國立臺南藝術大學
個人資訊管理制度內部稽核底稿

紀錄編號：_____ 填表日期：　　年　　月　　日

檢　查　項	是	否	不適用	備註與說明
1. 個資管理政策				
1.1 是否訂定個資管理系統範圍、政策與目標？	□	□	□	
1.2 組織是否定期審查政策之有效性與適切性？是否定期針對各項目標進行量測？	□	□	□	
1.3 高階管理是否提供適切資源？並展現承諾支持管理系統運作？	□	□	□	
1.4 是否制定個資管理系統中角色權責？	□	□	□	
1.5 是否有專人擔任個資管理系統管理代表，並負責溝通協調責任？	□	□	□	
1.6 組織是否曾透過教育訓練或觀念宣導等方式來強化組織內人員對於個資安全	□	□	□	
1.7 政策是否含有應用個人資料處理的各種例外狀況？	□	□	□	
1.8 政策是否含有提供資料分享方案之建議？	□	□	□	
1.9 是否持續確認法律、實務與科技的變化對PIMS帶來的改變？	□	□	□	
1.10 是否公告明確告知當事人其個人資料將如何被使用及被誰使用？	□	□	□	
1.11 是否公告組織應維護一份個人資料檔案名稱？	□	□	□	
1.12 是否公告組織個人資料檔案名稱？	□	□	□	

1.13 是否指派一位或多位合適或具經驗的同仁負責日常個人資料管理政策的遵循？	□	□	□	
2. 個資資產鑑別與風險評鑑				
2.1 是否識別出範圍內所有個人資料檔案？	□	□	□	
2.2 是否識別出特種個人資料檔案？	□	□	□	
2.3 是否各項個人資料檔案，皆可歸類於特定類別？	□	□	□	
2.4 是否各項個人資料檔案，皆具有蒐集之特定目的？	□	□	□	
2.5 是否訂定風險評鑑程序，以確保組織能瞭解在處理各種特定類型之個人資料 所可能產生的風險？	□	□	□	
2.6 是否於處理個人資料前，清楚識別法令上的各項要求？	□	□	□	
2.7 是否識別個人資料分享時的相關法令？	□	□	□	
2.8 是否定期執行隱私衝擊分析（如PIA）？	□	□	□	
2.9 是否定期執行風險評鑑作業？	□	□	□	
2.10 是否確保所有新識別個人資料之風險皆經評估？	□	□	□	
3. 個人資料的蒐集、處理、利用、傳輸、儲存與銷毀				
3.1 是否各項個人資料檔案蒐集、處理、利用之目的，皆取得當事人之同意？	□	□	□	
3.2 向當事人蒐集個人資料時，是否已具有明確告知當事人應知事項之程序？	□	□	□	
3.3 是否提供當事人拒絕行銷之選擇權利？	□	□	□	
3.4 蒐集個人資料時，是否符合「適當、相關、不過度」的原則？	□	□	□	
3.5 是否建立程序以主動或應要求維護個人資料之正確性？	□	□	□	

3.6 是否含有尊重當事人對其個人資料所能行使之權利，包含其請求閱覽；複 製；補充或更正；停止蒐集、處理或利用；刪除等權利？	□	□	□	
3.7是否建立程序以確保組織保留個人資料所需的保存期限？	□	□	□	
3.8 是否建立並實作個人資料檔案銷毀程序，當特定目的消失或保存期限屆滿時				
3.9 是否有跨國個資傳輸之行為? 是否建立並遵循跨國個資傳輸之控管？	□	□	□	
3.10 是否建立程序於組織處理個人資料之過程有任何疑慮時的聯絡方式？	□	□	□	
3.11 是否建立程序於確保第三方得正當且合法取得個人資料之程序？	□	□	□	
3.12 是否建立程序於確保為特定目的所蒐集之個人資料不逾越其目的？	□	□	□	
3.13 是否建立程序於確保個人資料被使用於其他特定目的以外時,應取得當事人	□	□	□	
3.14 是否建立當事人同意紀錄之保存機制？	□	□	□	
3.15 是否建立程序以定期檢視處理個人資料之科技與程序，以持續符合使用目	□	□	□	
4. 個資管理制度技術安全				
4.1 所有涉及個人資料的資訊設備，是否皆位於良好實體環境安全管制之區域？	□	□	□	
4.2 所有涉及個人資料的資訊設備，攜出入實體環境是否皆有管制？	□	□	□	
4.3 所有涉及個人資料的文件與紀錄，是否皆位於良好實體環境安全管制之區域？	□	□	□	
4.4 所有涉及個人資料的文件與紀錄，攜出入工作環境是否皆有管制？	□	□	□	
4.5 所有涉及個人資料的資訊設備，是否皆具備適切的防毒管制？	□	□	□	
4.6 所有涉及個人資料的資訊備份，其備份回復測試作業是否定期執行？	□	□	□	

4.7 所有涉及個人資料的資料庫權限，任何存取紀錄是否妥善保存？	☐	☐	☐	
4.8 所有涉及個人資料的應用系統權限，任何存取紀錄是否妥善保存？	☐	☐	☐	
4.9 所有涉及個人資料的伺服器作業系統權限，任何存取紀錄是否妥善保存？	☐	☐	☐	
4.10 是否制訂相關程序，以確保當個人資料以電子或人工方式在組織內外傳輸的				
4.11 是否制訂相關程序以確保個人資料的授權與存取作業應在合法目的下執行？	☐	☐	☐	
4.12 組織是否訂定個資管理系統資安事件管理程序？	☐	☐	☐	
4.13 組織是否訂定個人資料交換政策與程序，以確實保障資料交換時之個資安	☐	☐	☐	
4.14 組織是否訂定委外管理程序，以確實保障委外廠商不會危害當事人個資安	☐	☐	☐	
4.15 組織是否定期審查或稽核委外廠商有關個資安全之遵循性？	☐	☐	☐	
4.16 組織與委外廠商之契約是否考慮個人資料保護要求？	☐	☐	☐	
5. 個人資料管理制度				
5.1 是否建立對PIMS認知訓練有效性評量程序？	☐	☐	☐	
5.2 是否建立內部稽核程序及計畫？	☐	☐	☐	
5.3 內部稽核計畫之範圍是否涵蓋所有具高風險之個人資料處理流程及所有由其他組織所執行之個人資料處理流程？	☐	☐	☐	
5.4 是否建立程序以確保定期執行稽核作業？	☐	☐	☐	
5.5 是否建立程序以因應當管理制度發生重大變更後的稽核作業？	☐	☐	☐	
5.6 稽核報告內容是否識別所有可能影響政策遵循之技術或程序？	☐	☐	☐	
5.7 稽核報告是否由管理階層審核？	☐	☐	☐	
5.8 是否定期舉辦管理審查會議？	☐	☐	☐	

5.9 是否於管理審查會議中討論八大議題？	☐	☐	☐	
5.10 是否建立矯正預防措施程序？	☐	☐	☐	
5.11 是否將矯正預防措施所引發之變更加以記錄，並保存？	☐	☐	☐	
5.12 是否鑑別潛在不符合事項之原因？	☐	☐	☐	
5.13 是否消除不符合事項之原因？	☐	☐	☐	
5.14 矯正後是否降低不符合事項之風險等級？	☐	☐	☐	
5.15 是否確保稽核結果、矯正與預防措施皆經管理階層審查？	☐	☐	☐	