

TIPAS：2021⁺

條文逐項實務指引

本指引依據 TIPAS：2021⁺ 規範編製，提供各條文之實務操作說明、
合規建議及注意事項，供組織建置與維運個人資料管理制度之參考。

財團法人資訊工業策進會 科技法律研究所

第三章 用語與定義（節錄：3.5～3.9）

以下各條文為 TPIPAS：2021+ 第三章用語與定義中，與組織內部管理角色及事件處理密切相關之定義，並附實務指引說明。

3.5 個人資料管理代表

條文意旨

個人資料管理代表係由最高管理階層（如代表人、執行長、董事長）正式指派之管理階層成員，負有監督組織整體個人資料管理制度（PIMS）運作之職責與權責。

實務指引

- 管理代表應以書面（如任命書、會議記錄等）正式指派，並明確記載職稱、姓名、任期及職權範圍。
- 管理代表應具備足夠之管理職位（如副總、處長級以上），以確保其能有效調度資源、推動制度。
- 管理代表應定期（至少每年）向最高管理階層提交個人資料管理制度執行成效報告，報告應包含風險狀態、稽核結果、事故摘要及改善措施。
- 管理代表不得與查核人員互相兼任，以確保評量之獨立性。

實務提示：建議於組織章程或內部規章中明文規定管理代表之設置、任免程序及替代機制，避免因人事異動造成制度運作中斷。

3.6 個人資料管理人員

條文意旨

個人資料管理人員係實際推動並確保個人資料管理制度有效運作之人員，應具備個人資料管理師、個人資料內評師或個人資料驗證師資格之一，得由管理代表兼任。

實務指引

- 組織應確認管理人員持有有效之 TPIPAS 認可資格證書，並留存證書影本備查。
- 管理人員應負責日常 PIMS 文件維護、教育訓練規劃執行、當事人權利請求處理及事故通報協調等工作。
- 若由管理代表兼任，應確保其有足夠時間處理管理人員職務，並在工作說明書中明列。
- 管理人員資格到期前，應完成換證或繼續教育，以維持資格有效性。

實務提示：建議組織至少培養兩名具備資格之人員，以應對人員離職或請假時之緊急替代需求。

3.7 查核人員

條文意旨

查核人員係指辦理組織個人資料安全稽核之人員，須具備稽核獨立性及專業性，且不得與執行個人資料管理之管理人員互相兼任。

實務指引

- 查核人員可為內部人員或委外之專業機構/顧問。
- 查核人員應具備相關稽核資格（如 TPIPAS 個人資料內評師、驗證師）或足夠之實務稽核經驗，並留存相關資格文件。
- 稽核前與受稽核單位確認無利益衝突；稽核報告應獨立出具，不受受稽核單位干預。
- 組織應在程序文件中明定查核人員之遴選標準、任命程序及不兼任之限制規定。

實務提示：若委外辦理稽核，應在委外合約中明確約定稽核人員之資格條件、保密義務、報告格式及交付時限。

3.8 組織人員

條文意旨

組織人員係指受組織直接監督、與個人資料蒐集、處理或利用相關之從業人員，包括正職、派遣、約聘及其他形式之人員。

實務指引

- 組織應建立完整之人員清冊，區分正職、派遣、約聘、兼職及實習人員，並依其接觸個人資料之程度給予不同等級之授權與監督。
- 接觸個人資料之人員，應先完成個人資料保護教育訓練並簽署保密切結書（搭配 A.8.8.2）。
- 派遣及約聘人員之管理應納入派遣合約或委任契約，明確約定其個人資料保護義務。
- 人員離職或職務異動時，應即時收回相關權限、設備及資料存取憑證，並完成保密義務之確認程序。

實務提示：建議每季定期盤點人員名冊與系統帳號清單，確保兩者一致，及時移除已離職人員之系統存取權。

3.9 事故

條文意旨

事故係指個人資料之外洩、滅失、毀損、竄改及其他侵害；或其他違反個人資料保護相關法令或本制度規範之情事。

實務指引

- 建立如「事故判定標準、知悉後內部通報、外部通報及通知、以及損害控管應變」的標準化作業程序。
- 事故定義應涵蓋實體（紙本外洩、設備遺失）與電子（系統入侵、誤傳電子郵件）等各類型情境。
- 組織應建立事故登錄表單，記錄事故發現時間、影響範圍、涉及資料類型及當事人人數等資訊。
- 即便最終確認非屬資料外洩，疑似事故之調查過程亦應留存書面紀錄，以備稽核查驗。

實務提示：建議定期（每年）進行實際演練，模擬事故發生情境，測試組織應變能力及通報流程熟悉度。

第四章 組織環境

4.1 內外部議題

條文意旨

組織應決定與個人資料管理制度有關，且可能影響制度運行有效性之內部與外部議題。

實務指引

- 內部議題包含：組織規模與業務性質、現有 IT 基礎設施成熟度、人員個資保護意識、內部政策及文化、近期組織變革（如併購、業務擴張）等。
- 外部議題包含：相關個資法令動態（個人資料保護法修正）、主管機關裁罰案例、行業特性風險（如醫療、金融保險）、合作廠商供應鏈風險、資安威脅趨勢等。
- 組織宜建立「議題盤點表」，定期（每年）更新，並與風險評估連結，透過交互參照確認議題是否產生新風險。
- 議題分析結果應反映於個人資料保護管理手冊之範疇設定及風險評鑑過程中。

實務提示：可透過 SWOT 分析或 PEST 分析工具，識別內外部議題，確保分析完整性。

4.2 利害關係人需求

條文意旨

組織應決定與個人資料管理制度相關之利害關係人，以及其相關要求事項。

實務指引

- 利害關係人可包含：個人資料當事人（客戶、員工）、主管機關（個資保護委員會、目的事業主管機關）、股東/董事會、業務合作夥伴及委外廠商、稽核機構及社會大眾。
- 宜建立「利害關係人清冊」，記錄各方需求（如：當事人要求權利行使、主管機關要求依法通報、合作夥伴要求安全維護措施）
- 定期檢視，以因應法規修訂或業務合作關係變動而更新。
- 將利害關係人之合規要求轉化為具體的制度設計要素（如：告知之方式、當事人申訴管道等）。

實務提示：建立利害關係人溝通流程，說明如何向各方傳遞個資保護相關資訊（如：隱私權聲明、年報等），增加信任。

4.3 管理制度範圍

條文意旨

組織應考慮 4.1 及 4.2 事項決定個人資料管理制度之範圍。

實務指引

- 管理制度範圍應明確列舉納入管理之部門、地點、業務流程及個人資料類型。
- 範圍聲明應書面形式呈現，納入個人資料保護管理手冊，並於揭露於驗證申請文件中。
- 當組織新增業務線、子公司或分支機構時，應即時評估是否需擴大管理制度範圍。

實務提示：若資源尚無法一步到位，管理範圍可先聚焦於實際蒐集、處理或利用個人資料之核心流程；全組織驗證應包含組織各部門所有涉及個資之流程，特定範圍驗證則可擇定部門、流程、或產品。

第五章 管理責任

5.1 最高管理階層

條文意旨

最高管理階層之責任應包括：

- (1) 決定個人資料管理制度目標，確保符合組織需求與發展策略。
- (2) 決定個人資料保護管理政策。
- (3) 決定資源管理。
- (4) 決定個人資料保護管理組織架構及權責劃分。
- (5) 定期檢視管理制度，確保管理制度達成預期效果。
- (6) 建立有效之溝通機制，適時指導與支援組織人員。
- (7) 傳達落實個人資料管理制度之重要性。

實務指引

- 最高管理階層應以書面（如公告、會議決議）承諾推動個人資料管理制度，並留存相關文件。
- 每年至少召開一次由最高管理階層主持或出席之管理審查會議，並製作會議紀錄。
- 最高管理階層應每年檢視及簽核組織個人資料檔案安全維護計畫。
- 資源分配（預算、人力、設備）應有具體之書面核准紀錄，如最高管理階層之簽名或蓋章。
- 最高管理階層應透過適當管道（如全員大會、內部通訊、教育訓練）向全體員工傳達個資保護之重要性。

實務提示：提供最高管理階層支持個資保護政策之書面紀錄，如政策決議、資源分配之書面簽核證明、或會議記錄等，有助於展示最高管理階層的重視程度。

5.2 個人資料保護管理政策

條文意旨

最高管理階層應將其內部保有及管理個人資料之依據、目的與組織所負責任等基本理念原則，以書面訂定並對組織人員加以公開周知。個人資料保護管理政策應包括以下事項：

- (1) 個人資料管理制度之目標。
- (2) 承諾落實本制度規範要求事項與法令。
- (3) 承諾定期檢視與持續改善。

實務指引

- 管理政策應由最高管理階層正式簽署（含簽署日期），並標注版本號及生效日期。
- 政策內容應包含三大要素：（1）個人資料管理之目標；（2）遵循本制度規範與相關法令之承諾；（3）定期檢視與持續改善之承諾。
- 政策應以全體員工易於取得的方式公開周知（如：公司內網、佈告欄、新人訓練教材），並留存公開周知之證明（如截圖、照片）。
- 政策至少每年重新檢視，於法令修訂、業務重大變更或事故發生後應即時檢討更新。

實務提示：管理政策宜簡潔清晰，避免過於冗長難以閱讀；可另行制定「隱私聲明」對外公告，管理政策則側重對內宣示。

5.3 權限與責任分工

條文意旨

最高管理階層應以書面明定個人資料管理制度相關人員之職務、職掌、選任方式、責任層級及權限內容，並向組織內部公開周知。

實務指引

- 組織宜建立「個人資料管理組織架構圖」，清楚呈現各角色（最高管理階層、管理代表、管理人員、各部門業務窗口）之層級關係。
- 明訂各角色在個資蒐集、處理、利用、安全管理、事故應變等環節之責任與授權範圍。
- 責任分工文件應向全體相關人員公開（如放置於內部網站或人事系統），並定期更新。

實務提示：可定期舉辦個資人員教育訓練，強化各級人員之責任意識。

5.4 管理代表

條文意旨

最高管理階層應指派管理階層成員之一，擔任個人資料保護制度管理代表，其應有之責任與職權包括：

- (1) 負責維持個人資料管理制度運作之有效性，並建立必要內部人員結構。
- (2) 確保職務執行過程之公正性與客觀性。
- (3) 確保個人資料管理制度所需之各項程序被建立、實施與維持。
- (4) 向最高管理階層報告個人資料管理制度之實施成效與改善措施。

實務指引

- 任命書應明確載明管理代表之姓名、職稱、任期及核心職責。
- 管理代表應定期彙整制度執行狀況，包括風險評鑑更新、稽核缺失改善、事故統計及教育訓練完成情況，提交最高管理階層審閱。

- 管理代表職務的執行過程中，若發現潛在利益衝突，應揭露並由最高管理階層決定處理方式。

實務提示：建議管理代表建立固定的月報或季報機制，定期追蹤個資管理制度之執行狀態，使最高管理階層保持即時掌握。

5.5 個人資料管理人員

條文意旨

組織應由取得下列資格之一者，擔任個人資料管理人員，以實際推動並確保個人資料管理制度之有效運作：

- (1) 個人資料管理師。
- (2) 個人資料內評師。
- (3) 個人資料驗證師。

個人資料管理人員得由個人資料管理代表兼任。

實務指引

- 任命管理人員前應確認其資格證書之有效性，並留存證書影本於人事檔案或個資管理制度文件中。
- 管理人員之職責應以工作說明書形式明列，涵蓋：日常個資保護程序維護、教育訓練規劃執行、內部評量協調、當事人請求處理協助等。
- 若由管理代表兼任，應確認其工作量可負荷，並在任命文件中明確說明兼任情形。
- 資格證書到期時應安排換證作業，避免資格中斷影響制度合規性。

實務提示：鼓勵管理人員持續進修個資保護相關知識（參加研討會、TPIPAS 課程與講座、閱讀主管機關最新公告），以保持對法令動態之掌握。

第六章 制度規劃

6.1 總則

條文意旨

組織應依其規模、特性及本制度規範之具體要求，建立、實施與維持個人資料管理制度，並持續改善，以維護其有效性。

實務指引

- 制度規劃應從整體性出發，考量組織的業務規模、資料敏感程度、法令適用範圍，訂定符合比例原則的管理措施。
- 建立制度時應確保所有必要程序均已書面化，並有明確的負責人、執行週期及紀錄要求。
- 持續改善機制應制度化（如透過年度管理審查、矯正預防措施追蹤），而非僅在稽核前臨時補救。

實務提示：制度建置初期可採分階段推進策略，優先完成核心要求（政策、風險評鑑、事故應變），再逐步完善附屬程序。

6.2 個人資料保護管理手冊

條文意旨

組織應製作個人資料保護管理手冊，訂定具體規則，包含識別法令、識別個資、蒐集處理利用程序、風險管控、事故應變、教育訓練、文件紀錄管理、當事人申訴及諮詢、內部評量、矯正預防措施及最高管理階層定期檢視等十八項主題。

實務指引

- 管理手冊應作為 PIMS 的核心文件，統整所有政策、程序及表單之索引，確保各程序文件互相連貫。
- 手冊應包含版本管理資訊（版本號、修訂日期、修訂摘要、核准人），並建立修訂審查機制。
- 新進個資小組人員應接受個資管理手冊之教育訓練，使其儘快熟悉組織個資保護框架。

實務提示：管理手冊不宜複製法條文字堆砌，應著重於「組織如何」落實各項要求的具體描述，使讀者一目了然各自的操作義務。

6.3 因應風險之規劃

組織於規劃個人資料管理制度時應將內外部議題、利害關係人需求與相關本制度規範納入考量，規劃風險管理之原則、框架及過程，辨識相關風險與因應管控措施，並得適時採納從設計與預設階段著手隱私保護（Privacy by design and default）之概念。

6.3.1 個人資料隱私衝擊風險評鑑

條文意旨

組織應建立個人資料相關之風險分析與評估程序，包含風險準則建立、一致性評估、風險識別與擁有者、風險分析（衝擊值、可能性、風險等級）及評估優先次序，且應納入組織與當事人雙方影響。

實務指引

- 組織應建立「個人資料風險盤點表」，分析組織所持有之個資所具有之潛在風險。
- 設計風險衝擊矩陣，定義衝擊值（I）、可能性（P）等級矩陣以及風險分區，以確保個資風險具可評估性及可控制性。
- 風險評鑑應以業務流程或個資類型為維度，逐一識別威脅情境（如：未授權存取、意外外洩、系統故障）及其可能影響。
- 每個風險宜擇定負責之管理人員，確保風險有明確的責任歸屬。
- 風險分析結果應同時考量對組織（如對法律責任、名譽受損）及對當事人（如對隱私侵害、財務損失）之影響。
- 風險評鑑結果應以文件記錄，並至少每年重新檢視，或於重大業務變更、法令修訂、事故發生後即時更新。

實務提示：隱私衝擊評估（PIA/DPIA）可作為高風險流程的深度風險分析工具，建立一致、有效、可比較之標準。

6.3.2 風險管控措施

條文意旨

組織應依風險評鑑結果決定適當的風險管控措施，並確保符合附表 A 所列之必要安全管理措施。

實務指引

- 風險處理選項包含：風險轉嫁（購買保險）、風險避免（禁止目的外利用）、風險接受（留存接受理由之書面決策）、風險控制（安全管理措施）。
- 管控措施應對應具體之風險，並在「個人資料風險評估表」中記錄個資流程所涉及之風險與其相應之安全管理措施。
- 應定期評估管控措施之有效性，以確認風險對策之實際效果。

實務提示：建立「個人資料風險評估表」中控制措施欄位，每年管理審查會議應決定可接受風險值，並對超出可接受風險之流程，評估適當之風險對策，並持續追蹤後續成果。

第七章 支援

7.1 資源

條文意旨

組織應提供並維持個人資料管理制度所需之人力及軟硬體資源，確保資源管理之有效性，並留存相關紀錄。

實務指引

- 人力資源：確保管理代表、管理人員及相關業務人員有足夠時間投入個資管理工作，避免職務衝突或時間不足。
- 技術資源：包含資安工具（防火牆、防毒軟體、加密系統、日誌管理系統）、個資管理系統或資料盤點工具，應確保維持有效運作。
- 財務資源：建立年度個資保護預算，涵蓋教育訓練費用、系統購置維護費用、驗證費用及緊急應變資源。
- 資源配置之核准紀錄（如預算簽核文件、採購紀錄）應納入管理制度文件，以作為合規佐證。

實務提示：在年度計畫或預算規劃中，明確列示個人資料保護相關支出項目，有助於展示組織資源投入的具體承諾。

7.2 教育訓練

條文意旨

組織應確保組織人員對個人資料管理、管理與獎懲制度具有正確認知及能力，並建立基本教育訓練、權責人員訓練、成果維持與改善機制。

7.2.1 總則

實務指引

- 教育訓練應依人員類型設計不同深度的課程：全員基礎課程（個資法概念、日常注意事項）及權責人員進階課程（風險評鑑、事故應變、稽核技術）。
- 訓練方式可採多元形式：面對面授課、線上學習（e-learning）、事故模擬或工作坊。

7.2.2 基本教育訓練

實務指引

- 所有組織人員應定期（至少每年一次）接受個人資料保護基礎教育訓練，內容涵蓋：個資法基本概念、組織個資保護政策、日常操作注意事項（如社交工程郵件、紙本文件管理）、事故通報程序。
- 訓練完成後應進行測驗或簽名確認，留存訓練出席紀錄及測驗成績，作為合規佐證。
- 新進人員應於到職後一個月內完成基礎教育訓練，並留存訓練完成紀錄。

實務提示：可製作淺顯易懂的個資保護手冊，作為訓練的補充教材，方便員工隨時查閱。

7.2.3 權責人員教育訓練

實務指引

- 個資管理制度相關權責人員（管理代表、管理人員、部門個資聯絡人）應接受進階專業訓練，包含：風險評鑑方法、內部評量技巧、當事人權利請求處理、事故應變演練等。
- 訓練需求應依年度需求評估結果規劃，考量法令變動、業務調整或過去稽核缺失等因素。
- 組織應留存權責人員之訓練計畫、出席紀錄、訓練教材及效果評估結果。

7.2.4 成果維持及改善措施

實務指引

- 訓練完成後應評估訓練成效（如：測驗成績趨勢分析、訓練滿意度調查、實際申訴案件趨勢分析）。
- 若訓練成效不佳或有特定缺失，應記錄改善措施並追蹤執行結果。
- 年度訓練計畫應依上一年度成效評估結果調整，確保課程內容持續優化。

實務提示：可採用個資保護意識調查 (Awareness Survey) 或社交工程郵件等工具，客觀衡量人員的個資保護意識與能力水準；高階管理人員，可透過工作坊、講座等方式，提升法遵意識。

7.3 文件及紀錄之控管

7.3.1 文件及紀錄之範圍

條文意旨

組織應製作及保存下列文件：

- (1) 個人資料保護管理政策。
- (2) 個人資料保護管理手冊，及其相關具體規則。
- (3) 個人資料內部管理程序相關表單。
- (4) 個人資料管理制度之相關紀錄。

實務指引

- 建立「文件清冊」，列舉所有受控文件的名稱、編號、版本、負責人及保存位置。
- 內部文件應包含一至四階文件分類。一階文件應包含政策類文件；二階文件應包含各式程序類文件，如流程、程序等；三階文件應包含作業規範/指導書；第四階文件應包含各式申請表單及內部活動記錄。
- 政策類文件 (Policy)：一階文件，說明組織意圖與承諾 (如個人資料保護管理政策)。
- 程序類文件 (Procedure)：二階文件，個人資料檔案安全維護計畫，說明如何執行特定活動 (如事故應變程序、當事人請求處理程序)。
- 作業規範/指導書 (Work Instructions)：三階文件，提供執行人員操作的詳細步驟 (例如：硬碟銷毀作業規範、備份執行步驟)。
- 表單類文件 (Form) 與紀錄類文件 (Record)：四階文件，提供標準化填寫格式 (如個資盤點表、風險評鑑紀錄表、事故報告表)，以及個資管理安全維護措施執行之證據 (如已完成之事故報告、教育訓練出席表)。

7.3.2 文件管理

條文意旨

組織應建立文件管理程序，包含文件製作及修正事項、版本差異標記、儲存位置及存取權限管理。

實務指引

- 文件修訂時應在修訂紀錄欄位標明版本號、修訂日期、修訂摘要及核准者，舊版文件應留存或標示為「廢止版本」。
- 文件應儲存於安全且可管理的位置 (如企業文件管理系統、SharePoint、受控的共用資料夾)，並設定存取權限 (限授權人員讀取或編輯)。
- 電子文件應有備份機制，紙本文件應有適當之實體保存場所 (如檔案室、上鎖文件櫃)。

實務提示：推薦採用文件編碼系統，例如「PIMS-POL-001」代表第 001 號政策文件，便於追蹤管理。

7.3.3 使用紀錄與證據管理

條文意旨

組織為證明其已符合制度要求，應製作必要之紀錄文件並確立管理程序，包含個資蒐集/處理/利用紀錄、安全維護措施證據、當事人權利行使紀錄，且相關紀錄應留存至少五年。

實務指引

- 各類紀錄應至少保存五年，並紀錄名稱、存放位置及銷毀方式。
- 個資蒐集紀錄：同意書、告知聲明、隱私權聲明
- 個資處理紀錄：系統操作日誌、資料異動紀錄

- 個資利用紀錄：內部傳輸紀錄、外部提供授權文件。
- 安全維護措施證據：包括風險評鑑報告、安全措施測試結果、系統設定截圖等。
- 當事人權利行使紀錄：包括申請書、身分核驗紀錄、處理結果通知書。

實務提示：建立統一的紀錄銷毀流程，確保超過保存期限的紀錄依安全方式銷毀（電子檔案覆寫或實體媒體毀損），並留存銷毀紀錄。

7.3.4 系統日誌管理

條文意旨

組織維運資通系統蒐集、處理或利用個人資料，應訂定日誌記錄週期及留存政策、確保系統具備記錄特定事件之功能，並記錄系統管理者帳號執行之各項功能。

實務指引

- 明訂各類資通系統（如 CRM 系統、資料庫、網頁應用程式）的日誌記錄項目（登入/登出、資料存取、修改、刪除、權限變更）及留存時間。
- 管理者帳號（Administrator/Root）之所有操作行為應完整記錄，包含執行時間、操作內容、操作前後狀態。
- 日誌應儲存於獨立於業務系統的安全位置，限制一般使用者存取，防止遭篡改或刪除。
- 定期（如每月）對日誌進行異常行為分析，及時發現未授權存取或可疑操作，並將分析結果留存。

實務提示：建議導入 SIEM (Security Information and Event Management) 工具有助於自動化日誌彙整與異常告警，減輕人工審閱負擔。

7.4 溝通或傳達

條文意旨

組織應建立有效之溝通或傳達機制與程序。

實務指引

- 對內溝通：定期（如季度）向各部門主管傳達個資保護制度執行狀況、重要法令動態及管理審查結果。
- 對外溝通：建立回應媒體、主管機關、合作夥伴詢問的標準程序，確保對外口徑一致且符合法令要求。
- 緊急溝通：事故發生時的溝通程序應預先規劃，包含對內通報（管理代表、最高管理階層）及對外通知（當事人、主管機關）之責任人、時限及方式。

實務提示：建立「個人資料保護聯絡窗口」機制，對外公告一個統一的聯繫管道（如電子郵件信箱、客服電話），便於當事人申訴及諮詢。

第八章 個人資料管理制度之實施

8.1 識別法令及其相關規範

條文意旨

組織應識別所須遵循之相關法令，明示個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令變動進行調整。

實務指引

- 建立「法令盤點清冊」，列舉組織適用之個資相關法規（個人資料保護法、各目的事業主管機關特別規定、子法等），並標注各法規之適用部門及對應之制度措施。
- 指定專人（如法務部門或管理人員）負責每年定期追蹤法令動態，於法規修訂時即時更新法令清冊，並評估對現行制度之影響。
- 當法令修訂對管理制度有實質影響時，應啟動文件修訂程序，並完成相應的人員教育訓練。

實務提示：留意個資保護委員會（籌備處）、目的事業主管機關及 TPIPAS 維運機構（資策會科法所）之官方公告，確保及時掌握法令變動資訊。

8.2 納入管理之個人資料範圍

條文意旨

組織應界定其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。

實務指引

- 進行全組織個人資料盤點，識別所有個資檔案（電子/紙本/混合），記錄資料類型、涉及當事人類型（員工、客戶、供應商）、儲存位置、存取權限及保存期限。
- 建立「個人資料檔案清冊」，欄位至少包含：保有單位；個人資料之項目、類別、型態、數量；蒐集之特定目的、方式、來源；向當事人告知之方式，或得免為告知之情形；蒐集、處理及利用相關業務或程序；為目的外利用之情形；保存方式、期限及銷毀方式。
- 建立「個人資料流程圖」，呈現資料從蒐集→處理→利用→儲存→銷毀各環節的流向及相關人員/系統。
- 個資清冊及流程圖應至少每年更新，或於新業務上線、系統異動時即時更新。

實務提示：可採用資料流程圖（Data Flow Diagram, DFD），系統化呈現個資在組織內外的流動全貌，有助於後續風險識別。

8.3 風險管控措施之實施

條文意旨

組織應就納入管理範圍之個人資料，識別組織因蒐集、處理、利用個人資料可能面臨之風險，考量個人資料隱私衝擊風險評鑑結果，落實適當風險管控措施。

實務指引

- 依據個資清冊及流程圖，針對每個資料處理活動識別潛在風險情境（如：網路攻擊、內部人員不當操作、紙本文件遺失等），並且訂定可接受之風險水準。
- 確認風險評鑑已針對每個識別之風險確定「風險擁有者」，並建立對應之管控措施（技術面及管理面）。
- 管控措施實施後應進行有效性驗證（如人員教育訓練、加密管理、模擬社交工程攻擊），確認措施能如預期降低風險。
- 定期更新風險評鑑及管控計畫，確保新興威脅（如新型惡意軟體、新業務模式）均已納入考量。

實務提示：採用「剩餘風險評估」機制：在實施管控措施後，重新評估殘餘風險是否已降至可接受水準，若仍超過接受準則，應繼續強化措施或由最高管理階層決定是否接受風險。

8.4 個人資料之蒐集、處理與利用

8.4.1 總則

條文意旨

組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。

實務指引

- 「資料最小化」原則：蒐集的個人資料應僅限於達成特定目的所必需者，應定期審視各業務流程中蒐集的個資欄位是否全部必要。
- 「目的限制」原則：個資不得超出蒐集時的特定目的範圍使用，若需挪作其他用途，應重新確認合法基礎（如重新取得同意）。

實務提示：在設計新業務流程或系統時，即於設計階段導入隱私保護（Privacy by Design），避免事後補救，例如：預設最高隱私保護設定、最小化個資蒐集欄位。

8.4.2 蒐集

條文意旨

組織針對個人資料蒐集程序應確認蒐集時具備特定目的及符合法律規定之特定情形、其他法令

規定之義務，並保存相關紀錄。

實務指引

- 蒐集前應確認合乎個資法基礎。
- 蒐集紀錄應包含：蒐集時間、蒐集方式（紙本/線上）、蒐集目的、法律基礎、當事人身分確認方式等資訊。

實務提示：定期（如每年）審視同意書格式，確認其符合最新法令要求；若超出原目的、或目的變更，應重新蒐集同意、規劃相應的補充蒐集作業。

8.4.3 處理

條文意旨

組織針對個人資料記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及內部傳送，其程序應確認符合蒐集時特定目的及特定情形、其他法令規定義務，並訂定刪除/銷毀及業務終止時之程序，留存相關紀錄。

實務指引

- 建立「個資生命週期管理程序」，明定個資從蒐集→處理→利用→刪除銷毀各階段之操作要求及負責人。
- 個資刪除及銷毀程序應明確：刪除、銷毀觸發條件（保存期限屆滿、當事人請求、業務終止）、方式（電子資料覆寫、實體媒體破壞、紙本文件碎紙）、紀錄留存。
- 業務終止時的個資處置：應在業務終止計畫中納入個資刪除、銷毀/返還章節，確保蒐集個資目的終止後不留存個資。
- 個資之內部傳送應有程序規定（如申請單或 SOP 等）。

實務提示：宜建立「個資保存期限對照表」，依資料類型（員工資料、客戶資料、交易紀錄等）明定最低及最高保存期限，並自動化提醒銷毀時限。

8.4.4 利用

條文意旨

組織對於個人資料利用程序應確認於蒐集之特定目的必要範圍之內利用個人資料，履行其他法令規定義務，並保存相關紀錄。

實務指引

- 確認是否具有非蒐集目的範圍之利用，並應確認是否合乎個資法規定。
- 個資提供予第三方（非委託關係）前，應確認是否有授權依據，並建立提供紀錄（含提供對象、提供內容、提供時間、目的）。
- 對外部供應商提供個資時，應評估其個資保護能力，並簽訂個資保護條款或保密協議。

實務提示：確認蒐集個資目的與利用手段是否具有合理關聯性、及最小侵害性。組織應留

存傳輸軌跡，紀錄曾提供個資之對象。

8.4.5 行銷

條文意旨

組織針對利用個人資料進行行銷，其程序應提供當事人至少首次免費表示拒絕接受行銷之方式、隨時拒絕管道並立即停止，並保存相關紀錄。

實務指引

- 行銷訊息（如電子郵件、簡訊）中應明確提供「退訂/拒絕接受行銷」的操作方式（如退訂連結、回覆指定文字），且首次提供無需費用。
- 當事人表示拒絕接受行銷後，應於合理期間停止向其發送行銷訊息，並在系統中標記「禁止行銷」狀態。
- 建立「拒絕行銷名單」管理機制，確保拒絕記錄在各行銷管道（電子郵件、電話、紙本郵件、曾提供個資合作商）中同步生效。
- 行銷活動前應確認名單中是否有已拒絕接受行銷的當事人，避免誤發。

實務提示：若進行電話行銷，應遵守相關規定（如不得在特定時段撥打）並建立「拒絕行銷名單」。電子郵件行銷建議採用具退訂功能的 ESP (Email Service Provider) 平台，自動處理退訂請求。

8.4.6 國際傳輸

條文意旨

組織於國際傳輸個人資料時，應確實檢視並遵循主管機關之限制；於傳輸前明確告知當事人擬傳輸之國家或區域，並保存相關紀錄。

實務指引

- 識別組織中所有涉及個資國際傳輸的業務場景（如：使用境外雲端服務、跨國集團內部傳輸、委託境外廠商處理）。
- 查詢中央目的主管機關或個資保護委員會（籌備處）公告之禁止或限制傳輸國家或地區名單，確認目標傳輸目的地不在限制範圍內，或已取得主管機關核准。
- 國際傳輸前應告知當事人傳輸目的地（國家或區域）及傳輸目的，並取得同意或確認其他合法基礎。
- 國際傳輸紀錄應包含：傳輸目的地、傳輸個資類型、傳輸目的、傳輸個資類別、接收方資訊及合法基礎。

實務提示：若有大量或定期性的國際傳輸需求，建議考慮申請 APEC 及 Global CBPR 驗證，以降低合規風險並增強國際信任。

8.4.7 特種個人資料之蒐集、處理及利用限制

條文意旨

組織針對病歷、醫療、基因、性生活、健康檢查、犯罪前科等特種個人資料，應符合：原則禁止蒐集處理利用、例外情形之符合法律特定情形、適當資料安全管理措施，並保存相關紀錄。

實務指引

- 明定組織人員「原則禁止」蒐集、處理及利用特種個資的規定，並說明例外情形（如：醫療機構依法處理病歷、雇主依法取得員工健檢紀錄）。
- 確認例外處理特種個資之合法基礎（個資法第 6 條規定之特定情形）。
- 特種個資應採取更高等級的安全管理措施，如：儲存媒介規範、報廢或轉作他用之規定、安全備份、安全加密、安全傳輸、安全銷毀等機制。
- 特種個資的處理應有明確的合法目的及業務必要性說明。

實務提示：在系統設計上對特種個資欄位進行標記，並提醒人員該資料的敏感性及確認是否具備蒐用之合理性及必要性。

8.4.8 告知義務之履行

條文意旨

組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知確認程序，符合法律規定之告知時點、適當告知方式、免告知理由確認方式，並保存相關紀錄。

實務指引

- 依據個資法第 8、9 條規定，確認各業務情境之告知義務內容（蒐集機關/非公務機關名稱、蒐集目的、個資類別、利用期間/地區/對象及方式、當事人可行使之權利、提供資料是否影響當事人權益）。
- 直接向當事人蒐集：應在蒐集時完成告知，告知方式可為：面對面告知、書面告知（附告知聲明之同意書）、電子告知（網頁上方顯著位置之隱私聲明）。
- 間接蒐集（非直接向當事人取得）：應在蒐集後、初次處理前或初次提供利用時完成告知。
- 免告知情形應以書面確認（如業務屬性屬於法定例外情形），並留存確認依據。

實務提示：設計組織隱私聲明範本，並置於官網明顯位置，並依不同蒐集管道（網站、紙本申請書、電話）客製化調整呈現方式，確保告知內容清晰且易於理解。

8.5 當事人之相關權利

8.5.1 個人資料之相關權利

條文意旨

組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程，並保存相關紀錄。

實務指引

- 建立涵蓋所有法定當事人權利之「當事人權利行使程序」，包含：請求管道、身分驗證方式、審核程序、回覆方式、費用規定（如製給複製本之費用）。
- 提供便民的請求管道：如線上申請表單、電子郵件、實體書面申請，確保當事人可輕易行使權利。
- 建立「當事人請求追蹤表」，記錄每件請求之接收日期、請求類型、處理進度及完成日期。

實務提示：建立制度化及文件化之「當事人請求標準作業程序 (SOP)」，並留存相關紀錄至少五年。

8.5.2 當事人行使權利之程序事項

條文意旨

組織處理當事人請求之程序應包含：請求方式、身分確認方式、確認是否得依法拒絕方式、拒絕申訴管道、法令規定期間內准駁、書面通知（拒絕附理由）、延長期間書面通知，並保存相關紀錄。

實務指引

- 身分核驗：應建立合理的身分驗證機制（如出示身分證、填寫帳號資訊），確認請求者確為當事人本人（或其法定代理人），並留存核驗紀錄。
- 依個資法規定，組織應在受理後一個月內給予准駁，如需延長不得超過三個月，延長時應以書面通知理由。
- 若拒絕當事人請求，應以書面通知且附理由（如：依法可拒絕之情形、技術不可行等）。
- 建立申訴管道（如：客服電話、電子信箱、書面申訴），並告知當事人可向主管機關申訴之管道。

實務提示：「當事人請求標準作業程序 (SOP)」應包含各步驟的處理程序、文件格式及確認當事人身分之標準作業程序，確保不同人員處理時的一致性。

8.5.3 申訴及諮詢之處理

條文意旨

針對申訴與諮詢事項，組織應確保適當且迅速回應當事人，必要時通報個人資料管理代表並由其決定回應內容與方式，並保存相關紀錄。

實務指引

- 建立「申訴及諮詢處理程序」，明定接收窗口（如客服部門）、初步回應時限、轉介標準（何種情況需升級至管理代表）。
- 申訴案件（涉及權利侵害、不滿意處理結果）應由管理代表參與，確認回覆立場與方式，避免個別人員自行處置造成前後不一致。
- 建立申訴及諮詢紀錄表，記錄接收時間、來源、內容摘要、處理過程及最終回覆結果。
- 定期分析申訴案件統計，識別是否有反覆出現的問題，作為制度改善的參考依據。

實務提示：在隱私聲明及各接觸點明確告知當事人申訴及諮詢的聯繫方式，並確保聯繫方式持續有效（避免信箱不回應或電話無人接聽）。

8.6 維持個人資料之正確性

條文意旨

組織應建立確保個人資料於處理過程中正確性不受影響、確認錯誤時適時更正、定期檢查正確性，以及因組織可歸責事由未更正後應通知曾提供利用對象之程序。

實務指引

- 在資料輸入端設置品質控管機制（如格式驗證、欄位必填設定、輸入錯誤警示），降低資料輸入錯誤率。
- 建立「個資更正程序」：當事人請求更正時，確認更正必要性並完成更正，同時通知曾接收該個資之第三方。
- 定期進行資料品質稽核（如每年對員工個資、客戶個資進行一致性檢查），識別並更正過期或錯誤的個資。
- 在個資更正紀錄中留存：更正前後的資料內容、更正原因、更正日期、更正執行人員，以及通知相關利用對象的紀錄。

實務提示：對長期未更新的個資（如超過一定年份的客戶資料），可主動發起確認作業（如寄送確認函），請當事人確認資料正確性。

8.7 安全管理措施

條文意旨

組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料被竊取、竄改、毀損、滅失或洩漏之必要且適當之安全管理措施，至少包含管理面及技術面安全管理措施（如附表 A 所示）。

實務指引

- 管理面安全管理措施：包含組織架構建立、個資保護政策制定、風險評鑑執行、教育訓練、人員監督、委外管理、事故應變等制度性措施。

- 技術面安全管理措施：包含存取控制、加密傳輸、防火牆、入侵偵測、日誌管理、防毒軟體、資料備份等技術控制工具。
- 安全管理措施應依風險評鑑結果確定優先實施項目，並定期驗證措施之有效性（測試、稽核）。
- 建立「安全管理措施清冊」，逐項記錄已實施之管理面與技術面措施，並對應至附表 A 各控制選項。

實務提示：安全管理措施應與組織整體資訊安全管理系統整合，避免重複投入或產生管理缺口。

8.8 組織人員之監督

條文意旨

組織應對組織人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。

實務指引

- 在工作規則或員工手冊中明定個人資料保護相關行為準則及違規懲處規定，並確認所有員工已知悉（如簽名確認）。
- 技術面監督：透過系統存取日誌、DLP（資料外洩防護）工具監控異常的個資存取或傳輸行為。
- 管理面監督：主管定期（如每月）抽查下屬之個資處理作業，確認符合程序規定。
- 對於接觸高敏感個資的人員（如財務、人資部門），應設置更嚴謹之內控與監督機制。

實務提示：監督措施應在聘僱協議中告知員工，避免事後產生爭議；同時確保監督範圍符合勞動法令規定，不過度侵犯員工隱私。

8.9 委託蒐集、處理或利用個人資料之監督

條文意旨

組織委託他人蒐集、處理或利用個人資料時，應建立選任受託人之標準及監督方式，並確認委託人/受託人權利義務、委託業務範圍、安全管理措施、複委託、保留指示、事故責任、終止時個資返還等規定，並定期確認與審查受託人執行狀況。

實務指引

- 建立「委外廠商選任評估程序」，評估項目包含：廠商個資保護之能力（如通過 TPIPAS 驗證）、安全管理措施現況、過往事故紀錄等。
- 委外合約中須明確約定：（1）處理個資之目的、類型、範圍；（2）安全管理措施要求；（3）禁止目的外利用；（4）事故即時通報義務；（5）複委託之約定；（6）終止時個資之返還及刪除；（7）委託方之查核權。

- 建立委外查核流程，明定對受託人之定期查核頻率（如每年實地查核或審閱自評報告）、查核項目及方式。
- 宜定期（如每年）要求受託人提交個資安全管理狀況報告，並留存查核結果及改善追蹤紀錄。

實務提示：對高風險委外廠商（如大量個資處理、跨境傳輸、特種個資處理）應加強監督頻率。

8.10 事故之緊急應變

條文意旨

組織應訂定並落實事故緊急應變措施，至少包含：通知當事人、採取即時應變措施並保存紀錄、避免類似事件再發、通報主管機關及授證機關；並將通知/通報之內容、方式、時限與應變措施及紀錄保存以供備查。

實務指引

- 制訂「個人資料事故應變計畫（Incident Response Plan）」，包含：事故分類分級標準、各級別之應變程序與時限、通報責任鏈（誰負責通報、向誰通報、何時通報）、通報模板（對當事人及主管機關）。
- 事故發生時應確認：（1）止損措施（防止擴大）→（2）評估影響（確認受影響資料及當事人）→（3）通報主管機關與通知當事人→（4）調查根因並預防再發。
- 對主管機關的通報應依法令規定時限完成（目前個資法無明文規定通報時限，但應參考目的事業主管機關之要求），並留存通報證明。
- 對授證機關（TPIPAS 維運機構）之通報：事故發生後應依授證機關規定期限（詳閱驗證規則）完成通報，並說明應變措施。
- 事故調查結束後，應出具「事故調查報告」，包含根本原因分析（Root Cause Analysis）、已採取之應變措施及未來預防措施。

實務提示：事前準備工作至關重要，宜建立「事故應變聯絡清冊」（含所有通報對象之聯繫方式）、準備通知模板（對當事人及主管機關），並每年進行至少一次事故應變演練，確保相關人員熟悉流程。

第九章 績效評估

9.1 有效性量測

條文意旨

組織應針對個人資料管理制度之實施，建立分析量測機制，藉由各項方式使管理代表能判定制度內所建立之程序與機制是否有效，並將分析量測作成紀錄，以確保制度之持續有效運作與改善。

實務指引

- 建立「個資管理制度績效指標 (KPI) 」，例如：教育訓練通過率 (目標：XX%) 、當事人請求於法定期間內處理率 (目標：XX%) 、事故平均響應時間、風險評鑑更新週期遵循率、稽核缺失改善完成率。
- 個資管理制度績效指標應具代表性，例如：教育訓練通過率不得低於 90% ，避免該教育訓練失去有效性。
- 定期 (如季度) 蒐集績效資料，做成量測報告，呈現制度執行趨勢及與目標之差距。
- 量測方法應多元化：包含數量統計 (如訓練人數) 、時效追蹤 (如請求處理時間) 及品質評估 (如稽核缺失嚴重程度) 。
- 量測結果應作為管理審查的重要輸入，並作為決定是否需要調整管理措施的依據。

實務提示：採用資料視覺化 (Dashboard) 工具將績效指標視覺化，讓管理代表及最高管理階層能快速掌握制度執行狀況，提升決策效率。若為上市櫃公司，可與 ESG 指標做結合 (ESG 評鑑指標-編號第 4.32) 。

9.2 內部評量

條文意旨

組織每年應依其特性規劃執行內部評量，以瞭解個人資料管理制度是否符合法規、本制度及政策手冊等要求；應規劃評量方式及流程；應製作書面之內部評量報告；內部評量計畫應由具備個人資料內評師或驗證師資格者規劃，並確保評量有效性及出具報告。

實務指引

- 每年至少執行一次全面性內部評量，涵蓋所有 PIMS 要求項目；高風險領域可增加評量頻率。
- 內部評量應採系統化方法：制定評量計畫 (範圍、時程、評量人員) → 準備評量核對清單 → 執行評量 (文件審閱、訪談、觀察、測試) → 記錄缺失 → 出具評量報告 → 追蹤改善。

- 評量人員需具備 TPIPAS 個人資料內評師或個人資料驗證師資格，且不得評量其本身負責管理的業務（避免利益衝突）。
- 書面評量報告應包含：評量範圍、評量方法、各條文符合性判定（符合/觀察事項/不符合事項）、缺失描述及改善建議。
- 評量缺失應依嚴重程度設定改善期限，並由管理代表追蹤改善完成狀況。

實務提示：內部評量前應召開「起始會議」，讓受評單位了解評量目的、範圍及準備事項，提高內評執行之效率。

9.3 定期檢視

條文意旨

個人資料管理代表應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄結果，並報告最高管理階層。檢視內容包含：制度執行狀況分析、矯正預防措施成效、有效性量測結果及法令修改狀況。最高管理階層決策調整制度時，應考量檢視報告、環境變遷、業務變化、改善建議及其他影響變更。

實務指引

- 年度管理審查會議：由管理代表主持，邀請最高管理階層出席（或確保其收到書面報告並有批示），各部門個資聯絡人與會。
- 會議中得討論事項：內部評量報告、事故統計報告、當事人請求統計、有效性量測結果、缺失追蹤事項、法令動態摘要。
- 會議應明確記錄：哪些制度需要調整、資源是否需要追加、改善目標調整方向，及各決議事項的負責人與完成期限。
- 管理審查會議紀錄應正式化，包含：與會人員名單（含簽名）、會議日期、議程、討論內容摘要、決議事項及追蹤清單。

實務提示：管理審查不僅應檢討過去，更要針對未來一年的環境變化（法令趨勢、業務發展）做出制度規劃調整。

第十章 改善

10.1 總則

條文意旨

組織針對內部評量及本管理制度實施之結果，應規劃矯正措施及預防措施，並確保相關措施之執行。

實務指引

- 建立「矯正與預防措施管理程序」，明定不符合事項的識別管道（評量、稽核、事故、客訴）、處理程序及追蹤機制。
- 區分矯正措施（已發生的不符合事項）與預防措施（潛在風險），採取不同的分析與處理策略。
- 確保矯正及預防措施的執行均有書面紀錄，包括提出者、核准者、執行者、完成日期及驗證結果。

實務提示：持續改善 (Continual Improvement) 應成為組織文化，鼓勵全體員工主動發現問題並提出改善建議，而非僅在稽核時才發現缺失。

10.2 矯正措施

條文意旨

組織針對不符合事項，應確認不符合事項內容及發生原因、評估需求並提出矯正方案、訂定合理執行期限、記錄執行結果，並檢視矯正方案成果。

實務指引

- 不符合事項的根本原因分析 (Root Cause Analysis) 應深入，避免過於空泛（如「員工疏失」），應探討系統性原因（如「缺乏適當的訓練」或「程序設計不合理」）。
- 矯正方案應針對根本原因而非症狀，例如：若根本原因是缺乏訓練，矯正方案應是「設計並執行相關訓練課程」，而非「告誡違規員工」。
- 設定合理期限：緊急性缺失（如重大安全漏洞）應在短期內完成（如一週），一般性缺失可設定一到三個月的改善期限。
- 矯正完成後應由管理代表或指定人員驗證矯正效果（如重新稽核相關控制點），確認缺失已實際改善且不再發生。

實務提示：建立「不符合事項追蹤表」，定期（如每月）確認各矯正事項的完成進度，避免改善措施被遺忘或延遲執行。

10.3 預防措施

條文意旨

組織針對潛在不符合事項之風險，應確認潛在不符合事項內容及原因、評估需求並提出預防方案、訂定合理執行期限、記錄執行結果、檢視預防方案成果，並持續改善個人資料管理制度。

實務指引

- 潛在不符合事項的識別管道：風險評鑑（高風險項目）、法令修訂（新增義務）、行業同業事故案例、內部流程審查（發現弱點但尚未發生問題）。
- 預防措施應具體可執行，例如：「針對識別出的社交工程攻擊風險，定期進行社交工程演練，並對點擊釣魚郵件人員提供額外訓練」。
- 預防措施執行結果應定期評估，確認預防措施確實降低了潛在風險發生的可能性。
- 持續改善：應將制度改善視為動態過程，定期回顧整個 PDCA 循環，確保管理制度跟上業務發展和外部環境的變化。

實務提示：建立法規動態及案例分享機制，促進知識傳播和學習型組織文化的形成。

第十一章 個人資料管理制度實施指引

本章為實施指引，各條文使用「宜」而非「應」，代表為建議性而非強制性要求，組織應依其規模、特性與需求判斷是否採納。

11.1 總則

條文意旨

組織宜考量其規模、特性與需求，針對本管理制度實施指引建立並落實相關程序。

實務指引

- 中小型組織可依本章指引，選擇與其業務相關且具實際效益的項目優先實施，並非強制全面落實。
- 大型組織或高個資風險行業（如醫療、金融）宜參照本章指引，納入進階個資保護措施。

實務提示：將本章實施指引的採納情形記錄於適用性聲明書 (SoA) 中，清楚說明採納理由及排除原因，有助於驗證時展現制度的完整性考量。

11.2 從設計與預設階段著手隱私保護

條文意旨

組織宜於產品、服務或系統等開發設計階段時，落實本制度規範、個人資料保護法與相關法令之精神。

實務指引

- Privacy by Design（從設計著手隱私保護）七大原則：（1）主動而非被動預防；（2）隱私保護為預設狀態；（3）隱私保護嵌入設計；（4）全功能性（正和而非零和）；（5）端到端安全；（6）可見度與透明度；（7）尊重使用者隱私。
- Privacy by Default（預設隱私保護）實作：新系統功能預設應採最高隱私保護設定（如：資料分享預設關閉、Cookie 預設最小化）。
- 在系統需求文件中明列隱私保護需求（如資料最小化、匿名化、加密要求），並在系統測試計畫中納入隱私保護功能測試案例。

實務提示：將個資保護需求列為產品開發規格的標準項目，與功能需求、效能需求並列，確保開發人員從一開始就納入隱私考量。

11.3 生物特徵個人資料

條文意旨

組織於蒐集、處理或利用指紋、掌紋或臉部辨識等生物特徵個人資料，宜遵循個人資料保護法關於特種個人資料等相關法令。

實務指引

- 生物特徵個資（指紋、掌紋、臉部辨識、虹膜、聲紋等）屬敏感性個人資料，應適用特種個資的管理要求（即使目前個資法未明列為特種個資）。
- 蒐集生物特徵個資前，應詳細評估蒐集之必要性及相應安全措施。
- 採取最嚴格的安全管理措施：加密儲存、嚴格存取控制、禁止將原始生物特徵資料傳送至第三方（可使用模板/特徵向量而非原始影像）。
- 提供替代方案：若某業務功能使用生物辨識，應同時提供不使用生物辨識的替代方案（如傳統密碼或實體憑證），以保障當事人自主選擇權。

實務提示：密切關注主管機關對生物特徵個資之最新規定，若未來被明確列為特種個資，應立即調整相關處理程序。

11.4 風險處置

條文意旨

組織針對個人資料隱私衝擊風險評鑑結果為高風險之行為或流程，且風險無法透過風險管控措施緩解時，宜事先與相關主管機關溝通或諮詢。

實務指引

- 識別「剩餘高風險」場景，例如：在實施所有可行管控措施後，風險仍高於可接受水準的業務活動（如：極大量特種個資的處理、高敏感性個資的跨境傳輸）。
- 與主管機關溝通前，應充分準備相關資料，包含業務描述、個資類型及規模、已採取的管控措施、剩餘風險評估、擬採取的額外措施。
- 溝通紀錄（包含向主管機關諮詢的往來函文或會議紀錄）應妥善保存，作為努力合規的證明。

實務提示：即使主管機關未明確要求，主動諮詢有助於展現組織的合規誠意。

11.5 當事人同意

條文意旨

組織於取得當事人同意時，宜注意同意給予之真摯性、自主性、任意性、具體特定且受充分告知；撤回同意之方式宜與給予同意之方式等同便利。

實務指引

- 有效同意的五個要素：（1）真摯（無欺騙或誤導）；（2）自主（無脅迫或強制）；（3）任意（拒絕不會帶來不合理不利後果）；（4）具體特定（針對特定目的的明確同意，非概括性同意）；（5）充分告知（在同意前已清楚說明用途）。
- 同意設計原則：不得採用預設勾選（Pre-checked boxes）、捆綁同意（將服務使用與行銷同意捆綁）或暗黑模式（Dark Patterns 如刻意隱藏退出選項）。
- 撤回同意的便利性：若同意是透過網頁表單取得，撤回應可透過同樣便利的線上方式完成，而非要求以書面郵寄方式申請。
- 留存同意紀錄：包含取得時間、取得方式、同意內容版本，以便事後驗證同意的有效性。

實務提示：定期審視同意機制的設計，確保符合最新監管趨勢（如參考歐盟 GDPR 的同意要求），並適時調整以提升當事人信任度。

11.6 當事人權利

條文意旨

組織宜建立並落實相關程序，以回應當事人行使修改或撤回同意權、反對權、限制處理權、資料近用權、資料可攜權、資料更正權、資料刪除權。

實務指引

- 修改或撤回同意權：提供便捷的方式讓當事人隨時修改或撤回其同意，並在撤回後停止依該同意進行的個資處理活動。
- 反對權：建立機制讓當事人表示反對其個資用於特定目的（尤其是直接行銷或剖繪），並在接受反對請求後立即停止。
- 限制處理權：於當事人請求限制處理期間（如正在確認資料正確性時），暫停對該個資的主動處理。
- 資料近用權：允許當事人查詢和閱覽其個人資料，提供其所有相關個資的概況，包含處理目的、類型、接收者等資訊。
- 資料可攜權：以結構化、常用的機器可讀格式（如 CSV、JSON）提供當事人其所提供的個資，以便轉移至其他服務提供者。
- 資料更正權：建立快速且有效的更正流程，確認更正後同步通知曾接收該個資的第三方。
- 資料刪除權：建立評估刪除請求的程序（確認是否有法定保留義務），對符合條件的請求完成刪除並通知相關第三方。

實務提示：考慮建立「隱私儀表板（Privacy Dashboard）」，讓已登入的用戶可自助查閱、修改或下載其個人資料，以及管理其同意狀態，大幅降低人工處理的負擔。

11.7 未成年人之保護

條文意旨

組織於蒐集、處理或利用未成年人個人資料時，宜有較高之注意義務與安全管理措施，並應確認已採取措施足辨識未成年之法定代理人已有效代為同意，或符合其他法律規定之特定情形。

實務指引

- 在服務設計中識別是否有未成年人（未滿 18 歲）使用的可能性，並建立年齡核驗機制（如生日輸入、身分證件驗證、法定代理人授權書）。
- 若服務對象包含未成年人，應有法定代理人同意機制，確認代理人同意的真實性（避免由未成年人自行代填）。
- 未成年人個資應採取更高標準的安全管理措施，且禁止用於任何可能對未成年人不利的目的（如行為剖繪、精準廣告）。
- 隱私聲明及告知文件應提供適合未成年人閱讀的版本（簡化語言、圖示輔助），確保其能理解告知內容。

實務提示：對於面向兒童的服務，應參考相關的兒童網路隱私保護規範，並在產品設計階段即考量對未成年人的特殊保護需求。

11.8 無障礙

條文意旨

組織於運行個人資料管理制度時，宜考量身心障礙者權益，並以適當方式協助之。

實務指引

- 確保個資相關告知文件（隱私聲明、同意書）具有無障礙版本，如：大字體版本、語音朗讀友善格式、手語解說影片（針對聽障者）、點字版本。
- 當事人行使權利的管道應考量身心障礙者的需求，提供電話（客服專線）、輔助科技相容的線上表單等多元途徑。
- 在客服培訓中納入協助身心障礙者之訓練，確保客服人員能有效協助其完成個資相關請求。

實務提示：遵循無障礙網頁設計標準（如 WCAG 2.1）改善網站及線上服務的可及性，有助於同時滿足無障礙需求和個資保護告知要求。

11.9 Cookie

條文意旨

組織於蒐集、處理或利用 Cookie 等類似科技，宜僅於必要範圍內為之，並取得當事人之同意與提供當事人拒絕之選項。

實務指引

- 對網站所使用的 Cookie 進行分類：（1）必要性 Cookie（維持網站基本功能，通常無需同意）；（2）功能性 Cookie（記憶使用者偏好）；（3）分析性 Cookie（統計使用行為）；（4）行銷性 Cookie（跨網站追蹤及精準廣告）。
- 建立 Cookie 同意橫幅（Cookie Consent Banner）：清楚說明各類 Cookie 的用途，並提供「接受全部」、「拒絕非必要」及「自訂設定」選項。
- 避免使用「Cookie Wall」（強制接受所有 Cookie 才能使用網站）或其他阻礙拒絕的設計模式。
- 定期（至少每年）審視網站 Cookie 清單，確認是否有新增的第三方 Cookie，並更新隱私聲明和同意設定。

實務提示：使用「同意管理平台（Consent Management Platform, CMP）」可自動化 Cookie 同意的蒐集、記錄及管理，降低合規負擔並確保同意紀錄的完整性。

11.10 暫存檔之處理

條文意旨

組織於蒐集、處理或利用個人資料所產生之暫存檔，宜確保於適當時間內刪除或銷毀。

實務指引

- 識別業務流程及系統中可能產生個資暫存檔的環節（如：報表匯出後的暫存、系統快取、應用程式 Temp 資料夾、Log 檔案中的個資）。
- 建立暫存檔刪除政策，明定各類暫存檔的最長保存期限（如：報表暫存檔在下載後 24 小時內自動刪除）。
- 在系統設計中實作自動化暫存檔清理機制（如 Schedule Job 定期清理）。
- 對於含有敏感個資的暫存檔，應採用安全刪除方式（如覆寫），而非僅執行一般刪除（可能可被恢復）。

實務提示：在年度個資盤點中，將暫存檔的識別及清除狀況納入稽核項目，確保暫存檔管理措施持續有效執行。

11.11 自動化決策與剖繪

條文意旨

組織於使用自動化決策、剖繪等類似科技且影響當事人權益時，宜賦予當事人請求人為介入之機會。

實務指引

- 識別組織中使用自動化決策或剖繪（Profiling）的業務情境（如：自動信用評分、自動推薦系統、AI 篩選履歷），評估對當事人的影響程度。

- 若自動化決策對當事人產生重大影響（如：貸款拒絕、面試篩選淘汰），應提供：（1）說明決策邏輯的機制；（2）申請人工複審的管道；（3）提出異議的程序。
- 在使用剖繪功能前，應以清晰易懂的語言告知當事人剖繪的目的、方式及其對當事人的潛在影響。

實務提示：在個資蒐集告知中，明確說明是否有自動化決策及剖繪行為，並在隱私政策中提供相關說明，以符合透明性原則。

11.12 國際傳輸

條文意旨

組織如有個人資料國際傳輸之流程，宜取得 APEC CBPR 或 Global CBPR 驗證，或取得歐盟 GDPR 所定認證或驗證。

實務指引

- APEC 跨境隱私規則（CBPR）：適用於 APEC 成員經濟體之間的個資跨境傳輸，驗證範圍涵蓋個資保護管理制度的整體符合性。若組織與 APEC 成員之業務夥伴有頻繁個資傳輸，建議申請 CBPR 驗證。
- Global CBPR：APEC CBPR 之全球延伸版本，適用於更廣泛的國際個資傳輸場景。
- GDPR 認證/驗證：若組織有向歐盟居民提供服務或蒐集歐盟居民個資，應關注 GDPR 適用性，並評估是否需取得 GDPR 相容的認證機制（如適足性認定）。
- 無論是否申請上述驗證，組織仍應在個別合約層面（如標準合約條款）確保國際傳輸的合法基礎。

實務提示：申請國際認證前，應先確保組織的 PIMS 已完整建置並有效運作，以 TPIPAS 驗證為基礎，進一步對接國際認證框架，可大幅降低重複建置的成本。

11.13 委託蒐集、處理或利用個人資料之監督

條文意旨

組織於委託他人蒐集、處理或利用個人資料之全部或一部時，宜確保受託人落實附表 A 所列安全管理措施。

實務指引

- 在委外合約中明確要求受託人落實附表 A 所列安全管理措施（存取控制、日誌管理、識別鑑別、媒體安全、實體安全、資訊傳輸、系統完整性、系統發展生命週期安全、網路安全、新興技術風險管理、資料可用性、人員管理）。
- 將附表 A 控制要求納入「受託人安全評估問卷」，在選任前及定期評估時要求受託人填答，並提供相應佐證文件。

- 要求高風險受託人（大量個資處理、特種個資）提供第三方驗證證明（如 TPIPAS 驗證報告、ISO 27001 驗證證書、SOC 2 報告）。
- 若委外合約明確要求受託人落實附表 A，應在合約中保留委託方的「現場查核權」，以備必要時進行現場稽查。

實務提示：建立「受託人個資安全評分卡」，定期（如每年）評估受託人在各附表 A 控制項目的落實程度，作為是否續約或調整合作條件的依據。

11.14 應對政府存取資料

條文意旨

組織宜建立應對程序，回應要求揭露組織所持有個人資料之國內、外司法或其他政府傳票、搜索令或其他命令，其內容應包含：確認要求與回應方式符合法律規定之特定情形，並保存相關紀錄。

實務指引

- 建立「政府存取資料應對程序」，明定收到傳票或搜索令時的標準作業流程：（1）即時通知法務部門及管理代表；（2）確認文件之合法性（主管機關、授權範圍、有效期限）；（3）評估是否符合法律規定的揭露條件；（4）確認回應方式（提供哪些資料、以何種格式）；（5）在合法範圍內儘早通知當事人（若法律允許）。
- 確認回應合法性：核實要求揭露的個資範圍是否在傳票/命令授權範圍內，避免過度揭露。若要求不合法或超出範圍，應由法務人員主導拒絕或質疑。
- 保存完整紀錄：留存所有接收的傳票/命令原件或影本、法律分析意見、回應過程、提供之個資清單及提供時間。
- 跨境政府要求：若接到外國政府的個資揭露要求，除確認其法律基礎外，還應評估是否符合我國個資法的規定，必要時諮詢法律意見。

實務提示：預先與法律顧問（內部法務或外部律師）建立快速諮詢機制，確保在收到政府存取要求時能即時獲得專業法律建議，在法定回應期限內做出正確決策。

TPIPAS：2021⁺

附表 A 安全管理措施

合規證據實務指引

本文件針對附表 A 控制選項，逐項說明企業實務上應提供之證據，
以確認組織符合 TPIPAS：2021⁺ 安全管理措施之要求。

財團法人資訊工業策進會 科技法律研究所

附表 A 合規證據指引說明

附表 A 係針對 TPIPAS：2021+ 管理措施制定之基本安全管理具體措施，分為「A8.7 資通安全」及「A8.8 組織人員之管理與監督」兩大類，共 14 個控制選項。

本文件就每一個控制選項說明：（1）管理目標與管理措施摘要；（2）組織應提供之具體合規證據；以確認組織在評量時能充分展現其合規狀態。

【證據充分性原則】：組織應具備「相關程序規定」並留有「證據、紀錄或軌跡」以供查核。

A8.7 資通安全

A8.7.1 存取控制

管理目標：

組織對個人資料之存取加以規範與保護，防止任何未經授權之存取與破壞。

管理措施摘要：

存取控制政策與機制、帳號管理（申請/開通/停用/刪除/清查）、職責分工、最小權限原則、遠端存取管控、行動裝置存取管控、資訊分享機制。

證據類別	具體合規證據
存取控制政策文件	存取控制政策應涵蓋：存取控制原則、帳號管理規則、最小權限原則等，且應有版本號及核准人簽署。
帳號管理紀錄	- 帳號申請表單（表單資訊如申請人、申請理由、核准人、開通日期等）。 - 帳號清查報告（至少每年一次，特權帳號應有更高頻率）：列示系統中所有帳號狀態。 - 對於已停用帳號、閒置帳號之處置，應保存相關紀錄。 - 人員離職、職務異動時帳號處置的作業紀錄。 - 系統自動登出閒置期限的設定截圖或設定文件。
存取控制清單	- 各系統之存取控制清單（Access Control List, ACL）或存取矩陣（Access Matrix），呈現各使用者對資料資源的存取權限。 - 特權帳號清單及特權帳號使用日誌（管理者操作紀錄）。 - 訂定職責分工規範文件，例如：個資輸入與稽核不得兼任。
遠端/行動存取	- 遠端存取政策，若允許遠端存取，應提供 VPN 設定文件、加密機制說明、遠端連線日誌及自動監控告警紀錄。 - 行動裝置管理（MDM）系統設定截圖，或行動裝置存取政策及相關管控措施文件（如：裝置安全設定要求、應用程式管理、裝置遺失時遠端清除等功能）。
稽核測試紀錄	- 存取控制有效性測試紀錄（如：嘗試以未授權帳號存取個資系統之測試結果）。 - 定期存取權限覆核（Access Review）紀錄，確認現有權限設定仍符合業務需要及最小權限原則。

A8.7.2 事件日誌與可歸責性

管理目標：

組織依據個人資料風險評鑑與業務所需，決定資訊系統需要被稽核與記錄之事件，並建立監控機制。

管理措施摘要：

記錄事件（未授權存取/修改）、定期檢視分析通報日誌紀錄、日誌紀錄之保存與維護（留存週期、防竄改、限制存取）。

證據類別	具體合規證據
政策與程序文件	- 日誌管理政策，涵蓋如：應記錄之事件、日誌留存時間、日誌保護措施及定期審閱程序。 - 事件記錄項目清單（Event Logging Specification），列明各系統應記錄之事件類型（登入、登出、失敗登入、資料存取、修改、刪除、權限變更等）。
系統日誌樣本	- 各關鍵系統（CRM、資料庫、ERP、個資相關應用系統）的日誌截圖或樣本，確認已記錄所需事件類型。 - 系統管理者（Administrator）帳號的操作日誌，應呈現所有管理操作紀錄（含時間戳記、帳號、操作內容）。 - 失敗登入嘗試及異常存取行為的日誌紀錄。
日誌檢查紀錄	- 定期檢查日誌紀錄（如每月）：說明檢查範圍、發現之異常事件。 - 異常行為調查報告：針對日誌中發現的可疑活動，記錄調查過程及後續處置。
日誌保護措施	- 日誌儲存系統設定文件，說明日誌如何與業務系統隔離儲存，以及存取權限管控設定。 - 日誌完整性保護機制說明（如：日誌簽章、日誌伺服器僅允許追加寫入）。 - 日誌保存期限設定截圖或設定文件（確認日誌保存時間符合政策規定）。

A8.7.3 識別鑑別

管理目標：

組織對於組織內部之系統使用者，應有特定之方式確認其所擁有之存取帳號與權限，以確保行為之明確可歸責性。

管理措施摘要：

使用者唯一識別與驗證（避免共用帳號）、身分驗證管理（預設密碼變更、安全傳輸、密碼規則與更新週期）。

證據類別	具體合規證據
政策文件	- 身分識別與驗證政策，涵蓋：唯一帳號要求、禁止共用帳號規定、密碼長度要求（宜參照 NIST 要求）、密碼更新週期、預設密碼強制更改規定。 - 特殊帳號（共用/服務帳號）管理規範（若有使用，應說明例外處理方式及額外控制措施）。
技術設定佐證	- 系統密碼政策設定截圖（Active Directory 或各系統密碼設定），確認密碼複雜度及有效期設定符合政策。 - 強制初次登入變更密碼功能的設定截圖或測試紀錄（確認新帳號或重設密碼後必須立即變更）。 - 多因素驗證（MFA）設定文件（若有實施，特別是特權帳號或遠端存取場景）。
帳號唯一性驗證	系統帳號清冊，確認每位使用者均有其唯一帳號，無共用帳號情形；若有服務帳號，說明其用途及管理措施，確認無閒置帳號。

A8.7.4 媒體安全

管理目標：

組織應確保儲存個人資料之媒體，其存取、保存、傳輸與汰除時之安全。

管理措施摘要：

媒體存取（特定授權人員、限制數位與非數位媒體存取）、媒體儲存（安全作業規定）、媒體傳輸（管控區域外之安全防護）、媒體汰除（安全汰除程序）。

證據類別	具體合規證據
政策程序文件	- 媒體安全管理辦法，涵蓋：媒體定義（USB、硬碟、光碟、紙本文件、磁帶等）、存取授權程序、儲存要求、傳輸要求及汰除程序。 - 媒體汰除程序（Secure Disposal Procedure），說明各類型媒體的安全汰除方法（如：覆寫、消磁、實體銷毀）及相關標準。
媒體存取管控	- 媒體（含可攜式儲存裝置）存取授權清單或登記紀錄。 - USB/外部儲存裝置管控設定文件（如：終端防護政策設定，禁止或限制未授權 USB 使用）。 - 紙本文件存取管控措施說明（如：文件室門禁紀錄、文件借閱登記簿）。
媒體儲存紀錄	- 媒體清冊，記錄組織持有之儲存媒體清單（含媒體類型、序號、儲存內容概述、存放位置）。 - 儲存環境安全措施說明或照片（如：文件庫房門禁、儲存設備上鎖）。
媒體傳輸紀錄	- 媒體運輸紀錄（含對象、內容、方式、日期、簽署）。 - 傳輸加密措施說明或設定（如：加密容器、安全快遞服務）。
媒體汰除紀錄	- 媒體銷毀/汰除紀錄文件（如汰除日期、媒體識別、汰除方法、執行人員及確認人員）。 - 若委外銷毀，應提供銷毀廠商出具之銷毀證明書。 - 紙本文件銷毀紀錄（含碎紙機使用紀錄或文件銷毀服務紀錄）。

A8.7.5 實體與環境安全

管理目標：

防止儲存個人資料場所受人為因素未授權入侵與存取而導致個人資料之洩漏或毀損。

管理措施摘要：

實體存取控制（識別安全周界、資訊機房及檔案庫房之安全措施及權限管控）、實體存取監視（定期檢視有效性、人員及個資進出監視機制、出入紀錄保存）。

證據類別	具體合規證據
安全區域規劃文件	▪ 機房/資料中心及敏感檔案儲存區域之安全周界定義文件，說明各安全區域的範圍及等級劃分。 ▪ 各安全區域之存取授權清單。 ▪ 訪客管理程序，說明外部人員進入敏感區域的申請、陪同及登記。
實體管控措施	▪ 機房/文件庫房門鎖及安全設備清單（如：電子門禁、保全系統、上鎖文件櫃）。 ▪ 門禁系統設定文件及門禁卡管理記錄（含卡片發放、掛失、回收）。 ▪ 機房環境控制設施說明（如：溫濕度監控、消防設施、不斷電系統）。
進出紀錄	▪ 機房或敏感資料存放區域之進出紀錄（含日期時間、人員、身分、進出事由、陪同人員），應留存合理期間。 ▪ 訪客登記簿或電子訪客管理系統紀錄。
監視系統	▪ CCTV 設置說明及監控畫面保存政策。 ▪ 定期有效性檢視紀錄（如：CCTV 畫面品質確認、鐘訊同步、門禁系統功能測試）。
實地查核佐證	▪ 機房/文件庫房安全措施列表（顯示門禁設施、安全設備等）。 ▪ 安全周界測試記錄（模擬未授權進入嘗試的測試結果）。

A8.7.6 資訊傳輸

管理目標：

防止個人資料傳輸時遭未授權揭露。

管理措施摘要：

邊界保護（系統外部邊界及內部關鍵邊界的監視與控制介面防護）、傳輸機密性（確保個資傳輸機密性之措施、加密協定設定截圖、加密證明文件或傳輸軌跡紀錄）。

證據類別	具體合規證據
政策與架構文件	- 資訊傳輸安全政策，規定個資傳輸應採用的加密標準（如 TLS 1.2 以上）及禁止明文傳輸個資。 - 網路架構圖，呈現系統外部邊界（防火牆、DMZ）及內部關鍵邊界（網段隔離）的設計。
邊界防護設定	- 防火牆設定文件或規則摘要（隱除敏感設定），確認已實施適當的邊界過濾。 - 入侵偵測/防護系統（IDS/IPS）部署架構及設定說明。 - Web 應用防火牆（WAF）設定文件（若有對外 Web 服務涉及個資）。
傳輸加密佐證	- SSL/TLS 憑證有效性截圖（如 SSL Labs 評等報告），確認對外 HTTPS 服務使用有效且合規的加密憑證。 - 加密協定設定截圖（如：伺服器 TLS 設定，確認已停用 SSL 3.0、TLS 1.0 等已知不安全協定）。 - VPN 或加密通道設定文件（用於遠端存取或系統間加密傳輸場景）。 - 電子郵件傳輸加密機制說明（如：S/MIME、TLS 傳輸加密設定），若以電子郵件傳輸個資應提供加密設定佐證。
傳輸軌跡紀錄	- 個資外部傳輸的紀錄（含傳送時間、接收方、傳送內容概述及加密方式），確認所有對外個資傳送均經授權且採加密。 - 系統間資料交換紀錄（API 呼叫日誌或資料傳輸日誌），確認傳輸均透過安全通道。

A8.7.7 系統與資訊完整性

管理目標：

確保個人資料資通系統安全控管措施之有效性。

管理措施摘要：

安全性檢測（脆弱性識別/報告/修正、更新前測試）、惡意程式防護（入出端點部署、自動更新病毒碼、即時防護、定期完整掃描、偵測後處置）、資通系統監看（監視內外向通訊、入侵跡象通報）、測試環境管理（區隔正式/測試環境、避免使用真實個資測試）。

證據類別	具體合規證據
脆弱性管理	▪ 弱點掃描報告（近一年，大型非公務機關至少每年一次）：覆蓋個資相關之關鍵系統，包含識別之弱點及其風險等級。 ▪ 弱點修補紀錄：對應弱點掃描結果，記錄各弱點的修補措施及完成日期（未修補項目應有風險接受或補償措施說明）。 ▪ 系統更新測試程序及測試紀錄：確認重要更新在部署前均經測試，評估對系統的影響。 ▪ 滲透測試報告（高風險系統、對外服務系統建議每年一次；組織進行重大系統變動 / 更新時亦建議執行）。
惡意程式防護	▪ 防毒/端點防護軟體部署清單：確認所有端點（伺服器、筆電）均已安裝且運作中。 ▪ 病毒碼更新設定截圖（確認自動更新至最新版本且即時防護已啟用）。 ▪ 防毒掃描日誌或報告。 ▪ 惡意程式偵測及處置紀錄（確認偵測到的惡意程式已依程序隔離、刪除或其他適當處置）。
系統監控	▪ 資通系統監控架構說明（監控範圍、監控工具、告警機制）。 ▪ 安全事件監控日誌樣本（確認系統內外向通訊已受監視）。 ▪ 入侵告警通報紀錄（若有觸發告警，記錄告警內容、通報對象及後續處置）。
測試環境管理	▪ 測試環境與正式環境隔離架構文件（說明兩者在網路、帳號、資料等方面的隔離機制）。 ▪ 測試資料管理政策：禁止使用真實個資作為測試資料，或若有例外，說明申請程序及安全使用規範。 ▪ 測試環境使用紀錄（若有例外使用真實個資測試，應有申請及使用紀錄，以及安全維護措施之適用）。

A8.7.8 系統發展生命週期階段之安全性

管理目標：

確保組織系統發展之安全需求（含機密性、完整性、可用性、遵循性）。

管理措施摘要：

（1）SSDLC 概念應用於需求評估、設計開發、測試及部署維運；（2）個資相關系統於各階段導入適當安全措施（帳號管理、存取控制、隱碼加密、日誌監控、入侵防護及備份等）；（3）委外開發維運應將安全需求納入合約；（4）對外服務系統上線前應辦理源碼檢測、弱點掃描及滲透測試，並完成弱點漏洞修補；（5）定期評估安全措施有效性。

證據類別	具體合規證據
SSDLC 程序文件	系統安全發展生命週期（SSDLC）管理辦法或程序文件，說明各階段（需求/設計/開發/測試/上線/維運）的安全要求及管控閘門（Gate）。
安全措施導入佐證	- 系統安全設計文件（說明帳號管理、存取控制、資料加密、日誌記錄等安全機制的設計方式）。 - 安全功能測試計畫及測試結果（確認安全功能符合設計要求）。 - 隱碼/加密實作說明（如密碼儲存採 hash+salt、個資欄位加密方式）。
委外開發合約	- 系統開發或維運委外合約樣本（確認已納入安全需求條款、源碼交付條款、弱點修補義務）。 - 委外廠商安全評估報告（上線前對委外廠商安全能力的評估紀錄、委外監督紀錄）。
上線前安全測試	- 源碼安全檢測報告（如 SAST/DAST 掃描報告）：確認源碼中無嚴重安全漏洞或已完成修補。 - 弱點掃描報告（上線前對系統環境的漏洞掃描）。 - 滲透測試報告（對外服務系統上線前的滲透測試，確認無可利用的高風險弱點）。 - 弱點及漏洞修補確認紀錄（記錄測試發現的問題及修補完成狀態）。 - 上線核准文件（確認安全測試通過且弱點已修補後方核准上線）。
持續維運安全評估	- 系統上線後的定期安全評估紀錄（如每年一次弱點掃描）。 - 安全措施有效性評估報告（確認各項安全控制仍有效運作）。

A8.7.9 網路安全防護

管理目標：

確保組織網路系統有效應對威脅與風險。

管理措施摘要：

制定有效網路安全防護政策，如定期維護網路設備軟硬體、韌體及元件，避免系統遭未授權存取、入侵，損害資料之機密性、完整性與可用性，並保存相關更新之紀錄。

證據類別	具體合規證據
政策與架構文件	- 網路安全防護政策，涵蓋：網路設備維護要求、更新/修補管理程序、未授權連線管控措施及事件處理程序。 - 網路拓樸圖（Network Topology Diagram），呈現網路架構、關鍵設備位置及安全控制點（防火牆、IPS、IDS、DMZ）。 - 網路區段（VLAN）規劃文件，說明如何隔離個資相關系統與其他網路環境。
設備維護紀錄	- 網路設備（防火牆、路由器、交換器）韌體/軟體更新紀錄（含更新前後版本、更新日期及執行人員）。 - 網路設備弱點掃描或安全評估報告。 - 網路設備組態管理紀錄（確認設備採用安全組態，如禁用不必要服務、更改預設帳密）。
存取管控設定	- 防火牆規則清單，確認有適當的進出站規則管控。 - 無線網路（Wi-Fi）安全設定文件（如採用 WPA3、企業級身分驗證、訪客網路隔離）。 - 遠端網路存取管控設定（如 VPN 設定、零信任網路存取設定）。
監控與告警	- 網路監控系統設定說明（監控範圍、告警規則、通報流程）。 - 網路異常告警通報紀錄（確認監控系統能有效偵測並通報異常網路行為）。 - 定期網路安全審查或滲透測試報告。 - 建置 EDR/MDR 端點偵測與託管回應機制，納入異常行為自動攔截、24/7 監控告警及威脅分析紀錄。

A8.7.10 新興技術風險管理

管理目標：

確保組織於採納及運用新興技術時，能適當識別、評估並管理其所衍生之相關風險。

管理措施摘要：

制定新興技術相關政策，就新興技術之採納與運用進行適當之風險評估及管理：（1）雲端服務：取得、環境設定及維運管理規範，確保雲端個資安全（存取控制、加密、備份），定期檢視更新；（2）人工智慧系統或服務：取得、環境設定及使用管理規範。

證據類別	具體合規證據
政策文件	▪ 新興技術採納管理政策或程序，說明新技術導入前應進行的風險評估程序及核准機制。 ▪ 雲端服務使用管理辦法（若有使用雲端服務），涵蓋：雲端服務選評標準、設定要求、存取控制、資料加密、備份及監控要求。 ▪ 使用雲端服務應要求供應商明確揭露資料儲存之實體國家/區域，以符合跨境傳輸之法規合規性。 ▪ 人工智慧系統使用管理辦法（若有使用 AI 系統），如涵蓋：AI 系統評估、使用規範、輸入個資管控、輸出結果品質管控。
雲端服務佐證	▪ 雲端服務清單（列出組織使用的所有雲端服務）。 ▪ 雲端服務商安全評估報告或其提供的合規認證文件（如 ISO 27001、SOC 2、CSA STAR 認證）。 ▪ 雲端服務存取控制設定文件（如 IAM 設定、存取金鑰管理）。 ▪ 雲端資料加密設定文件（確認靜態資料及傳輸中資料均已加密，金鑰管理方式）。 ▪ 雲端環境備份設定及定期備份測試紀錄。 ▪ 雲端安全設定定期審查紀錄（如：雲端設定合規掃描報告）。
AI 系統佐證	▪ AI 系統評估紀錄（採購或自行開發前的風險評估）及使用規範（哪些資料可輸入 AI 系統、輸出結果的使用限制）。 ▪ AI 系統個資輸入管控機制文件（如：輸入個資前的去識別化程序）。 ▪ AI 系統供應商合約（確認有無個資保護條款，如 AI 供應商是否承諾不將客戶資料用於訓練）。
風險評估紀錄	▪ 新興技術採納風險評估報告（針對雲端遷移、AI 導入等重大技術變更所進行的個資風險評估）。 ▪ 定期新興技術風險審查紀錄（確認現有技術使用的風險狀況仍在可接受範圍內）。

A8.7.11 資料可用性維護

管理目標：

確保組織所留存之個人資料具實現蒐集目的所必要之可用性，減少因個人資料滅失或無法存取致當事人受侵害之風險。

管理措施摘要：

訂定資料備份政策（合理備份頻率）、定期測試備份資訊（驗證備份媒體可靠性及資訊完整性）、備份資料採與原始資料相同之安全防護措施（確保機密性與完整性）。

證據類別	具體合規證據
備份政策文件	資料備份政策或程序，涵蓋：備份範圍（哪些系統/資料需備份）、備份頻率（每日/每週/每月增量/差異/完整備份）、備份保存期限、備份儲存位置（含異地備份要求）及備份安全措施。
備份執行紀錄	- 備份作業執行日誌（各系統備份執行紀錄，確認備份頻率符合政策要求）。 - 備份失敗告警及處置紀錄（確認備份失敗時有適當的告警及補救措施）。 - 備份媒體清冊（記錄備份媒體的位置、內容及保存狀態）。
備份還原測試	- 備份還原測試計畫及測試紀錄（至少每年一次）：記錄測試範圍、測試方法、還原成功率及發現的問題。 - 備份資料完整性驗證紀錄（確認備份資料未損毀，可成功還原）。 - 備份系統功能測試紀錄（確認備份系統本身正常運作）。
備份安全措施	- 備份資料加密設定文件（確認備份資料在儲存及傳輸中均已加密）。 - 備份存取控制設定（確認備份系統有適當的存取控制，防止未授權存取或竄改）。 - 異地備份設施說明（確認異地備份地點及其安全保護措施，符合備份 321 原則）。

A8.8 組織人員之管理與監督

A8.8.1 選任監督

管理目標：

確保組織人員適任其角色。

管理措施摘要：

組織聘用人員時，應進行適當篩選。

證據類別	具體合規證據
選任程序文件	- 人員選任程序文件，說明不同職位類型（一般員工、接觸敏感個資職位、特權帳號使用者）適用的選任標準及項目。 - 篩選流程納入聘雇程序的說明，確認篩選為聘雇前的必要步驟。
聘用條件文件	- 聘雇合約中涵蓋個資保護義務的條款（如：個資保密責任、違規懲處）。 - 新進人員個資保護義務告知/簽署確認紀錄（確認新進人員已被告知並同意遵守個資保護規定）。
派遣/約聘管理	- 派遣/外包人員管理合約（確認其個資保護義務、適用相同篩選標準或等效要求）。 - 派遣公司對其人員進行篩選的確認文件。

A8.8.2 保密契約

管理目標：

確保組織人員瞭解其所承擔之責任。

管理措施摘要：

組織與人員簽訂僱傭或委任契約時，應一併簽訂個人資料相關保密契約，並確保於人員離職或職務變動時，異動人員有義務配合個人資料媒介物之交接、返還或資料刪除措施；同時，異動人員於合理期間內仍須負有保密義務。

證據類別	具體合規證據
保密契約文本	- 員工保密契約範本（NDA），涵蓋：保密義務範圍（包含個人資料）、保密期間（含離職後保密義務年限）、違反義務之法律責任。 - 派遣/約聘人員保密契約範本（確認外部人員同樣受保密義務約束）。
簽署紀錄	- 員工已簽署保密契約之簽收紀錄清單（確認所有在職員工均已簽署）。 - 新進人員到職日簽署保密契約的紀錄（確認簽署為到職程序的必要環節）。
離職/職務異動管理	- 離職作業程序文件，涵蓋個資媒介物交接/返還/刪除的具體步驟及確認機制。 - 離職程序查核表（Offboarding Checklist），包含：個資相關設備及媒體的返還確認、系統存取帳號停用確認、離職人員簽署離職確認書（確認已瞭解保密義務延續）。 - 離職確認書範本，明定離職後保密義務仍持續的期間及範圍。 - 職務異動時的個資媒介物交接紀錄（確認職務交接過程中個資的控管）。
委任/委外契約	- 業務合作夥伴或顧問委任合約（確認含個資保密條款）。 - 委外廠商合約之個資保護及保密條款（確認受託廠商之人員亦受保密義務約束）。

A8.8.3 教育訓練

管理目標：

確保組織人員獲得應有資通安全專業課程訓練或資通安全職能訓練，以利管理制度推動與運作。

管理措施摘要：

組織應制定教育訓練計畫，並訂定評量機制。

證據類別	具體合規證據
訓練計畫文件	▪ 年度教育訓練計畫書，涵蓋：訓練對象（全員/權責人員/特定職能）、訓練主題（個資法基礎、個資保護實務、資通安全意識、特定職務技能訓練）、訓練方式（課堂/線上/演練）、訓練時數及預計時程。 ▪ 各類人員訓練需求分析文件（說明不同職位訓練需求的評估依據）。 ▪ 教育訓練評量機制說明（如何評估訓練成效，測驗機制、通過標準）。
訓練執行紀錄	▪ 訓練出席紀錄（含訓練日期、訓練主題、參訓人員名單及簽名、訓練時數）。 ▪ 訓練教材（簽到表、課程講義、測驗等），確認訓練內容涵蓋個資保護相關主題。 ▪ 新進人員到職訓練紀錄（確認新人已完成基礎個資保護訓練）。 ▪ 年度訓練完成率統計報告（呈現各部門/全員的訓練完成情況）。
訓練評量紀錄	▪ 訓練測驗結果（含測驗題目及成績，可匿名化呈現，以確認學習成效）。 ▪ 未通過測驗人員之補訓紀錄（確認成效不足者已接受補充訓練）。 ▪ 訓練滿意度調查結果（確認訓練品質持續改善依據）。
外部訓練及資格	▪ 個資管理人員及查核人員的資格認證書（個資管理師、個人資料內評師、個人資料驗證師）。 ▪ 外部個資保護/資通安全訓練課程參訓紀錄（如主管機關辦理之研習、TPIPAS 講座課程）。