

TIIPAS:2021+與 2021 年版規範修正對照表

TIIPAS:2021+	TIIPAS：2021	修正理由
3.7 查核人員 <u>指為辦理組織個人資料安全稽核，具有稽核之獨立性及專業性之人員。組織應要求查核人員與執行個人資料管理之管理人員不得互相兼任。</u>	(本條新增)	對應個人資料檔案安全維護管理辦法草案(下稱「安維管理辦法草案」)§17，規定組織應確保管理專責人員及查核人員不得兼任，以確保查核獨立性與客觀性。
7.2.2. 基本教育訓練 <u>組織針對組織人員應定期提供必要之個人資料管理教育訓練。</u>	7.2.2. 本教育訓練 組織針對組織人員應提供必要之個人資料管理教育訓練。	對應安維管理辦法草案§8、§21，明定組織人員應「定期」接受個資教育訓練。若為組織則應定妥適頻率定期辦理管理制度及差異化(如通識及專業課程)之個人資料保護教育訓練。
7.2.3. 權責人員教育訓練 組織應決定個人資料管理制度相關權責人員之必要能力與 <u>定期</u> 教育訓練需求，並規劃與執行。	7.2.3. 權責人員教育訓練 組織應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。	
7.2.4. 成果維持及改善措施 組織應針對組織人員 <u>定期</u> 教育訓練成果建立紀錄與持續改善機制。	7.2.4. 成果維持及改善措施 組織應針對組織人員教育訓練成果建立紀錄與持續改善機制。	
7.3.3. 使用紀錄與證據管理 組織為落實且證明其已符合本制度所要求之事項，應製作必要之紀錄文件並確立實施相關之管理程序，其紀錄包含： (1) <u>個人資料之蒐集、處理或利用紀錄。</u>	7.3.3. 記錄管理 組織為落實且證明其已符合本制度所要求之事項，應製作必要之紀錄文件並確立 實施相關之管理程序。	對應安維管理辦法草案§25，為使組織妥善保存個人資料檔案安全保護制度之落實紀錄，以杜相關個資法上爭議，對應個資法§30之保存期限，相關使用紀錄與證據應保存至少五年。

TPIPAS:2021+	TPIPAS：2021	修正理由
(2) <u>落實安全維護措施之證據。</u> (3) <u>當事人權利行使之紀錄。</u> (4) <u>保存前三款相關紀錄，應留存至少五年。</u>		
7.3.4. 系統日誌管理 <u>組織維運其資通系統蒐集、處理或利用個人資料，應執行下列事項：</u> (1) <u>訂定日誌之記錄時間週期及留存政策，並保存適當時間。</u> (2) <u>確保資通系統具備記錄特定事件之功能，並決定應記錄之特定資通系統事件。</u> (3) <u>記錄資通系統管理者帳號所執行之各項功能。</u>	(本條新增)	對應安維管理辦法草案§13，為落實資通系統之安全管理，強化個人資料保護之追查與鑑識能力，增列本條。其要點如下： 1. 確保可歸責性：組織維運或委外開發資通系統涉及個資處理者，應採取安全控制措施，以利事故發生後之追蹤與鑑識。 2. 明確日誌規範：組織應訂定系統日誌之記錄範圍、頻率及留存政策。 3. 強化行為監控：應完整記錄重要系統事件（如登入、權限變更、個資存取及刪除等），並針對特權帳號之操作執行監控與記錄。
8.2. 納入管理之個人資料範圍 <u>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，劃定其納入個人資料管理制度之範圍，建立並</u>	8.2. 納入管理之個人資料範圍 <u>組織應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，</u>	文字微調，組織應每年界定個人資料檔案之管理範圍，並建立個人資料盤點清冊及流程說明文件等文件化資訊。

TPIPAS:2021+	TPIPAS：2021	修正理由
維護個人資料檔案清冊及流程說明。	建立並維護個人資料檔案清冊及流程說明。	
8.4.3. 處理 組織為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送，其程序應符合下列要求： (1) 確認處理時符合蒐集時之特定目的及特定情形。 (2) 其他法令規定處理時應履行之義務。 (3) 組織應訂定適當且合法之程序，<u>以處理刪除、銷毀及業務終止時組織所保有之個人資料，並留存個人資料之刪除、停止處理或利用、移轉及其他銷毀行為之方法、時間、地點及銷毀證明。</u> (4) 保存前三款相關紀錄。	8.4.3. 處理 組織為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送，其程序應符合下列要求： (1) 確認處理時符合蒐集時之特定目的及特定情形。 (2) 其他法令規定處理時應履行之義務。 (3) 組織應訂定適當且合法程序，處理刪除暨銷毀及業務終止時組織所保有之個人資料。 (4) 保存前三款相關紀錄。	為落實個人資料生命週期管理，確保組織於資料銷毀或業務終止時之安全性與可追溯性，增列組織於刪除、銷毀及業務終止時之安全維護措施。其要點如下： 1. 明定相關程序：組織應訂定合法之刪除、銷毀及業務終止處置程序。 2. 留存紀錄與軌跡：針對個資之刪除、移轉、停止處理或銷毀，應留存包含方法、時間、地點及銷毀證明之完整紀錄。
8.4.7. 特種個人資料之蒐集、處理及利用限制 組織針對病歷、醫療、基因、性生活、健康檢查、犯罪前科等個人資料，其	8.4.7. 特種個人資料之蒐集、處理及利用限制 組織針對病歷、醫療、基因、性生活、健康檢查、犯罪前科等個人資料，其	對應安維管理辦法草案S 11，鑑於特種個人資料具高度敏感性，一旦洩漏將嚴重侵害當事人權益，爰強化其管理規範：

TPIPAS:2021+	TPIPAS : 2021	修正理由
程序應符合下列要求： (1) 組織人員原則禁止蒐集、處理及利用特種個人資料之要求。 (2) 例外得蒐集、處理或利用特種個人資料時，<u>符合法律規定之特定情形</u>。 (3) <u>針對載有特種個人資料之紙本或電子檔案，採取適當之安全管理措施，包括紙本及可攜式設備或儲存媒體之管制、媒介物之安全處置(如銷毀、報廢或轉用)、備份資料之保護，以及檔案加密、資料傳輸與銷毀機制。</u> (4) 保存前<u>三款</u>相關紀錄。	程序應符合下列要求： (1) 組織人員原則禁止蒐集、處理及利用特種個人資料之要求。 (2) 例外得蒐集、處理或利用特種個人資料時，係屬合乎法律要求。 (3) 保存前二款相關紀錄。	1. 訂定紙本及使用可攜式設備或儲存媒體之管制規範。 2. 保有個人資料檔案之媒介物於銷毀、報廢或轉作其他用途時，應採取適當防範措施。 3. 處理過程有備份個人資料之需要時，應比照原件予以保護。 4. 建置檔案安全加密及資料安全傳輸措施。 5. 落實安全銷毀機制，確保資料不可回復，並留存相關紀錄。
8.7. 安全管理措施 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<u>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</u>。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措	8.7. 安全管理措施 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，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措	為使所列事故類型及用語與新修正之個資法條文一致，修正為「竊取、竄改、毀損、滅失或洩漏」。

TPIPAS:2021+	TPIPAS：2021	修正理由
施。 (2) 技術面安全管理措施。	施。 (2) 技術面安全管理措施。	
8.10. 事故之緊急應變 為避免事故可能產生之 不利益及影響，組織應 訂定並落實事故緊急應 變措施。相關措施應至 少包括： (1) <u>知悉事故時於適當時機及方式通知當事人事故發生，並提供後續查詢與處理管道。</u> (2) <u>採取即時有效之應變措施，防止事故之擴大，及記載相關事實、影響、已採取之因應措施，並保存相關紀錄。</u> (3) 避免類似事件再次發生之方法。 (4) <u>將事故即時通報主管機關及其他依組織所識別之法令應通報之政府機關。</u> (5) 將事故即時通報授證機關。 <u>組織應將通知之內容、方式、時限與通報範圍、應變措施及紀錄保存，以供備查。</u>	8.10. 事故之緊急應變 為避免事故可能產生之 不利益及影響，組織應 訂定並落實事故緊急應 變措施。相關措施應至 少包括： (1) 查明後於適當時機及方式通知當事人事故發生，並提供後續查詢與處理管道。 (2) 防止組織所受損害擴大之方法。 (3) 避免類似事件再次發生之方法。 (4) 將事故即時通報授證機關。	因應個資法§12 修訂，調修部分文字： 1. 明確通知當事人義務：為使當事人能即時評估並關注權益損害，組織知悉個資事故發生時即負有通知義務。個資法條文修正說明亦指出原條文易生「須先確認違法」或「查明時點爭議」之誤解，明定通知義務不以確認違法為前提。 2. 應變措施與紀錄留存：組織於事故發生後應採取即時有效之應變作為以防止損害擴大，並應詳實記載事故事實、影響、已採取之因應措施及留存相關紀錄。 3. 通報義務：配合個資法§48II，明定組織知悉個資事故且符合法定通報範圍時，負有主動通報主管機關之義務，以利監理機關及時介入調查與協助，確保個資保護之落

TPIPAS:2021+	TPIPAS：2021	修正理由
		實。 4. 確保可追溯性：組織應將事故通知之內容、方式、時限與通報範圍、應變措施及處置紀錄詳實留存，以確保事故之可追溯性，並於當事人主張權利或主管機關為行政調查時，作為釐清爭議與合規證明之依據。
11.7. 未成年人之保護 <u>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，或足辨識具其他符合法律規定之特定情形。</u>	11.7. 未成年人之保護 <u>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。</u>	配合 Global CBPR 計畫要求更新內容，鑒於未成年人自我保護能力較弱，組織於蒐集、處理或利用其個資時，應履行較高之注意義務。其要點如下： 1. 強化安全管理機制：針對未成年人個資應採取更嚴謹之安全控管措施。 2. 確認同意有效性：組織應採取有效措施，確認已取得法定代理人之同意，或確認符合其他法定特定情形。
11.14. 應對政府存取資料 <u>組織應建立應對程序，回應要求揭露組織所持有之個人資料之國內、外司法或其他政府傳</u>	(本條新增)	配合 Global CBPR 計畫要求更新內容，明定組織應建立應對程序，以規範回應國內外司法或政府機關調閱個人資料之請求。確保調閱要求與回應方式均符合法律

TPIPAS:2021+	TPIPAS：2021	修正理由
<u>票、搜索令或其他命令，其內容應包括：</u> <u>(1) 確認要求與回應方式符合法律規定之特定情形。</u> <u>(2) 保存相關紀錄。</u>		規定，並保存相關紀錄。

附表 A：本制度規範安全管理措施

修正與公告日期：2026 年 06 月 01 日

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
前言 附表 A 係針對本制度規範管理措施制定基本安全管理措施，組織應<u>制定符合附表 A 所列各項管理措施</u>，確保組織蒐集、處理及利用個人資料流程符合法令遵循，並已採取防止個人資料被竊取、竄改、毀損、<u>滅失或洩漏及其他侵害之必要且適當之安全管理措施</u>。	前言 附表 A 係針對本制度規範管理措施制定基本安全管理措施，組織應符合附表 A 所列各項管理措施，確保組織蒐集、處理及利用個人資料流程符合法令遵循，並已採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。	為使所列事故類型及用語與新修正之個資法條文一致，修正為「竊取、竄改、毀損、滅失或洩漏」，現行「或其他侵害」一語，易生誤解，爰此予刪除。
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： 1. <u>存取控制實施政策</u> 組織應透過存取控制政策與存取實施機制(如存取控制清單)對個人資料之存取進行管控。 2. 帳號管理 組織應建立帳號管理機制，包含帳號之申請、開通、停用、<u>去識別化或及刪除</u>	A8.7.1 存取控制 管理目標：組織對個人資料的存取加以規範與保護，防止任何未經授權的存取與破壞。 管理措施： 1. 存取控制實施 組織應透過存取控制政策與存取實施機制(如存取控制清單)對個人資料之存取進行管控。 2. 帳號管理 組織應建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序，並應刪	1. 落實存取政策核定：組織應訂定經權責人員核定之存取控制政策與實施機制，並納入去識別化為帳號管理機制之一；針對特權帳號應至少每年定期清查，以防範閒置帳號遭非法提權導致之個資事故。 2. 深化最小權限原則：組織應識別業務涉及個資之人員，限縮授權範圍於達成任務之必要存取行為。另配合安維管理辦

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
<u>之程序，並應至少每年定期辦理帳號清查，或就特權帳號評估設定較高頻率之清查週期，以檢視並刪除或禁用已逾期之臨時或緊急帳號、閒置帳號，及其他不再使用或有異常情形之帳號。當使用者逾組織所訂定之閒置時間未進行操作時，系統應自動將其登出。</u> 3. 職責分工 組織對於個人資料之存取應落實職責分工。 4. 最小權限 組織應<u>識別業務內容涉及個人資料蒐集、處理或利用之人員，並落實最小權限</u>之概念，僅允許使用者依組織任務與業務功能需要，完成指派任務授權之存取行為。 5. 遠端存取 組織應透過政策訂定選擇禁止或嚴格限制遠端存取個人資料，倘允許遠端存	除或禁用已逾期之臨時或緊急帳號、閒置帳號。逾組織所訂定之時間時，系統應自動將使用者登出。 3. 職責分工 組織對於個人資料之存取應落實職責分工。 4. 最小權限 組織應落實最小權限的概念，僅允許使用者依組織任務與業務功能需要，完成指派任務授權的存取行為。 5. 遠端存取 組織應透過政策訂定選擇禁止或嚴格限制遠端存取個人資料，倘允許遠端存取，組織應確保傳輸過程經過適當加密，並應建立自動監控措施，以確保從遠端連線至資通系統之活動，均符合遠端存取政策。 6. 行動裝置存取 組織應透過政策訂定選擇禁止或嚴格限制，來自於可攜式或行動裝置對個人	法草案§23，明定大型非公務機關自行維運或委外設置、開發之資通系統蒐集、處理或利用資通系統應採取個人資料顯示隱碼機制，以強化資料呈現之安全性。 3. 資訊分享紀錄留存：組織應建立個人資料分享機制，明確要記載分享之對象與方式，並確保所有存取授權均符合內部政策規範，以達成軌跡留存之目標。

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
取，組織應確保傳輸過程經過適當加密，並應建立自動監控措施，以確保從遠端連線至資通系統之活動，均符合遠端存取政策。 6. 行動裝置存取 組織應透過政策訂定選擇禁止或嚴格限制，來自於可攜式或行動裝置對個人資料之存取。如果行動裝置經允許存取個人資料，組織應確保該裝置被適當保護，並定期檢視或確認該裝置以確認其安全狀態。 7. 資訊分享 組織應制定個人資料資訊分享機制，<u>該機制應保存分享方式與對象之紀錄</u>，並確保對個人資料存取之授權符合政策規定。	資料的存取。如果行動裝置經允許存取個人資料，組織應確保該裝置被適當保護，並定期檢視或確認該裝置以確認其安全狀態。 7. 資訊分享 組織應制定個人資料資訊分享機制，確保對個人資料存取之授權符合政策規定。	
A.8.7.2 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紀錄之事件，並建	A.8.7.2 技術檢視 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紀錄的事件，並建立監控機制。	1. 因應資通安全責任等級分級辦法修訂，以及表十、資通系統防護基準修訂，為使用語與一致，爰修訂本制度

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
立監控機制。 管理措施： 1. <u>記錄事件</u> 組織應監控影響個人資料機密性、<u>完整性</u>之事件，例如對個人資料之未授權存取或修改。 2. <u>日誌紀錄之檢視、分析、通報</u> 組織應定期檢視與分析資通系統之<u>日誌紀錄</u>，以發現<u>可能影響個人資料機密性或完整性之不當或異常活動跡象</u>；並應就可疑活動或疑似違規情形進行調查，將調查結果報告權責主管，並採取適當措施。 3. <u>日誌紀錄之保存與維護</u> 組織應訂定日誌之紀錄時間周期及留存政策，並採取措施避免紀錄遭毀損或竄改。如對日誌之存取管理，僅限於有權限之使用者。	管理措施： 1. 稽核事件 組織應監控影響個人資料機密性的事件，例如對個人資料的未授權存取。 2. 稽核紀錄的檢視、分析 組織應定期檢視與分析資通系統稽核紀錄，以發現個人資料的不當或不尋常活動的跡象、調查可疑的活動或可疑的違規、將發現報告給權責主管並採取適當措施。	用詞。 2. 強化資料完整性控管：組織除監控個人資料之機密性外，應同步加強對「完整性」之保障。針對未經授權之存取或惡意竄改等影響資料正確性之事件，應納入核心稽核項目與監控機制。 3. 明定日誌留存規範：配合安維管理辦法草案§23，組織應訂定資通系統日誌之記錄時間週期及留存政策，並明確規範日誌紀錄應至少保存六個月，以落實事故調查之可追溯性。 4. 日誌紀錄：為確保日誌內容之真實性，應採取存取控制措施，防止日誌遭非法毀損或竄改，僅限經授權之特定人員始得存取。
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	A8.7.3 識別鑑別 管理目標：組織對於組織內部的系統使用者，	因應安維管理辦法草案§12 規定，爰增訂使用者設置符合一定複雜性要

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
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： 1. 使用者之識別與鑑別 組織內之使用者使用資通系統，組織應賦予其唯一之識別與驗證方式，避免使用共用帳號。 2. 身分驗證管理 使用預設密碼登入系統時，應於登入後要求立即變更。身分驗證相關資訊不以明文傳輸。<u>應依需要制定並落實密碼規則與更新週期，落實密碼管理原則。</u>	應有特定的方式確認其所擁有的存取帳號與權限，以確保行為之明確可歸責性。 1. 管理措施： 使用者之識別與鑑別 組織內之使用者使用資通系統，組織應賦予其唯一的識別與驗證方式，避免使用共用帳號。 2. 身分驗證管理 使用預設密碼登入系統時，應於登入後要求立即變更。身分驗證相關資訊不以明文傳輸。	求之密碼，並定期更換。
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： 1. 媒體存取 組織應採用特定防護措施，對特定授權人員，限制其對數位與非數位媒體類型的存取。	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： 1. 媒體存取 組織應採用特定防護措施，對特定授權人員，限制其對數位與非數位媒體類型的存取。	鑒於數位化環境下，實體或邏輯標記已不足以防範未授權存取，現行實務已轉向以身分驗證與權限控管為核心之防禦機制，故刪除媒體標記之管理措施。

TIIPAS:2021+ 附表 A	TIIPAS：2021 附表 A	修正理由
~~2. 媒體標記~~ 組織應建立媒體標記之方法且進行適當標記。 2. 媒體儲存 組織應建立並落實個人資料媒體儲存之安全作業規定。 3. 媒體傳輸 個人資料儲存媒體運輸或傳輸到管控區域外時，應採用適當安全防護措施。 4. 媒體汰除 組織於媒體汰除時應透過適當程序加以安全汰除，確保無法被還原。	2. 媒體標記 組織應建立媒體標記之方法且進行適當標記。 3. 媒體儲存 組織應建立並落實個人資料媒體儲存之安全作業規定。 4. 媒體傳輸 個人資料儲存媒體運輸或傳輸到管控區域外時，應採用適當安全防護措施。 5. 媒體汰除 組織於媒體汰除時應透過適當程序加以安全汰除，確保無法被還原。	
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： 1. 實體存取控制 組織應識別儲存個人資料之安全周界，於存放個人資料場所，<u>如資訊機房及檔案庫房</u>，採取適當安全措施，並針對<u>進入</u>場所之<u>權限</u>加以管控。	A8.7.5 實體與環境安全管理目標：防止儲存個人資料場所不受人為因素非 授權入侵與存取而導致個人資料之洩漏。 管理措施： 1. 實體存取控制 組織應識別儲存個人資料之安全周界，於存放 個人資料場所採取適當安全措施，並針對場所之進出加以管控。 2. 實體存取監視 組織應定期檢視已	1. 強化實體場域防護：配合安維管理辦法草案§10 規定，針對紙本或電子檔案之儲存場所，組織應建立實體安全周界，尤其針對資訊機房與檔案庫房等敏感區域。 2. 落實權限與監控：明定應實施場域進出管制、設置監視系統及建立實體障礙，並控管進入人

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
2. 實體存取監視 組織應定期檢視已實施安全措施之有效性，<u>並就人員及個人資料之進出，建立監視與環境控管安全機制，並制定合理保存期間，保存相關出入紀錄。</u>	實施安全措施之有效性，並建立個人資料儲存場所監視與環境控管安全機制。	員之權限；並針對各類實體出入紀錄（如門禁 Log、監視影像、進出登記簿）制定合理之保存期間，以確保發生資安事故或個資爭議時，具備充足之資訊。
A8.7.6 資訊傳輸 管理目標：防止個人資料傳輸時遭非授權揭露。 管理措施： 1. 邊界保護 組織於系統外部邊界與系統內部的關鍵內部邊界，應建立適當監視與控制通訊的介面防護。 2. 傳輸機密性 組織應採取適當措施確保個人資料傳輸的機密性，<u>並提供傳輸加密協定之設定截圖、加密證明文件或傳輸軌跡紀錄。</u>	A8.7.6 資訊傳輸 管理目標：防止個人資料傳輸時遭非授權揭露。 管理措施： 1. 邊界保護 組織於系統外部邊界與系統內部的關鍵內部邊界，應建立適當監視與控制通訊的介面防護。 2. 傳輸機密性 組織應採取適當措施確保個人資料傳輸的機密性。	組織應提供傳輸加密協定（如 TLS 1.2 以上）之設定截圖，或其他加密機制之佐證，以資證明管理措施之有效性。
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： 1. 安全性檢測 組織應進行資通系	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： 1. 安全性檢測	1. 收攏稽核規範：原「稽核事件」管理措施性質屬事件日誌紀錄，爰併入「A.8.7.2 事件日誌與可歸責性」統一管理，以維持制度邏輯一致性。

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
統脆弱性識別、報告與修正作業。系統更新前應事先進行測試，瞭解該更新對資通系統可能產生之結果與衝擊。 ~~2. 稽核事件~~ ~~組織應規劃資通系統有稽核特定事件之功能，並決定應稽核之特定系統事件，對稽核紀錄之存取管理，僅限於有權限之使用者。~~ 2. 惡意程式防護 組織應針對資通系統可能之出入端點部署有效之惡意程式防護機制。<u>防毒軟體應設定自動更新至最新版本之病毒碼，並啟用即時防護功能；另應定期執行完整系統掃描，並依程序針對偵測到之惡意程式進行隔離、刪除或其他適當處置。</u> 3. 資通系統監看 組織應透過資通系統監視內向與外向通訊，發現資通系統有被入侵跡象時，依	組織應進行資通系統脆弱性識別、報告與修正作業。系統更新前應事先進行測試，瞭解該更新對資通系統可能產生之結果與衝擊。 2. 稽核事件 組織應規劃資通系統有稽核特定事件之功能，並決定應稽核之特定系統事件，對稽核紀錄之存取管理，僅限於有權限之使用者。 3. 惡意程式防護 組織應針對資通系統可能的出入端點、工作站、伺服器或可攜式媒體等設備，有效部署惡意程式防護機制。 4. 資通系統監看 組織應透過資通系統監視內向與外向通訊，發現資通有被入侵跡時，應依程序通報特定人員。	2. 強化惡意程式防禦：因應安維管理辦法草案§9 規定，組織應於系統出入端點部署有效之防護機制，包含自動更新至最新病毒碼、啟用即時防護及定期執行完整掃描。針對偵測到之威脅，應確實執行隔離或刪除處置。 3. 落實開發測試安全：考量測試環境之安全層級通常低於正式環境，組織應實施環境區隔及避免使用真實資料。如需使用真實個資，須經申請核准之程序。

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
程序通報特定人員。 4. <u>測試環境管理</u> <u>組織應區隔正式環境與測試環境，且應避免使用真實個人資料作為系統之測試資料。如有使用真實個人資料測試系統之必要，應制定程序及安全使用規範，依循程序申請使用。</u>		
A8.7.8 系統發展生命週期階段 管理目標：<u>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)。</u> 管理措施： 1. 組織應<u>運用安全系統發展生命週期(SSDLC)概念於系統發展生命週期之需求評估、設計開發、測試及部署與維運階段，合理滿足系統之安全需求。</u> 2. <u>資通系統如涉及個人資料之蒐集、處理或利用，應於系統發展及維運各階段，依相關法規導入適當之安全措施，包含帳號管理與身分鑑別、</u>	A8.7.8 系統發展生命週期階段 管理目標：組織於系統發展生命週期需求、設計開發、測試及部署與維運階段運用安全系統發展生命週期(SSDLC)概念之安全設計概念。	1. 強化開發安全週期：組織應導入安全系統發展生命週期(SSDLC)概念，確保系統自需求、設計至維運階段均符合機密性與完整性要求。委外開發時，應將各階段安全需求納入契約規範。 2. 落實預防性檢測：配合安維管理辦法草案§23，明定系統上線前須執行源碼檢測、弱點掃描及滲透測試，並完成漏洞修補。 3. 建立持續維護機制：考量資訊安全威脅具動態性，明定系統上線後仍應

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
<u>存取控制、隱碼及加密、日誌紀錄與監控、入侵防護及備份等機制。</u> 3. <u>組織資通系統開發、維運如委外辦理，應將系統發展生命週期各階段所必要之安全需求納入委外契約。</u> 4. <u>提供對外服務之資通系統，於上線前應辦理源碼檢測、弱點掃描及滲透測試，並完成弱點、漏洞修補作業；系統上線後應持續辦理。</u> 5. <u>組織應定期評估各項安全措施之有效性，並持續檢討及改善。</u>		定期辦理安全性檢測與修補作業，以確保個資防護與時俱進。
(整併進 A8.7.8)	A8.7.9 系統發展生命週期委外階段 管理目標：確保組織系統發展之委外安全管理。 管理措施：組織資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、完整性、可用性）	為強化系統發展生命週期（SDLC）管理之完整性，將原「A.8.7.9 系統發展生命週期委外階段」相關規範併入「A8.7.8 系統發展生命週期階段」，以落實開發至維運階段之一致性控管。

TIIPAS:2021+ 附表 A	TIIPAS：2021 附表 A	修正理由
	納入委外契約。	
A8.7.9 網路安全防護 <u>管理目標：確保組織網路系統有效應對威脅與風險。</u> <u>管理措施：組織應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，避免系統遭未經授權存取、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。</u>	（本條新增）	配合安維管理辦法草案S23，為確保組織網路系統有效應對威脅與風險，增列本條管理規範。組織應制定網路安全防護政策，包含定期維護網路設備之軟硬體、韌體及相關元件，以避免系統遭未經授權之存取或入侵。
（整併進 A8.7.7）	A8.7.10 獲得程序與系統文件 <u>管理目標：確保資料流管控與文件管理之機制</u> <u>管理措施：組織系統開發、測試及正式作業應為區隔，且應避免使用真實個人資料作為系統之測試資料，如有使用真實個人資料測試系統之必要，應透過相關程序申請並經許可始可採用，並管理相關系統文件。</u>	為強化資通系統整體防禦之連貫性，將原「A8.7.10 獲得程序與系統文件」併入「A8.7.7 系統與資訊完整性」，統籌管理系統之完整性。
A8.7.10 新興技術風險管理 <u>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</u>	（本條新增）	鑑於雲端運算及人工智慧（AI）等新興技術之廣泛應用，為確保組織能有效識別並管理其衍生之個人資料安全風

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
<u>並管理其所衍生之相關風險。</u> <u>管理措施：組織應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。</u> 1. <u>資通系統如部分或全部採用雲端服務，應就其取得、環境設定及維運管理訂定相關規範，並保存更新紀錄。</u> 2. <u>組織如開發、部署或採購人工智慧系統或服務，應就其取得、環境設定及使用管理訂定相關規範。</u>		險，爰增列本條。 1. 組織如採用雲端服務，應針對服務獲取、環境設定及管理維護制定專門政策，並詳實記錄相關更新與調整。 2. 人工智慧倫理與安全：組織開發、部署或採購人工智慧服務時，應建立獲取規範、環境設定及使用規則，落實風險評估與控管措施。
A8.7.11 資料可用性維護 <u>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，減少因個人資料減失或無法存取致當事人受侵害之風險。</u> <u>管理措施：組織應訂定資料備份之政策，決定資料備份之合理頻率，並定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。備份資料應比照原件予以保護。</u>	A8.7.11 營運持續計畫 管理目標：確保組織業務運作正常，訂定最大可容忍中斷時間（MTPD）與最低可接受服務水準。 管理措施： 1. 系統備份 組織應訂定系統可容忍資料損失之時間要求，執行系統碼與資料備份，並定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整	配合安維管理辦法草案§11、§22 規定，將重點調整為針對個資之「備份」管理。

TPIPAS:2021+ 附表 A	TPIPAS：2021 附表 A	修正理由
~~2. 系統備援~~ ~~訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。於原服務中斷時，於可容忍時間內，由備援設備取代提供服務，提供最低可接受服務水準。~~	性。 2. 系統備援 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。於原服務中斷時，於可容忍時間內，由備援設備取代提供服務，提供最低可接受服務水準。	
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：組織與人員簽訂雇傭或委任契約時，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<u>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。</u>	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：組織與人員簽訂雇傭或委任契約時，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後適當期間內仍負有保密義務。	配合安維管理辦法草案S7 規定，針對職務上直接或間接具取得個資可能性之人員，組織應與其約定保密義務，以降低未經授權濫用之風險。明定人員異動（含離職、調職）時，應履行個資媒介物之交接、返還或資料刪除義務。此外，異動人員於合理期間內仍負有保密義務，以確保個資安全不因人員更迭而產生個資保護真空期。