論述 》管理 · 資訊

導入個人資料保護經驗分享

國立中興大學 101 年 3 月啓動導入「個人資料保護與管理制度」，至當年底取得英國標準協會 BS 10012 ：2009 國際標準認證，成為全國第 1 所符合個人資料保護管理制度之頂尖標竿大學。本文簡述實施過程，並說明主計室具體實行措施，提供各主（會）計機構因應「個人資料保護法」之施行參考。

林妙冠（國立中興大學主計室組長）

壹、前言

「個人資料保護法」（以下簡稱「個資法」）於 101 年 10 月 1 日施行，本校李校長德財具前瞻性遠見，於 100 年 10 月 26 日第 365 次行政會議中宣達，全校將導入「個人資料保護與管理制度」，經數月籌劃，於 101 年 3 月 22 日召開第 1 次「資訊安全暨個人資料保護推動委員會」，正式啓動導入個資保護管理制度，並由財團法人中華民國國家資訊基本建設產業發展協進會（簡稱 NII）協助，於 101 年 12 月 27 日完成 19 個一級行政單位英國標準協會（BSI, British Standards Institution）BS 10012：2009 國際標準認證，成爲全國第 1 所通過個資保護管理認證之頂尖大學，去（102）年持續擴大推動至各院、系、所等教學單位，於 6 月 28 日通過 SGS（Societe Generale de Surveillance S.A.）驗證公司之認證，成爲全國第 1 所行政單位及教學單位全面通過個資認證之頂尖標竿大學。茲將實施過程簡述如次，並詳細說明主計室具體實行措施，提供各主（會）計機構參考，以符合「個人資料保護法」之要求。

貳、個資法規定

「個資法」係避免人格權受侵害，促進個人資料合理利用之法規，其中規範公務機關對個人資料之蒐集、處理及利

用，並對違反規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，需負刑事及民事責任，重要規定說明如下：

一、何謂「個人資料」？

個資分類如下：

（一）一般個資

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、聯絡方式、財務情況、社會活動。（第 2 條）

（二）特殊個資

醫療、基因、性生活、健康檢查及犯罪前科。（第 6 條）

（三）其他

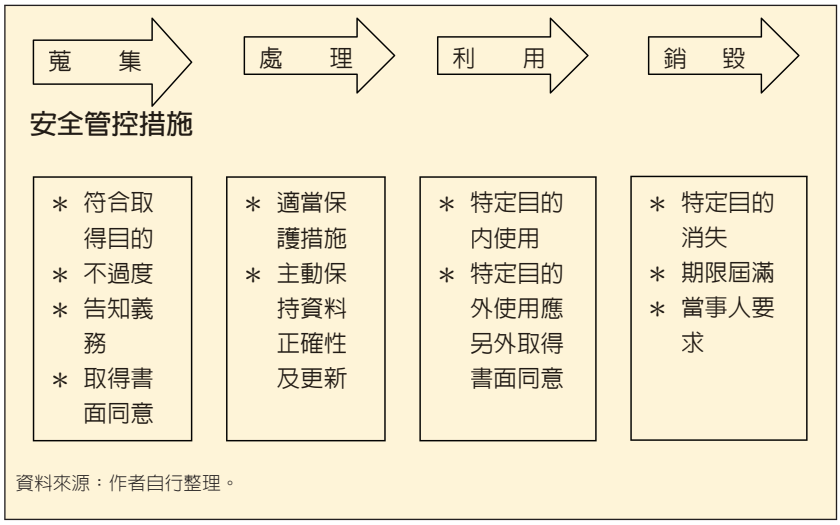
其他得以直接或間接方式識別該個人之資料。（第 2 條）

二、個資生命週期及安全管控措施

個人資料蒐集、利用、處理（包括傳輸及儲存）、銷毀等過程，即構成「個資生命週期」，各項過程中需具適當之安全管控措施，以防止不當處理個資事件，如圖 1。

三、公務機關相關責任

圖 1　個資生命週期



資料來源：作者自行整理。

（一）誠實信用責任

個人資料之蒐集、處理或利用，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。（第 5 條）

（二）個資管理責任

公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。（第 18 條）

（三）損害賠償責任

公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。依侵害情節，以每人每一事件 500 元以上 2 萬元以下計算，對於同一原因事實造成多數當事人權利依侵害事件，合計最高總額以 2 億元為限。（第 28 條）

參、本校實施過程

一、範圍及時程

論述 》管理 · 資訊

（一）第一階段

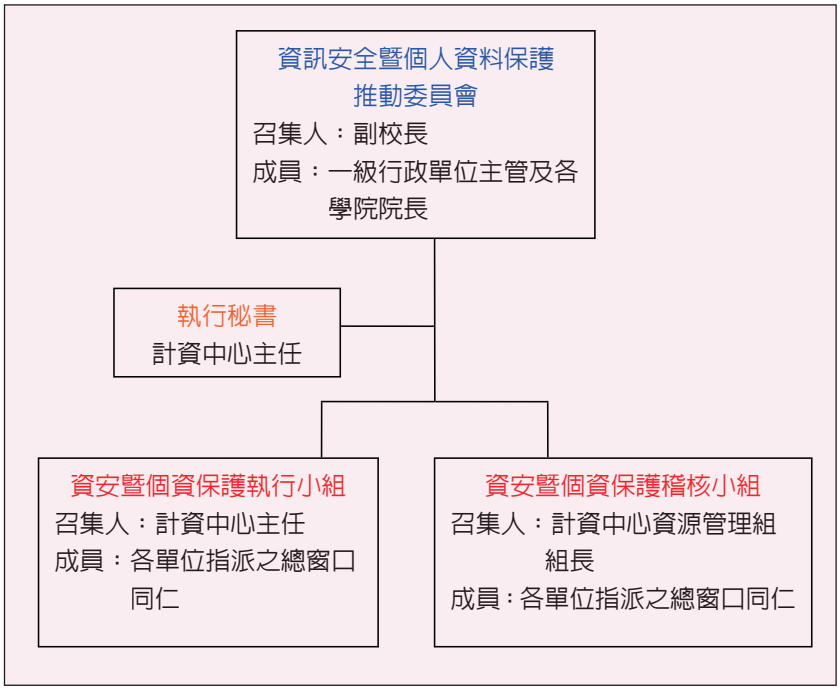
101 年 3 至 12 月底，由一級行政單位－校長室、副校長室、秘書室、教務處、學生事務處、研究發展處、國際事務處、總務處、人事室、主計室、圖書館、創新產業推廣學院、體育室、計算機及資訊網路中心、產學智財營運中心、環境保護暨安全衛生中心、師資培育中心、校友中心、藝術中心等 19 單位辦理導入「個人資料保護與管理制度」，於 101 年 12 月 27 日通過第三方英國標準協會臺灣分公司稽核驗證，成為全國第 1 所通過個資保護管理認證之頂尖大學。

（二）第二階段

102 年 3 至 6 月底，農業暨自然資源學院、文學院、理學院、工學院、生命科學院、獸醫學院、管理學院、法政學院及所屬各系、所等教學單位納入「個人資料保護與管理制度」，第一階段之行政單位亦持續推動，行政及教學單位均接受第三方稽核驗證，於 6 月 28 日通過第三方 SGS 臺灣分公司稽核驗證，成為全國第 1 所行政單位及教學單位全面通過個資保護管理認證之頂尖標竿大學。

二、組織架構（圖 2）

圖 2　資訊安全暨個人資料保護推動組織架構圖



資料來源：作者自行整理。

三、執行過程

（一）成立資訊安全暨個人資料保護推動組織，各單位指派總窗口同仁。

（二）各單位總窗口同仁，接受 35 小時訓練，取得 BS 10012:2009 PIMS 個人資訊管理系統（Personal Information Management System）主導稽核員之國際證照，成為各單位推動種子人員。辦理 20 多場全校性教育訓練，使各同仁均具個資保護與管

理觀念。

（三）成立本校個人資料保護與管理專屬網頁（圖3），俾利同仁隨時查閱相關規定及表單。

（四）訂定個人資料保護管理制度及審查作業。

（五）辦理個人資料檔案盤點及清查，填列「個人資料檔案清冊」。

（六）辦理個人資料檔案衝擊分析及風險評鑑，填列「個人資料檔案風險評鑑彙整表」。

（七）辦理個人資料檔案風險處理，填列「個人資料檔案風險處理計畫表」。

（八）辦理個資侵害事故緊急應變計畫作業。

（九）辦理內部稽核暨矯正預防作業，由各單位指派之總窗口同仁交互稽核非其所屬單位，填列「內部稽核報告」，受稽單位依據「內部稽核報告」所列稽核發現，立即辦理改善措施並填列「矯正預防處理單」。

（十）第三方外部稽核（書面及實地訪評）。

四、完成文件

訂定「國立中興大學個人資料保護與管理政策」及各項程序書及表單，如下頁附表。

圖 3　個人資料保護與管理專屬網頁

資料來源：國立中興大學計算機及資訊網路中心。

肆、主計室具體實行措施

一、實務作爲

（一）會計資訊委外廠商管理

目前各國立大專院校及國立高中、職校均採「艾富資訊股份有限公司」所設計開發之會計資訊系統，辦理預、決算及會計作業，依「政府採購法」規定程序辦理限制性招標，並訂定合約，以規範雙方權利義務。惟依「個資法」第4條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」，換言之，若委外廠商故意或過失洩漏個資，當事人可逕向學校求償，故對委外廠商管理，爲必須且立即需辦理事項，其實務作法如下：

1. 要求委外廠商簽訂本校制訂之「委外廠商保密切結書」，其重要內容主要規

論述 》管理 · 資訊

範廠商，如有違誤願負法律上之責任。

2. 下年度續約時，其合約內容增訂個資保密條款與資訊安全、著作之使用與發行、侵權行爲之規範等三項條款；另增訂本校定期或不定期派員檢查或稽核該公司個資保護管理措施。

3. 委外廠商要求連線作業時，填列「遠端連線申請單」，始依其申請時段，開啓遠端軟體供委外廠商使用，俟作業完成後，立即關閉該軟體，並先以電話確認維護人員身分。

（二）資訊安全管理

1. 主計室網頁、會計線上請購系統等辦理弱點掃描檢測。

2. 會計資訊系統主機之更新及遷移：汰舊換新超過耐用年限老舊主機，並將主機遷移至計資中心機房統一管理，以確保實體環境溫度、溼度等安全控制。

3. 主機之使用者僅保留系統

附表　各項程序書及表單

序號	項　　目	細項程序書及表單
（一）	個人資料文件管理程序書	1. 個人資料文件管理程序書 2. 員工個人資料保密同意書 3. 委外廠商保密切結書 4. 個人資料管理制度文件清冊 5. 文件新增 / 異動 / 廢止申請表 6. 個人資料使用資訊服務申請表 7. 個人資料紀錄銷毀申請單
（二）	個人資料檔案風險評鑑與管理程序書	1. 個人資料檔案風險評鑑與管理程序書 2. 個人資料檔案清冊 3. 個人資料檔案威脅暨弱點分析評分構面表 4. 個人資料檔案威脅及弱點評估表 5. 個人資料檔案風險評鑑彙整表 6. 個人資料檔案風險處理計畫
（三）	個人資料蒐集處理利用管理程序	1. 個人資料蒐集、處理、利用與安全管理程序書 2. 個人資料提供同意書（中、英文範本） 3. 個人資料申訴事件紀錄單
（四）	個人資料當事人之權利聲明	1. 個人資料當事人之權利聲明 2. 個人資料特定目的範圍變更需求同意書 3. 隱私權政策聲明範本（網站使用中、英文範本） 4. 隱私權政策聲明範本（通用版）
（五）	個人資料稽核作業程序書	1. 個人資料稽核作業程序書 2. 個人資料管理制度有效性量測表 3. 個人資料管理制度內部稽核計畫 4. 個人資料管理制度內部稽核底稿 5. 個人資料管理制度內部稽核報告
（六）	個人資料矯正預防管理程序書	1. 個人資料矯正預防管理程序書 2. 個人資料管理制度矯正預防處理單
（七）	個人資料安全控管作業說明書	1. 個人資料安全控管作業說明書 2. 主機系統帳號暨權限申請表 3. 帳號清查紀錄表 4. 遠端連線申請單
（八）	個人資料保護緊急應變處理作業說明書	1. 個人資料保護緊急應變處理作業說明書 2. 個資事故通報及受理流程 3. 個人資料侵害事故通報與紀錄表
（九）	個人資料檔案安全維護計畫	個人資料檔案安全維護計畫
（十）	業務終止後個人資料處理方法	業務終止後個人資料處理方法

資料來源：作者自行整理。

管理者帳號及資料庫管理帳號，並關閉 Guest 帳戶。

4. 存放資料庫之主機，計資中心網管設定其連線網域，只限定校內 IP。
5. 資料庫備份及異地存放。
6. 資料備份還原測試排定作業。

（三）會計資訊系統管理

1. 增列隱私權政策聲明。
2. 會計資訊系統中，主計室同仁依職責分工辦理個人權限管控。
3. 辦理帳號清查及應用系統權限管理與資料庫帳號定期審查並作記錄。
4. 會計資訊系統中設定有關個人身分證號碼、金融帳號、廠商金融帳號等個資，列印出紙本時，其中間部分號碼予以隱藏及戶籍地址未印出等功能，期使紙本於公文傳送過程中避免洩漏個資。
5. 定期或不定期辦理資料備份回復測試，並留有相關測試紀錄。

（四）其他事項

清查於主計室網頁公告之各項表格，若涉及個資者，於表格下方備註個資保護相關聲明。

二、填列下列相關表格

（一）個資檔案清冊。

（二）威脅及弱點評估表。

（三）個資檔案風險評鑑彙整表。

（四）風險處理計畫表。

（五）個資管理制度矯正預防處理單。

（六）個資侵害事故應變計畫。

（七）個資管理維護進度表。

（八）主計室保有個資檔案公開項目彙整表。

三、同仁配合事項

（一）參加個資宣導研習課程。

（二）簽訂「員工個人資料保密同意書」（含工讀生）。

（三）個人電腦密碼長度至少設定 8 碼及不記憶密碼。

（四）設定個人電腦螢幕保護裝置（至多 15 分鐘）。

（五）個資檔案傳送時需加密。

（六）個人電腦資源回收筒、垃圾郵件或寄件備份不可留有含個資檔案。

（七）影印機、傳眞機上不可留有含個資文件資料。

（八）刪除非法軟體（解壓縮工具、影片、音樂 ... 等）。

（九）確實做好桌面淨空（例：桌上不可放置電話簿、隔板不可黏有同仁通訊資料、浮貼法院債權扣款函等）。

（十）退件時若文件含有個資者，以傳遞袋傳送。

伍、結語

本校在李校長德財領導下，積極推動建置「個人資料保護與管理制度」，依

論述 》管理 · 資訊

PDCA（Plan 規劃→ Do 執行→ Check 檢查→ Act 行動）循環原則，確保個資安全維護管理政策整體持續改善，維持有效性。各同仁除於業務執掌中，依制度規範貫徹落實外，更於本次建置過程中，重新檢視相關個人資料蒐集、處理與利用之法令依據，惟下列事項未來仍需持續關注：

一、目前「個資法」第 6、54 條凍結之條款，未來行政院之修訂方向與內容。

二、目前主計相關法規對於個資蒐集、處理、利用之規定，是否必要做修訂或明確說明，以利各主（會）計人員依循？

三、內部控制流程應納個資保護管理規範。

四、持續研讀法務部、中央目的事業主管機關暨司法單位對於個資法條文之解釋與案例。

五、持續參加「個資法」相關教育訓練。

102 年 7 月 1 日起至 12 月底，教育部資訊及科技教育司與本校合作推動「教育體系個人資料保護安全管理施行專案計畫」，建置「教育體系個資導入交流平台」（網址：http://epims.nchu.edu.tw/），研訂公立大學個資保護安全管理所需政策、程序與稽核項目，並提供範本開放下載，且設諮詢專線 04-22840307 轉 722 及電子信箱（nchu-pims@nchu.edu.tw）等服務，以上為本校導入個人資料保護經驗分享，希為各主（會）計機構因應「個資法」之施行有所助益。

● 102 年 8 月 16 日教育部資訊及科技教育司楊司長鎮華（左 3）、興大李校長德財（左 4）共同宣布合作平台正式啓動（照片來源：本校計資中心）

參考文獻

1. 國立中興大學個人資料保護與管理政策（民 102）。
2. 朱瑞陽（民 102）。個人資料保護法介紹。地方行政研習 e 學中心。數位學習課程講義。
3. 蒲樹盛（民 102）。個人資訊管理系統國際標準介紹－以 BS 10012 為例。地方行政研習 e 學中心。數位學習課程講義。
4. 英國標準協會 BSI 臺灣分公司 BS 10012：2009PIMS 個人資訊管理系統主導稽核員訓練課程講義（民 101）。❖