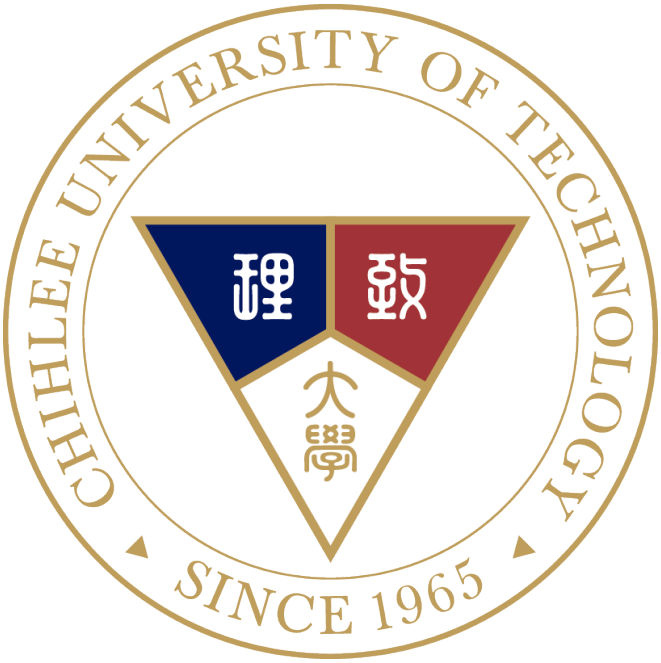
# 致理科技大學

## 個人資料管理手冊




機密等級：■一般 □敏感 □機密

編號：P-1-01

版本：5.0

發行日期：111 年 1 月 4 日

# 文件制／修訂紀錄頁

| 版次 | 發行日期 | 修訂摘要 | 修訂者 | 文管人員 |
|---|---|---|---|---|
| 1.0 | 106.4.20 | 初次發行 | 呂瑞茹 | 呂瑞茹 |
| 1.1 | 106.6.15 | 修正第 9 頁個人資料蒐集、處理與利用管理程序之第十一條 | 呂瑞茹 | 呂瑞茹 |
| 2.0 | 107.5.28 | 依據 BS 10012:2017 標準要求修正程序書內容 | 呂瑞茹 | 呂瑞茹 |
| 3.0 | 107.7.24 | 新增組織 PIMS 全景評鑑表相關條文及表單；修改管理審查會議參與人員。 | 呂瑞茹 | 呂瑞茹 |
| 4.0 | 109.7.7 | 新增使用生物特徵管理規範相關說明 | 呂瑞茹 | 呂瑞茹 |
| 5.0 | 111.1.4 | 修改召集人及副召集人為主任委員及副主任委員 | 呂瑞茹 | 呂瑞茹 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

目錄

壹、前言：

致理科技大學（以下簡稱本校）為落實個人資料保護法要求，以及維護校園之個人資料安全，規劃本校個人資料保護之框架，發展具適法性及有效性之個人資料保護管理機制，建立本校個人資料保護管理系統(PIMS)之共同性規範、程序指引與參考表單，以落實個人資料保護與管理。

貳、個人資料保護政策：

為使個人資料保護推動委員會執行方向能有所依據，訂定個人資料保護政策聲明，作為個人資料保護工作之最高指導方針。聲明內容如下：

致理科技大學個人資料保護政策聲明

本校認知個人資料保護的重要性，為展現對個人資料與隱私保護之決心，特訂定下列政策聲明為本校個人資料保護最高指導方針。

一、 本校基於合法的組織目的，蒐集最少的必要個人資料，並採行適當安全措施，確保個人資料被公平合法的處理及利用。

二、 本校將維持學校處理的個人資料檔案清單。

三、 本校將維持所經手個人資料於正確與最新狀態。

四、 本校尊重個人對其個人資料所受保障的相關權利。

五、 本校僅在確實必要且有適當充分保護的狀況下，將個人資料移轉到其他的地方。

六、 本校將發展和實行個人資料管理系統，落實個人資料保護政策。

七、 本校針對涉及個人資料之個案，會確認內部和外部的利害關係人，以及這些利害關係人涉及學校個人資料管理系統治理的程度，每年定期完成組織 PIMS 全景評鑑。

八、 本校確保個人資料管理系統之管理皆由特定職責且承擔責任的人員負責。

參、適用範圍、目標與義務

一、 範圍

本管理系統適用範圍包含全校各單位，涉及個人資料的蒐集、處理與利用相關業務，包含之文件紀錄、資訊系統、軟硬體設備、人員與作業程序。

二、目標

本校依據我國個資保護法規暨 BS 10012 國際標準，制定 PIMS 目標，作為本校評鑑個資保護機制運作良窳之基準， PIMS 目標由個人資料保護技術評估小組負責制訂，經個人資料保護推動委員會審核後實施，並應將執行結果紀錄於「PIMS 目

標執行成效評鑑表」，納入管審會議審核。

三、義務

本校蒐集、處理與利用個人資料時應履行下列之義務：

（一） 個人資料之蒐集、處理與利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

（二） 本校依個人資料保護法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：

1. 本校名稱。
2. 蒐集之目的。
3. 蒐集個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人依個人資料保護法第三條規定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。

（三） 非由當事人提供之個人資料，應於處理或利用前，或對當事人首次利用時，向當事人告知個人資料來源及前條所列事項。

（四） 本校應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。

（五） 本校應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。

（六） 本校若發生違反個人資料保護法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

肆、適用法律規定

本校個人資料管理系統適用個人資料保護法、個人資料保護法施行細則、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實施辦法等法規。

伍、名詞解釋

一、 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理

之個人資料之集合。

三、 蒐集：指以任何方式取得個人資料。

四、 處理：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。

五、 利用：指將蒐集之個人資料為處理以外之使用。

六、 當事人：指個人資料之本人。

七、 資訊安全：保護資訊的機密性、完整性與可用性。

八、 風險評估：以有系統的方式使用資訊，進而辨識風險的來源，將預估與既定的風險標準比較，以決定風險的重要性。

九、 風險處理：選擇與實施修正風險的措施。

十、 機敏等級：個人資料檔案依其個人資料內容可能包含多種的個人資料類別。機敏等級指對不同的個人資料類別所隱含的機密性與敏感度所給予的評價。一般個人資料的機敏等級可對應成個人資料的價值。

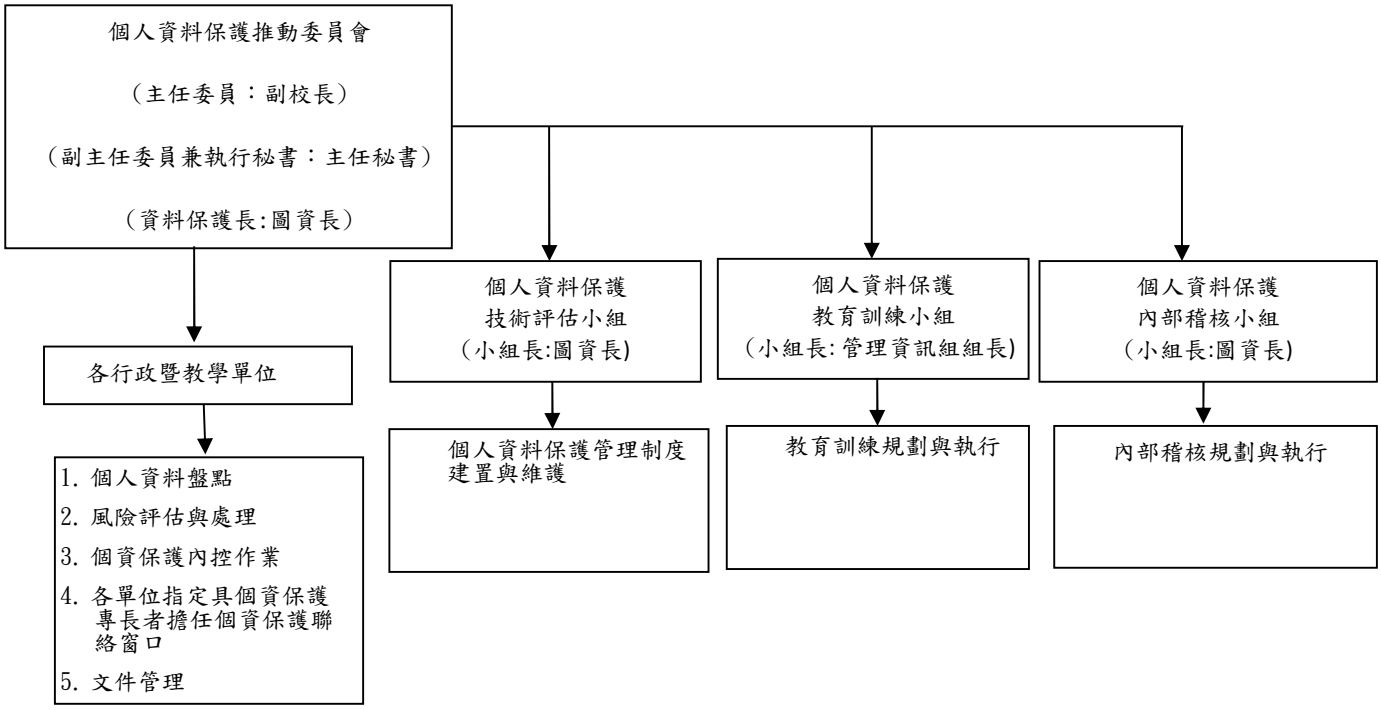
十一、 機密等級：個人資料檔案依其個人資料內容可能包含多種的個人資料類別。個人資料檔案依其所含個人資料類別中最高之機敏等級，對應為該個人資料檔案之機密等級。

十二、 個人資料類別清單：考量本校實際蒐集之個人資料，依據個人資料保護法個人資料之類別，修改為適用本校之個人資料類別清單，並定義各種個人資料類別的機敏等級。

## 陸、組織與職責

### 個人資料保護推動組織架構與工作職掌

一、 個人資料保護推動組織架構如下圖所示：




二、 個人資料保護推動組織各層級之工作職掌分述如下：

| 推動組織 | 職稱 | 負責單位/人員 | 職責 |
|---|---|---|---|
| 個人資料保護推動委員會 | 主任委員 | 副校長 | ● 督導本校個人資料保護業務推動<br>● 副主任委員兼任本校個人資料保護業務對外聯絡窗口<br>● 資料保護長應確保適當的隱私衝擊評估與風險評估符合法律、法規與營運要求，並確實完成<br>● 資料保護長應於必要時向主管機關回報(現階段無回報必要)<br>● 組織 PIMS 全景評鑑審核 |
| | 副主任委員兼執行秘書 | 主任秘書 | |
| | 資料保護長 | 圖資長 | |

| | | | |
|---|---|---|---|
| 個人資料保護內部稽核小組 | 小組長 | 圖資長 | ● 內部稽核規劃與執行作業<br>● 出列席個人資料保護管理審查會議 |
| | 成員 | 由具專業證照人員擔任(BS 10012或其他個資保護相關) | |
| 個人資料保護技術評估小組 | 小組長 | 圖資長 | ● 小組長擔任執行秘書職務代理人<br>● 個人資料保護管理制度建置與維護<br>● 執行個人資料保護政策、目標研擬及各階文件增修訂管制<br>● 定期執行個人資料保護驗證、稽核及管理審查等業務<br>● 定期召開個人資料保護推動委員會 |
| | 成員 | 由小組長遴選 | |
| 個人資料保護教育訓練小組 | 小組長 | 圖書資訊處管理資訊組組長 | ● 本校教職員工個人資料保護教育訓練規劃與執行<br>● 建立年度個人資料保護教育訓練計畫表<br>● 訓練紀錄建立與維持<br>● 訓練經費編列與運用 |
| | 成員 | 由小組長遴選 | |
| 各行政暨教學單位 | ● 個人資料盤點<br>● 風險評估與處理<br>● 個資保護內控作業<br>● 各單位指定具個資保護專長者擔任個資保護聯絡窗口<br>● 辦理委外作業廠商之個人資料委外安全評估或查核<br>● 文件管理 | | |

三、 個人資料保護推動組織重要會議暨召開時機：

| 會議名稱 | 會議主持人 | 召開時機 | 參與人員 | 會議重點 |
|---|---|---|---|---|
| 個人資料保護推動委員會 | 主任委員（副校長） | 每學年至少召開一次 | 個人資料保護推動委員會委員 | ● 審查本校個人資料保護政策、目標及一階文件<br>● 審查年度個人資料保護績效指標<br>● 審查各單位個人資料保護 |

| | | | | |
|---|---|---|---|---|
| | | | | 年度工作報告<br>● 審查本校對個人資料保護法律及優良實務的遵循狀況<br>● 審查個人資料保護策略<br>● 審查個人資料管理制度<br>● 組織 PIMS 全景評鑑審核 |
| 管理審查會議 | 副主任委員 | 視需要不定期召開、每年至少召開一次 | 主任秘書為當然委員。<br>行政單位現任或曾任主管之代表 1-2 人、教學單位現任或曾任主管之代表 1-2 人、圖資長、圖書資訊處管理資訊組組長、以及具有個資保護實務經驗之校內外學者專家 1-2 人等組成，委員人數以 6-9 人為原則。委員由校長遴選聘任之。 | ● 審核個人資料檔案風險處理計畫<br>● 審查各單位個人資料盤點結果<br>● 審查各單位風險評估結果<br>● 決定本校之可接受風險值<br>● 檢討年度個人資料保護績效指標<br>● 審查內部稽核報告<br>● 本校二、三、四階文件增修訂審查<br>● 訴願處理<br>● 個人資料事件處理、管制與向上通報<br>● 組織 PIMS 全景評鑑 |

柒、資源提供

透過個人資料保護推動委員會決議事項，籌獲個人資料保護作業所需之適當資源，以持續改善其運作之績效。

捌、教育訓練

一、 教育訓練應確保各行政暨教學單位在處理個人資訊及相關業務時可知悉個人資料保護職責，得以遵循個人資料保護相關標準、法規與優良實務要求，全體人員並應接受適合本身職責所需之教育訓練。

二、 教育訓練的類型：教育訓練依類型可分為新進人員訓練、一般訓練、專業訓練。

（一） 新進人員訓練：配合人事室新進人教育訓練，課程內容應包含個人資料保護觀念與本校個人資料管理作業流程介紹。

（二） 一般訓練：一般訓練包含意識提升與作業流程說明。課程內容置重點於個人資料保護政策、責任、程序等要求事項或觀念之傳達，並應考量相關安全要求，以提昇整體處理個人資料之風險覺知。

（三） 專業訓練：強化負責個人資料保護業務執行人員之專業知識與技能，應提供相關人員個人資料專業教育或技術訓練。

三、 教育訓練實施：

（一） 教育訓練小組，應於每年度結束前，規劃下一年度之個人資料保護教育訓練計畫表。

（二） 教育訓練成效除依年度「個人資料保護教育訓練計畫表」執行外，應蒐集其他個資保護教育訓練成果紀錄備查。

## 玖、個人資料管理程序

一、 個人資料保護原則

（一） 公平及合法的處理。

（二） 僅為了特定目的取得，且不進行不合於該目的之處理。

（三） 適當、相關且不過度。

（四） 保持正確及最新。

（五） 不保存超過需求的時間。

（六） 遵循法定的個人權利包括個人資料當事人對於其資料的存取。

（七） 確保安全。

（八） 不將資料傳輸到法令所不允許及沒有足夠保護的國家。

二、 本校依據 BS 10012、個人資料保護法、施行細則，建立「P-1-01-01 個資文件階層參照表」，以對應四階程序文件，落實個資保護管理系統建置。

三、 個人資料檔案風險評估與管理

制訂相關程序書並要求本校各一、二級單位應針對個人資料檔案進行風險分析採取措施，以確保個人資料檔案可受到適當之保護，相關單位作業應包含：

（一） 進行個人資料盤點，並依類別建立個人資料類別清單。

（二） 個人資料盤點清冊應定期與不定期檢視並修訂。

（三） 評估個人資料之價值，檢視評估個人資料類別清單中發生被竊取、竄改、毀損、滅失或洩漏等事件，將對個人與組織所可能產生之衝擊程度。

（四） 進行風險值評估，應檢視個人資料類別清單，判定可能存在的威脅與弱點，並評定其風險等級，產生風險評估報告。

（五） 依據校定之可接受風險等級，應針對不可接受風險之個人資料相關資產，規劃風險處理計畫並進行處理。

四、 個人資料蒐集、處理與利用管理

制訂相關程序書並要求本校各一、二級單位應確保蒐集的個人資料在特定目的下適當且不過度，並且讓當事人的個人資料能被公平與合法的處理，相關單位作業應包含：

（一）確認具備特定目的，並符合法律規定之特定情形。

（二）蒐集資料應依法向當事人告知法定事項。

（三）提供當事者都可容易取得的隱私權公告或聲明。

（四）特種個人資料之蒐集、處理、利用要求與限制。

（五）向第三方蒐集資料應建立契約或協議。

（六）除已經以任何方式公開之個人資料外，均應依資料類別建立相關安全作業的機制。

（七）記錄、輸入、編輯及更正個人資料應該進行資料審核並留下紀錄。

（八）因可歸責於本校的事由而未進行更正或補充之個人資料，應於更正或補充後，通知當事人。

（九）含個人資料之書面文件與磁性媒介，應建立安全保護措施。

（十）書面文件與磁性媒介的傳輸，應依機密等級採用適當傳遞方式。

（十一）建立個人資料蒐集特定目的消失或期限屆滿或業務終止之處理方式。

（十二）應明確界定本校執行相關業務服務或為行銷、研究調查目的之使用的必要範圍。

（十三）利用個人資料對當事人進行第一次行銷或研究時，應提供當事人拒絕行銷或研究的機制，並支付所需費用。

（十四）個人資料的公開，應有公開特定目的，並對個人資料做適當處理，保障個人隱私。

（十五）對於資料的傳輸方式應做規範，並有依據經過審核同意，且留下紀錄，

以保護傳輸期間的資料安全。

（十六）因業務需求需將個人資料移轉到本國以外的地方，確保個人資料的處理與利用符合法令規範並受到保護。

五、 個人資料權利行使管理

制訂相關程序書並要求本校各一、二級單位應依個人資料法規定個人資料當事人享有之權利，訂定本校對於個人權利行使之方式與流程，相關單位作業應包含：

（一）提供當事人依個人資料法享有之權利。

（二）當事人各項權利行使方式與流程。

（三）當事人各項權利行使所需費用評估。

（四）對當事人請求之回覆要求。

（五）當事人針對個人資料案件申訴作業。

六、 隱私權告知管理

制訂相關程序書並要求本校各一、二級單位應依據個人資料法規定，向當事人蒐集個人資料時，應明確對當事人履行告知義務。對於隱私權告知內容與方式應有規範，各單位作業應包含：

（一）隱私權告知時機與方式

（二）隱私權告知聲明內容修(新)訂

（三）隱私權公告版本控制與紀錄保留

七、 個人資料安全作業管理

制訂相關程序書並要求本校各一、二級單位應確保個人資料能受到安全保護，對於如資訊系統、資訊設備或個人電腦之使用需有安全作業規定，相關作業需保存紀錄，並定期進行檢核，確保作業安全，相關單位作業應包含：

（一）資訊應用系統開發與建置、系統使用、系統資料交換與連結等安全機制建立。

（二）資訊應用系統的稽核與資料備份。

（三）資訊設備使用與維護安全。

（四）資訊設備報廢作業。

（五）資訊系統與個人電腦密碼安全規定。

（六）個人資料檔案稽核管理。

（七）紀錄與證據之保存。

八、 個人資料事件管理

制訂相關程序書並要求本校各一、二級單位應針對個人資料安全事件的發生，即刻進行反應，並採取適當的處理措施，降低損害的擴大，列入後續改正參考，以杜絕類似事件再發生，有效降低威脅，相關單位作業應包含：

（一）建立資訊與個人資料安全事件通報流程，包含內部通報與外部通報。

（二）資訊與個人資料安全事件處理，作業內容應記錄備查，並經由權責人員審視確認。

（三）事件處理前，應確實做好證據保存工作，如為數位證據應先備份。

（四）定期彙總進行事件分析，以採取適切管控措施。

九、 個人資料委外作業管理

制訂相關程序書並要求本校各一、二級單位應於委託他人蒐集、處理或利用個人資料時，對委外單位做適當之監督。對於涉及個人資料之委外作業應做管制，相關單位作業應包含：

（一）委外廠商應訂定選擇標準並進行評鑑。

（二）各項管理措施均應明文規範於委外合約或相關契約文件中。

（三）委外廠商或人員個人資料保護措施，包含資訊安全措施與員工管控。

（四）受託單位再轉包其工作之管制與管理。

（五）委託關係終止或解除之設備歸還與資料刪除。

（六）委託者之行政監督義務。

十、 內部稽核管理

制訂相關程序書並要求本校各一、二級單位應針對個人資料保護各項管理機制，需經由內部稽核機制進行監控與審查，以確保個人資料管理系統運行達到預期目標。藉由內部稽核作業，瞭解各項作業執行之成效，以作為持續維護個人資料管理制度之參考。透過稽核結果進行改善與預防，確保個人資料管理制度之有效性及持續改善，相關單位作業應包含：

（一）稽核規劃與稽核人員的選擇。

（二）建立個人資料保護稽核檢查表。

（三）定期或不定期進行管理階層審查。

十一、 矯正預防管理

制訂相關程序書並要求本校各一、二級單位應確保任何有關現有或潛在不合格事

項能及時採取有效之對策，經由適當的矯正及預防措施處理，防止類似問題再次發生，達到持續改善之目的，相關單位作業應包含：

（一）發現呈異常情況時須進行矯正改善。

（二）依據適切的資料來源採取預防措施。

十二、使用生物特徵管理規範

制訂相關規範並要求本校各一、二級單位應確保蒐集生物特徵個人資料不逾越特定目的之必要範圍，尊重當事人之權益，並遵循教育部使用生物特徵辨識技術個人資料保護指引之規範，相關單位作業應包含：

（一）蒐集資料應依法向當事人告知法定事項。

（二）確認具備特定目的，並符合法律規定之特定之情形。

拾、管理責任

本校管理階層需規劃符合校方或政府相關法令規範要求之個人資料政策及目標，每年應訂定並發布績效衡量指標、完成內部稽核，並應於個人資料保護推動委員會議中，提出績效指標達成現況統計值，透過管理審查活動，瞭解本管理系統之適法性與有效性，進而修正本管理系統，以達持續改善之目的。

一、 PIMS 監控、量測、分析和評估

（一） 應決定何者需要被監控和量測，監控、量測、分析和評估方法宜確保其有效之結果、監控和量測應律定執行時機、對監控和量測結果進行分析與評估的時機。應留存適當的文件化資訊，作為監控、量測、分析和評估之證據，應評估 PIMS 的績效與有效性。

（二） 應將執行結果紀錄於「PIMS 目標執行成效評鑑表」，並納入管審會議審核。

二、 於內部稽核執行後召開管理審查會議，檢討稽核結果處理狀況、管理系統可改善之機會，及審查管理系統是否可維持其適法性、充分性與有效性。

三、 管理審查會議中需檢討下述各項資訊：高階管理者應在規劃期間內審查組織的 PIMS，以確保其持續的適切性、充分性及有效性。管理審查應考量:

（一） 上次審查會議議決事項之成果追蹤檢討。

（二） 與 PIMS 有關之內外部議題的變更。

（三） 內、外部稽核報告及矯正與預防措施效果確認。

（四） 個資目標執行績效審查，包括下列趨勢:不符合事項與矯正措施、監控與量測結果、稽核結果。

（五） 程序審查和紀錄及個資管理系統意見回饋。

（六） 持續改善機會，包括改善資源需求規劃、技術升級及持續不斷改善狀況報告。

（七） 組織 PIMS 全景評鑑、上級主管機關的正式評估請求、檢查結果及要求改善等。

（八） 由人員識別風險及變化、風險評估結果與風險處理狀態。

（九） 使用者回饋、訴怨及當事人權利行使處理。

（十） 已經發生的違反與安全事件。

（十一） 資料保護長法律、法規與營運要求遵循性檢討與報告。

（十二） 臨時動議。

四、 管理審查會議結果需包含以下事項之決策目標及行動方式：

（一） 個人資料管理制度之政策、程序、作業及表單，是否需要進行修正。

（二） 審查會議依據審查及討論事項之內容，應將個人資料管理審查結果製作成會議紀錄，以利後續之改善追蹤。

（三） 管理審查之輸出包括與持續改善機會有關之決策，及任何對 PIMS 變更之需要，例如:確認可能影響遵循的政策、程序或技術修正。應保存管理審查文件化資訊，以作為管理審查結果之證據。如遇重大變更，應在執行完畢後盡快完成稽核。

拾壹、使用表單：

一、 個資文件階層參照表。(P-1-01-01)

二、 個人資料保護教育訓練計畫表。(P-1-01-02)

三、 PIMS 目標執行成效評鑑表。(P-1-01-03)

四、 組織 PIMS 全景評鑑表。(P-1-01-04)