輔仁大學

個人資料保護管理手冊

機密等級：公開使用

文件編號：PIMS-A-001

版　　次：1.0

發行日期：103.12.05

修訂紀錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	103.12.05			發佈

個人資料保護管理手冊					
文件編號	PIMS-A-001	機密等級	內部使用	版次	1.0

個人資料保護管理手冊					
文件編號	PIMS-A-001	機密等級	內部使用	版次	1.0

1 目的

遵循「個人資料保護法」、「個人資料保護法施行細則」及教育部行政命令、函釋等，建立個人資料安全管理規範，以確保輔仁大學(以下簡稱本校)各項業務所蒐集、處理及利用之個人資料相關作業，能有效進行管理與保護並不逾越法律規範。

2 適用範圍

本校內含有與個人資料相關的業務流程及個人資料檔案(包括備份檔案)

3 權責

3.1 個人資料管理委員會

3.1.1 本校個人資料保護政策之研議。

3.1.2 本校個人資料管理制度之審議、評估及推展。

3.1.3 本校個人資料隱私風險之評估及管理。

3.1.4 本校個人資料保護教育訓練之規劃。

3.1.5 本校個人資料損害預防及危機應變之處理。

3.1.6 本校個人資料保護管理跨部門協調與整合。

3.1.7 本校個人資料保護全般執行審查及持續改善。

3.2 執行分組

3.2.1 政策研擬與提案

3.2.2 辦理推廣訓練

3.2.3 協助各項個資業務管理之落實

(1) 協助管理代表（召集人）推行個資管理。

(2) 依相關法令辦理安全維護及保管事項。

(3) 傳達管理代表（召集人）之決策，以貫徹個資管理。

(4) 協調各組使組織相關個人資料保護之運作更落實。

(5) 彙集、轉陳各組之意見、資料，供管理代表（召集人）作最佳決策。

(6) 協助追蹤、管理個人資料保護稽核所提相關建議事項。

(7) 定期蒐集、分析及陳報個資相關通報及執行狀況之報告。

3.3 稽核分組

3.2.1 研提年度個人資料與隱私保護管理稽核計畫。

3.2.2 配合年度稽核計畫執行相關稽核活動並提供改善建議事項予管理委員會。

3.2.3 對外查核業務之規劃與執行作業。

3.2.4 配合主管機關的行政檢查作業。

3.4 全體同仁

3.4.1 遵守本校「個人資料保護管理手冊」內規定事項。

4 名詞定義

4.1 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。

4.2 個資檔案

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、整理之個資之集合。

4.3 蒐集

指以任何方式取得之個人資料。

4.4 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。

4.5 利用

指將蒐集之個人資料為處理以外之使用。

4.6 國際傳輸

指將個資作跨國（境）之處理或利用。

4.7 公務機關

指依法行使公權力之中央或地方機關或行政法人。

4.8 非公務機關

指公務機關以外之自然人、法人或其他團體。

4.9 當事人

指個人資料之本人。

4.10 個人：

指現生存之自然人。

5 個資管理原則

5.1 個資蒐集或蒐集非由當事人提供之個人資料，除以下免告知項目外，均應於處理或利用前，向當事人告知個人資料來源：

5.1.1 依法律規定得免告知。

5.1.2 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

5.1.3 告知將妨害公務機關執行法定職務。

5.1.4 告知將妨害第三人之重大利益。

5.1.5 當事人明知應告知之內容。

5.1.6 當事人自行公開或其他已合法公開之個資。

5.1.7 不能向當事人或其法定代理人為告知。

5.1.8 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

5.2 有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料（以下簡稱特殊個人資料)，不得蒐集、 處理或利用。但有下列情形之一者,不在此限:

5.2.1 法律明文規定。

5.2.2 履行法定義務所必要，且有適當安全維護措施。

5.2.3 當事人自行公開或其他已合法公開之個人資料。

5.2.4 基於醫療、衛生或犯罪預防之目的,為統計或學術研究而有必要,且經一定程序所為蒐集、處理 或利用之個人資料。

5.3 蒐集、處理及利用時應確認符合本校業務相關法定目的，並符合下列情形：

5.3.1 執行法定職務必要範圍內。

5.3.2 經當事人書面同意。

5.3.3 對當事人權益無侵害。

5.4 如遇進行本校業務相關法定目的或行使法定職權目的外的蒐集、處理及利用時，應符合下列情形之一：

5.4.1 法律明文規定。

5.4.2 為維護國家安全或增進公共利益。

5.4.3 為免除當事人之生命、身體、自由或財產上之危險。

5.4.4 為防止他人權益之重大危害。

5.4.5 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

5.4.6 有利於當事人權益。

5.4.7 經當事人書面同意。

5.5 應尊重當事人對其個資的權利，資料當事人查詢或請求閱覽個資，給予複製本，或要求補充、更正、刪除、停止使用個資，應依據個資請求相關流程辦理。

5.6 使用個資應正確告知資料使用目的與使用方式，非免告知事項並應以書面方式取得同意。

5.7 蒐集個資僅以業務所需為範圍，對於非業務所需資料應避免蒐集與使用。

5.8 個資應保持正確性與即時性，並保護個資之蒐集、處理、利用及儲存時的安全性，防止個資被竊取、竄改、 毀損、滅失或洩漏。

5.9 個資如需傳遞出國境，應確認接受或處理資料單位具有安全保護機制後，始得進行資料傳遞作業。

5.10 蒐集或處理者知悉或經當事人通知禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

5.11 個資被竊取、洩漏、竄改或其他侵害事件，則應依據事件情節將安全事件等級列為 3 或 4 級資安事件。

5.12 本校所有與個人資料相關之作業流程的個資檔案需要進行盤點及風險評估，作業說明詳見 PIMS-B-003「個人資料盤點及風險評估作業管理程序書」。

5.13 本管理原則應依照 PIMS-B-004「個人資料文件及紀錄管理程序書」，進行相關文件審查作業。

6 個資管理程序

6.1 建立當事人通知管道

6.1.1 建立對個資當事人的通知管道，如書面通知、隱私權聲明或個資作業公告，告知當事人個資行使之權利及方式。

6.1.2 隱私權聲明或個資作業公告內容應包含下列資訊：

6.1.2.1 保有單位名稱及聯絡方式

6.1.2.2 個資檔案名稱

6.1.2.3 個資之類別

6.1.2.4 個資檔案保有之依據及特定目的

6.1.2.5 個資利用之期間、地區、對象及方式。

6.1.2.6 當事人可以行使之權利及方式，包括：

6.1.2.6.1 查詢或請求閱覽。

6.1.2.6.2 請求製給複製本。

6.1.2.6.3 請求補充或更正。

6.1.2.6.4 請求停止蒐集、處理或利用。

6.1.2.6.5 請求刪除。

6.1.2.7 可自由選擇提供個資業務，應說明當事人不提供資料時將對其權益所產生的影響。

6.1.2.8 該業務是否其個資會傳遞出其他沒有適切保護個資的國家。

6.2 個資蒐集

6.2.1 直接蒐集資料應告知目的與書面同意

6.2.1.1 蒐集的個資如非屬法律規定、執行法定業務或免告知（見本手冊 5 個資管理原則）事項，應該在文件表單明顯位置說明告知事項，並視需求規劃同意欄位。

6.2.1.2 個資告知事項包括資料具體的使用目的、範圍及同意與否對其權益之影響。

6.2.1.3 提供下列書面同意方式其中一項，由資料當事人同意後，始能使用該資料。

6.2.1.3.1 書面同意：於紙本文件表單上簽名同意。

6.2.1.3.2 契約同意：以契約或協議方式，如以定型化契約行為表達同意。

6.2.1.3.3 電子簽章同意：以符合電子簽章法規範之機制表達同意。

6.3 個資處理

6.3.1 個資處理包含記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送等作業，除了經任何方式已合法公開之個資外均應依資料類別建立相關安全作業的機制。

6.3.2 記錄、輸入、編輯、更正與輸出

6.3.2.1 記錄、輸入、編輯及更正個資應該進行資料審核並留下紀錄。

6.3.2.2 應訂定資料錯誤更正的作業流程，並應留下資料更正紀錄。

6.3.2.3 記錄、輸入、編輯及更正等作業應定期進行審查，確保資料的正確性與完整性。

6.3.2.4 業務處理過程中產生與使用個資之資料及報表，應依資料類別標示機密等級，並僅供已授權單位或人員使用。

6.3.2.5 資料輸出報表與交換使用，應經核可並保存相關紀錄。

6.3.2.6 因可歸責於本校的事由而未進行更正或補充之個資，應於更正或補充後，通知當事人。

6.3.3 儲存

6.3.3.1 含個資之書面文件與磁性媒介存放時，需加鎖或以管制區域保護，避免遭人任意檢視或拿取，僅開放給授權存取之人存取，並不可在公開場合使用。

6.3.3.2 個人使用含個資之書面文件與磁性媒介時，確實遵守安全保護要求，離座或下班時不可遺留於桌面或機器設備上。

6.3.3.3 含個資之書面文件與磁性媒介，未經部門主管同意並作成紀錄不得攜帶外出或拷貝複製。

6.3.3.4 磁性媒介在媒介上依資料類別標示機密等級，磁碟片或磁帶貼上紅色圓貼紙，CD 光碟片，則以手寫方式直接書寫於 CD 光碟片上。

6.3.3.5 電子檔案存放時以硬體設備或加密方式保護，避免遭人任意檢視或複製。

6.3.3.6 個人使用電子檔案時，確實遵守要求，離座時需啟動電腦螢幕保護裝置，下班時除非特殊考量，需將個人使用設備關機或以密碼鎖定保護。

6.3.3.7 重要個資備份應異地存放，並置有防火設備及可上鎖檔案櫃保護，以防止資料滅失或遭竊取。

6.3.4 傳輸

6.3.4.1 含個資之書面文件與磁性媒介於內部人工傳送時，請親自或專人負責傳送。

6.3.4.2 含個資之書面文件與磁性媒介以郵件方式傳送到外部時，須以雙信封封

存，並於內封加蓋「密」字，再以掛號方式寄出。

6.3.4.3 含個資之書面文件掃瞄、列印、影印或傳真時，應由處理人員立即取走，不可任由文件遺留於機器上。

6.3.4.4 含個資之電子檔案如需以 e-mail 或 FTP 等電子傳送方式須加密始得傳輸。並以適當的方式保存與傳送密碼予對方。密碼可透過電話告知或另外發一封 e-mail 告知，勿打在同一封 e-mail 內。

6.3.5 刪除與報廢

6.3.5.1 含個資之書面文件之資料，不可再生利用，一律使用碎紙機將文件銷毀。

6.3.5.2 含個資之磁性媒介須報廢或不堪再使用時，依媒介性質則由個人或資訊單位人員以燒毀、粉碎或使用其他應用程式或工具清除資料或銷毀該媒介，使其無法以任何工具或方法復原。

6.3.5.3 含個資之電子檔案需刪除時，應由保管人確認其已被確實刪除。

6.4 個資利用

6.4.1 應明確界定單位上執行相關業務服務或為行銷或研究調查目的之使用的必要範圍，包括業務承辦單位與受委託單位。

6.4.2 利用個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。

6.5 國際傳輸（處理利用）

如因業務需求需將個人資訊移轉到本國以外的地方，確保個資的處理與利用符合法令規範並受到保護，包括：

6.5.1 確認教育部或其他與本校有關主管機關是否明令禁止或限制與本校持有個人資料進行國際傳輸。

6.5.2 在資料傳輸雙方的合約或協議中載明個資保護與符合目的處理與利用的條件，以確保個資與該資料的處理受到保護及規範。

6.5.3 在移轉到外國前，應先確認個資將被移轉的單位是否已提出符合該國個資與貿易相關法令要求的證明。

6.5.4 確認目的地國家或地區是否已被評估為能夠提供充足的保護。

6.5.5 建立對該資料傳輸目的地組織進行監督與評估，以確保個資處理及利用的安全。

6.6 個資蒐集特定目的消失或期限屆滿之處理方式

6.6.1 應定期檢視個資是否為執行職務或業務所必需資料，或已經當事人書面同意者，並登錄於個資類別清單。

6.6.2 應定期檢視個資項目是否可能發生特定目的消失或期限屆滿事件，如可能發生則應確認是否為執行職務或業務所必需資料，或已經當事人書面同意者，而可以停止利用代替刪除。否則應準備個資刪除、停止處理或利用個資相關作業。

6.6.3 經檢視若非職務或業務所必需資料，但仍有保留處理與利用之需求，則應於期限屆滿前取得當事人書面同意延長保留期限。

6.6.4 個資蒐集之特定目的消失或期限屆滿，而需進行刪除作業者，應確認該項資料已完成刪除作業，並留下相關的紀錄與證據。

6.6 業務執行之作業說明書

6.6.1 PIMS-B-001 個人資料蒐集處理利用管理程序書

6.6.2 PIMS-B-002 個人資料告知作業管理程序書

6.6.3 PIMS-B-004 個人資料文件及紀錄管理程序書

7 當事人權益請求個資程序

7.1 請求項目

7.1.1 提供當事人資料，其流程應包含下列事項：

7.1.1.1 查詢或閱覽

7.1.1.2 製給複製本

7.1.1.3 補充或更正

7.1.1.4 停止蒐集、處理或利用

7.1.1.5 刪除

7.1.2 若當事人要求答覆查詢、提供閱覽或製給複製本等事項，涉及下列情況，則可依規定不提供該項請求：

7.1.2.1 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

7.1.2.2 妨害公務機關執行法定職務。

7.1.2.3 妨害該蒐集機關或第三人之重大利益。

7.2 請求與駁回期限

7.2.1 受理當事人個資之答覆查詢、提供閱覽或複製本等請求項目，應於十五日內，完成同意處理駁回或的決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

7.2.2 受理當事人個資更正或補充請求，應於三十日內，完成同意處理或駁回的決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

7.3 請求費用

7.3.1 查詢或請求閱覽個人資料或製給複製本者，相關作業產生之費用依據本校各項資料申請流程合理計算，經權責主管核定納入作業規定辦理。

7.4 請求流程

7.4.1 由當事人填寫本校個資處理表單 PIMS-D-001「個人資料當事人權益申請書」以作為申請依據。

7.4.2 當事人填寫後之表單交由各單位個資聯絡人受理（應指定一位代表），個資聯絡人需依據業務類別直接處理或轉至本校其他單位個資聯絡人進行後續處理作業。

7.4.3 當事人亦可將填寫後之表單交由資訊中心人員受理（應指定一位代表），並由資訊中心直接處理或轉至本校其他單位個資聯絡人進行後續處理作業。

7.4.4 查詢或請求閱覽個人資料或製給複製本者，如需繳交費用，則依本校原有繳費方式進行繳費。

7.4.5 請求管理作業

7.4.5.1 資料查詢或閱覽

由業務承辦人員向當事人確認身份後提供查詢結果，或請當事人到該業務單位進行資料閱覽，亦可在安全控制下提供線上查詢或閱覽。

7.4.5.2 提供複製本

由業務承辦人員於申請單陳核後依據申請人選擇方式交付文件，完成當事人真實身分核對後，取件方式如下：

7.4.5.2.1 親自領取。

7.4.5.2.2 郵寄方式：郵寄至申請人指定之地點，須繳納掛號郵資。

7.4.5.2.3 電子郵件：寄至申請人指定之電子郵件信箱。

7.4.5.2.4 傳真。

7.4.5.3 補充或更正

應查明或請當事人補充佐證資料，確認其資料補充或更正是否正確，如為正確資料，應於經陳核後進行補充或更正作業。

7.4.5.4 停止蒐集、處理或利用

查明是否為依法規或執行職務或業務所必需之資料，若為必需之資料而無法停止，則應以書面函覆當事人說明原由，以取得瞭解。非必需之資料，則於陳核後進行停用作業。

7.4.5.5 刪除

查明是否為依法規或執行職務或業務所必需之資料，若為必需之資料而無法刪除，則應以書面函覆當事人說明原由，以取得瞭解。非必需之資料，則於陳核後進行刪除作業。

7.5 請求駁回作業

7.5.1 所有請求如依據規定或因執行職務或業務所必需，而無法同意其請求，均應以正式書面函覆，並以掛號方式寄出。

7.5.2 函覆內容應包含申請項目、駁回原因、申訴管道及相關連絡資訊。

7.6 請求申訴作業

7.6.1 個資請求申訴作業由本校各單位內之「個資聯絡人」(應指定一位代表）處理，接受當事人申訴案件。

7.6.2「個資聯絡人」收到申訴案件如屬本校業務時，應由本校「個資專人」陪同個資聯絡人進行調查，並依據調查結果建議處理方式。

7.6.3 調查結果與建議處理方式經由本校業務主管及相關主管同意後，以書面函覆結果，並進一步與申訴人取得聯繫與同意。

7.7 業務執行之表單

7.7.1 PIMS-D-001 個人資料當事人權利行使申請書

8 個資保護作業程序

8.1 設備管理—資訊應用系統安全

處理含有個資之資訊應用系統應符合一般處理作業要求，檢視並建立具有保護個資機密性、完整性、可用性與不可否認性等安全機制。其作業包含：

8.1.1 系統開發與建置

8.1.1.1 規劃資訊系統的個資保護的安全要求。

8.1.1.2 建立記錄、輸入、編輯、更正及刪除等資料驗證及錯誤更正的機制。

8.1.1.3 系統輸出之資料及報表，依權限與報表使用之性質，設定使用者權限，並僅供已授權單位或人員使用。

8.1.1.4 系統產生的資料、顯示畫面或報表，應標示機密等級。

8.1.1.5 資料輸出與交換使用，應經核可並保存相關紀錄。

8.1.1.6 系統應具有查詢檢索及複製個人資料功能，以利當事人查詢與複製，並設定適當的權限控制。

8.1.1.7 建立資料輸入、運算與輸出控制應相互配合機制，並於程式控制中需有適當之檢查方式。

8.1.1.8 系統建置階段即應同時於系統中建立安全機制，如權限控管功能、加密、系統稽核功能及完善之系統文件。

8.1.1.9 應於系統設計之相關文件說明安全控管措施，以利使用者及承包廠商人員明瞭電腦系統內建之安控系統功能。

8.1.2 系統使用

8.1.2.1 使用資訊應用系統應建立記錄、輸入、編輯及更正等資料審核流程及資料錯誤更正的作業程序，並明定資料輸入與異動過程中相關人員的責任。

8.1.2.2 系統內記錄、輸入、編輯及更正等作業應定期進行審查，確保資料的正確性與完整性。

8.1.2.3 系統產生的資料或報表，應確認標示機密等級，並僅供已授權單位或人員使用。資料輸出報表與交換使用，應經核可並保存相關紀錄。

8.1.3 系統資料交換與連結

資訊系統如連結其他單位資料系統或資料庫時，應注意僅能使用於已告知且相容的目的的資料，並先取得雙方資料交換協議。

8.1.4 系統稽核

8.1.4.1 經要求系統產生系統稽核日誌，記錄內容應包括使用者識別碼、登入登出之日期時間、電腦的識別資料或其網址及事件描述等事項。

8.1.4.2 系統稽核紀錄每月應作備份至少需保存三個月，禁止未經授權之刪除及修

改，以為日後稽核調查及監督之用。

8.1.5 系統備份與復原

8.1.5.1 系統資料應定期執行備份作業，由負責同仁檢視備份結果，並追蹤備份失效之原因，需確定所有備份作業成功。

8.1.5.2 各系統主機之資料備份至少保留三代。

8.1.5.3 每半年將所備份之系統資料，進行資料還原測試並作紀錄。

8.1.5.4 應訂定系統毀損之回復作業程序，並建立妥適的回復措施。

8.2 設備管理—資訊設備安全

8.2.1 設備使用與維護

8.2.1.1 建置個資之個人電腦，不應直接作為公眾查詢工具。

8.2.1.2 資訊設備應定期保養維護，並應注意資料備份及相關安全措施。

8.2.1.3 移動或攜出含個資之資訊設備，應申請核准並留下紀錄。

8.2.2 設備報廢

8.2.2.1 設備超過年限或無法修理申請報廢、轉售或廢棄者時應經權責主管核准後，請資訊單位刪除資產所儲存之相關資料。並視情況需要使用適當工具再次進行資料清除作業。

8.2.2.2 資訊系統儲存媒體損壞、無法執行其功能或無需繼續保存使用時，應銷毀該儲存媒體。

8.3 其他安全維護事項

8.3.1 通行碼（密碼）管理

8.3.1.1 個資檔案應釐定使用範圍及使用權限，密碼應保密不得與他人共用。

8.3.1.2 個人通行碼應保密，且需定期變更密碼，以防被竊取使用。

8.3.2 個人電腦儲存個資檔案者時，應設定登入密碼、啟動螢幕保護程式及安裝防毒軟體等安全措施。

8.4 資料稽核

8.4.1 個資管理單位應定期及不定期稽核個人資料檔案管理情形。

8.4.2 以電腦處理個資時，應檢視記錄、輸入、編輯、更正及刪除是否與原檔案或正確資料相符。

8.4.3 個資提供使用時，應核對與檔案資料是否相符，如有疑義，應調原檔案或作業申請文件查核。

8.4.4 指派個資稽核人員定期檢核含有個資之資訊設備使用者之權限清單，確認使用者對資訊存取是否符合規範，實施稽核時，得調閱有關資料，並請相關處理人員

說明。

8.4.5 其餘稽核作業詳見 PIMS-B-005「個人資料稽核管理程序書」。

8.5 紀錄與證據之保存

8.5.1 所有的事件紀錄，包含紙本或電子形式，應放置於安全處所或安全的儲存設備，並依業務權限控管，以防止非授權人員的塗改或破壞。

8.5.2 事件紀錄表單應加以定時或不定時審查，並將審查結果陳報相關主管核備後保存。

8.5.3 審查事件紀錄表單時需特別注意其完整性及是否有任何異常，並追蹤其原因，留下稽核紀錄。

8.5.4 電腦稽核軌跡及相關的證據，每月應作備份至少需保存三個月，禁止未經授權之刪除及修改，以為日後稽核調查及監督之用。

8.5.5 其餘紀錄保存作業說明詳見 PIMS-B-004「個人資料文件及紀錄管理程序書」。

8.6 人員管理及教育訓練

8.6.1 員工安全管理

8.6.1.1 員工報到時，應要求其閱讀並充分瞭解個資保護與資訊安全相關規定，並簽署「保密切結書」(結合學校現行表單，個資專案不另行提供)。

8.6.1.2 員工執行業務時，並遵守政府資訊安全相關法令及本校個資保護與資訊安全相關規定，若違反時應依相關法令及本校相關規定懲處。

8.6.1.3 員工離職時，辦理各項離職相關事宜，應包括資訊設備回收、帳號及權限停用或刪除。

8.6.1.4 處理個資檔案人員職務異動時，應將所保管之儲存媒體及有關資料列冊移交，接辦人員應另行設定密碼，以為護安全。

8.6.1.5 員工離職後，其離職員工曾接觸過之密碼均需取消或更改為新密碼。

8.6.2 個資保護教育訓練

8.6.2.1 應定期及不定期對各單位實施個資安全防護教育訓練。

8.6.2.2 包含個資保護觀念及作法宣導、法律相關規範及正確使用資訊設備等。

8.7 委外管理

8.7.1 委外廠商在執行業務時會接觸校內個資

8.7.1.1 委外廠商應簽署 PIMS-D-002「保密同意書」，保密同意書內至少應包含保密的責任、義務及違反時的罰則等。

8.7.1.2 本校應保存委外廠商存取個資的紀錄。

8.7.1.3 可行時，請委外廠商參與本校個資安全保護教育訓練。

8.7.2 本校委外業務，其內容包含個資的蒐集、處理及利用等

8.7.2.1 委外廠商應簽署 PIMS-D-002「保密同意書」，保密同意書內至少應包含保密責任、義務及違反時之罰則等。

8.7.2.2 委外廠商需遵守本校 PIMS-A-001「個人資料保護管理手冊」之規範。

8.7.2.3 需要求委外廠商依個資法規定制定個人資料安全維護計畫，內容可能包含如下：

8.7.2.3.1 配置管理人員及適當資源。

8.7.2.3.2 界定個人資料之範圍。

8.7.2.3.3 個人資料之風險評估及管理機制。

8.7.2.3.4 事故之預防、通報及應變機制。

8.7.2.3.5 個人資料之蒐集、處理及利用之內部管理程序。

8.7.2.3.6 資料安全管理及人員管理。

8.7.2.3.7 認知宣導及教育訓練。

8.7.2.3.8 設備安全管理。

8.7.2.3.9 資料安全稽核機制。

8.7.2.3.10 使用紀錄、軌跡資料及證據保存。

8.7.2.3.11 個人資料安全維護之整體持續改善。

8.7.2.4 委外合約至少需明確說明本校委託蒐集、處理及利用個資的範圍、特定目的及委託期間。

8.7.2.5 本校需監督委外廠商使用個資情形，每年至少需稽核一次委外廠商執行 8.7.2.3 項目之成效，委外廠商需依個資法及合約內規定配合及接受，無正當理由不得拒絕。

8.7.2.6 委外合約結束後，需確保委外廠商已歸還並刪除所接觸及保有之本校個人資料。

8.8 業務執行之表單

8.8.1 PIMS-D-002 保密同意書

9 緊急應變措施及通報程序

9.1 安全事件通報

9.1.1 內部通報

9.1.1.1 發現個資被竊取、洩漏、竄改或其他侵害事件，應先通報個資專人。

9.1.1.2 判定事件狀況後，由個資專人通報本校對外個資聯絡窗口（秘書室）。

9.1.1.3 並依據本校 PIMS-B-007「個人資料安全事件通報、應變及管理作業管理程序書」進行通報。

9.1.2 外部通報

9.1.2.1 安全事件發生後，由對外個資聯絡窗口(秘書室)以電話、電子郵件或書函方式通知個資當事人事件發生狀況、所產生的影響、處理情形及後續作業等。

9.1.2.2 依據本校 PIMS-B-007「個人資料安全事件通報、應變及管理作業管理程序書」之要求填寫 PIMS-D-012「個資安全事件通報單」並進行通報。

9.2 安全事件處理

9.2.1 事件發生後，依據本校 PIMS-B-007「個人資料安全事件通報、應變及管理作業管理程序書」進行相關處理作業，並依據規範進行矯正預防措施。

9.2.2 事件處理作業時間應於指定時間完成，作業內容應記錄備查，並經由權責人員審視確認。

9.2.3 事件處理前，應先備份數位證據（例如系統紀錄、稽核軌跡），確實做好證據保存工作。

9.2.4 應鑑別事件發生根本原因，以利事件處理作業，如為外來攻擊事件，應適當鑑別攻擊來源。

9.2.5 如發現可能為資訊系統漏洞或脆弱點，應通知本校技術服務組協助獲得解決方案，並執行修復動作。

9.2.6 完成事件處理後，個資專人應提供處理結果報告，交由對外個資業務聯絡窗口（秘書室）彙整，並以電話、電子郵件或書函方式通知個資當事人。

9.2.7 對外個資業務聯絡窗口（秘書室）應彙總及分析個資安全事件相關資訊。

9.3 業務執行之作業程序

9.3.1 PIMS-B-007 個人資料安全事件通報、應變及管理作業管理程序書

9.3.2 PIMS-D-012 個資安全事件通報單

10 管理改善程序

10.1 執行時機

當本校各單位內部及外部稽核發現個資類缺失或是發生個資類安全事件時，應進行原因分析與改善措施。

10.2 原因分析

分析問題發生之原因及影響程度，決定處理的優先順序與處理時限。

10.3 改善對策

提出改善措施時，區分為暫時性對策及永久性對策，以期有效防止類似事件發生，並應考慮成本效益及可行性。

10.4 追蹤執行狀況

10.4.1 各項改善措施計畫，發生單位應指派人員追蹤，並應於改善措施計畫上留存追蹤紀錄。

10.4.2 彙整相關改善措施之執行狀況，於本校「個人資料管理委員會」會議提出報告。

10.5 業務執行之作業說明書

10.5.1 PIMS-B-006 個人資料矯正及預防管理程序書