據
釐清保存期限

安全性與風險評估

5

評估存放環境安全
識別洩漏與存取風險
制定保護措施

維護與持續改善

6

定期稽核與更新檔案
執行資料銷毀與歸檔
提升人員資安意識

資料生成：Gemini_Generated_Image_2026_05_26_HC

個資盤點時，資料流向未釐清或不知去向

可能造成的資安風險！

可能造成的資安風險

個資外洩
資料被未授權存取或外流，導致個資外洩事件。

難以追蹤與稽核
無法掌握完整流向，影響調查與法遵。

資料重複與分散
多處留存、版本混亂，增加誤用與洩漏風險。

過度保存與管理失控
不必要的資料持續留存，增加被濫用與洩漏風險。

法遵與罰則風險
違反個資法等法規，面臨罰鍰與商譽損害。

盤點清楚，掌握流向，降低風險！

1. 找出所有個資來源
2. 釐清資料流向與保存位置
3. 確認傳輸與分享對象
4. 落實存取控管與權限管理
5. 定期檢視與刪除不必要資料

看得見流向，才能守住個資！

資料生成：ChatGPT Image 2026年5月26日 上午09_35_59_HC

認識您的「個人資料」

中華民國個人資料保護法第2條宣導

自然人所擁有的資料受法律保護

1. 識別資料

姓名、出生年月日、身分證字號
護照號碼、相片、指紋

2. 特徵與社會活動

特徵、性生活、職業
教育程度

3. 聯絡資料

電話號碼、地址
電子郵件

4. 財務資料

財務狀況
信用卡卡號

5. 醫療與敏感資料

醫療狀況、基因
犯罪前科

敏感個資
應注意蒐集之法
遵及管理之責

6. 其他類別

合約內容
會員卡資料
社會團體活動

保障隱私，尊重個資，您的資料受法律保護！

依據中華民國個人資料保護法第2條定義。

資料生成：Gemini_Generated_Image_2026-05-26-09_17_HC

中華民國個人資料保護法

個人資料盤點及風險評鑑

完整盤點・有效管理・降低風險・保障權益

盤點是管理的基礎，
風險評鑑是保護的關鍵！
落實個資盤點，強化機關資安與隱私保護！

個資盤點從「點、線、面」三個角度，完整掌握機關內所有個人資料檔案

點（點狀盤點）

以「個人資料檔案」為單位逐一清查

盤點重點

- 找出機關內所有含個資的檔案、表單、文件、資料庫或電子檔案。
- 確認個資檔案的名稱、保存地點及負責單位。
- 盤點個資類別、蒐集目的、利用對象、保存期限等基本資訊。

常見盤點對象

紙本表單　紙本文件　電子檔案（如Excel、PDF、Word）　資料庫（如SQL、Access）

盤點成果：形成「個人資料檔案清冊」

線（流程盤點）

以「業務流程」為主軸追蹤個資流向

盤點重點

- 描繪業務流程中個資的產生、蒐集、處理、利用、傳輸、保存與銷毀等流向。
- 確認流程中涉及的個資檔案、系統、單位及外部機關或廠商。
- 找出個資在流程中可能的風險環節。

常用工具

流程圖（Flowchart）　資料流程圖（DFD）　個資流向圖（Data Flow）

盤點成果：建立「個資流程地圖」，掌握個資流向

面（系統／單位盤點）

以「系統或單位」為範圍全面清查

盤點重點

- 針對機關內所有單位、資訊系統、應用程式及設備進行全面清查。
- 確認各單位或系統持有之個資檔案及其關聯性。
- 掌握委外廠商、雲端服務等外部處理個資之情形。

常見盤點對象

業務單位　資訊系統　儲存設備（含行動裝置）　雲端服務／委外廠商

盤點成果：「產出個資與系統關聯清單」

為什麼要盤點個人資料？

遵法義務
個資法第27條要求公務機關定期進行盤點與風險評鑑。

風險控管
掌握個資分布與流向，才能有效評估風險並採取適當防護措施。

資源配置
依風險高低優先改善，提升資安與隱私保護效能。

建立信任
落實個資保護，增進民眾對機關的信任。

盤點成功的關鍵

- 高階支持，明確指派權責單位與人員
- 跨單位協作，確保資訊完整
- 定期更新，盤點非一次性工作
- 文件化保存，作為後續風險評鑑與管理依據

溫馨提醒

盤點不是目的，管理才是關鍵！
透過持續盤點、風險評鑑與改善，
落實個資保護，守護民眾權益！

個資盤點建議步驟

1. **規劃準備**：確認盤點範圍、目標、時程與資源，指派盤點人員。
2. **資料蒐集**：透過訪談、問卷、文件檢視等方式蒐集相關資訊。
3. **盤點彙整**：依「點、線、面」方法彙整個資檔案與流程資訊。
4. **確認與驗證**：與各單位核對確認，確保盤點結果完整正確。
5. **建立清冊**：產出個資檔案清冊、流程地圖或系統清單等成果文件。
6. **後續應用**：作為風險評鑑、資安管理、教育訓練及內部稽核之基礎。

小提醒：常見的個人資料類別

- 辨識個人者（姓名、身分證號等）
- 特徵資料（性別、出生年月日等）
- 社會情況（職業、學歷、婚姻等）
- 教育或訓練（成績、學籍等）
- 聯絡方式（電話、地址、Email 等）
- 財務情況（所得、財產、帳戶等）
- 其他經中央主管機關公告之資料類別

落實個資盤點與風險評鑑，打造安全、可信賴的政府服務環境！

保護個資，你我有責！

更多資訊請參考
個人資料保護委員會（https://www.pdpc.gov.tw）

資料生成：ChatGPT Image 2026年5月21日 下午03_32_59_HC

個人資料檔盤點-重點

- 應包含全機關之個人資料檔案，如電子檔、紙本文件、資料庫
- 同時應注意來源及流向
- 對於其生命周期應有明確起、迄
- 涉及委外或個資外送（揭露或利用）應加強管理
- 機敏個資及特種個資之管理與法遵依據要作業要求要落實
- 有蒐集個資就應有蒐集之告知聲明
- …

個人資料檔案盤點-基本欄位

- 個人資料檔案清冊 (參考資料) https://reurl.cc/O63KWy

個人資料檔案清冊（單位名稱：　）僅供參考

處室	組別	個資資產編號	流程名稱	個人資料檔案名稱	個人資料檔案施行單位	資料形式	是否委外	法律依據	個人資料類別	個人資料之範圍	個資保管數量	個資保管總數量	特種資料	蒐集或處理之目的
					□資料控制者 □資料處理者 □共同資料控制者									

蒐集			處理		利用				保存		銷毀		揭露			現有控制措施	資產價值
來源	方式	單位	方式	單位	期間	地區	單位	方式	單位	期限	形式（方式）	頻率	對象	方式	個資範圍		

關於個資檔案施行單位-角色

- **資料控制者 (Data Controller)**
  - 決定蒐集、處理個人資料之「目的」（Why）與「方法」（How）的組織或個人。通常是發起業務、擁有資料並直接面對當事人的**組織或單位**，如人事室、教務處。-**主導該作業流程/業務**
- **資料處理者 (Data Processor)**
  - 依據「資料控制者」的指示與授權，替控制者實質處理個人資料的**外部實體或個人**，如學生事務處、受託托印製學生證之外部單位、繳費單印製銀行。-**協助或經手該作業流程/業務**
- **共同資料控制者 (Joint Controllers)**
  - 當「兩個或兩個以上」的組織或個人**共同決定處理個人資料的目的與方法**時，即為共同控制者，如資訊中心與教務處共同具有資通系統的特定操作。-**有兩方(含)以上主導該作業流程/業務**

GDPR 將**資料控制者**定義為對**收集和處理個人資料的方式和目的做出決定的實體**，將**資料處理者**定義為通常**代表資料控制者處理個人資料的實體**。

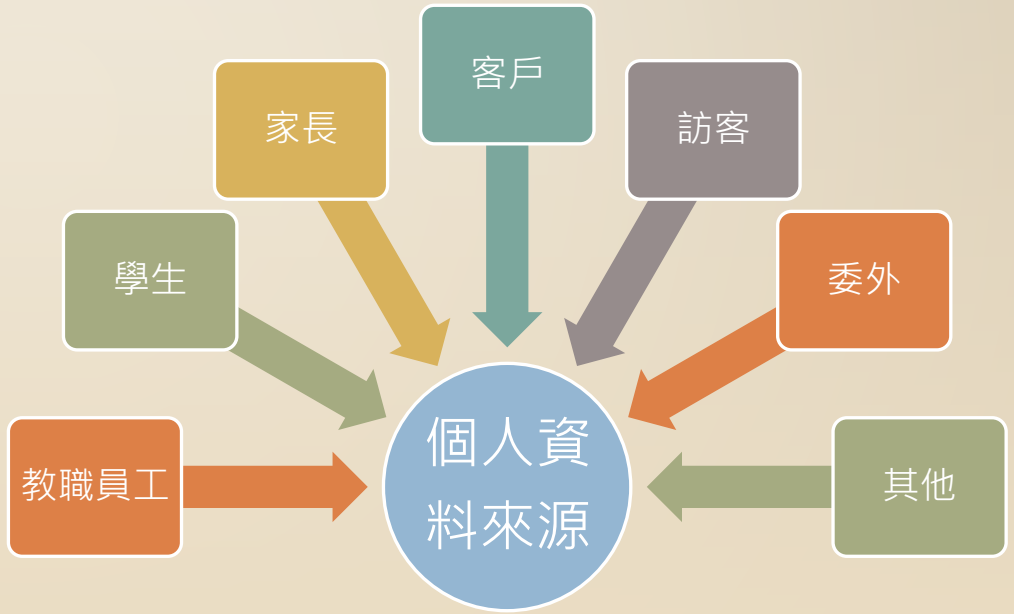
風險評估

https://reurl.cc/Dxklx5

個資檔案盤點(清冊)的完整性-蒐集1/2

五、規範行為(蒐集)			五、規範行為(處理)		五、規範行為(利用)				六、保存管理			七、銷毀方式及頻率		八、揭露		
來源	方式	單位	方式	單位	期間	地區	單位	方式目的	保管人	單位/地點	保存年限	方式	頻率	對象	方式目的	個資範圍

- 蒐集定義：
  - 指以任何方式取得個人資料。
- 蒐集來源：
  - **當事人-直接**
    - 當事人自行填寫
    - 網站或問卷。(務必確認為自行蒐集)
  - **非當事人-間接**
    - 校外機關(構)。
    - 其他單位提供。



個資檔案盤點(清冊)的完整性-蒐集2/2

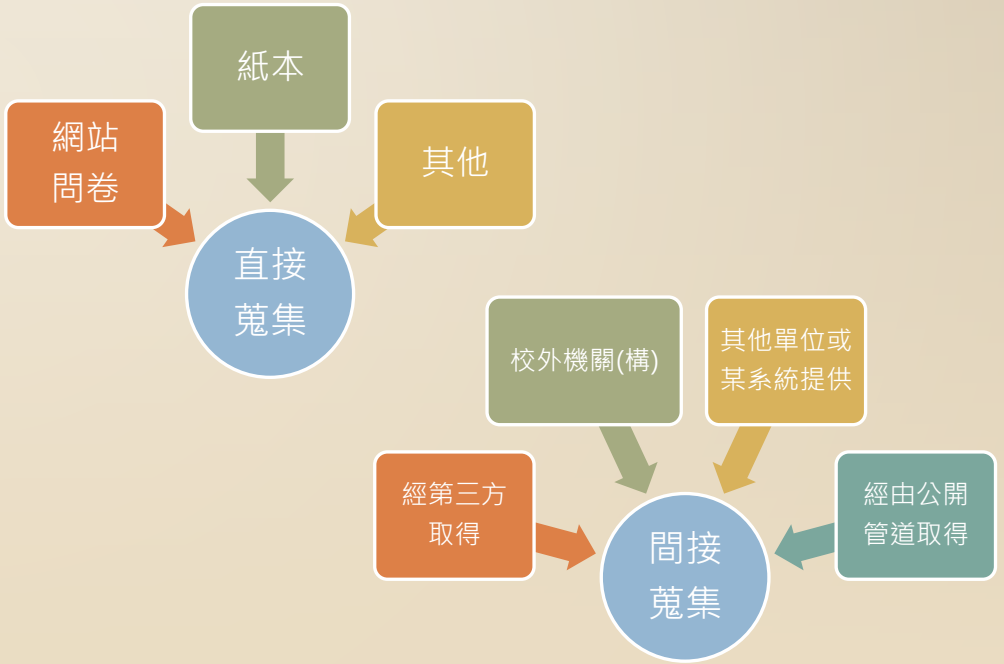
五、規範行為(蒐集)			五、規範行為(處理)		五、規範行為(利用)				六、保存管理			七、銷毀方式及頻率		八、揭露		
來源	方式	單位	方式	單位	期間	地區	單位	方式目的	保管人	單位/地點	保存年限	方式	頻率	對象	方式目的	個資範圍

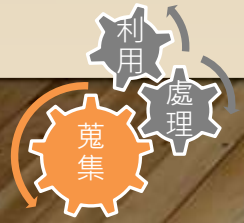
- 蒐集方式
  - 直接蒐集：直接從當事人取得個人資料。
    - 直接填寫表單或藉由組織對外網站上填寫資料。
  - 間接蒐集：透過第三方取得個人資料。

藉由媒合平台取得、合作夥伴介紹、外部機關(學校傳染病監視通報系統...) / 非內部系統取得之個人料檔案

    - 委外：如合作廠商、104、市調公司、信用卡業務。
    - 非委外：如主管機關提供、其他學校。

- 蒐集單位：對當事人蒐集個資的單位/機關。





個資檔案盤點(清冊)的完整性-“處理”與“利用”--處理

五、規範行為(蒐集)			五、規範行為(處理)		五、規範行為(利用)				六、保存管理			七、銷毀方式及頻率		八、揭露		
來源	方式	單位	方式	單位	期間	地區	單位	方式目的	保管人	單位/地點	保存年限	方式	頻率	對象	方式目的	個資範圍

- 處理定義：
  - 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。**
  - 新增文件、建置檔案、輸入系統。
  - 編輯檔案、刪除檔案、儲存檔案、複製檔案。
  - 檢索查詢何系統、更正錯誤、製作連結。
  - 內部傳送至部門。

- 處理方式：**(可以從工作流程內識別)**
  - 依據表單彙整統計建置word表單（或輸入至XX系統）
  - 列印使用
  - 內部傳送至XX、YY、ZZ部門會簽
  - 儲存至個人電腦

  若其他單位有備份留存，由該單位自行盤點。

- 處理單位：包含有資料傳輸的內部其他單位。
  - 彙整單位、列印單位、儲存存放部門、傳送單位傳送至XX、XX傳送至YY、YY傳送至ZZ部門

個資檔案盤點(清冊)的完整性-“處理”與“利用”--利用

五、規範行為(蒐集)			五、規範行為(處理)		五、規範行為(利用)				六、保存管理			七、銷毀方式及頻率		八、揭露		
來源	方式	單位	方式	單位	期間	地區	單位	方式目的	保管人	單位/地點	保存年限	方式	頻率	對象	方式目的	個資範圍

- 利用定義：
  - 指將蒐集之個人資料為**處理以外之使用**。
  - 對當事人使用其個資：如使用通訊錄打電話或寄信、E-mail。
  - 揭露第三方：如提供檢調單位調查、提供主管機關備查、提供勞健保給勞健保機構、提供報稅資料給國稅局、稅捐單位。
  - 一旦有【利用】行為，相對會有【揭露】的可能性，請務考量揭露之識別。
- 期間：
  - 利用個資期間，如業務期間。無【利用】情形→僅需於本欄位填無。
- 地區：
  - 利用地區，如中華民國、國外。(國內使用及國際傳輸)
  - 上傳成績，無須傳至國外網站→國內
- 單位：
  - 揭露對象(有哪些單位利用到)，如國稅局、教育部、檢調單位、主管機關、勞健保局。
- 方式目的：
  - 揭露方式、揭露目的或利用個資方式、目的。

何謂風險？

風險是尚未發生、也不一定會發生的事情；但如果發生，可能對組織造成影響。

外部威脅

來自外部環境或攻擊者

- 釣魚郵件
- 駭客攻擊
- 偽冒網站

內部弱點

來自內部管理或行為不足

- 弱密碼
- 未啟用多因素驗證
- 隨意點擊連結

風險

還沒發生、不一定會發生，但值得提前思考與管理。

聲譽受損

信任下降、品牌受影響

財務損失

罰款、賠償、收入損失

重挫營運

流程中斷、服務受影響

法律責任

違規責任、裁罰、法律風險

思考風險時，請聚焦兩件事

A 發生可能性

- 它發生的機會高不高？
- 外部威脅多嗎？
- 內部弱點明顯嗎？
- 目前控制措施足夠嗎？

B 發生後的衝擊與影響

- 一旦發生，影響會多大？
- 會影響誰？
- 損失有多大？
- 是否影響聲譽、財務、營運與法遵？

外部威脅 ＋ 內部弱點 → 形成風險

評估重點 =
發生可能性 ＋ 發生後的衝擊與影響

提前思考、主動管理，才能降低風險！

資料生成：ChatGPT Image 2026年6月2日 上午08_20_58_HC

風險評估-以個資管理為主體-供參

- **威脅：會造成個資事故的事件或來源**
  - 駭客攻擊
  - 員工誤寄郵件、誤上傳
  - 離職員工惡意攜出
  - 勒索軟體
  - 委外廠商外洩、或違約
  - 紙本資料遺失
  - 火災水災
  - ...等
- **弱點：讓威脅容易發生或擴大的缺口**
  - 權限過大(未落實最小權限原則或進行職務區隔)
  - 未加密、未隔離、寄送資料未有覆核機制
  - 沒有 MFA
  - 沒有紀錄軌跡、調閱無紀錄
  - 未定期刪除
  - 委外契約未約定安全義務、未執行委外監督
  - 紙本櫃未上鎖、庫房進出未管制及紀錄(如未設監視系統)
  - 教育訓練未落實、未辦理還原演練
  - ...等

風險評估-以個資管理為主體-供參

- **可能性：威脅實際利用弱點並造成事件的機率或可能程度**
  - 可能性不是單看威脅，也不是單看弱點，而是看「威脅是否可信、弱點是否存在、暴露程度多高、現有控制是否有效」
  - 可採量化數值，如1~5或1~3...數值區間愈少，風險被低估之可能性愈高
    - 低分特徵：很少發生、攻擊誘因低
    - 高分特徵：常見攻擊、資料有高價值、曾發生事件...
- **衝擊/影響：發生事故後對組織造成的衝擊或影響程度**
  - 衝擊高、中、低
    - 可回復程度或財務影響（含法律責任...）
    - 可採量化數值，如1~5或1~3...數值區間愈少，風險被低估之可能性愈高
  - 高可能性不表示高衝擊、很少發生不表示衝擊性低...

衝擊程度應另外評定，不且混在可能性裡

風險評估-個資可能的衝擊-供參

衝擊構面	評估重點
個資敏感度	是否包含身分證字號、財務、病歷、醫療、基因、性生活、健康檢查、犯罪前科等資料
資料量	筆數、當事人人數、是否大量資料
可識別性	是否可直接或間接識別特定自然人
當事人權益影響	是否可能造成詐騙、歧視、財損、身分冒用、名譽損害
法遵影響	是否涉及告知、同意、特定目的外利用、委外、跨境傳輸、保存期限
營運與聲譽	是否造成服務中斷、主管機關調查、媒體曝光、客訴

風險評估-供參

- **風險等級可用「可能性 × 衝擊」決定，如採5*5矩陣(未納入個資價值)**

風險值	建議等級	處置建議
1~4	低	例行管理，維持紀錄
5–9	中	訂定改善措施，納入定期追蹤
10–15	高	指定負責人、期限與補強控制
16–25	極高	優先處理，必要時暫停該處理活動或限制使用範圍

個資法施行細則第 12 條，也將適當安全維護措施定義為防止個資被竊取、竄改、毀損、滅失或洩漏所採取的技術上及組織上措施，且列舉包含人員與資源配置、界定個資範圍、風險評估與管理、事故應變、內部管理程序、資料與人員管理、教育訓練、設備安全、稽核、軌跡保存與持續改善等項目。

建立風險評估-供參

- 個人資料檔案風險評估表 (參考資料) https://reurl.cc/O63Kxr

個人資料檔案風險評鑑彙整表

個人資料檔案風險評鑑彙整表（單位名稱：　　）僅供參考

紀錄編號：　　填表日期：　　年　　月　　日

項次	評鑑別	資產編號	資料形式	流程名稱	資產名稱	保有單位	衝擊		可能性			資產價值(V)	衝擊(I)	可能性(P)	風險值 R=V*I*P
							構面1	構面2	構面3	構面4	構面5				
							對當事人損害程度	對學校財務影響程度	教育訓練	內部監督稽核	個資安全通報紀錄				

個資不當存取或外洩

價值(V) 、可能性(P) 、衝擊(I) 評估因子-範例

設定各評估**值**時，宜考量過高或偏低之因子，避免造成風險檢視/評估失準！！

衝擊評估表

項目/評估值	對當事人損害程度	對學校財務影響程度
1	個資檔案機敏等級低，資料外洩對不致影響個人權益或僅導致個人權益輕微受損。（如：個資價值「1」者）	個資檔案500筆以下，若發生損害賠償對學校財務影響範圍較小
2	資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益部份受損。（如：含身分證號、財務資訊，個資價值「2」者）	個資檔案500筆（含）以上5000筆以下，若發生損害賠償對學校財務影響範圍較小
3	資料外洩資料外洩可能導致個人隱私遭冒犯，當事 人個人權益嚴重受損。（如：含身分證號、財務資訊，個資價值「3」）	個資檔案5000筆(含)以上50000筆以下，若發生損害賠償對學校財務影響範圍較大
4	資料外洩將造成個人身心受到危害、社會地位受到損害、或衍生財物損失，當事人個人權益非常嚴重受損。（如：含特種個資、特種身分、輔導紀錄等，個資價值「4」以上者）	所含個資檔案50000筆(含)以上，若發生損害賠償對學校財務影響範圍非常大

風險評估資料範本來源 https://reurl.cc/O63Kxr

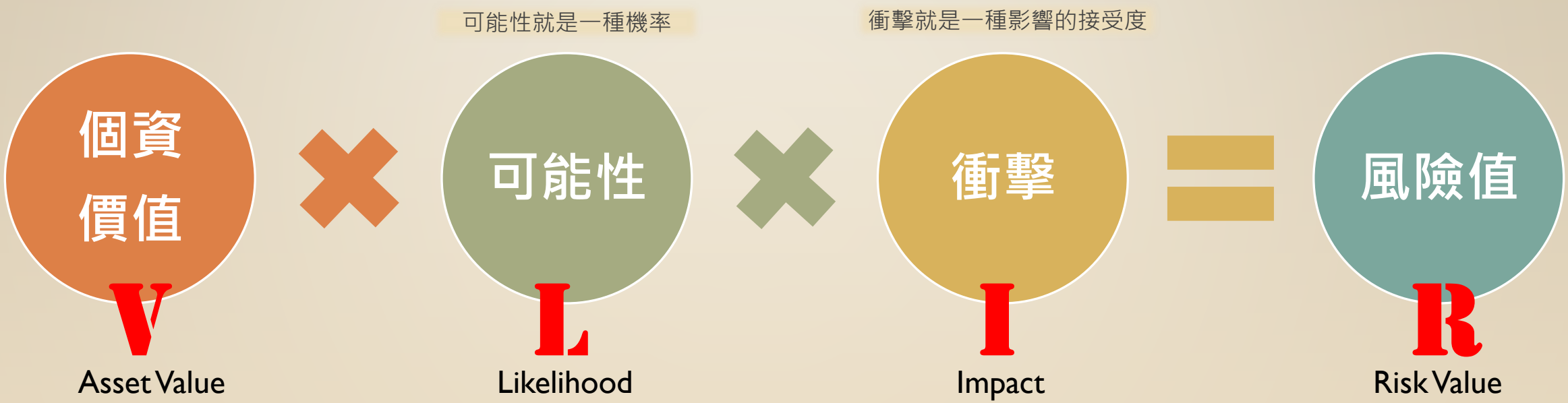
資產價值等級表

資產價值	個人資料範圍
極高(4)	自然人之姓名或國民身分證統一編號（或護照號碼）及特種個人資料。
高(3)	1.含自然人之姓名及國民身分證統一編號（或護照號碼），但不含特種個人資料。 2.含自然人之姓名或國民身分證統一編號（或護照號碼）及財務情況（如：薪資、局帳號），但不含特種個人資料。
中(2)	1.含自然人之姓名或國民身分證統一編號（或護照號碼），但不包含特種資料。 2.含自然人之姓名及員工編號（或學號），但不含特種個人資料。
一般(1)	不含自然人之姓名及國民身分證統一編號（或護照號碼）。

可能性評估表

項目	教育訓練	內部監督稽核	個資安全通報紀錄
1	業務相關人員近一年接受3小時以上個資教育訓練課程	單位已建立內部稽核或監督管理機制，單位於每年執行稽核，並確實執行持續改善	近三年內未發生過個資安全通報紀錄
2	業務相關人員近一年接受3小時以內個資教育訓練課程	單位有建立內部稽核或監督管理機制，但單位並未每年執行稽核或監督管理機制	近三年內曾發生個資安全二次以內(含二次)通報紀錄
3	業務相關人員近一年未接受個資相關教育訓練	單位未建立內部稽核或監督管理機制	近三年內曾發生個資安全三次以上(含三次)通報紀錄

產出風險值



P Potentiality

個人資料檔案：產生風險值-供參

- 一般風險值的考量來自於「發生的**可能性**」及「發生後造成的**衝擊程度**」

個人資料檔案清冊暨風險評估表（參考資料）

盤點日期：2026/6/3

盤點單位	個資檔案名稱	個資價值(V)	發生可能性評估(L)				衝擊程度評估(I)				風險值(R)=V*L*I
			作業管理規定落實度(1)	教育訓練達成度(2)	個資檔案不當存取(3)	評估值Max(1,2,3)	對當事人損害影響(4)	對對組織財務影響(5)	對組織營運影響(6)	評估值Max(4,5,6)	
系統網路組（範例）	電子郵件帳號管理系統	2	1	1	1	2	1	2	1	1	4
系統網路組（範例）	電子郵件帳號申請表	2	1	1	1	1	1	2	1	2	4
註冊組（範例）	學籍系統	3	2	1	1	2	2	3	3	3	18
人事室（範例）	員工管理系統	2	2	1	1	2	2	2	3	3	12
人事室（範例）	員工健康建查資料	3	1	1	1	1	3	2	3	3	9

核決、確認可接受風險值-供參

決定可接受風險值

需有相關核決之紀錄、主官管簽署之文件資訊，如日日期、會議名稱等...

規劃與執行風險改善計畫

需針對**高於**可接受風險者進行風險處置，應有相關紀錄及處理結果等資訊。

評估風險改善執行成效

宜有改善後之成效與追蹤紀錄。

超過可接受風險值之風險處理策略

風險處理策略-舉例

處理方式	說明	舉例
降低	採取控制措施來**減少風險的發生機率或影響程度**。	● 安裝防毒軟體以防惡意程式感染 ● 實施多因素認證以防帳號被盜，強化管理控施與監控。
轉移	把風險轉嫁給第三方，通常是**保險或外包**。	● 購買資安保險以分擔資安事件損失 ● 將伺服器管理外包給具資安認證的廠商、雲端服務或委外機房管理。
接受	若風險在可接受範圍內，選擇**不採取行動**。	● 某些舊軟體只支援Windows 7，因經費有限，不升級繼續使用。
避免	**完全不進行高風險活動**，以迴避風險。	● 限制電腦連接外網，以避免惡意軟體及資料外洩。

超過可接受風險值-風險處理計畫-供參

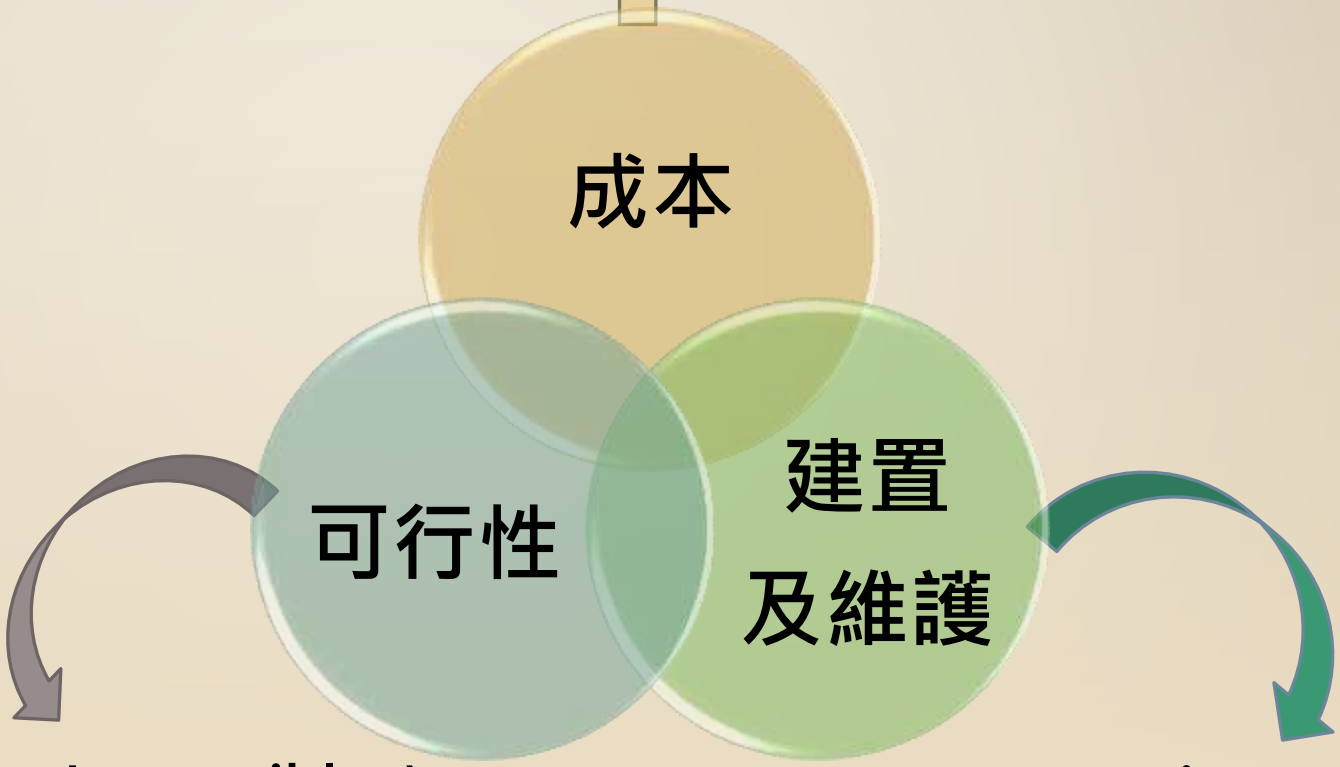
個資風險處理計畫

單位名稱：　　填表日期：　　年　　月　　日

個資檔案識別暨風險說明					風險處理措施			風險進度追蹤				
編號	個人資料檔案名稱	風險說明	風險值 (R)=V×P×I	風險等級	風險處理型式	改善活動/控制措施	改善後風險值 (R)=V×P×I	負責人	預定完成日期	實際完成日期	覆核人員	處理結果
					□接受風險 □降低風險 □轉移風險 □避免風險							
					□接受風險 □降低風險 □轉移風險 □避免風險							
					□接受風險							

風險處理考量原則

比資產本身昂貴？
（More expensive than assets）



（Difficult or Impossible ）
困難度高或不可能做到

（Time and Cost）
時間和成本因素

個資威脅、弱點識別與改善處理-供參

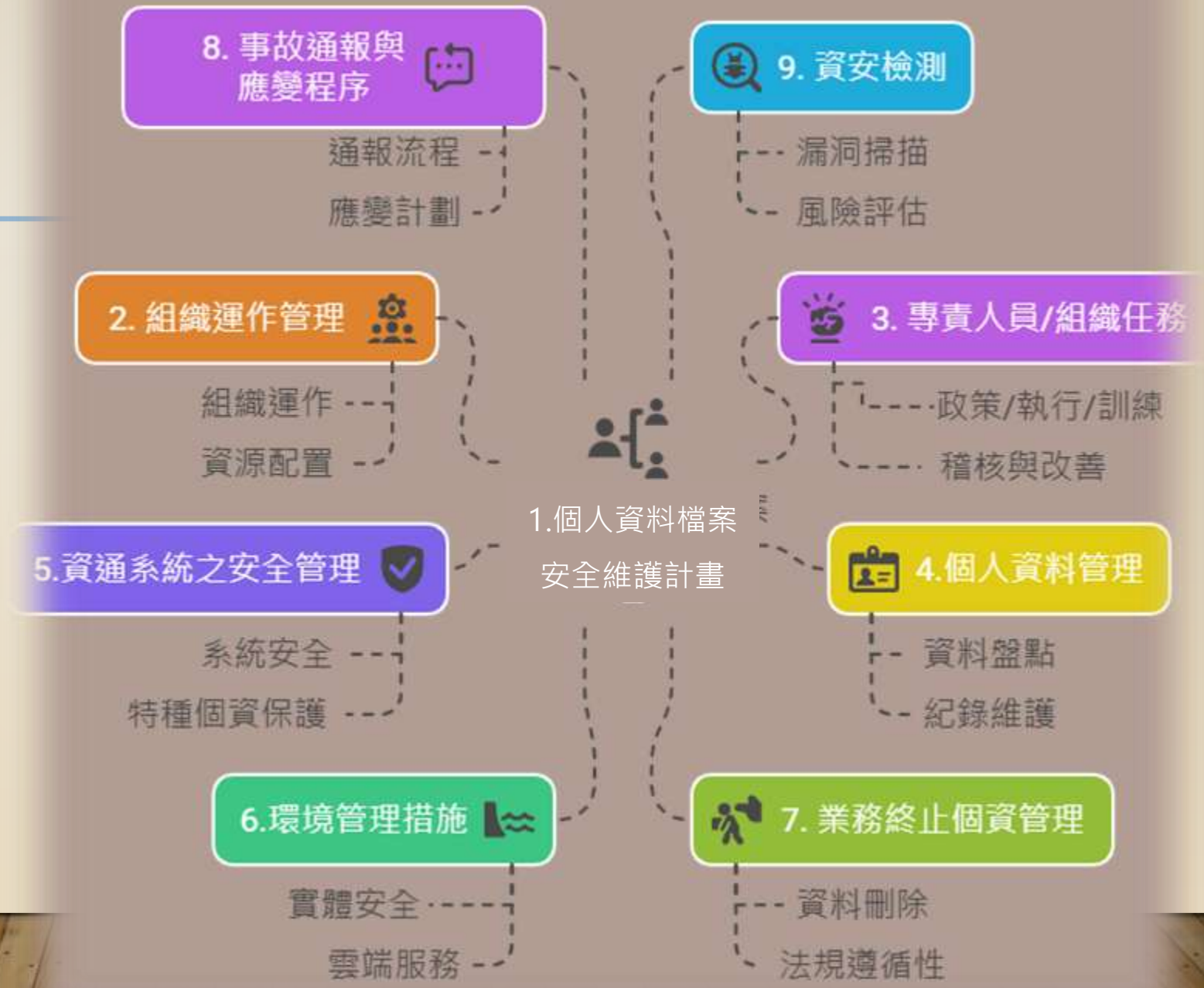
編號	個資檔案名稱	個資內容／類型	威脅情境	弱點	現有控制	建議處置
1	學員資料庫	姓名、電話、Email、生日、學員消費紀錄	外部駭客利用網站弱點取得學員資料	網站程式未定期弱掃、帳號無MFA、資料庫權限過大	有防火牆、帳號密碼控管、每日備份	導入 MFA、弱掃、權限最小化、加密
2	員工薪資資料	姓名、身分證字號、薪資、帳戶資料	內部人員誤寄或未授權下載薪資檔	Excel 未加密、無寄送覆核、共用資料夾權限過寬	主管核准後可存取	限縮權限、檔案加密、寄送覆核、建立存取紀錄
3	客服錄音檔	姓名、電話、交易問題、申訴內容	錄音檔被未授權人員調閱或外洩	查詢權限未分級、下載無管制、保存期限不明	系統登入帳號控管	建立調閱申請、下載限制、保存期限與刪除機制
4	紙本申請書	姓名、地址、聯絡方式、簽名、身分證影本	紙本文件遺失、被非授權人員翻閱	文件櫃未上鎖、調閱無紀錄、銷毀無證明	辦公室門禁管制	上鎖保存、調閱登記、定期清理、碎紙銷毀紀錄
5	行銷名單	姓名、電話、Email、購買偏好	超出原蒐集目的使用或寄送給未同意對象	未標示同意來源、退訂名單未同步、跨部門共用	有行銷系統帳號控管	補強同意紀錄、退訂同步、目的外利用審查
6	委外客服名單	姓名、電話、訂單編號、服務紀錄	委外廠商外洩或違反約定另作利用	契約未明定刪除、事故通知、轉委外限制；未稽核廠商	有簽署一般保密條款	補簽個資條款、要求稽核證明、建立事故通報時限
7	系統備份檔	完整客戶及交易資料	勒索軟體加密備份，或備份檔被竊取	備份未加密、未離線隔離、未定期還原測試	每日自動備份	備份加密、離線備份、還原演練、權限隔離
8	測試環境資料	客戶姓名、電話、交易紀錄	測試環境遭入侵或測試資料被開發人員誤用	使用真實個資測試、未遮蔽、測試環境防護較弱	開發人員帳號登入	資料去識別化、測試環境隔離、刪除真實資料
9	人事履歷資料	姓名、學經歷、聯絡方式、證照、面試紀錄	履歷資料保存過久或被非人資人員存取	保存期限未訂、共用資料夾未分權、離職主管仍可存取	人資部門管理	訂定保存期限、權限覆核、逾期刪除
10	門禁刷卡紀錄	員工姓名、卡號、進出時間	內部人員濫用紀錄進行不當監控	查詢無審核、無使用目的控管、無調閱紀錄	系統帳號密碼控管	建立調閱申請、限制查詢目的、保存軌跡

檢查表各項內容填寫
與
佐證檢附範例/原則

配合檢查 *9*大項

1. 個人資料檔案安全維護計畫
2. 組織及運作管理情形
3. 專責人員或專責組織任務
4. 個人資料盤點、管理與紀錄
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**
6. 環境管理措施
7. 業務終止之個資管理
8. 事故通報與應變程序
9. 資安檢測

各項目所需要求請詳參PDSAI專案計畫網站之「填表說明」



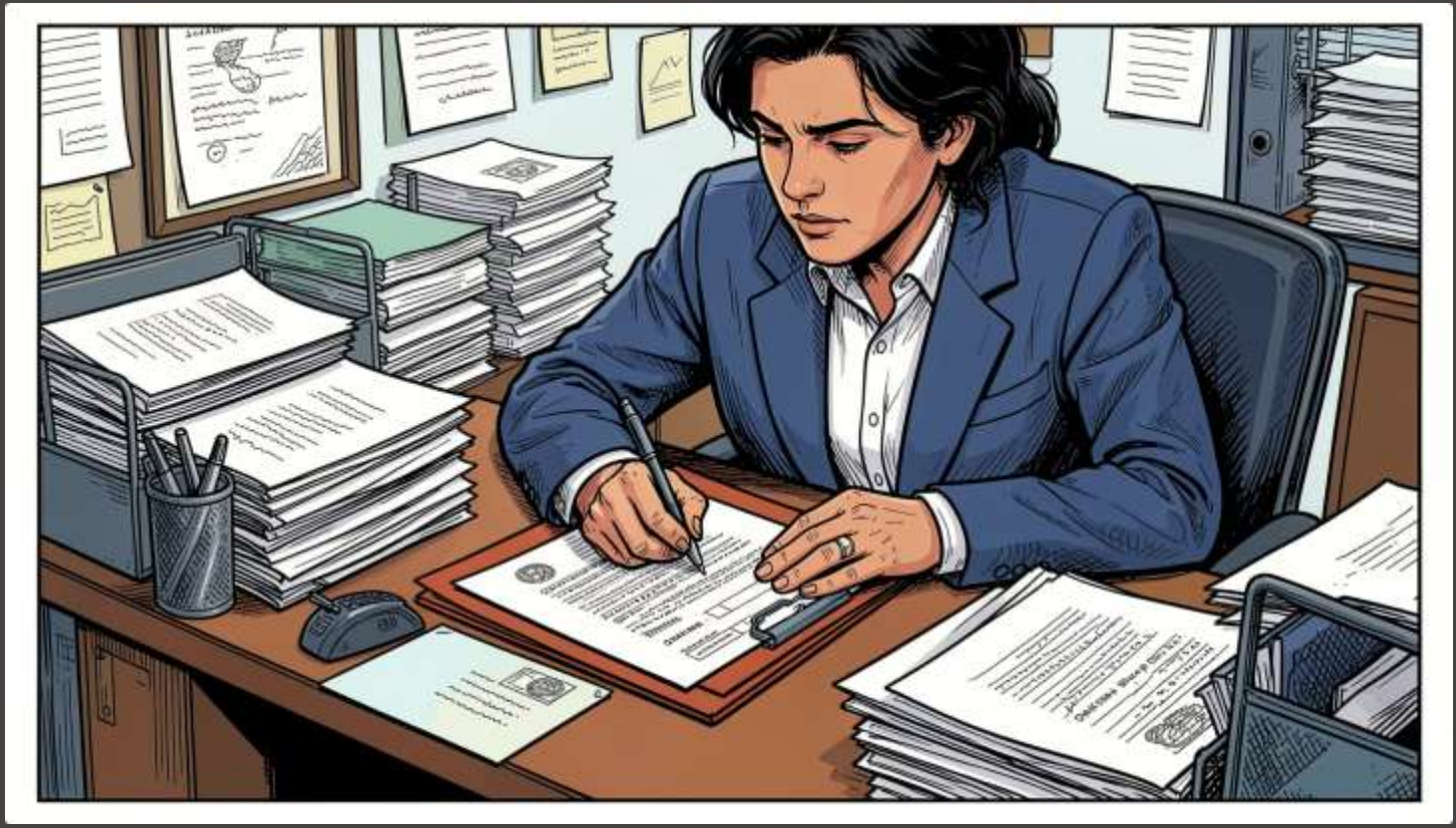
請參PDSAI網站-下載專區之填表說明

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—協助各類私立教育機構依法完成個資保護自評作業

個資保護　自我檢查

壹、受檢單位基本資料



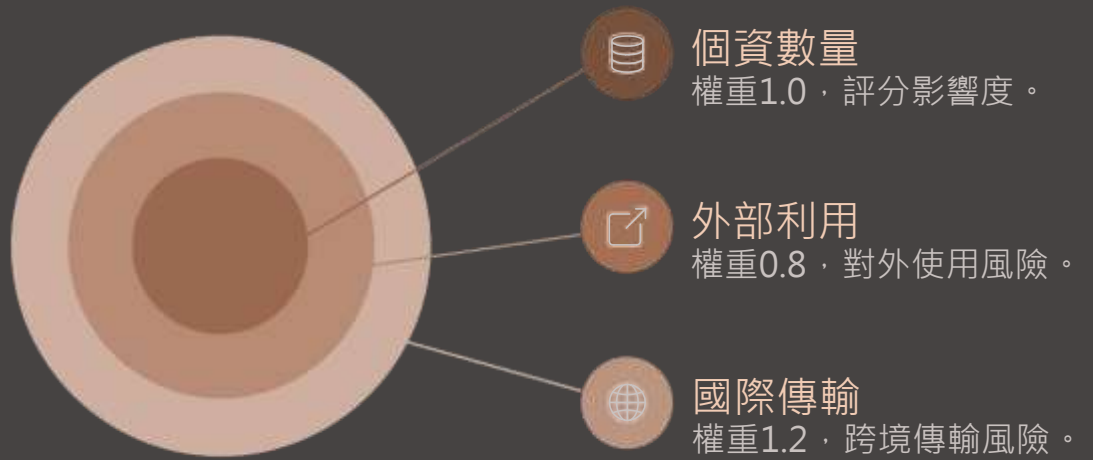
必填項目說明

- **單位名稱**：依教育部核定之學校中文名稱填報
- **填寫日期**：依實際填寫日期填報
- **經營業別**：依對應代號填寫（A私立專科以上、B兒童課後照顧、C補習班、D私立高中、E私立國中、F私立國小、G私立幼兒園等）

電子商務或具特種個資之資通系統，需特別標示安全管理情形。

個資保護要求強度等級評估

依個資數量（A）、外部利用（B）、國際傳輸（C）三構面加權計算總分，決定適用等級。



個資數量
權重1.0，評分影響度。

外部利用
權重0.8，對外使用風險。

國際傳輸
權重1.2，跨境傳輸風險。

普（1–4分）

少量一般性個資及特種個資

中（4.1–7分）

一定數量個資，或有對外電子商務系統

高（7.1–9分）

大量個資、特種個資，或對外電子商務系統

壹、個人資料檔案安全維護計畫

1

1.1 安全維護計畫

訂定個人資料檔案安全維護計畫，含業務終止後個資處理方法。

個人資料檔案安全維護計畫

依據《個人資料保護法》~~第27條第2項~~及相關實施辦法，落實個人資料之安全維護與管理，防止竊取、竄改、毀損、滅失或洩漏。

依據、目的與適用範圍

法規依據

個人資料保護法**~~第27條第2項~~**及「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4條第1項。

學校適用範本

目的

落實個人資料安全維護與管理，防止被竊取、竄改、毀損、滅失或洩漏。

適用對象

全校師生、員工、臨時約聘人員及受委辦派駐本校之人員。

權責單位與管理人員

管理人（召集人）

負責整體個資保護計畫制定與推動。

執行秘書

協助推動個資保護相關業務執行。

個資專職人員

負責風險評估、教育訓練及安全措施強化。

個資保護聯絡窗口

受理當事人行使個資相關權利之申請。

個人資料蒐集範圍與特定目的

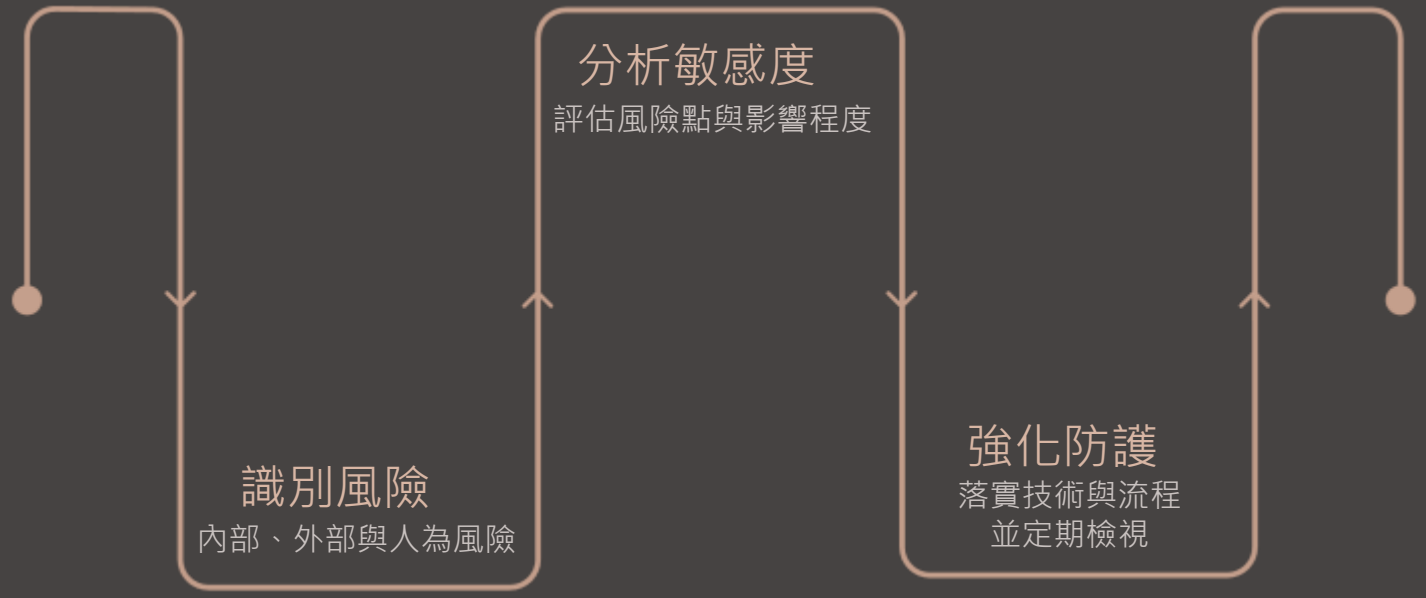
資料類別

依個資法第2條規範之19項個人資料，含特種個人資料（如健康檢查、醫療資訊），須經當事人書面同意方可蒐集。

盤點要求

需全面盤點現持有、受委託及委外蒐集之個人資料，產出**個人資料盤點清冊**，並對未列清冊之資料類別進行當事人告知。

風險評估與管理機制



完成風險評鑑後，需產出**個人資料檔案風險評鑑彙整表**，由權責單位維護管理。

技術防護

資料加密、身份驗證、系統防火牆，落實最小存取原則。

流程監控

針對駭客攻擊、內部濫用、資料外洩設定防範措施。

定期檢視

定期審查資料安全性與合規性，確保符合法令要求。

事故預防、通報與應變

1

預防

指定專人管理；限承辦人員存取；加密儲存媒體；安裝防毒軟體；定期演練。

2

發現事故

立即向負責人或管理組織通報，啟動應變程序。

3

72小時內

依法遵要求向主管機關通報，填寫「個人資料事故通報及紀錄表」。

4

通知當事人

以電話、電子郵件或公開說明通知事故事實、處理措施及聯絡窗口。

5

改善追蹤

深入分析原因，研擬改進措施，留存通報紀錄、事故分析報告及改善記錄。

個人資料內部管理措施

蒐集告知與同意

蒐集時需告知目的、類別、利用期間及方式，並取得當事人同意。

當事人權利

當事人得請求閱覽、更正、停止利用或刪除個人資料，拒絕時應附理由通知。

資料刪除與移交

利用期限屆滿或人員離職時，主動刪除或銷毀個資，並留存相關紀錄。

委外監督

委託第三方蒐集或處理個資時，需明確約定監督事項並適當監管。

實體、資料與人員安全管理

1

設備安全

指派專人管理儲存媒體；重要備份異地存放；報廢前確實刪除資料。

2

資料安全

設置識別密碼與保護程式；100筆以上個資需建置隱碼機制與加密傳輸；紙本文件上鎖保管，丟棄前碎紙處理。

3

人員管理

依業務需求設定存取權限；定期變更密碼；離職時立即取消帳號並確實移交個資。

教育訓練、稽核與紀錄保存

教育訓練

每年至少3小時個資保護訓練；新進人員給予特別指導；留存簽到表等佐證資料。

內部稽核

每半年/一年稽核1次計畫執行情形，向負責人提出報告；不符合法令時提出改善措施，相關文件保存至少5年。

紀錄保存

個資使用查詢紀錄每年備份並設密碼；紙本紀錄上鎖保管；使用紀錄、軌跡資料及相關**證據**至少留存5年。

持續改善與業務終止後處理

持續改善

隨時參酌業務執行狀況、技術發展及法規修訂，定期檢討本計畫是否合宜，必要時予以修正並保存備查。

業務終止後個資處理

- **銷毀**：紙本送焚化或碎紙；電子資料以消磁、擊毀硬碟等物理方式破壞，並留存佐證照片。
- **移轉**：因合併或業務移交他校時，依個資法規定辦理，明確記錄移轉對象、方法及合法依據。

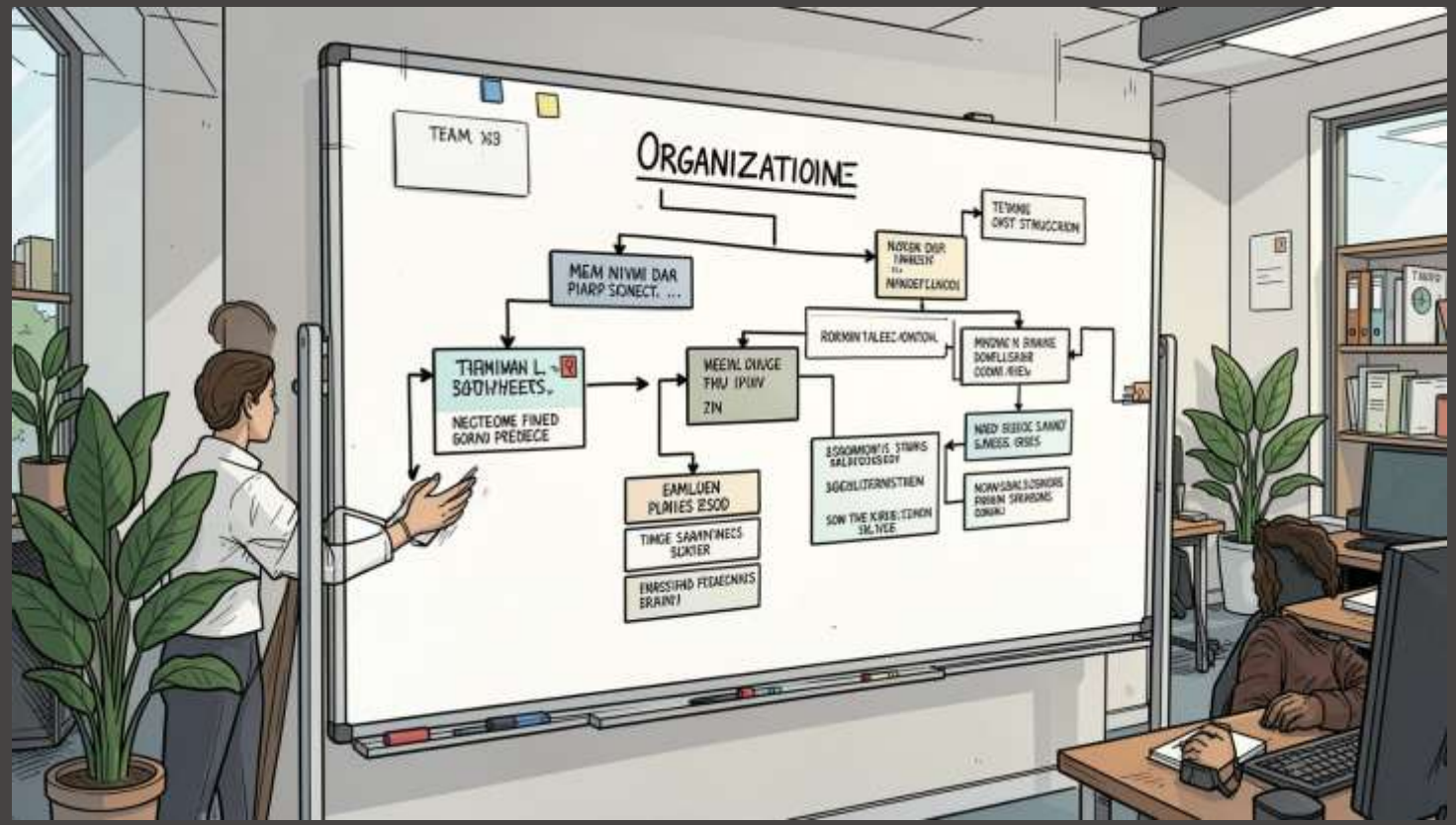
✓ **相關紀錄報送事業主管機關備查。**

貳、組織及運作管理

1

2.1 專責組織

指定專人或建立專責單位，依等級檢附組織架構或核准紀錄。



2.1 指定專人或建立專責組織

依個資保護要求強度等級提交佐證：

- ✓ 個資管理組織架構或職務分配說明文件
- ✓ 指派專責（職）人員或專責單位之核准紀錄
- ✓ 核准紀錄或專責組織設置法規

佐證亦包含個資管理組織圖、分工辦法、會議紀錄等。

參、人員與組織任務

1

3.1 安全維護計畫

訂定個人資料檔案安全維護計畫，含業務終止後個資處理方法。

2

3.2 定期報告

每年至少一次向管理人 / 代表人報告，紀錄須有簽核及日期。

3

3.3 稽核及檢討

每年至少一次向管理人 / 代表人報告，紀錄須有簽核及日期。

4

3.4 管理政策

具有訂定個人資料保護政策相關公開之紀錄(如紙本或電子的公告紀錄)。

個資保護強度等級高者

參、人員與組織任務

5

3.5教育訓練

定期對所屬人員進行個資保護宣導或教育訓練，檢附簽到紀錄與教材。

3.1 規劃、訂定、修正與執行安維計畫

核心要求

各經營業別需規劃、訂定、修正並執行所訂定之安全維護計畫。

佐證資料

可檢附同 1.1 項佐證資料，且需包含**計畫管理人核准紀錄**。

核准紀錄須由計畫管理人簽署，並註明日期。

3.2 定期向管理人暨代表人報告

報告對象

含管理人、代表人或其他代表權人

報告形式

核准紀錄、會議記錄或其他形式（需註明）

頻率認定

建議每年度至少一次，佐證日期需在受檢期間內

3.2 依經營業別提交佐證資料

學校及學術機構

私立專科以上學校、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

- 書面定期報告紀錄
- 核准紀錄及會議紀錄

課後照顧中心及補習班

私立兒童課後照顧服務中心、短期補習班

- 定期報告紀錄（不限形式）
- 需有報告對象簽核

相關名詞說明

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。

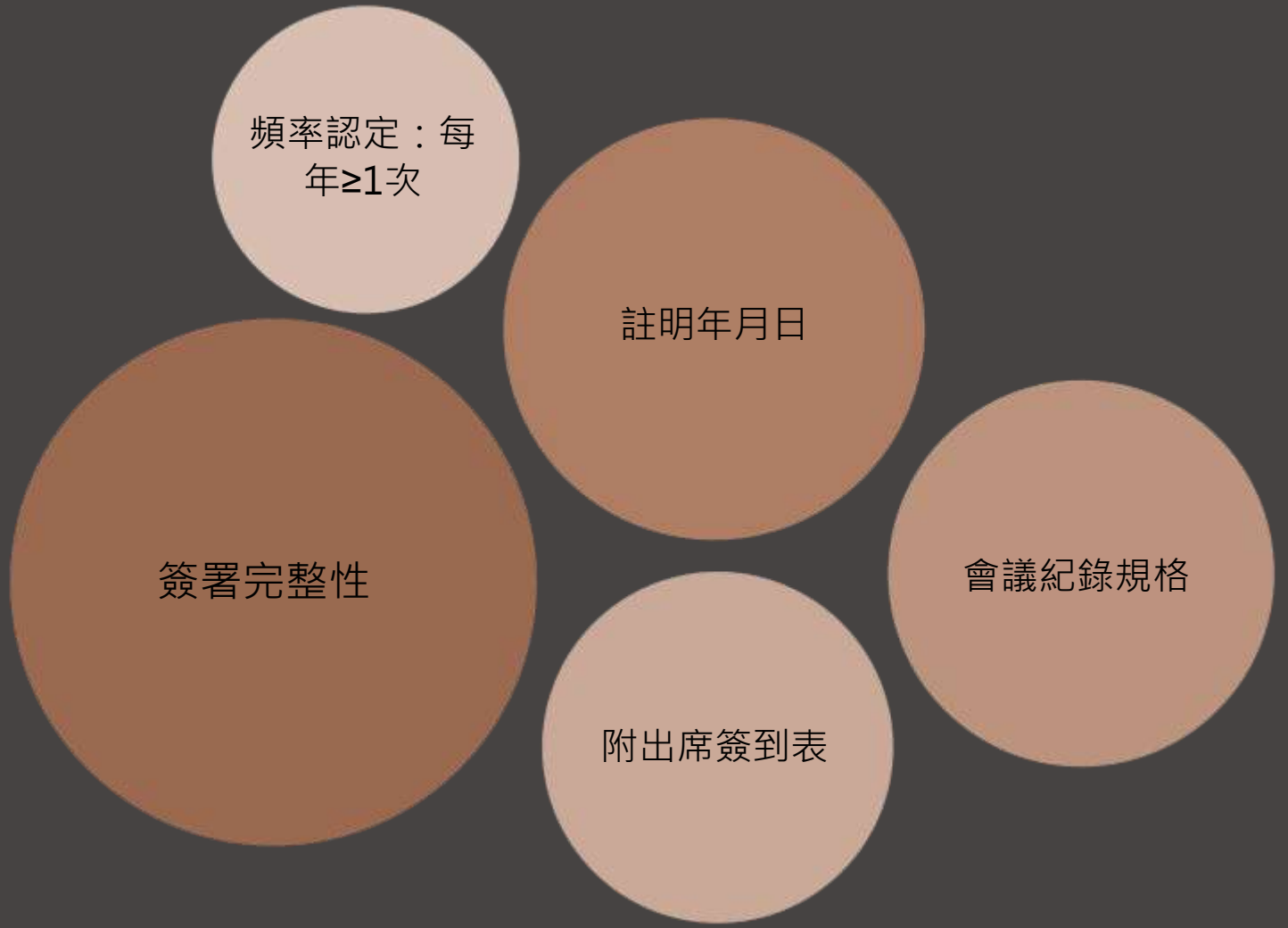
負責人

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。

3.2 補充說明：簽章與會議紀錄



所有紀錄文件均須由報告對象簽核，並註明「年月日」。
若以會議紀錄為佐證，建議一併檢附「出席簽到表」，以證明報告對象確實參與該次會議。

3.3 依稽核結果檢討改進並提出書面報告

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）。

稽核紀錄

檢附稽核紀錄及稽核之不符合事項

追蹤改善紀錄

針對缺失提出具體改善措施與完成證明

結果報告

向管理人提出結果報告之紀錄

3.3 依經營業別提交佐證資料

學校、學術機構、課後照顧中心

私立專科以上學校、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

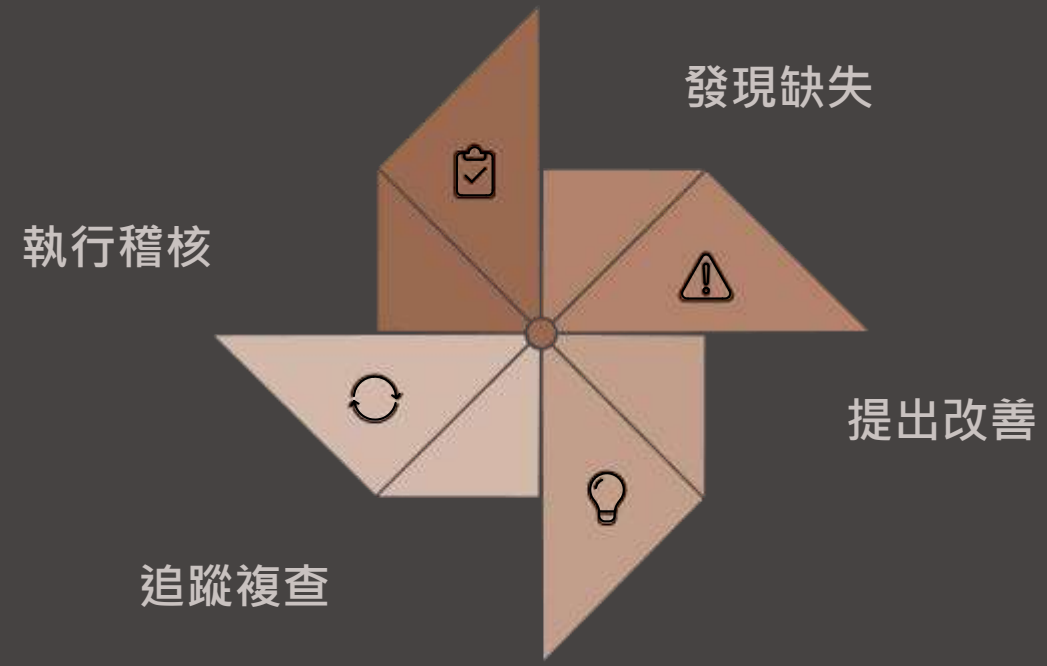
- 稽核紀錄
- 稽核之不符合事項追蹤改善紀錄
- 向管理人提出結果報告之紀錄

短期補習班

⚠ **注意事項：**查核人員與指定之專責人員**不得為同一人**。

- 個人資料檔案安全維護計畫執行之檢查紀錄
- 向負責人提出結果報告之紀錄

➢ 稽核與改善流程

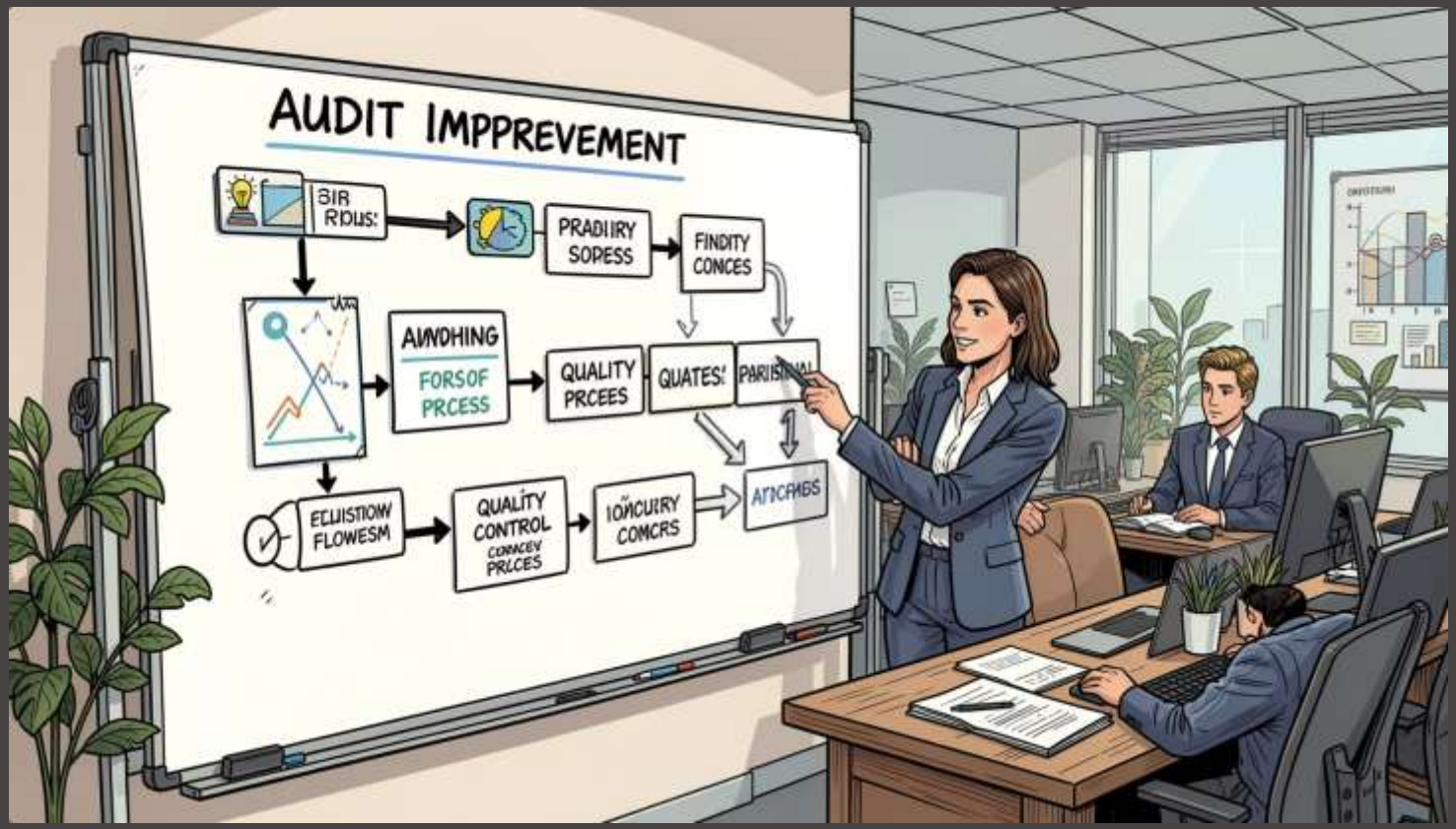


3.3 稽核重點說明

- ✓ 填寫稽核日期及改善報告提出日期
- ✓ 佐證須呈現完整「發現缺失→改善→追蹤」流程
- ✓ 若無缺失，仍需檢附稽核紀錄並註明持續維持

⚠ 查核人員與指定專責人員不得為同一人（短期補習班適用）。

3.3 補充說明：改善邏輯與報告內容



改善邏輯一致性

改善報告日期需在稽核日期**之後**，佐證資料應呈現完整「發現缺失 → 進行改善 → 追蹤結果」流程，不可僅檢附稽核表。

無缺失情況

若稽核結果為「合格 / 無缺失」，仍需檢附稽核紀錄，並於報告中註明「經查核各項要點均符合規範，將持續維持」。

書面報告建議內容

- 稽核時間
- 稽核發現（含優 / 缺點）
- 缺失改善對策
- 追蹤複查結果

3.4 管理政策與 3.5 教育訓練

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 定期宣導或專業教育訓練

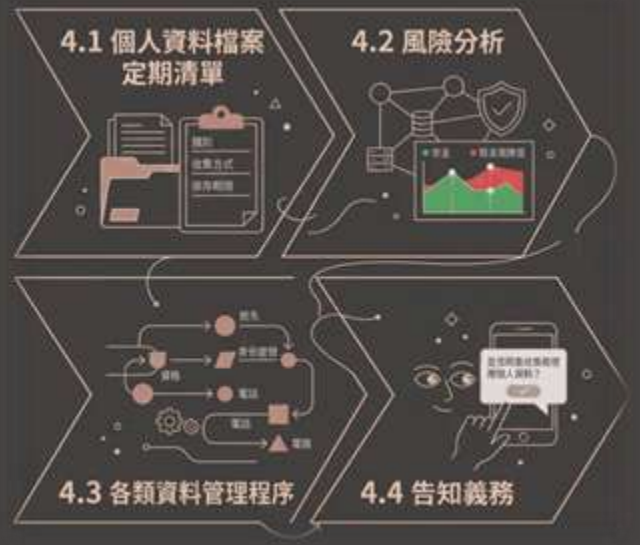
請填寫近期宣導、教育訓練次數及日期，並檢附相關紀錄：

- 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

建議專責人員具備專業證照或培訓紀錄。

⚠ ⚠ 課程內容須與個人資料保護法相關。

肆、個人資料盤點與管理



4.1 定期盤點

填寫盤點日期，檢附個資檔案盤點清冊，涵蓋類別、蒐集、處理、保存及銷毀方式。

4.2 風險評估

檢附經負責人核定之風險評估文件，包含風險識別、分析與評核，建議呈現去年改善成效。

4.4 告知義務

蒐集個資前須明確告知當事人蒐集目的、類別、利用方式及當事人權利（個資法第8、9條）。

4.9 權限與保密

依人員性質設定不同存取權限，所有接觸個資人員（含兼職、工讀）均須簽訂保密切結書。

4.1 定期盤點個人資料

請填寫近期個資檔案盤點日期，並勾選盤點欄位內容項目，檢附**個資檔案盤點清冊紀錄**。

資料類別

一般個資 / 特殊種類個資（病歷、基因、犯罪前科等）

蒐集與處理

蒐集方式、處理方式、利用方式

保存與銷毀

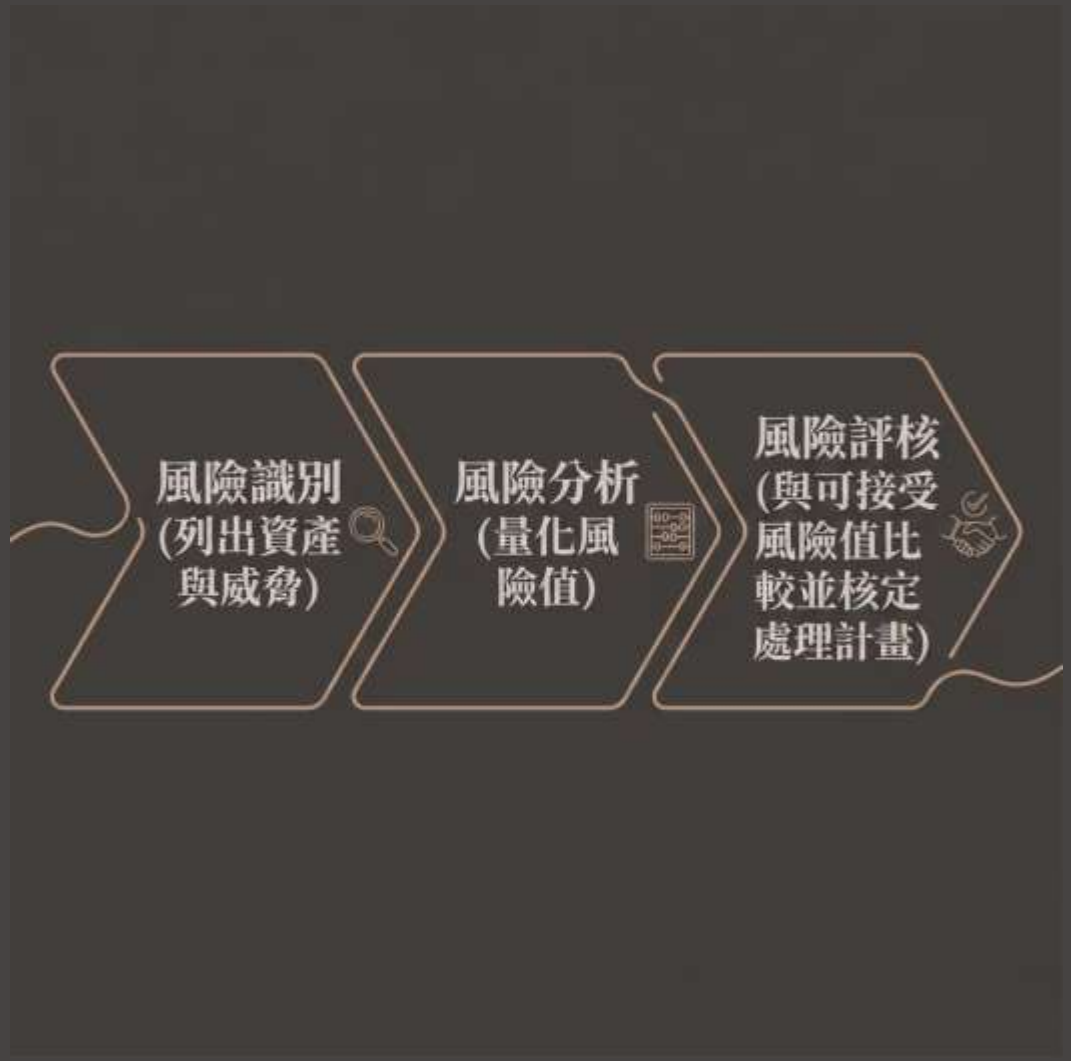
保存期限、銷毀方式、控制措施

4.2 風險分析及管控措施

請檢附經負責人、管理人**核定之風險評估文件**，並確認超出可接受風險值之處理計畫已核定（含核可紀錄）。

> ⓘ 風險評估文件須包含：風險識別、風險分析、風險評核，並明確列出資產、威脅與弱點。

建議呈現「去年風險處理後的成效」，例如高風險項目已降為中低風險，證明管控具實質效力。
若無去年資料，應有今年盤點結果之風險評估結果與後續處理規劃等資料。



4.3–4.5 管理程序、告知義務與蒐集合規

4.3 依資料屬性訂定管理程序

檢附安維計畫，須包含一般個資與特殊種類個資之不同管理程序章節。

4.4 告知義務（個資法第8、9條）

蒐集前或利用非當事人提供之個資前，須告知機關名稱、目的、類別、利用方式及當事人權利。

4.5 符合個資法第19條要件

檢附安維計畫檢查報告、個資蒐集紙本表單及系統截圖，確認蒐集處理具特定目的且符合法定情形。

個人資料保護法（個資法）第8、9、20條：蒐集告知、利用與法律責任綜合指南

第一部分：個資蒐集之告知要求

第8條：向當事人直接蒐集

應告知事項

- 蒐集者名稱
- 蒐集目的
- 個資類別
- 利用期間/地區/對象/方式
- 當事人權利
  - 查詢
  - 請求閱覽
  - 補充/更正
  - 停止利用
  - 停止利用
  - 刪除
  - 刪除
- 未提供之影響

第9條：非向當事人蒐集（間接蒐集）

得免告知

- 法定免除、法定免陰
- 已知悉
- 緊急
- 公開

第二部分：個資之處理與利用

第20條：利用原則與特定目的外利用

原則（本文）

- 在蒐集特定目的範圍內利用，並有正當合理關聯

特定目的外利用之例外
（經當事人事前同意或特定情形）

- 法定理由
- 公共利益
- 免除危險
- 防止危害
- 學術研究
- 有利權益

第三部分：違反法定義務之法律責任

民事責任（第29、30條）

- 損害賠償
- 慰撫金（精神損害）

案例：故意或過失造成損失

刑事責任（第41-43條）

- 有期徒刑
- 罰金

意例：意圖不法利益或損害他人

行政責任（第47-50條）

- 罰鍰
- 命令停止
- 沒入個資
- 停業

資料生成： Gemini_Generated_Image_2026-05-27_HC

落實個資法第19條，合規利用更放心

蒐集與特定目的

1. 明確告知蒐集機關、目的、類別與權利

- 確保第8條告知義務
- 使用者知情權

2. 按特定目的利用

- 一般利用：符合原始蒐集目的
- 禁止逾越目的範圍

個資蒐集與處理流程

逾越目的利用之例外情形（第20條第1項）

3. 為增進公共利益

- 為增進公共利益
- 免除當事人生命生命身體威脅

目的外利用與同意

3. 目的外利用需求

業務需要超出原始特定目的範疇

4. 引導使用者進行利用同意蒐集

- 主動告知新利用目的與範圍
- 提供明確勾選同意
- 尊重使用者選擇權

【合規利用避坑指南】

- ✗ 未經同意逾越目的利用：嚴重違反第19條要求
- ✗ 默認同意：不可設為預設勾選！
- ✗ 未經同意之例外使用不當：濫用公共利益等例外情形
- ✓ 完善紀錄：妥善保存同意紀錄提供查核。

資料生成： Gemini_Generated_Image_2026-05-26_HC

4.6 委外監督與 4.7 首次行銷告知

4.6 委外監督

如有委外，請填寫近期檢核日期，並檢附**委外監督紀錄**（依個資法施行細則第8條）。監督項目應包含：

- 蒐集範圍、類別、目的與期間
- 受託者違法時之通知與補救措施
- 委託關係終止時個資載體之返還與刪除

4.7 首次利用個資行銷

依個資法第20條，首次利用個資進行行銷前，須完成告知作業並留存紀錄。

無首次行銷(利用)者免附告知紀錄。

告知內容：機關名稱、蒐集目的、個資類別、利用方式、當事人權利。

個資法 第20條

什麼是「利用」？ 首次利用應注意！

善用個人資料・合法利用・保障權益・建立信任

法條依據

個人資料保護法 第20條

非公務機關違反第六條第一項、第八條第一項規定，利用個人資料者，處新臺幣五萬元以上五十萬元以下罰鍰。」

什麼是「利用」？

指將個人資料為處理以外之使用，
例如：查詢、傳送、傳播、提供、
轉讓、公開、作成統計或學術研究等。

常見的利用行為

- 寄送行銷資訊（EMAIL、簡訊、DM）
- 會員資料提供予第三方進行行銷
- 將資料用於原蒐集目的以外的新用途
- 進行資料分析、統計、研究
- 其他任何形式的使用或提供

EMAIL/簡訊 | 提供第三方行銷 | 資料分析統計研究 | 其他利用行為

首次利用應注意事項（個資法第20條）

首次利用個人資料時，應依下列事項辦理：

1. **告知當事人**
   首次利用時，應以顯著方式向當事人告知下列事項，並給予合理期間表示意見。
2. **提供拒絕之方式**
   告知內容應包含當事人得表示拒絕利用之方式，並確保當事人可輕易行使。
3. **不得預先勾選同意**
   不得以預設勾選、預設同意或其他不當方式，使當事人難以拒絕。
4. **當事人表示拒絕時**
   當事人表示拒絕利用時，應立即停止利用其個人資料。

應告知事項（個資法第20條第1項）

首次利用個人資料時，應以顯著方式告知當事人下列事項：

1. 機關或團體名稱
2. 利用之目的
3. 個人資料之類別
4. 個人資料利用之期間、地區、對象及方式
5. 當事人得行使之權利及方式
6. 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

小提醒： 告知內容應清楚、簡明且容易理解，以確保當事人知情並可自主決定。

情境範例：是否屬「首次利用」？

不是首次利用（已有告知並取得同意）

會員註冊時已告知將用於行銷，並取得同意，後續寄送優惠資訊。

可以利用

是首次利用（未告知或用途不同）

會員註冊僅用於「出貨」，後續想用來寄送行銷資訊，屬首次利用。

應依第20條告知

首次利用流程建議

1. **確認利用目的**
   確認是否超出原蒐集目的。
2. **準備告知內容**
   依第20條規定準備告知事項。
3. **告知當事人**
   以顯著方式告知，提供拒絕方式。
4. **取得同意或等待意見**
   給予合理期間，當事人可表示意見。
5. **紀錄與管理**
   留存告知與同意或拒絕之紀錄。

當事人拒絕時
應立即停止利用其個人資料，並不得再行利用。

違法利用的風險

- 處新臺幣5萬元以上50萬元以下罰鍰
- 造成當事人損害，可能負損害賠償責任
- 損害機關/企業信譽與客戶信任
- 影響個資安全與營運風險

貼心提醒

- 定期盤點個人資料用途，確保符合蒐集目的
- 建立內部審查機制，確認是否屬首次利用
- 落實告知與紀錄保存，強化個資保護管理
- 尊重當事人選擇，建立透明可信的關係

☆ 重點總結

首次利用個人資料時，務必依法告知並取得當事人同意或給予拒絕機會！

知情 才能安心 → 選擇 才有尊重 → 信任 才能長久 → 守法 才能永續

更多資訊

法務部個人資料保護專區
https://mojlaw.moj.gov.tw
個人資料保護委員會
https://www.pdpc.gov.tw

保護個人資料・從合法利用開始・尊重隱私・共創信任社會

4.8–4.9 個資正確性與人員權限管理

重點提醒

- 請填寫個資受理窗口人員姓名及職稱
- 權限區分建議檢附「權限對照表」，標示不同職稱之存取等級
- 保密切結書須涵蓋**所有**接觸個資之人員

4.10–4.11 系統設備安全管理與銷毀程序

4.10 系統設備防護措施

針對電腦、伺服器、USB、硬碟等**媒介物**採取防護措施，並留存作業紀錄。建議具體描述管控措施（如每季更換密碼、紙本文件加鎖）。

應檢附具有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。

4.11 設備報廢或轉用之銷毀程序

請檢附**個資紙本、電子資料及設備之銷毀程序**與**作業紀錄**、**硬體清除紀錄（格式化或物理破壞）**。

銷毀程序建議區分：紙本（碎紙）、電子檔（格式化）、硬體（消磁）。

4.11⇔7.2

4.12 個資使用軌跡紀錄留存

請填寫個資使用及軌跡紀錄之**保存期限**，並檢附留存紀錄與**系統主機軌跡紀錄檔**設定畫面。

留存個人**資料使用紀錄**及系統軌跡紀錄檔，資料須保存**5年**，符合個資法第30條規定。

> 軌跡紀錄範疇：系統登入、資料查詢、修改、匯出紀錄。無電子系統者可提供紙本「存取登記簿」或「調閱申請單」。

保存年限須明訂於內部個資安維計畫，並確保歷史紀錄完整保存。

§30 損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。

再次提醒

資料生命週期管理

4.6 委外監督

委託他人蒐集、處理個資時，應定期確認受託者執行狀況，監督項目依個資法施行細則第8條辦理，並留存監督紀錄。

4.11 報廢與銷毀

設備或媒介物報廢時，需訂定銷毀程序：紙本碎紙、電子檔格式化、硬體消磁，並留存銷毀作業紀錄。

4.12 軌跡紀錄

留存個資使用紀錄及系統軌跡紀錄，包含登入、查詢、修改、匯出等，保存期限須明訂於安維計畫中。

4.7 行銷告知

首次利用個資進行行銷前，須依個資法第20條完成告知作業並留存紀錄。

紀錄保存期限建議明訂於內部個資安維計畫，並確保歷史紀錄完整保存。

伍、電子商務與資通系統安全管理

5.1 身分確認

帳號申請、異動及定期盤點紀錄

5.2 隱碼機制

螢幕顯示或紙本輸出時遮罩敏感欄位

5.3 傳輸加密

採用SSL/TLS或VPN等加密機制

5.4檔案存取控制與保護監控 / 5.5 防外部入侵

存取管理與保護措施 / 防火牆、防毒、IPS/IDS及內外網路區隔

5.6 異常監控

LOG日誌、自動警示及行為分析機制

5.7 定期演練

演練個資外洩、入侵等情境並留存檢討紀錄

5.1–5.2 身分確認與隱碼機制

5.1 使用者身分確認及保護機制

應採取身分確認與保護機制，並檢附帳號申請及異動紀錄、帳號定期盤點紀錄。無保護機制者須說明理由。

5.2 個人資料顯示之隱碼機制

系統輸出個資（螢幕顯示或紙本列印）時，須採用隱碼遮罩處理。如：身分證後四碼遮罩 **A22345****。請檢附螢幕截圖或紙本輸出隱碼佐證。

5.3–5.4 傳輸加密與資料庫存取控制

5.3 網際網路加密傳輸

傳輸加密機制

- SSL/TLS 加密協議
- VPN 安全遠端存取
- 其他加密方式

請檢附螢幕截圖或產品購買/建置證明。

5.4 個人資料檔案及資料庫之存取控制與保護監控措施

檔案及資料庫存取控制措施

- 資料檔案存取管理...（存放個資的設備，如:NAS、存放個資的系統，如:學籍系統DB）
- 強化身份驗證與權限管理
- 存取紀錄與系統日誌審查
- 資料庫加密與定期漏洞掃描
- 安全訪問控制（IP/時段限制）

請檢附存取控制截圖或作業紀錄。

5.5–5.6 外部入侵防護與異常行為監控

5.6 異常使用行為監控

- LOG 日誌記錄（系統/防火牆/Web）
- 自動警示機制
- 行為監控系統與行為分析
- 存取控制管理

若發生異常，請檢附「異常事件處理紀錄」；若無異常，請檢附「異常演練紀錄」或「定期監控分析報告」。

5.7 定期演練及檢討改善

01

演練主題規劃

對應「風險分析」中高風險項目，涵蓋個資外洩、勒索軟體、釣魚攻擊、社交工程、自然災害等情境。

02

多角色分工執行

演練紀錄應呈現發現者、通報者、決策者、執行者等不同角色分工。

03

檢討與改善追蹤

演練後須檢附「檢討紀錄」，誠實記錄缺失（如通報過慢、備份還原時間過長），並提出改善措施與追蹤紀錄。

5.5–5.7 應有所對應
外部入侵防護、異常監控與定期演練

演練涵蓋情境

- ✓ 個資外洩、外部網路入侵
- ✓ 勒索軟體、釣魚攻擊、社交工程
- ✓ 系統服務中斷、自然災害

⚠ 演練紀錄須呈現不同角色分工：發現者、通報者、決策者、執行者。

演練主題建議對應4.2風險分析中的高風險項目，演練後須誠實記錄缺失並提出改善措施與追蹤紀錄。

陸、 環境管理措施 / 柒、 業務終止個資管理

6.1 環境管理措施

針對個資存取媒介物及環境（機房、雲端）採取管理措施，主要適用於**中高**等級單位。

- 等級中：存取記錄、可攜式媒體申請管控紀錄、資料備份記錄
- 等級高：另需檢附合規性文件（第三方驗證證書）

7.1 業務終止之個資措施與處置 / 7.2 留存相關紀錄

應訂定業務終止之個資處置措施，並留存相關紀錄。

- 列舉本年度業務中止之個資檔案清冊
- 銷毀需檢附銷毀紀錄與照片
- 移交需檢附移交簽收清單
- **紀錄至少留存五年**（適用部分業別）

7.2⇔4.11

捌、事故通報與應變程序

1

8.1 72小時內通報

知悉個資洩漏起72小時內完成通報，明確列出內部（個資專責人員、負責人）及外部（主管機關）通報窗口。

2

8.2 應變措施控制損害

訂定應變措施以控制損害擴大，依安維辦法規定執行並留存佐證。

3

8.3 通知當事人

查明事故後以適當方式通知當事人，並告知已採取之因應措施。

4

8.4 研議預防機制

若發生事故，須填寫案發日期、檢附矯正預防單及預防機制說明。

玖、資安檢測

9.1 系統弱點掃描

針對處理個資之資訊系統執行，請檢附弱點掃描紀錄及修補紀錄。

9.2 滲透測試

針對處理個資之資訊系統執行，請檢附滲透測試紀錄。

9.3 資安健診

無論是否處理個資皆需執行，項目含網路架構、防火牆設定、資料庫安全等檢視。

9.4 APP 檢測

如有處理個資之APP，請檢附APP檢測紀錄，並選用數位部認可之認證實驗室執行。

合規重點總結

系統安全
身分驗證、隱碼機制、傳輸加密、資料庫存取控制、入侵防護

監控與演練
異常行為監控、定期演練、多角色分工、檢討改善追蹤

環境與終止管理
機房環境管控、業務終止個資處置、紀錄留存至少五年

事故通報與資安檢測
72小時通報機制、應變措施、預防機制、弱點掃描與資安健診

所有佐證資料建議參照各章節「同1.1項佐證資料」格式，並依個資保護要求強度等級（普 / 中 / 高）提交對應文件。

哪裡找資料...

- 教育體系個資安維行政檢查計畫(PDSAI)官網
  - https://sites.google.com/ntub.edu.tw/personaldata/
- 檢查表及教育部各事業別安維辦法對應表
  - https://reurl.cc/7VpqnN

	A	B	C	D	E	F	G	H	I	J
1	查 核 重	查 核 內 容	紀錄文件	私立專科以上學校及私	私立高級中等以下學校	海外臺灣學校及大陸地	私立兒童課後照顧服務	短期補習班個人資料檔	運動彩券業個人資料檔	個資法暨施行細則
2	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」	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)。	第3條 依私立學校法核准設立之私立專科以上學校（以下簡稱學校）及依學術研究機構設立辦法核准設立之私立學術研究機構（以下簡稱機構）**應訂定個人資料檔案安全維護計畫**（以下簡稱安全維護計畫），落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第4條1項 學校及幼兒園**應依本辦法規定訂定安全維護計畫**，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第4條 依海外臺灣學校設立及輔導辦法設立之海外臺灣學校及依大陸地區臺商學校設立及輔導辦法設立之大陸地區臺商學校(以下簡稱境外臺校)**應訂定個人資料檔案安全維護計畫**，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第4條 課照中心**應依本辦法規定，訂定安全維護計畫**，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第3條第1項 短期補習班（以下簡稱補習班）**應訂定個人資料檔案安全維護計畫**（以下簡稱計畫），落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	第3條第1項 運動彩券業**應訂定個人資料檔案安全維護計畫**（以下簡稱計畫），落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	(個資法授權主管機關訂) 個資法第27條第2項規定中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

查檢表 https://reurl.cc/aXbMbQ