長榮大學

個人資料檔案安全維護計畫

機密等級：一般
文件編號：PI-A-0200
版　　次：1.2
修訂日期：113.10.01

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	112.11.01		俞怡中	112.11.01. 經「112 學年度第 1 次資訊安全執行小組、個人資料保護執行小組聯席會議暨管理審查會議」審議通過
	112.11.03		俞怡中	呈資安長簽核通過
1.1	113.06.14	5	俞怡中	新增管理組織一節
		9	俞怡中	配合智慧財產權與資訊安全暨個人資料保護宣導及執行委員會設置辦法修正，個人資料保護長修訂為個資管理長
1.2	113.10.01		俞怡中	修正程序書名稱，將【資安暨個資】修訂為【資訊安全暨個人資料保護】 同時內文相關字樣一併修正。

目錄

1 依據與目的 3
2 適用範圍 3
3 權責 3
4 名詞定義 4
5 作業說明 4
5.1 個人資料管理安全 4
5.2 個人資料保護推動組織 5
5.4 個人資料保護 7
5.5 內部稽核管理 8
5.6 實體環境與設備安全管理 8
5.7 人員管理及認知宣導教育訓練 9
5.8 個人資料安全持續改善 9
6 審議 9
7 相關文件 9

個人資料檔案安全維護計畫

1 依據與目的

依據教育部「私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法」第三條定訂個人資料檔案安全維護計畫，以落實長榮大學(以下簡稱本校)個人資料檔案管理之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏，特訂定本實施計畫。

2 適用範圍

本校所有有關個人資料保護相關作業均適用之。

3 權責

3.1 「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」

3.1.1 個人資料保護管理政策之研擬與管理制度之審查。

3.2 「個人資料保護執行小組」

3.2.1 個人資料保護事項權責分工之協調，並提供必要資源予以執行任務。

3.2.2 對所採用之技術、方法及程序之研議及評估。

3.2.3 個人資料保護相關事件之檢討及監督。

3.3 「個人資料保護執行小組」之「作業工作小組」

3.3.1 協助各單位進行個資盤點與彙整。

3.3.2 各單位個人資料管理、保護及維護等事項，並落實於相關業務及人員。

3.3.3 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。

3.4 「個人資料保護執行小組」之「稽核工作小組」

3.4.1 實施個人資料管理制度內部稽核。

3.4.2 確認個人資料管理制度實施之有效性，並鑑別潛在之風險。

3.4.3 協助追蹤矯正預防措施之處理與完成情形。

3.5 本校所有同仁

3.5.1 落實個人資料保護相關作業規範。

3.5.2 執行本校於各項個人資料保護之決策及交辦事項。

4 名詞定義

無。

5 作業說明

5.1 個人資料管理安全

5.1.1 個人資料範圍包含自然人姓名、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。

5.1.2 建立個人資料保護管理組織，並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。

5.1.3 建立可再現性之風險識別方法機制，以鑑別組織處理相關個資作業於個資生命週期過程中可能產生之風險，釐清並配合適當控制措施，降低風險於可接受範圍內。

5.1.4 對個人資料之蒐集、處理、利用、傳輸與銷毀應訂定相關管理規範，且符合適當、相關且不過度之使用原則，記錄個人資料之紙本文件、電子檔案、資料庫，應妥善保管並建立存取管控機制，執行重點：

5.1.4.1 蒐集個人資料時應向當事人盡到告知義務，並取得同意。

5.1.4.2 個人資料之蒐集、處理與利用須評估目的及範圍為適當、相關且不過度，不處理無關或超過原來所陳述使用目的之個人資料。

5.1.4.3 個人資料檔案應建立保存期限，並確實辦理保存與銷

毀。

5.1.4.4 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。

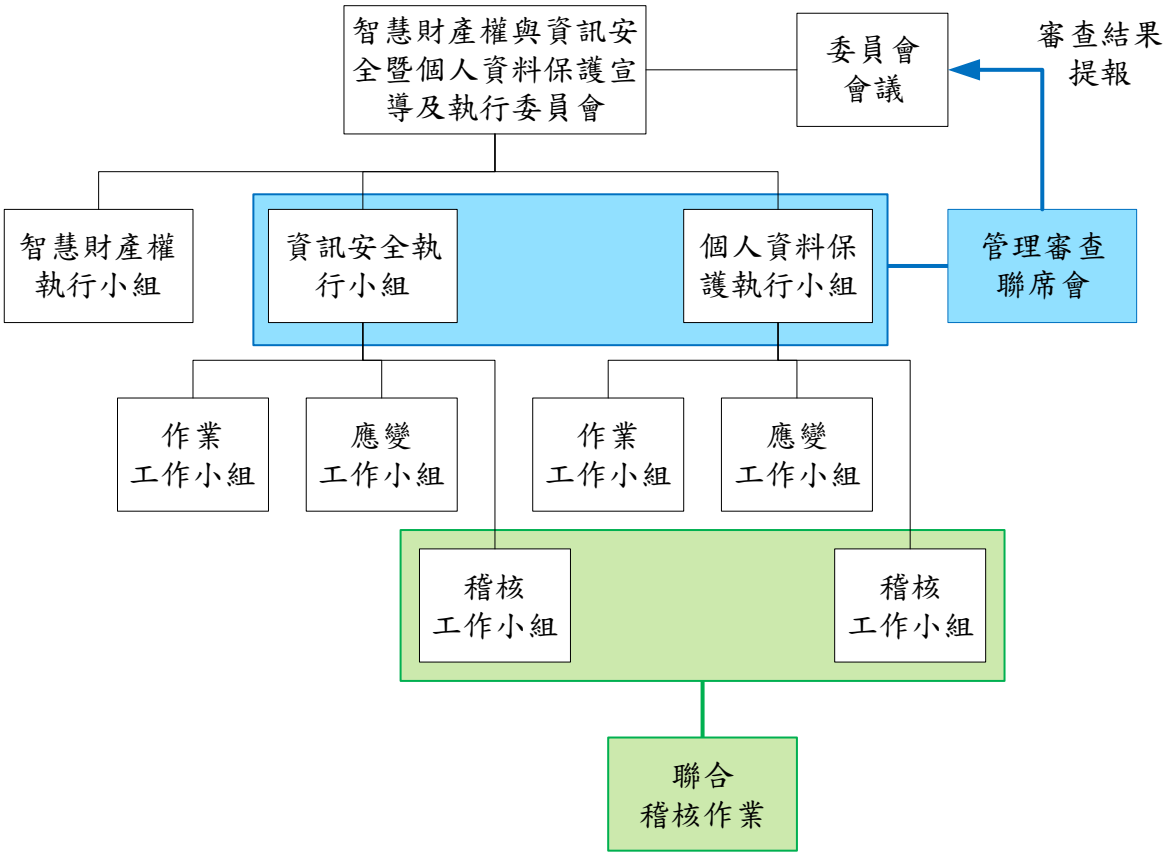
5.1.4.5 個人資料存取權限之授權管理，必須依人員執掌角色所需，且以執行業務及職務所必要的最低資源存取授權為限。

5.1.4.6 含有個人資料之紙本文件、資料庫資料，非日常作業之讀取、列印、存檔、交換、分享及銷毀等處理及利用行為，應提出申請，經核准後方可執行，以建立授權、監督及行為記錄機制。

5.1.4.7 業務單位個人資料蒐集之特定目的消失或個人資料檔案保存期 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。

5.2 個人資料保護推動組織

5.2.1 本校以「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」(以下簡稱委員會)為推動組織，由校長、副校長、各行政及教學單位一級主管、法學專家、學生會會長及各學院學生代表組成。校長擔任召集人並為會議主席，由督導相關業務之副校長擔任個資管理長；下設個人資料保護執行小組，由圖書資訊長擔任召集人，統籌個人資料保護相關之推動與執行事項。委員會每學期召開一次委員會議，由個人資料保護執行小組提報執行情形，並提案審議相關事項。



5.2.2　委員會之設置，依本校「長榮大學智慧財產權與資訊安全暨個人資料保護宣導及執行委員會設置辦法」規範施行。

5.2.3　各執行小組與工作小組之權責與職掌，依本校個人資料管理制度文件「資訊安全暨個人資料保護組織程序書」程序書規範施行。

5.3　事故預防、應變與通報機制

5.3.1　本校提供單一窗口受理當事人之請求或申訴事件，及建立個人資料事故通報程序，確實紀錄通報與處理情形，並追蹤應變措施之有效性。

5.3.2　提供單一窗口受理當事人之請求，提供其個人資料之查詢、閱覽、製給複製本。單一窗口以本校「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」網頁公告資訊為準。

5.3.3　當事人對本校處理個人資料不滿時，可透過電話或電子郵件方式提出申訴，並由專人受理，並記錄於「個人資料申訴/侵害事

故通報與紀錄表」。

5.3.4 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程序書」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。

5.3.5 建立完整之內部個人資料事故通報流程，於發生個資外洩事故時，必須告知當事人並留下通報與處理紀錄。

5.3.6 權責單位個資管理人應將相關異常通知、事故判斷及處理情形等相關資訊確實記錄，並陳報權責單位主管審核。

5.3.7 權責單位個資管理人於處理完成時，應確認應變措施之有效性，隨時回報權責主管及相關單位，並視情況調整應變措施。

5.4 個人資料保護

本校應確保個人資料受到妥善保護，避免非經授權之閱覽、存取。

5.4.1 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。

5.4.2 各單位公務文書及紙本郵件應有專人負責收發。

5.4.3 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。

5.4.4 有備份必要之個人資料，除必要時採取加密機制，儲存備份資料之媒體亦應以適當方式保管，且宜定期進行備份資料之還原測試，以確保備份之有效性。

5.4.5 儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之，以避免資料不當外洩。

5.4.6 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。

5.4.7 電腦系統中應安裝防毒軟體，並定期更新病毒碼，避免惡意程式與系統漏洞對作業系統之威脅。

5.4.8 為確認所訂定之相關程序是否落實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，各單位應保存相關紀錄以供查驗。

5.5 內部稽核管理

透過定期內部稽核管理，確認個人資訊管理制度與矯正預防措施之實施情形。

5.5.1 建立內部稽核管理機制，確認個人資訊管理制度實施之有效性與落實情形。

5.5.2 每年至少辦理一次內部稽核，並針對控管結果之不符合事項與潛在風險，規劃改善及預防措施。執行改善及預防措施時，應完成以下事項：

- 確認不符合事項根本原因。
- 提出改善及預防措施。
- 紀錄執行結果。

5.6 實體環境與設備安全管理

為確保個人資料存放環境與設備之安全，避免未經授權之人員進出辦公環境，處理或儲存大量個人資料之資訊設備，應規劃安全防護程序，或採取適當隔離控管措施，執行重點：

5.6.1 本校同仁應保持警覺，留意陌生人員進出辦公環境，若發現身份不明或可疑的人員，應主動詢問其身份，並視需要通知相關單位處理。

5.6.2 委外廠商及訪客應於本校各單位指定之區域內活動。

5.6.3 網路環境應建立安全防護機制，網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

5.6.4 存放個人資料之伺服器、應用系統及資料表(Database Table)等於系統效能許可下宜啟用稽核日誌，以保存相關稽核日誌與軌

跡資訊。

5.6.5 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。

5.7 人員管理及認知宣導教育訓練

本校應對組織內部人員規劃訓練課程，以提升人員個人資料保護之安全認知及警覺意識，並要求委外廠商人員遵循本校個人資料保護相關規定。

5.7.1 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。

5.7.2 權責單位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。

5.7.3 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」及本校個人資訊管理制度相關規定，且不得對外透露。

5.8 個人資料安全持續改善

本校應建立個人資料管理持續改善機制，透過適當的矯正或預防措施，矯正因內部或外來威脅所產生之風險，以達成持續改善之目標，提升整體個資保護安全的強度。

6 審議

本計畫經「個人資料保護執行小組」管理審查會議審議，簽請個資管理長簽准後公告施行，修訂時亦同。

7 相關文件

7.1 個人資料保護法。

7.2 私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施

辦法

7.3 資訊安全暨個人資料保護組織程序書。

7.4 資訊安全暨個人資料保護稽核作業程序書。

7.5 個人資料蒐集處理利用與安全管理程序書。

7.6 個人資料保護緊急應變處理程序書。

7.7 個人資料安全控管作業說明。

7.8 個人資料申訴/侵害事故通報與紀錄表