

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：111 年 06 月 06 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」、「附錄B 個人資料管理規範」及貴校個人資料管理制度文件要求執行稽核，以檢視個人資料管理之落實情形。

本作業將採專案查核方式進行，判斷個人資料管理的流程及程序是否符合法令法規及貴校之個人資料管理制度文件要求，以作為後續改進參考

二、稽核範圍

- (一) 學務處：學雜費減免業務及學生校內及校外獎助學金業務。
- (二) 人事室：教職員退休、資遣及撫卹案件之辦理業務。

上述作業過程中蒐集、處理及利用個人資料及使用該資料或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) 學務處：學雜費減免業務及學生校內及校外獎助學金業務

- 經查碎紙機內碎紙後，其資訊內容容易被拼湊。

(二) 人事室：教職員退休、資遣及撫卹案件之辦理業務

- 經查「0200-04-02電子式資產」個人資料範圍多列了戶籍謄本、學歷、帳戶資訊。
- 經查碎紙機內碎紙後，其資訊內容容易被拼湊。

(三) 口頭提醒：

- 請再評估教職員退休、資遣及撫卹案件之辦理業務，其紙本個資（副本）永久保存適當性。(人事室)
- 組織採用行動硬碟備份資料，應注意其硬體或資料失竊的風險。(人事室)

(四) 其他共通性建議

- 勞動契約缺少學生未滿20歲應有法定代理人同意並簽名或蓋章欄位。
- 相同之個人資料檔案保存期限，電子與紙本定義不一致，經查因為電子資料存放於MIS系統中單位無法刪除。【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，因此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。（去年已提出之議題）】。