

個人資料管理制度 (PIMS)

長庚大學

個人資料管理制度

內部稽核報告

文件等級：限制使用

版 次：1.0

稽核日期：110 年 11 月 30 日

一、稽核目的

為實際了解長庚大學（以下簡稱 貴校）個人資料管理落實執行之情形，依據「個人資料保護法」、「個人資料保護法施行細則」、「教育體系資通安全暨個人資料管理規範」、「教育體系資通安全暨個人資料管理規範-附錄B 個人資料管理規範」及貴校個人資料管理制度文件執行稽核，以確保個人資料管理之落實執行。

本作業將採獨立查核方式，判斷個人資料管理的控制目標、方法、流程及程序是否符合法令法規及貴校之個人資料管理暨資料保護要求，以作為後續改進參考。

二、稽核範圍

- (一) 資訊中心-軟體組(與註冊組、研究生教務組相關之系統個人資料管理作業流程)。
- (二) 教務處-註冊組、研究生教務組。

上述單位作業過程中蒐集、處理及利用個人資料管理作業流程及使用資訊設備之相關人員。

三、稽核項目

個人資料保護法施行細則第12條中適當安全維護措施，說明如下：

- (一) 配置管理之人員及相當資源。
- (二) 界定個人資料之範圍。
- (三) 個人資料之風險評估及管理機制。
- (四) 事故之預防、通報及應變機制。
- (五) 個人資料蒐集、處理及利用之內部管理程序。
- (六) 資料安全管理及人員管理。
- (七) 認知宣導及教育訓練。
- (八) 設備安全管理。
- (九) 資料安全稽核機制。
- (十) 使用紀錄、軌跡資料及證據保存。
- (十一) 個人資料安全維護之整體持續改善。

教育體系資通安全暨個人資料管理規範本文與附錄B 個人資料管理規範要求，說明如下：

- (一) 本文。
- (二) 個人資料管理政策。
- (三) 個人資料管理組織。
- (四) 人員認知與訓練。
- (五) 個人資料之識別與風險管理。
- (六) 公正與合法的處理。
- (七) 個人資料特定目的處理。
- (八) 適當相關與正確性。
- (九) 保存與處置。
- (十) 當事人權利。

- (十一) 資料安全議題。
- (十二) 國際傳輸。
- (十三) 委外管理。

四、稽核結果及其他建議事項

(一) 資訊中心：軟體組

1. 個人資料檔案清冊內容的完整性應再調整
 - 0420-01多勾選了委外作業（台塑網）；0420-07資料存放欄位及保存期限誤植（中心目前無存放資料）。
2. 資料保存期限與銷毀作業應再行評估適切性
 - 系統修改需求單中涵蓋個資資訊，目前已銷毀但未留存銷毀紀錄。
3. 個人資料控管措施宜再強化
 - 抽查發現個人電腦(陳○○)，未依規定設定螢幕保護程式10分鐘（目前設30分鐘）。

(二) 教務處：註冊組

1. 個人資料檔案清冊內容的完整性應再調整
 - 0610-06、0610/0650-09-01 委外作業未勾選，0610/0650-09-01來源漏列大考中心。
2. 個人資料保存期限應再評估目前訂定之適切性
 - 抽樣個人資料檔案清冊內容發現個人資料保存期限多數均設為永久保存，應再考量個人資料保存期限之合理性。
3. 個人資料控管措施宜再強化
 - 抽查個人電腦(陳○○)安裝WinRAR5.7破解版，應移除。
 - 抽查個人電腦(莊○○)作業系統仍為Windows 7，應更新。

(三) 教務處：研究生教務組

1. 個人資料檔案清冊內容的完整性應再調整
 - 0610/0650-09-01、0610/0650-14-01委外作業未勾選，0650-08-01 放置位置誤植，應更新為公文櫃，0610/0650-15-01無利用作業，0610/0650-06-01有利用（教育部）。
 - 0610/0650-11-01漏列委託書。
1. 個人資料保存期限與銷毀作業應再評估適切性
 - 個人資料保存期限多數設為永久保存，請再考量合理性。
 - 個人資料銷毀目前未落實填寫組織已制訂核准之「CGU-PIMS-I-04-003 個人資料

紀錄銷毀申請單」。

2. 個人資料控管措施宜再強化

- 個人電腦(林○○) 安裝WinRAR5.01破解版，請移除；作業系統為Windows 10 1903請更新。

(四) 其他共通性建議

- 學生資料蒐集後，目前直接匯入ERP(MIS)系統，但該系統管理控制權在總公司（企業）非學校內，如何在個資告知中呈現資訊蒐集後會存放於非學校內的問題，煩請組織應審慎考量。
- 含有個人資料之資訊於傳遞過程建議應加密傳送，學校可考量統一規範密碼設定方式。