

華梵大學

Huaan University

個人資料保護法 & 資訊安全管理系統(ISMS)

報告人：李仁鐘

日期：104年10月5日

大綱

- 緣起
- 個人資料保護法介紹
- 如何實施個人資料保護法 & ISMS
- 工作事項



緣起

教育部統合視導

- 智慧財產權 (40%)
- 個人資料保護法 (30%)
- 資訊安全管理系統 (30%)



個人資料保護法架構

第一章 總則

第二章 公務機關對個人資料之蒐集、處理及利用

第三章 非公務機關對個人資料之蒐集、處理及利用

第四章 損害賠償及團體訴訟

第五章 罰則

第六章 附則

個人資料保護法

- 立法院於 **99年4月27日**，將電腦處理個人資料保護法，修訂並三讀通過為「個人資料保護法」
- 「個人資料保護法」 **99年05月26日** 總統府正式公布修正之全文



個人資料保護法

- 為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

➤ 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。

P.S.

1. 所謂人格權，指一般人格權而言，乃關於人之價值與尊嚴的權利。
2. 每個生物學意義上的個人都是自然人。只有自然人才有資格享有基本人權。



安全維護事項（細則第12條）

保護標的：

防止個人資料被竊取、竄改、毀損、滅失或洩漏

1	配置管理之人員及相當資源
2	界定個人資料之範圍
3	個人資料之風險評估及管理機制
4	事故之預防、通報及應變機制
5	個人資料蒐集、處理及利用之內部管理程序
6	資料安全管理及人員管理
7	認知宣導及教育訓練
8	設備安全管理
9	資料安全稽核機制
10	使用紀錄、軌跡資料及證據保存
11	個人資料安全維護之整體持續改善



賠償責任與罰則

■ 調整賠償義務及罰則：

- 民事賠償：新台幣→2億元
- 刑事處罰：新台幣→100萬元
- 有期徒刑：→5年以下
- 意圖營利犯罪者，非告訴乃論
- 行政處罰：新台幣→50萬元

■ 企業需負舉證責任

- 除能證明無故意或過失，否則需負損害賠償責任



個資法統合視導

- 個資法遵循性(10%)
- 教育部頒訂「教育體系個人資料安全保護基本措施及作法」配合度(12%)
- 個人資料保護持續改善管理流程(8%)



視導項目	視導指標	評分標準
(一) 個資法遵循性(10%)	1. 已建立個人資料保護組織？並指定機關高層為個資業務之機關召集人？(2分)	已建立個人資料保護組織並指定機關高層為個資業務之機關召集人：2分。（檢附機關個人資料保護組織相關規範）
	2. 已定期界定並清查機關內「個人資料檔案」？(2分)	已定期界定並清查機關內「個人資料檔案」：2分。（提供歷年及最新「個人資料檔案」清冊）
	3. 已指定具備適當資格或經驗之專人依法令規定辦理個資安全維護及保管事項？(2分)	已指定具備適當資格或經驗之專人依法令規定辦理個資安全維護及保管事項：2分。（檢附受指定專人相關經驗或資格文件(如具BS 10012 LA或相關個資證照等))
	4. 已設置「個資保護聯絡窗口」，協調聯繫個資事宜，並將聯繫方式（如：電話、email）置於單位網站以便利民眾提出申訴與救濟？(2分)	已設置「個資保護聯絡窗口」並將聯繫方式置於單位網站：2分。（提供個資聯繫之網頁資料）
	5. 已訂定個人權利行使的流程，並於法律允許之範圍內提供資料當事人下列權益：(2分) (1) 查詢或請求閱覽 (2) 請求製給複製本 (3) 請求補充或更正 (4) 請求停止蒐集、處理或利用 (5) 請求刪除	已訂定個人權利行使的流程且包含提供5種資料當事人權益：2分。（提供已訂定個人權力行使的流程規範）

(二)教育部頒訂「教育體系個人資料安全保護基本措施及作法」配合度(12%)	1. 已依據「教育體系個人資料安全保護基本措施及作法」，辦理「人員管理措施」？(2分)	提供佐證資料：2分。（提供「人員管理措施」相關說明文件）
	2. 已依據「教育體系個人資料安全保護基本措施及作法」，辦理「作業管理措施」？(2分)	提供佐證資料：2分。（提供「作業管理措施」相關說明文件）
	3. 已依據「教育體系個人資料安全保護基本措施及作法」，辦理「物理環境管理措施」？(2分)	提供佐證資料：2分。（提供「物理環境管理措施」相關說明文件）
	4. 已依據「教育體系個人資料安全保護基本措施及作法」，辦理「技術管理措施」？(2分)	提供佐證資料：2分。（提供「技術管理措施」相關說明文件）
	5. 已依據「教育體系個人資料安全保護基本措施及作法」，辦理「認知宣導及教育訓練」？(2分)	提供佐證資料：2分。（提供當年度辦理「個資認知宣導及教育訓練」相關佐證資料）
	6. 已依據「教育體系個人資料安全保護基本措施及作法」，辦理「紀錄機制」？(2分)	提供佐證資料：2分。（提供「紀錄機制」相關說明文件）



(三)個人資料保護持續改善管理流程(8%)	1. 已進行個資風險評鑑，設定資料保護要求？(2分)	提供佐證資料：2分。（提供風險評鑑報告書）
	2. 已定期執行稽核作業，以確保相關個人資料保護管理措施之有效性(2分)	提供佐證資料：2分。（提供稽核結果報告書）
	3. 已將個資業務委外監督管理機制納入合約條款，並進行適當之稽核(4分)	(1)已將個資業務委外監督管理機制納入合約條款且有進行相關監督稽核紀錄：4分。 (2)僅有委外監督管理機制之合約條款，仍未進行相關監督稽核作業2分。（a. 提供個資委外契約範本 b. 提供委外監督相關稽核紀錄）



統合視導時程

- 前置作業階段：自104年6月1日起
- 自我檢核階段：自104年9月1日起至105年8月31日
 - 105.8 下半年受訪學校上傳並提交各項目訪視表及附件
- 實地訪視階段：自105年10月1日起至105年12月31日
- 結果決定階段：自106年1月1日起至106年6月30日

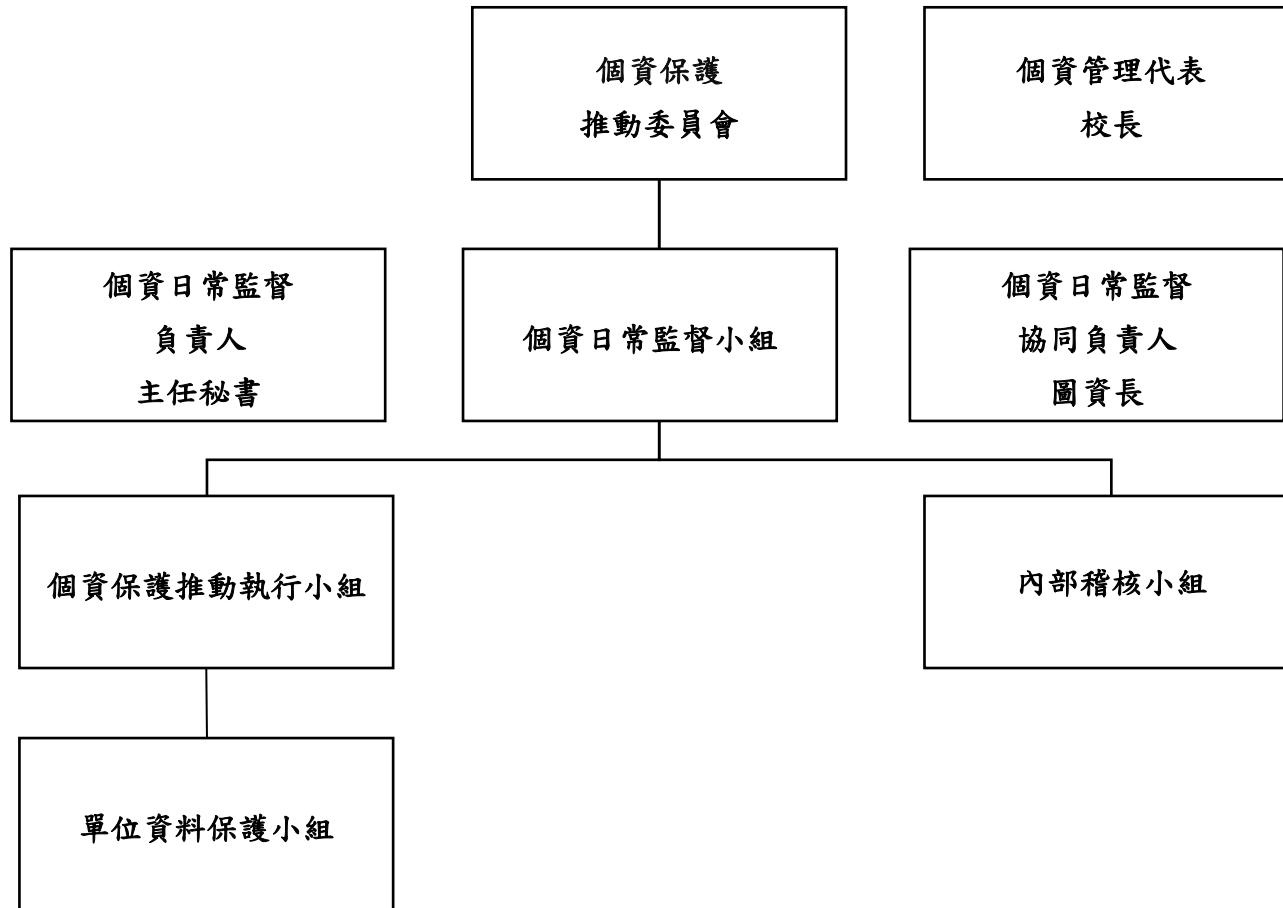


個人資料保護管理政策聲明

HFU-PIMS-A-001-個人資料保護管理政策聲明



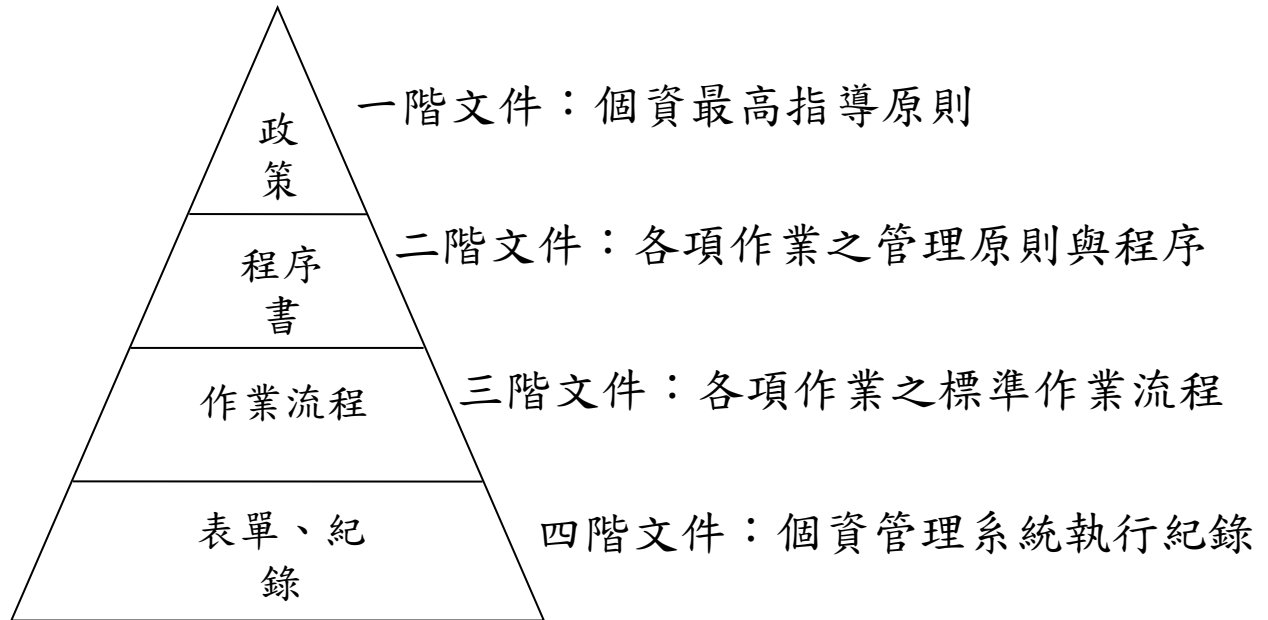
個人資料保護推動組織架構



HFU-PIMS-B-001-個人資料保護推動組織程序書

個資法文件

四階文件



HFU-PIMS-D-002-個人資料管理制度文件清冊

四階文件教育訓練

- 圖資長 HFU-PIMS-A-001、HFU-PIMS-B-001
- 孫明綢組長 HFU-PIMS-B-005、HFU-PIMS-B-006
- 高俊君組長 HFU-PIMS-B-003、HFU-PIMS-B-004
- 張維世組長 HFU-PIMS-B-002、HFU-PIMS-B-008、
HFU-PIMS-B-009、HFU-PIMS-B-012
- 郭昕周組長 HFU-PIMS-B-007、HFU-PIMS-B-010、
HFU-PIMS-B-011
- 顧問

P. S. 包含相關之三、四階文件



內部稽核小組

- 張組長
- 郭組長
- 禧慧
- 各一級行政單位
- 各學院代表



個資保護推動執行小組

- 文管成員
 - 張組長
 - 各行政單位
 - 各學院代表
- 盤點&風險評估成員
 - 郭組長
 - 各行政單位
 - 各學院代表
- 技術支援成員
 - 圖資處(梁光玉 李光晟)



相關工作事項

- 個資不執行外部稽核及申請驗證
- 資訊安全管理系統(ISMS)改版
- 建立個人資料保護法網頁專區
 - <http://pims.hfu.edu.tw>

工作事項(1/2)

項次	工作事項	主辦單位	協辦單位
1	草擬及公告本校個人資料保護管理政策規範	圖書資訊處	
2	盤點及公告本校個人資料檔案	圖書資訊處	各單位
3	本校個人資料聯絡窗口	秘書室	圖書資訊處
4	各單位個人資料聯絡窗口	各單位	
5	召開個人資料保護推行委員會會議	圖書資訊處	各單位
6	訂(修)定單位個人資料管理作業流程、保護規範或表單	各單位	
7	檢視單位蒐集、處理及利用個人資料之特定目的、適用法規是否適法	各單位	秘書室
8	本校教職員工之個人資料保護法規教育訓練	人事室	
9	本校學生之個人資料保護法規教育訓練(含社團)	學生事務處	
10	執行個人資料保護政策、制度及措施	各單位	



工作事項(2/2)

項次	工作事項	主辦單位	協辦單位
11	委外作業要求受託單位辦理個人資料保護管理措施	各單位	
12	稽核本校個人資料保護作業之運作情形	個人資料保護稽核小組	
13	回應處理當事人請求查詢、更正、停止蒐集、處理、利用或刪除個人資料	各單位	
14	個資違規事件通報、應變	各單位	秘書室、圖書資訊處
15	個資違規事件調查及賠償	各單位	秘書室、圖書資訊處(彙整數位證據)



工作時程(1/2)

工作項目	備註	期程
行政會議通過個人資料保護委員會設置要點	法規委員會	104/09/22
資訊服務委員會	相關系統開發	104/09/23
一級主管教育訓練	1hr	9/29
行政會議 #153		104/09/30
個人資料保護委員會會議	通過： 1. 組織架構 2. 個人資料安全保護基本措施 3. 個人權利行使的流程 4. 四階文件	104/10/07-21
調查各單位資料保護小組成員		104/10/07~104/10/28
教育訓練（一）	內容： 個資法 四階文件 年度工作排程 個資盤點	104/10/28(三)下午 個資盤點 104/11/04(三)下午 個資盤點 104/11/25(三)下午 個資盤點進階課程
個資盤點：紙本/電子檔案	同時進行系統分級	104/10/28~105/01/06

工作時程(2/2)

工作項目	備註	期程
教育訓練 (二)	內容： 風險評鑑 風險處理 風險複評	(105/01/06 風險評鑑) (105/01/13 風險評鑑)
風險評鑑		105/01/13~105/03/29
風險評鑑審查會議		105/03/30
風險處理		105/03/31~105/04/26
風險處理審查會議		105/04/27
風險複評		105/04/28~105/5/25
內部稽核教育訓練		105/06/01
內部稽核		105/06/01~105/06/22
內部稽核會議		105/06/29
管審會	內部稽核一月內	105/07/06

校長指示事項

- 同意個人資料保護法推動，先以內部稽核即可，經費部份先自行調整勻支，不足部份再行討論
- 有關資安、兩性、個資、智財權等，納入新生教育訓練宣導
- 加強同仁教育訓練(心態及知識)



敬請指教

