（十三）共通事項

◎個人資料安全保護管理作業

1. 流程圖：如圖5_13_1（置於文件後）。

2. 作業程序：

2.1. 人員管理：

2.1.1. 指定蒐集、處理及利用個人資料個別作業（以下簡稱「作業」）流程之負責人員。

2.1.2. 就個別作業設定所屬人員不同之權限並控管之，以一定機制管理其權限，且定期確認權限內容設定之適當與必要性。

2.1.3. 要求所屬人員負擔相關之保密義務。

2.2. 作業管理：

2.2.1. 運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，依循「電腦設備安全暨資訊機密維護規則」。

2.2.2. 針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。

2.2.3. 作業過程有備份個人資料之需要時，比照原件，依個人資料保護法（以下簡稱「個資法」）規定予以保護之。

2.2.4. 個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，嗣該媒介物於報廢或轉作其他用途時，採適當防範措施，以免由該媒介物洩漏個人資料。

2.2.5. 委託他人執行前款行為時，對受託人依個資法施行細則第八條規定為適當之監督，並明確約定相關監督事項與方式。

2.3. 物理環境管理：

2.3.1. 依作業內容之不同，實施必要之門禁管理。

2.3.2. 妥善保管個人資料之儲存媒體。

2.4. 技術管理：

2.4.1. 於電腦、相關設備或系統上設定認證機制，帳號及密碼使其具備一定安全之複雜度並定期更換密碼。

2.4.2. 於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。

2.4.3. 對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。

2.4.4. 具備存取權限之終端機不得安裝檔案分享軟體。

2.4.5. 定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。

2.5. 認知宣導及教育訓練：

2.5.1. 各單位應要求所屬人員參與個資法認知宣導及教育訓練，使其明瞭個人資料保

護相關法令之要求、所屬人員之責任範圍及各種作業程序。

2.6. 紀錄機制：

2.6.1. 個人資料交付、傳輸之紀錄。

2.6.2. 確認個人資料正確性及更正之紀錄。

2.6.3. 提供當事人行使權利之紀錄。

2.6.4. 所屬人員權限新增、變動及刪除之紀錄。

2.6.5. 個人資料刪除、廢棄之紀錄。

2.6.6. 教育訓練之紀錄。

2.7. 委外與自我檢核管理：

2.7.1. 進行個人資料之蒐集、處理及利用時須自我檢核是否符合法令法規，並於每學期填報「慈濟科技大學個人資料保護管理制度檢核表」，送交本校個資保護聯絡窗口備查。

2.7.2. 委外進行個人資料之蒐集、處理及利用時須於契約中明確約定相關監督事項與方式，並要求受任人(廠商)填報「慈濟科技大學委外處理個人資料保護管理制度檢核表」自我檢核後，送交委任單位複檢。

3. 控制重點：

3.1. 人員管理

3.1.1. 是否指定進行個人資料之蒐集、處理及利用個別作業流程之負責人員。

3.1.2. 是否就個別作業流程設定所屬人員不同之權限並控管。

3.1.3. 處理個人資料檔案之人員，是否簽訂保密同意書。

3.2. 作業管理

3.2.1. 是否建立與維護個人資料檔案清冊。

3.2.2. 是否依個資法規定進行告知並徵求同意。

3.2.3. 是否依循本校「電腦設備安全暨資訊機密維護規則」。

3.2.4. 是否針對保有之個人資料檔案採取適當之防護或加密機制。

3.2.5. 是否針對有備份必要之個人資料，定期進行備份資料之還原測試，以確保備份之有效性。

3.2.6. 儲存個人資料之媒體於廢棄或移轉與他人前，是否確實刪除媒體中所儲存之資料，或以物理方式破壞之，以避免資料不當外洩。

3.2.7. 委託他人執行前款行為時，是否對受託人依個資法施行細則第八條規定為適當之監督，並明確約定相關監督事項、方式、義務及責任。

3.3. 物理環境管理

3.3.1. 針對個資蒐集之書面或電子資料，是否妥善保管並存放至有門禁管理或上鎖之鐵櫃內。

3.3.2. 是否指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施。

3.4. 技術管理

3.4.1. 個人資料檔案之處理行為是否設置使用者代碼及密碼。

3.4.2. 處理個人資料檔案終端主機登入密碼是否依循設定規則(每六個月至少更換一次，長度應至少8碼，且包含文數字)。

3.4.3. 儲存個人資料之終端主機是否安裝防毒軟體，並定期更新病毒碼。

3.4.4. 儲存個人資料之終端主機是否定期檢視、更新作業系統、應用程式漏洞。

3.4.5. 是否對轉交或傳輸行為加以記錄流向備查。

3.4.6. 處理個人資料檔案之人員，其職務如有異動，是否將所保管之儲存媒體及有關資料列冊移交。

3.4.7. 個人資料檔案是否禁止存放於網路芳鄰分享目錄。

3.4.8. 是否禁止個人資料檔案處理人員使用如Skype等即時通訊軟體傳輸個人資料檔案。

3.4.9. 是否禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案。

3.4.10. 是否禁止使用點對點(P2P)軟體及Tunnel相關工具下載或提供分享檔案。

3.4.11. 是否禁止在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。

3.5. 認知宣導及教育訓練

3.5.1. 處理個人資料檔案之人員是否參與資訊安全與個資隱私保護之教育訓練（內、外訓皆可）。

3.5.2. 是否定期於單位內宣導個資隱私保護之重要性。

3.6. 紀錄機制

3.6.1. 單位所管理之網站或網頁內容，於確有必要公布個人資料時，是否經所屬單位主管核准。

3.6.2. 對於個人資料之調閱是否經申請並核准。

3.6.3. 是否加以記錄調閱個人資料者之身分及行為。

3.6.4. 是否針對以下個人資料處理相關活動，評估及進行紀錄的保存，以為未來舉證等用途。

3.6.4.1. 個人資料交付、傳輸之紀錄。

3.6.4.2. 確認資料正確性及更正之紀錄。

3.6.4.3. 提供當事人行使權利之紀錄。

3.6.4.4. 權限新增、變動及刪除之紀錄。

3.6.4.5. 個人資料刪除、廢棄之紀錄。

3.6.4.6. 參與教育訓練之紀錄。

3.7. 委外與自我檢核管理

3.7.1. 是否定期填報「慈濟科技大學個人資料保護管理制度檢核表」。

3.7.2. 個資委外處理是否填報「慈濟科技大學委外處理個人資料保護管理制度檢核

表」。

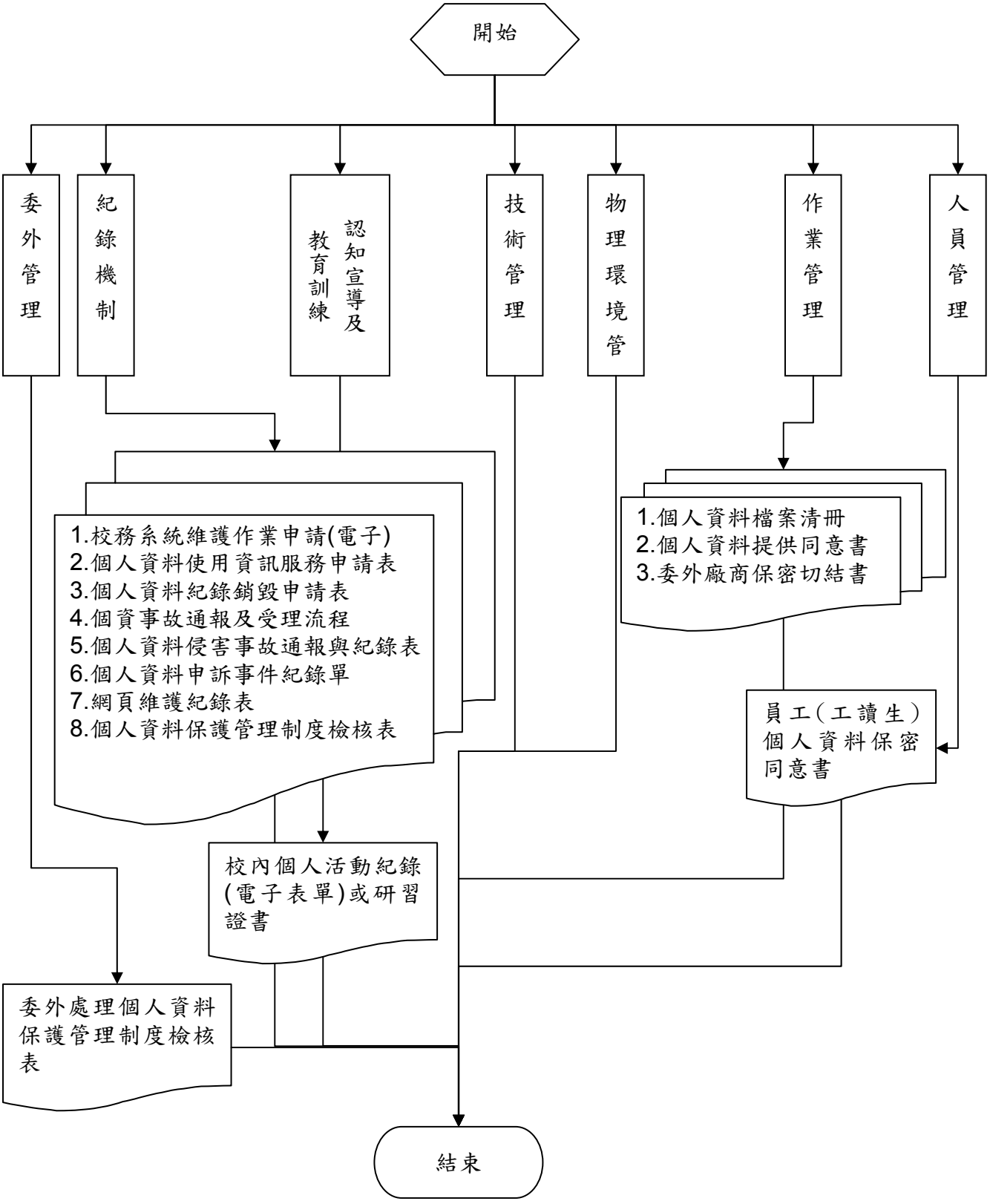
4. 使用表單：

4.1. 員工(工讀生)個人資料保密同意書。
4.2. 委外廠商保密切結書。
4.3. 個人資料檔案清冊與風險評鑑表。
4.4. 個人資料使用資訊服務申請表。
4.5. 個人資料紀錄銷毀申請單。
4.6. 個資事故通報及受理流程。
4.7. 個人資料侵害事故通報與紀錄表。
4.8. 個人資料申訴事件記錄單。
4.9. 個人資料提供同意書。
4.10. 網頁維護紀錄表。
4.11. 校務系統維護作業申請(電子表單)。
4.12. 校內個人活動紀錄(電子表單)。
4.13. 慈濟科技大學委外處理個人資料保護管理制度檢核表
4.14. 慈濟科技大學個人資料保護管理制度檢核表。

5. 依據及相關文件：

5.1. 個人資料保護法。
5.2. 個人資料保護法施行細則。
5.3. 慈濟學校財團法人慈濟科技大學電腦設備安全暨資訊機密維護規則。
5.4. 慈濟學校財團法人慈濟科技大學校園網路使用管理規範。
5.5. 隱私權政策聲明。
5.6. 慈濟學校財團法人慈濟科技大學個人資料保護管理要點。
5.7. 102年度教育機構個人資料保護工作事項

5.8. 圖5_13_1


開始
委外管理
紀錄機制
認知宣導及教育訓練
技術管理
物理環境管
作業管理
人員管理
1.校務系統維護作業申請(電子)
2.個人資料使用資訊服務申請表
3.個人資料紀錄銷毀申請表
4.個資事故通報及受理流程
5.個人資料侵害事故通報與紀錄表
6.個人資料申訴事件紀錄單
7.網頁維護紀錄表
8.個人資料保護管理制度檢核表
1.個人資料檔案清冊
2.個人資料提供同意書
3.委外廠商保密切結書
員工(工讀生)個人資料保密同意書
校內個人活動紀錄(電子表單)或研習證書
委外處理個人資料保護管理制度檢核表
結束