國立中興大學
National Chung Hsing University

個人資料管理文件宣導教育訓練

NII產業發展協進會 專業講師群

財團法人中華民國國家資訊基本建設產業發展協進會

課程目的

- 協助　貴校人員瞭解個人資料保護管理實際執行面相關控管要求。
- 備註：本教材內容有部份執行調整，實際執行內容以最後公佈之版本為主。

目錄

目錄

個人資料保護管理政策

蒐集 | 處理 | 利用 | 儲存 | 銷毀 | 管理

- 本校因營運所需取得或蒐集之包括但不限於個人之姓名、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、職業等個人資料，應遵循我國個人資料保護法（以下簡稱個資法）等法令，不過度且符合目的、相關且適當並公平與合法地從事個人資料之蒐集與處理。

個人資料保護管理政策(續)

蒐集 | 處理 | 利用 | 儲存 | 銷毀 | 管理

- 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務及重要性，考量其他輔助安全措施。

個人資料保護管理政策(續)

蒐集 | 處理 | 利用 | 儲存 | **銷毀** | 管理

- 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應釐定使用範圍及調閱或存取權限。

個人資料保護管理政策(續)

蒐集 | 處理 | 利用 | 儲存 | 銷毀 | 管理

- 本校於利用個人資料時，除需依個資法之特定目的必要範圍內為之外，如需為特定目的以外之利用時，將依據個資法第二十條之規定辦理；倘有需取得用戶之書面同意之必要者，本校應依法取得用戶之書面同意。
- 本校所蒐集、處理之個人資料，應遵循我國個資法及本校個資管理制度之規範，且個人資料之使用為本校營運或業務所需，方可為本校承辦同仁利用。
- 本校取得之個人資料，如有進行國際傳遞之必要者，定謹遵不違反國家重大利益、不以迂迴方法向第三國傳遞或利用個人資料規避個資法之規定等原則辦理，又，倘國際條約或協定有特別規定、或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞者，本校將不進行國際傳遞，以維護個人資料之安全。
- 當本校接獲個人資料調閱或異動之需求時，應依個資法及本校所訂之程序，於合法範圍內進行當事人之個人資料查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除 。

個人資料保護管理政策(續)

蒐集 | 處理 | 利用 | 儲存 | 銷毀 | 管理

- 本校因業務上所擁有之個人資料負有保密義務，除當事人之要求查閱或有下列情形外，應符合個資法第二十條及相關法令規定，並以正式公文查詢外，本校不得對第三人揭露。
- 本校對個人資料之利用，除個資法第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。
- 本校已成立個人資料保護組織，明確定義相關人員之責任與義務。
- 本校已建立與實施個人資料管理制度(PIMS)，以確認本政策之實行；全體員工及委外廠商應遵循個人資料管理制度（PIMS）之規範與要求，並定期審查PIMS之運作。
- 為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校設置資安暨個資保護執行小組，統籌各項資安暨個資保護作業原則規劃事宜，由各一級單位推派1人組成之，計算機及資訊網路中心主任擔任召集人，並依相關法令規定辦理個人資料檔案及個人資料清冊安全維護及更新事項。

個人資料保護管理政策(續)

蒐集 | 處理 | 利用 | 儲存 | 銷毀 | 管理

- 個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。
- 為確保所有個人資料安全，應強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核。
- 本校各組如遇有個人資料檔案發生遭人惡意破壞、毀損或作業不慎等安全事件，應進行緊急因應措施，並依本校計算機及資訊網路中心之【資訊安全事件通報管理辦法】及【個人資料保護緊急應變處理作業說明書】通報程序辦理。
- 本校係以嚴密之措施、政策保護當事人之個人資料，包括但不限於本校之所有員工，均受有完整之個資法、或隱私權保護之教育訓練，本校之委外廠商或合作廠商與本校業務合作時，均簽有保密契約，使其充分知悉個人資料保護之重要性及洩露個資相關之法律責任，倘有違反保密義務之情事者，將受嚴格之內部懲處或嚴重之違約求償，並追究其民、刑事法律責任。
- 本校個人資料保護及管理決議事項應納入資訊安全暨個人資料保護推動委員會報告，會議紀錄將提報主管機關（教育部）及相關利害關係人，如有任何回饋事項，將列入下次管理審查會議之討論議題。

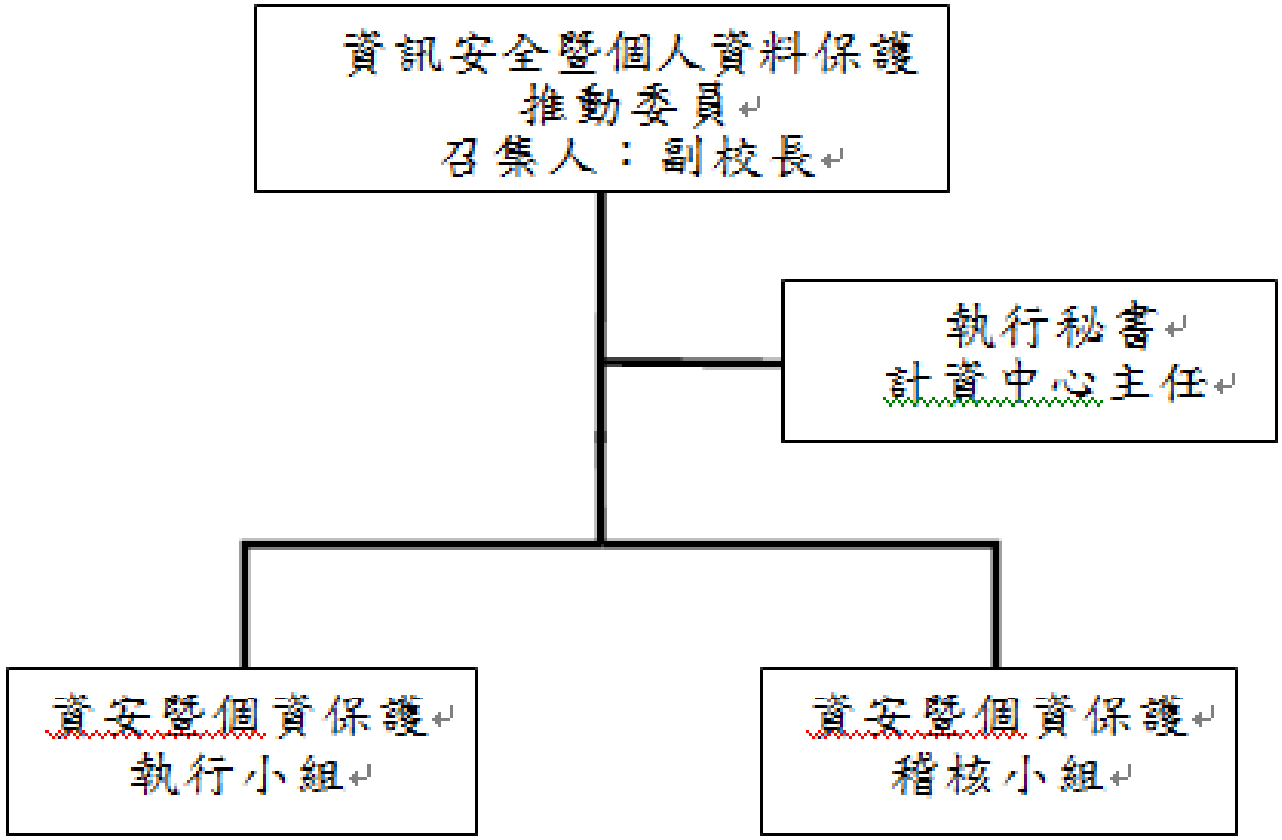
目錄

個人資料保護組織程序書

目的

- 為有效推動與辦理個人資料管理制度（以下簡稱PIMS）各項工作，特成立個人資料保護組織，以擬訂本校各項個人資料保護之目標、策略及管理程序，促進其執行之有效性，並達成既定之目標。

資訊安全暨個人資料保護推動委員會



個人資料保護組織程序書(續)

組織成員

- 本校設立「資訊安全暨個人資料保護推動委員會」（以下簡稱本會），負責本校資安暨個資保護之政策、計畫、資源調度等統籌、協調與研議之整體資通安全個資維護任務，人員組成詳「資訊安全暨個人資料保護推動委員會組織成員表」，工作說明如下：
  - **當然委員**
    - 副校長1人、主任秘書、教務長、學務長、總務長、研發長、國際長、各學院院長、創新產業推廣學院院長、圖書館館長、人事主任、會計主任、法律系系主任及計算機及資訊網路中心主任為當然委員。

個人資料保護組織程序書(續)

組織成員

- 召集人
  - 由副校長擔任資訊安全長（召集人），負責督導綜理本校資訊安全暨個人資料保護管理政策之推動、協調及督導。
- 執行秘書
  - 計算機及資訊網路中心主任為執行秘書，負責本校資訊安全暨個人資料保護之推動事宜。
    - 負責資訊安全暨個資保護作業之監督與審核工作。
    - 協調資訊安全暨個人資料保護推動委員會執行個資保護及緊急事故處理等相關作業。

個人資料保護組織程序書(續)

◆資安暨個資保護執行小組

- ✓ 統籌各項資訊安全暨個資保護作業原則規劃事宜，由本校各一級單位推派1人組成之，計算機及資訊網路中心主任擔任召集人，其工作如下
  - ■ 協助各單位進行個資盤點與彙整。
  - ■ 所轄業務之個人資料管理、保護及維護等事項，並落實於相關業務及人員。
  - ■ 負責規劃個人資料管理制度之維運工作及文件之制/修定作業。
  - ■ 負責日常個人資料保護管理政策的遵循並承擔下列責任：
  - ■ 發展個人資料保護管理政策及個人資料處理程序。
  - ■ 隱私權公告的管理與溝通。
  - ■ 處理來自當事人之需求。
  - ■ 個人資料的蒐集與處理。

個人資料保護組織程序書(續)

資安暨個資保護執行小組(續)

- 抱怨事件的處理。
- 事故的管理。
- 委外的管理。
- 與組織內負責風險管理與安全議題的單位/人聯繫。
- 提供有關資料保護法令相關事項的專家意見與參考文件。
- 說明與應用個人資料處理的各種例外狀況。
- 提供資料分享方案之建議。
- 確保組織可存取與資料保護法令相關之法例修訂及合適的指導綱要。
- 持續確認法律、實務與科技的變化對個資保護帶來的改變。
- 在個人資料保護法的要求下，填寫、提交及管理隱私權通告予權責主管。
- 考量任何具強制或諮詢性單位針對個人資料處理所制定之法規，經評估其適用性後於組織內實行。

個人資料保護組織程序書(續)

資安暨個資保護稽核小組

- 負責資安暨個資保護稽核事宜，本校各一級單位應派一人參加稽核小組，該小組成員必須受過資安暨個資保護稽核訓練，由計算機及資訊網路中心執行資安業務組組長擔任召集人，其工作如下：
  - 擬定個資保護內部稽核計畫。
  - 執行個資保護內部稽核。
  - 撰寫個資保護內部稽核報告。
  - 追蹤不符合事項之改善執行情。

個人資料保護組織程序書(續)

- **為確保本校矯正預防措施之有效運作，應落實管理審查機制，每年舉行一次管理審查會議，並確實討論下列議題：**
  - 來自PIMS使用者之回饋。
  - 由組織人員所辨識及提升之風險。
  - 稽核結果。
  - 程序審查及紀錄。
  - 資訊技術提升及替換之結果。
  - 來自主管機關評估後之正式要求。
  - 抱怨事件的處理。
  - 已發生之資安事故及資料外洩事件。
  - 控制措施持續改進之有效性評量。

個人資料保護組織程序書(續)

◆ 組織間的合作及協調：

- ✓ 須建立與管理個人資料管理制度相關之「外部單位聯絡清單」，並由資訊安全暨個人資料保護推動委員會指派專人負責維護及更新。

目錄

個人資料文件管理程序書

目的

- 確保各相關單位能適時獲得適當且有效之最新文件，特訂定本程序書。

個人資料文件管理程序書(續)

◆個人資料保護管理制度文件等級分為4級

- 公開使用：無特殊之機密性要求，可對外公開之資訊。
- 內部使用：僅供組織內部人員或被授權之單位及人員使用。
- 內部限閱：僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。
- 機密：為組織、主管機關或法律所規範之機密資訊。

個人資料文件管理程序書(續)

◆個人資料保護管理制度文件編碼

- 學校名稱：學校簡稱。
- 管理制度類別：文件所屬之管理制度，如個人資料管理制度(PIMS)。
- 文件類別：A-一階文件，B-二階文件，C-三階文件，D-四階文件。
- 文件流水號：採三碼流水號(000)，例如： NCHU-PIMS-A-001個人資料保護管理政策、 NCHU-PIMS-B-001個人資料保護組織程序書
- 文件管理人員對個人資料保護管理制度文件應編號列表管制，並紀錄於「個人資料管理制度文件清冊」中，文件編碼不得有重覆之情形，以利文件管控。

個人資料文件管理程序書(續)

◆個人資料保護管理制度文件管制作業程序

- 各單位至少設一名文件管理人員，負責該單位個資相關文件之管理。
- 一階文件之內容適用性應由資訊安全暨個人資料保護推動委員會每年至少一次進行審查。
- 二、三、四階文件之內容適用性應由資訊安全暨個人資料保護推動委員會視需要進行審查，以維持管理制度之可運行性。
- 各階文件如有新增/異動/廢止，版本更新或內容更新需填寫「文件新增/異動/廢止申請表」。

個人資料文件管理程序書(續)

文件存取管制

- 本校內部限閱等級(含)以上文件/紀錄之存取調閱，除業務權責人員、權責單位主管以外，其他人員均需填寫「個人資料使用資訊服務申請表」，說明文件調閱申請需求，由權責單位主管進行核准後始能調閱使用。

文件/紀錄保存方式

- 本校之內部限閱等級(含)以上書面文件與電子資料，皆應由各單位業務負責人放置於安全處妥善保管。

個人資料文件管理程序書(續)

文件/紀錄銷毀

- 各業務單位超過保存期限，不予保留而須進行銷毀時，應由經辦人員填寫「個人資料紀錄銷毀申請單」，經權責主管核准後，可以碎紙機絞碎或撕毀等無法回復之安全方式處理。
- 紀錄銷毀申請單辦理後，交由文件管理人員存檔備查，並至少保留3年。

目錄

個人資料檔案風險評鑑與管理程序書

目的

- 為建立國立中興大學（以下簡稱本校）個人資料檔案風險評鑑與管理規範，提供共同遵行之風險評鑑標準，採取適當之對策或控制措施，以有效降低個人資料檔案遭受損害的風險，特訂定本程序書。

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料資產分類

- 個人資料資產分為電子與紙本兩類別，其分類說明如下：
  - 電子資料(Data：DA)：係指儲存於儲存媒介等相關數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔案。
  - 紙本資料(Document：DC)：係指以紙本形式存在之文書資料、報表等相關資訊，包含公文、報表、表單、計畫書、合約、外來文件等紙本資料。

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料檔案鑑別

- 資安暨個資保護執行小組(各單位聯絡窗口)應進行組織業務個資盤點作業。
- 依據作業流程分析結果，執行個人資料檔案鑑別作業，並建立「個人資料檔案清冊」(詳下頁)。
- 每年應至少執行一次個人資料檔案鑑別作業，於下列情形發生時，亦得針對變動範圍內的作業程序與個人資料檔案進行個人資料檔案鑑別之作業：
- 組織變更。
- 作業流程改變。
- 個人資料檔案異動。

個人資料檔案風險評鑑與管理程序書(續)

◆「個人資料檔案清冊」

個人資料檔案清冊

機密等級：□公開使用 ■內部使用 □內部限閱 □機密

文件編號：NCHU-PIMS-D-008　　版　　次：1.0

紀錄編號：　　填表日期：　　年　　月　　日

個資盤編號	流程名稱	個人資料檔案名稱	資料形式	法律依據或內部規定	特定目的	個人資料類別	個人資料之範圍	有否特種資料？何種特種資料？	有無監督管理之非公務機關及其名稱	蒐集			處理		利用				保存		銷毀		揭露			現有控制措施	衝擊值
										來源	方式	單位	方式	單位	期間	地區	單位	方式目的	單位	期限	形式	頻率	對象	方式目的	個資範圍		

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料檔案隱私衝擊分析

個人資料檔案價值之判定

- 各單位針對「個人資料檔案清冊」內容，依據 「個資衝擊影響程度表」(詳下頁)每年應至少進行一次個人資料檔案資產之衝擊影響程度分析，並產出個人資料檔案隱私衝擊分析報告。

個人資料檔案風險評鑑與管理程序書(續)

「個資衝擊影響程度表」

衝擊影響程度	資產價值(衝擊值)	個人資料範圍
極高	4	自然人之姓名或國民身分證統一編號（或護照號碼）及特種個人資料。
高度	3	1. 含自然人之姓名及國民身分證統一編號（或護照號碼），但不含特種個人資料。 2. 含自然人之姓名或國民身分證統一編號(或護照號碼)及財務情況（如：薪資、局帳號），但不含特種個人資料。
中度	2	1. 含自然人之姓名或國民身分證統一編號(或護照號碼)，但不包含特種資料。 2. 含自然人之姓名及員工編號（或學號），但不含特種個人資料。
一般	1	不含自然人之姓名及國民身分證統一編號(或護照號碼)。

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料檔案風險評鑑

- 依上述個人資料檔案隱私衝擊分析鑑別個人資料檔案資產價值。
- 個人資料檔案風險評鑑作業應於每年個人資料保護內部稽核作業活動前至少執行一次，各單位主管可視實際狀況，決定執行之時機與範圍，於下列情形發生時亦得為之：
  - 營運組織變更。
  - 作業流程改變。
  - 個人資料檔案新增或變更。
  - 發生重大資訊安全事件。

其他特殊執行時機

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料檔案威脅及弱點影響分析

- 個人資料檔案之威脅及弱點評估依據「個人資料檔案威脅及弱點評估表」(詳下頁)進行風險分析，分析構面係依據「個人資料保護法」內容與控管設計「個人資料檔案弱點暨威脅分析評分構面表」（詳下頁)以利評估組織在面臨個資風險時可能產生之影響程度。
- 個人資料檔案之威脅及弱點評估後，產出個人資料檔案風險值，**風險值計算方式為衝擊影響程度(PIA）×（構面值1*權重+構面值2*權重+構面值3*權重+構面值4*權重+構面值5*權重）=個人資料檔案風險值。**

第34頁之
評估結果

個人資料檔案風險評鑑與管理程序書(續)

「個人資料檔案威脅及弱點評估表」

個資資產編號：					流程名稱：					
個人資料檔案名稱：					蒐集單位：					
保存單位：					資產價值(衝擊值)：					
個資範圍：										
	威脅	弱點	構面1 財務影響	構面2 違反個資法影響組織營運與聲譽	構面3 個資蒐集、處理、利用範圍與目的	構面4 保存、銷毀	構面5 安全管理制度	不適用	風險值	0
		加權	1	1	1	1	1			
蒐集	資料外洩	委外蒐集資料(1235)							0	
		缺乏監督機制(1235)							0	
		教育訓練不足(1235)							0	
	不符合蒐集程序	委外蒐集資料(1235)							0	
		缺乏監督機制(1235)							0	
		教育訓練不足(1235)							0	
	未遵循法令法規	未告知蒐集目的(1235)							0	
		未取得當事人同意(1235)							0	
		蒐集特種資料(1235)							0	
		收集過度資訊(1235)							0	
		教育訓練不足(1235)							0	
		未提供拒絕提供個資之權利(25)							0	

個人資料檔案風險評鑑與管理程序書(續)

「個人資料檔案弱點暨威脅分析評分構面表」

項目 評估值	財務影響	違反個資法影響、 組織營運與聲譽	個資蒐集、處理、利用 之範圍與目的	保存、銷毀	安全管理制度
1.	個資保管數量 500 筆(含)以內，全數外流或處理不當，造成財務影響；或可能遭受法院判賠金額 1,000 萬元(含)以下。	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資，影響組織聲譽但不影響該業務流程運作。	已取得當事人同意蒐集、處理、利用個資，且未超過範圍與目的。	已建立保存、銷毀、監督程序，且已落實該等作業。	已建立安全控管程序及相關文件，且已落實。
2.	個資保管數量逾 500 筆~5,000 筆(含)以內，全數外流或處理不當，造成財務影響；或可能遭受法院判賠逾 1,000 萬元，1 億元(含)以下。	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資會影響組織聲譽及該業務流程運作。	1. 已取得當事人同意蒐集、處理、利用個資，雖資料蒐集範圍（過度）與目的不同（目的外之處理、利用），已進行告知，但未取得書面同意。或 2. 已取得當事人同意蒐集、處理、利用個資，未逾越目的，且有進行告知但未取得書面同意。	已建立保存、銷毀、監督程序，但未落實。	已建立安全控管程序及相關文件，但部分未落實。
3.	個資保管數量逾 5,000 筆~5 萬筆(含)以內，全數外流或處理不當，造成財務影響；或可能遭受法院判賠逾 1 億元，2 億元(含)以下。	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資影響組織聲譽及部門業務運作。	已取得當事人同意蒐集、處理、利用個資，但資料蒐集、處理、利用範圍（過度）與目的不同（目的外之處理、利用），且未進行告知或已告知但不同意。	尚未建立保存、銷毀、監督程序，但有部分實施。	尚未建立安全控管程序及相關文件，但有實施部份安全控管。
4.	個資保管數量逾 5 萬筆，全數外流或處理不當，造成財務影響；或可能遭受法院判賠逾 2 億元。	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資影響組織聲譽及組織業務運作。	未取得同意而蒐集、處理或利用個資，也未進行告知。(例如:購買名單或於臉書上搜尋[處理或利用])。	尚未建立保存、銷毀、監督程序，亦無實施任何措施。	未建立安全控管程序及相關文件，亦無任何安全控管。
備註	【損害賠償請參酌個資法第 25(非公務)】。營利之個資外流事件，組織或業務承辦人可能依判決有刑責。	N/A.	未告知違反個資法第 54 條。	N/A.	N/A.

個人資料檔案風險評鑑與管理程序書(續)

風險評鑑報告產出

- 上述評估資料之風險值由各單位彙整後產出「個人資料檔案風險評鑑彙整表」(詳下頁)。
- 依據個人資料檔案風險評鑑結果撰寫個人資料檔案風險評鑑報告，並由資安暨個資保護執行小組提出可接受之風險等級建議。

個人資料檔案風險評鑑與管理程序書(續)

◆「個人資料檔案風險評鑑彙整表」

機密等級：□公開使用 ■內部使用 □內部限閱 □機密

填表日期： 年 月 日

個人資料檔案風險評鑑彙整表　　紀錄編號：

項次	評鑑別	資產編號	資料形式	流程名稱	資產名稱	保有單位	資產價值	個資處理階段	風險事件		構面1	構面2	構面3	構面4	構面5	風險值
									威脅	弱點						
	第一次評鑑															
	風險再評鑑															
	第一次評鑑															
	風險再評鑑															
	第一次評鑑															
	風險再評鑑															

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料檔案風險管理

- 決定可接受風險值
  - 個人資料檔案風險評鑑之可接受風險值，需經「資訊安全暨個人資料保護推動委員會」開會決議，並記載於會議紀錄中。
  - 除決定可接受風險值外，亦可訂定風險處理之補償條件，篩選出可接受風險值以下，但仍須進行風險處理之個人資料檔案項目。
  - 「資訊安全暨個人資料保護推動委員會」應每年召開會議檢討可接受風險值，其可接受風險值得考量本行作業環境及安全控管現況作適當調整。

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料檔案風險處理計畫作業

- 依個人資料檔案風險評鑑結果及可接受風險值之決議，由各單位「個人資料檔案清冊」之各風險項目負責人針對需降低風險值之個人資料檔案擬訂「個人資料檔案風險處理計畫」，以期將風險降至可接受程度。
- 個人資料檔案風險處理計畫之風險處理措施，應根據「個人資料保護法」對各項個人資料保護之安全要求目標，擬訂適當之處理措施及相關執行資源之資訊。
- 個人資料檔案風險處理計畫應提報「資訊安全暨個人資料保護推動委員會」審查後執行，並列入追蹤管理。

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料檔案風險處理計畫作業

- 風險處理計畫之風險處理措施及說明、改善活動與其所需資源、預訂完成日期等規劃項目應記錄於「個人資料檔案風險處理計畫」（詳下頁）之「風險處理進度」欄，並於預訂完成日期結束後，至少每年應彙整提報「資訊安全暨個人資料保護推動委員會」審查。
- 個人資料檔案風險處理計畫若為長期之專案計畫，則應於執行前進行風險評估，確認其預期效益可達到風險處理之目標，並於專案各階段驗收後，提報「資訊安全暨個人資料保護推動委員會」討論執行之成效與進度。

個人資料檔案風險評鑑與管理程序書(續)

「個人資料檔案風險處理計畫」

機密等級：□公開使用 □內部使用 ■內部限閱 □機密

填表日期： 年 月 日

紀錄編號：

個人資料檔案風險處理計畫

資產識別暨風險說明											風險處理措施		風險進度追蹤				
項次	單位	資產編號	流程名稱	個資檔案	型式	個資階段	威脅	弱點	風險說明	風險值	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	風險處理進度

個人資料檔案風險評鑑與管理程序書(續)

◆風險處理計畫執行成效暨殘餘風險處理

- 風險處理計畫於預訂完成日期結束後，須由各單位相關業務承辦人執行風險再評鑑，以確認風險處理計畫執行達到風險減緩預期效益，並將風險再評鑑之結果填寫於「個人資料檔案風險評鑑彙整表」，提報「資訊安全暨個人資料保護推動委員會」會議。
- 實施控制的風險，若處理結果已降至風險可接受等級之下，應於「資訊安全暨個人資料保護推動委員會」會議中提出討論，決定是否列入下次風險評鑑審查事項。
- 若處理後之風險值無法降至風險可接受等級之下，應於「資訊安全暨個人資料保護推動委員會」會議中提出討論，決定是否接受此風險或增加其他控制。

個人資料檔案風險評鑑與管理程序書(續)

◆個人資料檔案風險評鑑結果審查

- 監控
  - 控制措施的實施應視需要建立相對應之有效性量測，以反映出控制措施實施狀況及成效，以利管理階層及相關人員定期或不定期審視。
- 持續改善
  - 為維持本風險評鑑方法之有效性，「資訊安全暨個人資料保護推動委員會」應每年辦理下列項目：
    - 檢討可接受風險值與「個人資料檔案威脅及弱點評估表」之威脅及弱點項目。
    - 視需要將發生個資事故或遭遇個資訴訟判決相關資訊，納入「個人資料檔案威脅及弱點評估表」威脅及弱點項目之檢討。

個人資料檔案風險評鑑與管理程序書(續)

「個人資料檔案風險評鑑彙整表」

機密等級：□公開使用 ■內部使用 □內部限閱 □機密

填表日期： 年 月 日

個人資料檔案風險評鑑彙整表　　紀錄編號：

項次	評鑑別	資產編號	資料形式	流程名稱	資產名稱	保有單位	資產價值	個資處理階段	風險事件		構面1	構面2	構面3	構面4	構面5	風險值
									威脅	弱點						
	第一次評鑑															
	風險再評鑑															
	第一次評鑑															
	風險再評鑑															
	第一次評鑑															
	風險再評鑑															

目錄

個人資料蒐集、處理、利用與安全管理程序書

目的

- 國立中興大學（以下簡稱本校）為落實辦理【個人資料保護法】（以下稱個資法）規定之個人資料蒐集、處理、利用與安全，特訂定本程序書。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆個人資料之蒐集控管原則

- 各單位蒐集個人資料時，應向當事人履行告知義務，並依據個資法規定，請當事人填寫「個人資料提供同意書」取得當事人書面同意，或與當事人有契約或類似契約之關係。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆個人資料之蒐集控管原則

- 各單位蒐集個人資料時，應明確告知當事人以下事項：
  - 本校名稱、聯繫方式。
  - 蒐集目的。
  - 個人資料的類別。
  - 向當事人說明資料使用期間、保存期限、使用範圍及使用方式。
  - 當事人可以行使之權利及方式，例如當事人可請求查詢、閱覽、製給複製本、補充、更正、刪除、停止蒐集、處理或利用。
  - 向當事人說明可自行判斷是否提供個人資料，若為本校提供服務時所必須之資訊，因而造成無法提供該服務情形時，當讓當事人瞭解對其個人權益之影響。
  - 本校如於網站上蒐集個人資料時，應說明採用之技術收集並儲存資訊之方式，如cookies等。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之蒐集控管原則

- 各單位於蒐集個人資料檔案時應注意：評估蒐集目的及範圍為適當、相關且不過度，不處理無關或超過蒐集目的之額外的個人資料。
  - 各單位因業務需求蒐集個人資料前，應先確認蒐集個人資料之目的與範圍。
  - 各單位定期透過內部稽核方式檢視蒐集之個人資料不逾越其目的。
  - 各單位處理個人資料之系統或業務，應每年定期檢視，確保個人資料處理之適當性及不過度使用。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之處理控管原則

- 處理個人資料檔案之個人電腦，應設置使用者登入帳號及密碼，並啟動螢幕保護程式密碼功能，相關存取原則依據本校【個人資料安全控管作業說明書】辦理。
- 應避免開啟個人網路分享目錄與檔案，或設定存取權限至指定之目錄。
- 本校處理個人資料之系統或業務，應每年定期檢視，確保個人資料處理之適當性及不過度使用。
- 處理個人資料檔案之應用系統，應將個人資料檔案的安全需求納入系統開發考量。
- 個人資料存取權限之授權管理，必須依人員執掌角色所需，且以執行業務及職務所必要的最低資源存取授權為限。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之處理控管原則(續)

- 本校應每年定期由個人資料檔案權責人員維護資料之正確性，或依當事人之請求更新或補充其個人資料，並應於個人資料變更後，通知曾提供利用之第三方。如個人資料正確性有爭議者，應主動停止處理或利用，但因執行職務或業務所必須或經當事人書面同意者，不在此限。
- 本校應主動或依當事人之請求補充、更正、停止蒐集、停止處理、停止利用或刪除個人資料。受[illegible]於30日內為准駁之決定，必要時得予延長，延長[illegible]書面通知請求人。

依據電腦處理個人資料保護法施行細則修正草案第十六條說明：
依本法第八條、第九條及第五十四條 所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之利用控管原則

- 個人資料的利用應先確認利用的目的是否和原先蒐集的特定目的相同。
- 公務文書及紙本郵件應有專人負責收發。
- 使用影印機、印表機、傳真機、掃描機或多功能事務機處理個人資料後，應立即將資料取走。
- 含有個人資料之報廢紙張不得回收及再利用。
- 針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於上鎖之抽屜或儲櫃內，以避免個人資料外洩。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之傳輸控管原則

- 個人資料採電子檔案進行傳輸時，應採取資訊加密技術傳輸執行（如壓縮軟體加密），且解密金鑰須分開傳送。
- 個人資料以紙本方式進行傳輸時，應採取彌封或專人遞送等其它具保密機制之傳遞方式進行。
- 個人資料以傳真模式進行傳輸時，應於傳真前通知對方，並於傳真後立即與對方進行確認。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之儲存控管原則

- 本校處理、儲存個人資料檔案之資訊設備，應由專人負責保管與維護。
- 各單位儲存個人資料檔案之磁碟、磁帶及紙本等相關儲存媒體，需指定專人管理，並置於實體保護之環境，例如上鎖之儲櫃、防潮箱或銀行保險箱等。
- 由廠商協助維修儲存個人資料檔案之電腦設備時，應指派專人在場確保資料的安全。
- 儲存個人資料檔案之儲存媒體，應建立定期備份或備援機制。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之銷毀控管原則

- 個人資料檔案超過保存期限，除審核有無永久保留外，應依規辦理銷毀作業。
- 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用，應刪除其所儲存之個人資料檔案。
- 超過保存期限之個人資料檔案應填寫「個人資料紀錄銷毀申請單」，經權責單位主管核准後辦理銷毀。
- 紙本若屬大量銷毀應指定專業廠商並有相關安全控管措施（如：人員全程陪同或全程錄影監控）。
- 紙本若少量則應以碎紙機銷毀。
- 若為電子檔案，應依規範辦理刪除，並清除「資源回收筒」。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之銷毀控管原則(續)

- 個人資料蒐集之特定目的消失或期限屆滿時，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，但因執行職務或業務所必須或經當事人書面同意者，不在此限。
- 個人資料蒐集之特定目的消失或期限屆滿時，由權責單位確定已無保存之必要後，電子之個人資料檔案應填寫「個人資料使用資訊服務申請表」、紙本之個人資料檔案應填寫「個人資料紀錄銷毀申請單」經權責單位主管核准後辦理刪除或銷毀。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆個人資料之申訴控管原則

- 當事人對本校處理個人資料有任何抱怨申訴時，可由下列管道進行：
  - 向本校提出申訴時，由各單位受理人員填寫「個人資料抱怨及申訴事件紀錄單」並陳核單位主管後，轉請本校之個人資料管理窗口判定抱怨申訴內容進行後續處理。
  - 當事人透過電話、E-mail、傳真等方式申訴時，由相關受理人員填寫「個人資料抱怨及申訴事件紀錄單」並陳核單位主管後，轉請本校之個人資料管理窗口判定抱怨申訴內容，再轉交業務權責單位進行後續處理。
  - 受理單位接獲個資當事人之抱怨與申訴後，應於10個工作日內回應當事人本校已受理申訴之訊息。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之申訴控管原則(續)

- 業務權責單位受理抱怨及申訴事件之處理流程如下：
  - 針對抱怨及申訴事件內容進行原因瞭解及處理。
  - 於合理期間內將處理結果回覆當事人，並留下回覆紀錄。
  - 將處理結果通知受理單位，於紀錄單上註明已通知受理單位。
  - 將處理紀錄及回覆內容交付個人資料管理窗口。
- 個人資料管理窗口應追蹤業務權責單位處理進度，其相關記錄應留存以備查。

個人資料蒐集、處理、利用與安全管理程序書（續）

◆ 個人資料之委外控管原則

- 委外處理個人資料檔案，應於委外合約中載明所處理之個人資料保密義務、個人資料安全相關責任及違反之罰則。
- 受本校委託處理個人資料之委外廠商，在簽訂正式書面協議或契約後，本校保留個人資料保護管理相關作業之稽核權，以確保當事人之個資安全。
- 若委外廠商將個人資料處理作業進行再轉包，所簽訂之書面協議或契約應有與該委外廠商相同之安全控管措施，委外廠商亦應保留對轉包廠商進行相關安控措施之稽核權。
- 與第三方廠商所簽訂正式書面協議或契約中，應明確陳述契約終止時，相關個人資料應被銷毀，或交還本校或業務承辦單位。

個人資料蒐集、處理、利用與安全管理程序書（續）

第三方揭露個人資料之要求

- 本校取得當事人的同意或其他法令之特別規定，始得將個人資料揭露予第三方或使用於蒐集目的以外之其他用途。
- 若需要於本校對外網站或網頁公布個人資料時，應進行適當之遮蔽或僅公告適當之資訊，並經權責主管核准後依相關法律及規範處理。

目錄

個人資料當事人之權利聲明

目的

- 國立中興大學（以下簡稱本校）為提供當事人行使個人資料保護法（以下稱個資法）第三條所規定之權利，規範當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除個人資料之規則與流程，並建立控制與紀錄機制，特訂定本聲明。

個人資料當事人之權利聲明(續)

◆提供查詢、閱覽、製給複製本之處理原則

- 針對當事人請求查詢、閱覽個人資料或製給個人資料複

第十三條

公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；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。

公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；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。

- 應具備收受請求及做出准駁之控制與紀錄保留機制。

個人資料當事人之權利聲明

◆ 當事人請求個人資料補充、更正、停止利用及刪除之處理

第十三條

公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；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。

公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；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。

- 應具備收受請求及做出准駁之控制與紀錄保留機制。

個人資料當事人之權利聲明

個人資料得拒絕申請之情形：

- 依「個人資料保護法」第十條或確認當事人之查詢、閱覽、

第十條

公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

一、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。

二、妨害公務機關執行法定職務。

三、妨害該蒐集機關或第三人之重大利益。

個人資料當事人之權利聲明

◆ 隱私權聲明：

- 本校所提供之服務若含個人資料，應制定及維護隱私權聲明。
- 本校相關隱私權聲明，可參酌「隱私權政策聲明範本」修訂，此聲明應讓當事人易於取得與閱讀。
- 本校所辦理之活動或業務需直接從當事人取得個人資料前，本校應以E-mail或書面方式提供當事人該隱私權聲明，或公告於網站上。

目錄

個人資料稽核作業程序書

◆稽核人員之要求

- 為確保稽核過程的客觀性與獨立性，稽核之執行應由非受稽人員擔任。可由下列方式組成稽核團隊執行稽核活動，依權責辦理各項個人資料保護稽核事務。

◆個人資料管理制度內部稽核

- 個人資料管理制度內部稽核每年至少辦理1次，並可視需要不定期舉行，當個人資料管理制度發生重大變更後，應立即執行稽核作業。
- 資安暨個資保護稽核小組應事先擬定稽核計畫，闡明稽核範圍與項目，陳核「資訊安全暨個人資料保護推動委員會」召集人核可後，方得實施。

個人資料稽核作業程序書(續)

個人資料管理制度內部稽核

- 內部稽核報告由資安暨個資保護稽核小組彙整後，呈報「資訊安全暨個人資料保護推動委員會」核定。內部稽核報告所列建議改善事項，應辦理追蹤複檢。

矯正預防處理

- 受稽部門於接獲內部稽核報告後，應依據【個人資料矯正預防管理程序書】之規定實施矯正，並於十五個工作天內將該單位之缺失原因分析及擬採行之矯正與預防措施填列於「個人資料管理制度矯正預防處理單」內，經單位權責主管核定後回覆資安暨個資保護稽核小組。

目錄

個人資料矯正預防管理程序書

◆個資外洩事故矯正與預防措施

- 個資外洩事故發生時，其發現者可依據本校【個人資料保護緊急應變處理作業說明書】進行相關通報作業事宜，並由該事故權責單位進行後續處理改善。
- 個資外洩事故時，權責單位負責人或業務負責人應填寫本校「個人資料管理制度矯正預防處理單」，並提出原因分析、可執行之預防措施、預計完成日期並實施處理追蹤。
- 資安暨個資保護稽核小組應對改善狀況執行成效進行確認及陳核，並負責「個人資料管理制度矯正預防處理單」的彙整與保管。

個人資料矯正預防管理程序書(續)

◆ 個人資料保護稽核缺失矯正與預防措施

- 由業務權責人員填寫本校「個人資料管理制度矯正預防處理單」，包含稽核缺失不符合原因之根因分析，並提出改善因應措施、可執行之預防措施、預計完成日期並實施之。
- 資安暨個資保護稽核小組應對改善狀況執行成效確認。將本校「個人資料管理制度矯正預防處理單」於完成狀況確認後，彙整及保管。
- 資安暨個資保護稽核小組應彙整「個人資料管理制度矯正預防處理單」辦理情形，於管理審查會議中呈報「資訊安全暨個人資料保護推動委員」進行審查與檢討。

目錄

個人資料安全控管作業說明書

目的

- 依據「個人資料保護法」、「個人資料保護法施行細則」、個人資訊管理制度(PIMS) BS 10012標準及國立中興大學(以下簡稱本校)「個人資料保護管理政策」等相關規定，制訂本校個人資料安全控管程序，以確保個人資料受適當的控管與監視，防止不當管控而造成資料外洩之風險。

個人資料安全控管作業說明書(續)

◆ 實體環境安全控制

- 未經授權不得將機敏文件攜出辦公環境區域。若有需要，須經主管人員核准，始得進行。
- 處理完之個人資料檔案(紙本、電子)，若無需保留應立即絞碎或刪除(電子檔案應確實清除「資源回收筒」)，含有個人資料之報廢紙張不得回收及再利用。
- 針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖，以避免外洩。
- 為確保本校相關資訊設施及資料保護之安全，非業管權責單位指定或授權之人員不得擅自進入處理與存放機敏資訊之場所。
- 存放機敏資訊之儲存空間應建立門禁管理，如透過鑰匙或門禁卡等方式進行管理。

個人資料安全控管作業說明書(續)

◆ 一般安全控制

- 各單位應對存有個人資料之系統伺服器應進行備份，並至少保留2代。備份作業應儘量於離峰時段進行。
- 備份資料至少每年執行資料回復測試，以確認備份資料之可用性。
- 存放重要機敏資料之備份媒體應另異地存放一份於安全場所。備份媒體運送過程中應存放於上鎖之媒體保護箱由專人親送。
- 本校同仁、接觸個人資料之外部人員、委外服務廠商人員於在職及離、退職後，均不得洩漏所知悉之機敏資訊，或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。
- 每年應對組織內部人員規劃訓練課程，或派員參加外單位辦理之專業課程，以提升人員個人資料保護之安全認知及警覺意識。

個人資料安全控管作業說明書(續)

一般安全控制

- 為確保教育訓練執行之成效，可採行隨堂抽問、案例討論、習題演練或隨堂測驗等方式進行成效評估。
- 本校個人資料保護安全教育訓練一般人員至少3小時，其簽到表及執行成效等紀錄應由資安暨個資保護執行小組留存備查。

個人資料安全控管作業說明書(續)

◆ 委外安全控制

- 委外廠商人員於專案服務期間所知悉之業務資訊，應遵守「個人資料保護法」及本校相關規定，且不得對外透露。廠商及專案人員並應分別簽署廠商保密切結書或人員保密切結書。
- 委外廠商履行契約所使用之軟體不得違反著作權法之規定，若因使用非法軟體造成本校單位個人資料外洩，委外廠商須承擔所有法律責任。
- 委外廠商於專案服務期間所使用之工具軟體及作業執行紀錄，本校有權進行稽核，廠商不得異議。
- 於專案期間，本校應透過稽核等方式監督委外廠商之個人資料管理作法，如個資蒐集、處理、利用、傳輸與銷毀之管理情形。
- 提供委外廠商測試之資料，應將個人資料欄位內容轉換為虛擬資料或移除。

個人資料安全控管作業說明書(續)

存取控制

- 個人資料之存取應與本身業務範圍相關，任何人未經授權不得存取與個人業務無關之個人資料。
- 若因特殊需要提供帳號予外部或非業務負責之人員，應填列「主機/系統帳號暨權限申請表」，並考量作業需求及個人資料之機敏性，授與適當之存取權限及有效期限。
- 權責主管應審慎評估重要系統特殊權限之授權管理。
- 因處理系統當機與異常狀況需視狀況授與適當之存取權限，並避免共用帳號，如特殊情況，需共用帳號時，應建立可歸責性之機制，以利識別身份。
- 公用程式路徑或公(共)用目錄之存取權限應適當控管，防止非授權使用者存取。含個人資料之檔案不得存放於公(共)用目錄。

個人資料安全控管作業說明書(續)

◆ 存取控制(續)

- 針對無人看管的資訊設備，應有適當控管程序，以防未經授權之存取或濫用。公共使用之影印機、印表機、傳真機或多功能事務機應每日應檢視有無個人資料遺留。
- 為確保個人資料之安全，對敏感性系統或處理大量個人資料之資訊設備，應採取適當控管程序或隔離措施。
- 伺服器、個人電腦及筆記型電腦應設定螢幕保護程式，並設定密碼或採取登出鎖定方式保護；自行啟動螢幕保護程式的時間設定應不超過15分鐘。

個人資料安全控管作業說明書(續)

使用者帳號管理

- 新進同仁報到後，由人事室建立人事資料，依工作職掌所需開立帳號並授予適當之權限。
- 本校具機敏性資料之應用系統帳號須經申請並核可後，方可建立帳號使用。非業務權責單位人員如需使用其資訊系統時，須經業務權責單位主管核可後方得使用。
- 除特殊規定外，員工離、退職時，系統管理人員於收到相關單位通知後，應進行帳號註銷或停用。
- 員工內部調職時，應提出異動申請，系統管理人員應確實刪除其原單位之存取權限。
- 員工留職停薪時，系統管理人員於收到人事室通知後，應停用其帳號。

個人資料安全控管作業說明書(續)

使用者帳號管理(續)

- 系統管理人員應避免共用管理者帳號，重要系統管理者帳號與密碼之文件，應密封並存放於上鎖之安全處所。
- 具機敏性資料之伺服器及資料庫，其特殊權限帳號應每年清查，查核結果填列於「帳號清查紀錄表」，並陳權責主管審核。
- 新購置之資訊設備或系統，應於安裝完成後刪除或關閉不必要之帳號及更改預設密碼。

個人資料安全控管作業說明書(續)

密碼管理

- 首次登入系統時，應立即變更密碼設定，並妥善保管帳號與維持密碼之機密性。
- 應避免將帳號密碼張貼或放置於伺服器、網路設備、個人電腦、螢幕或其他場所。
- 除特殊需求外，應避免使用者共用帳號密碼。
- 登入系統時應避免使用記錄密碼之功能，以免開機時自動登入系統。
- 使用者密碼須為英數字混合，且不得與帳號名稱相同、密碼長度至少為6碼，且不得與前次設定相同，原則上密碼至少1年變更1次；使用者密碼遺忘時，應提出申請並由主管核可或經本人身份確認無誤後，始得進行密碼變更，並保留相關紀錄以備查核。

個人資料安全控管作業說明書(續)

使用者存取權限

- 對於職務異動如調、離職、留職停薪人員等，依本程序書之使用者帳號異動辦理，據以異動、註銷或停用存取權。
- 使用者存取業務相關之個人資料須經授權，其帳號應為唯一之識別碼，禁止借用他人之帳號或共用帳號。
- 久未登入系統之帳號應妥善管理，經確認無須使用後，應予以刪除。

個人資料安全控管作業說明書(續)

◆作業系統存取控制

- 系統紀錄存取，應限定僅由系統管理人員或被授權者存取。
- 帳號名稱應避免顯示任何足以辨識為特殊權限的訊息，如管理者或監督者。

◆應用系統之存取控制

- 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。
- 應用系統之敏感等級以上資訊，應與一般資訊作適當區隔，並加強權限控管措施。
- 應視系統情形，進行會談期逾時(Session timeout)控制，以防止未經授權使用者的存取及阻絕服務之攻擊。

個人資料安全控管作業說明書(續)

網路存取控制

- 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

遠端存取之限制

- 非經授權禁止執行遠端存取作業。
- 連線存取個人資料時，應限定標的範圍，並填列「遠端連線申請表」，並陳權責主管審核。

個人資料安全控管作業說明書(續)

資料庫存取控制

- 資料庫存取應啟動作業系統或資料庫之身份識別機制。
- 具機敏性資料之資料庫系統存取帳號，應依功能區分為應用系統及資料庫管理之帳號，並給予適當之權限。
- 具個人資料之資料庫系統帳號之密碼須為英數字混合，且不得與帳號名稱相同，密碼長度至少為8碼，並嚴禁管理人員轉知他人。
- 具機敏性資料之資料庫最高權限帳號存取授權，應僅限於資料庫管理人員或職務代理人。
- 具機敏性之測試資料，應僅由系統管理人員進行存取，且應將個人資料內容轉換為虛擬資料、模糊化或遮蔽。

個人資料安全控管作業說明書(續)

系統開發安全管理

- 系統測試環境所使用之設備環境應予獨立，不應與提供服務之設備環境共用。
- 具機敏性資訊之應用系統，應設計加密傳輸機制(如SSL或https等)，必要時應針對資料內容加以保護如資料庫加密，並記錄傳輸的相關資訊，包含傳輸來源、接收目的位址、傳送時間與傳輸成功或失敗等資訊。
- 應對具個人資料之重要資訊系統定期實施弱點掃描或滲透測試，以鑑別各單位應用系統與作業環境之風險，並針對弱點部分實施修補與改善，並保留相關紀錄以備查核。

個人資料安全控管作業說明書(續)

系統開發委外安全控管

- 為確保應用系統之安全性與可靠性，應於契約或建議書徵求文件中明訂下列安全管理事項：
  - 系統需求分析時，應考量現況及未來應用系統之運作環境配置、資料之重要性及遭受攻擊之可能性，據以發展應用系統之安全需求及系統功能。
  - 程式測試時，應進行相關安全性檢測，並提供相關測試報告與記錄。
  - 應用系統須進行源碼檢測，並提供相關檢測報告，以驗證程式碼之安全性。
  - 委外廠商每次交付之應用程式版本，應進行應用程式安全弱點掃描及程式碼安全檢測，若有弱點存在，委外廠商須負責修改。

個人資料安全控管作業說明書(續)

系統開發委外安全控管(續)

- 為確保應用系統之安全性與可靠性，應於契約或建議書徵求文件中明訂下列安全管理事項：
  - 契約期間如發生程式錯誤或資料漏失，經確認屬委外廠商責任者，應由委外廠商負責更正；另損及他人權益時，亦由委外廠商負責。
  - 委外廠商對業務上所接觸之資料，應採必要之保密措施。委外廠商及專案相關人員均應依本校規定填具保密切結。
  - 委外廠商應配合本校安全控管要求，辦理應用系統弱點修補、異常排除、事件通報及進行相關演練作業事宜。

目錄

個人資料保護緊急應變處理作業說明書

目的

- 為建立個人資料事故管理作業準則，並規範事故處理之作業事項，針對個人資料侵害之情形，決定其影響範圍及緊急程度，並能快速解決問題，確保事故能有效處理，特訂本說明書。

控制重點

- 制定個人資料事故通報及受理流程。
- 評估管理涉及個人資料之事故並紀錄發生原因及處理情形。
- 個資事故應定期管理及追蹤處理進度，以利管理階層有效掌握資訊。
- 個資事故應進行宣導，避免相同事故重覆發生。

個人資料保護緊急應變處理作業說明書(續)

◆個資事故定義

- 單一或一連串機率可能危害與威脅個資安全之非蓄意或非預期的個資事故；簡而言之，泛指對組織已構成傷害之事故。例如：
  - 個人資料檔案遭遇竊取、竄改、毀損、滅失或洩漏等相關事故。
  - 洩漏個人資料或違反個資政策之故意行為或重大人為疏失。
  - 販賣個人資料圖利。
  - 個人資料檔案遭受誤用。
  - 超過蒐集之特定目的處理或利用。
  - 未經同意蒐集個人資料。
  - 個人資料未應當事人請求修改、刪除、停止使用、製給複製本及閱覽權利。

個人資料保護緊急應變處理作業說明書(續)

◆建立個資事故通報、受理與分析

- 應建立完整之內部個人資料通報流程，當
  若無任何主管檢調機關和當事人之通報
  和罰則。
- 個資事故通報後，須依所通報之內容
  事故，則由「個人資料管理窗
  (詳下頁)。
- 違反「個人資料保護法」之規定，導致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。
- 應建立通報機制，確保所使用之方式(例如電話、郵寄、email等)可以通知到當事人，並留下紀錄。
- 個資事故通報人員依據各種管道向「個人資料管理窗口」進行通知，由「個人資料管理窗口」判斷是否為個資事件，若確定為個資事件後，將問題轉予權責單位進行處理，待權責單位處理完成後，將處理結果回覆「個人資料管理窗口」，由「個人資料管理窗口」判斷事件是否違反「個人資料保護法」，並回覆個資事故通報人員，且保留相關紀錄。
- 個資事故之當事人通報及受理程序，請依「個人資料事故通報及受理流程」(詳下頁)辦理。

依據電腦處理個人資料保護法施行細則修正草案第二十一條說明：
本法第十二條所稱適當方式通知，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。

個人資料保護緊急應變處理作業說明書(續)

- 「個人資料侵害事故通報與紀錄表」

文件編號	NCHU-PIMS-D-025	機密等級	內部限閱	版次	1.0

本表單蒐集之個人資料，僅限於特定目的使用，非經當事人同意，絕不移做其他用途，亦不會公佈任何資訊，並遵循本校資料保存與安全控管辦理。

一、通報單位基本資料

通報人單位／職稱／姓名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

通報人電話／傳真／E-mail＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

二、發生情形

發現日期	年　月　日　時　分
簡述發生經過與內容	
事故原因	☐ 個人資料檔案遭通竊取、竄改、毀損、滅失或洩漏等相關事故。 ☐ 洩漏個人資料或違反個資政策的故意行為或重大人為疏失。 ☐ 販賣個人資料圖利。 ☐ 個人資料檔案遭受誤用。 ☐ 超過蒐集之特定目的處理或利用。 ☐ 未經同意蒐集個人資料。 ☐ 個人資料未應當事人請求修改、刪除、停止使用、製給複製本及閱覽權利。 ☐ 其他：

二、個人資料管理窗口分派業務權責單位

業務權責單位：＿＿＿＿＿＿單位

個人資料管理窗口	組長	單位主管

三、業務權責單位處理情形

處理人員資料	單位：＿＿＿＿＿＿　職稱：＿＿＿＿＿＿ 姓名：＿＿＿＿＿＿　電話：＿＿＿＿＿＿		
簡述經過及結果			
經辦	組長	單位主管	

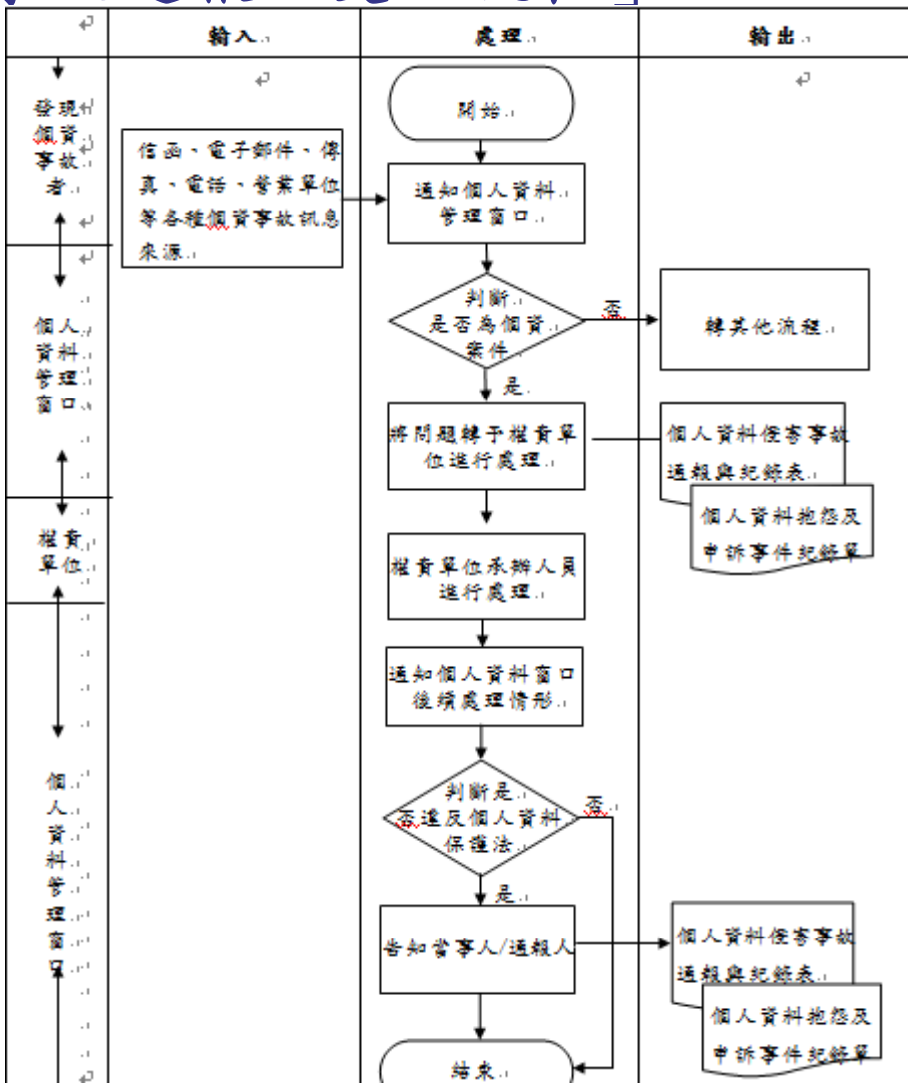
四、個人資料管理窗口覆核

結案日期＿＿＿年＿＿＿月＿＿＿日		
個人資料管理窗口	組長	單位主管

1. 緊急連絡電話：(04) xxxxxxxx　[秘書室]：(04)xxxxxxx
2. 本單所通報事件若非為個資事故，應指定權責單位主管。
3. 本單需由通報單位視自檢會受事故影響單位，未受影響單位需落實代理人制度，相關層級負責人員不在即由代理人或該單位主管代簽該批就必要處置，再轉知負責人員，以加速通報時效。

個人資料保護緊急應變處理作業說明書(續)

「個人資料事故通報及受理流程」



個人資料保護緊急應變處理作業說明書(續)

◆個資事故通報

- 同仁於發現個資遭侵害時，應通知個人資料管理窗口，由「個人資料管理窗口」判斷是否發生個資事故。
- 通報原則：
  - 個資事故發生時，應依通報順序逐級陳報。
  - 當上述任何一層級人員無法依層級順序被通報時，負責通報人員應往上一層級逕行陳報，以確保通報程序之即時性。

個人資料保護緊急應變處理作業說明書(續)

◆個資事故通報

- 判斷個資事故
  - 「個人資料管理窗口」接獲相關個資案件通知時，應立即協同相關人員蒐集相關跡證，初步判斷是否發生個資事故及其影響程度與範圍。
  - 若經判斷為個資事故，事故處理之業管單位應立即依據「個人資料事故通報及受理流程」，啟動個資應變措施相關處理作業。

個人資料保護緊急應變處理作業說明書(續)

◆記錄個資事故，啟動個資應變措施

- 應變措施應符合限制、處理、復原等三階段的事故處理原則，說明如下：
  - 針對可即時解決之個資事件，業務權責單位陳報主管審核後，並通報「個人資料管理窗口」。
  - 若個資遭到人為竄改或失竊等涉及民、刑事案件時，應即時通報警政或檢調單位請求處理。
  - 事故處理作業所留存之相關紀錄應至少保留1年備查。
  - 為提高個資侵害發生時之處理效率及應變能力，計畫內容包含計畫之說明、系統架構、緊急連絡人員清單、協力廠商清單及作業程序(含備援及復原程序)說明。

個人資料保護緊急應變處理作業說明書(續)

◆記錄個資事故，啟動個資應變措施

- 確認狀況排除：
  - 個資事故處理人員於處理完成後，應確認應變措施之有效性，並回報「個人資料管理窗口」及業務權責單位主管，視情況調整應變措施。
  - 個資事故發生之業務權責單位主管於初步認定事故排除後，仍應嚴密監控相關資訊，並進行必要之安全清查，防止潛伏之可疑行為再發生。
  - 個資事故確認排除後，業務權責單位主管應再回報「個人資料管理窗口」後續處理情形，且由其通知受事故影響之相關單位或回報上級單位。
  - 「個人資料管理窗口」應留存紀錄，並決定是否通報主管機關或通知個資當事人。
  - 「個人資料管理窗口」應儘速將損失彙整後，提供給「資訊安全暨個人資料保護推動委員」，負責協助召集人對外說明情況與處置方式。

個人資料保護緊急應變處理作業說明書(續)

◆記錄個資事故，啟動個資應變措施

- 檢討及改善：
  - 個資事故確認處理完成後，事故發生單位應檢討現行安全控制措施之完整性，並適當修訂相關作業管理規範或建置控制措施，且於必要時召開檢討會議。
  - 事故發生單位應於事故處理完畢後，進行相關矯正預防措施，避免同類型之個資事故重複發生。
  - 各單位權責主管應監督個資事故之後續處理及安全控制之有效性。
  - 個資事故之發生單位應為個人資料內部稽核作業之重點，並列入追蹤管理。
  - 由「個人資料管理窗口」彙整「個人資料侵害事故通報與紀錄表」，並在無牽涉個人隱私與本校業務機密之情況，將事件發生原因、過程、處理方式、注意事項及改善建議等內容，以網站或電子郵件等方式提供予員工，以做為內部個人資料保護安全宣導及事故預防之參考。

&

Thank You !