德明財經科技大學個人資料檔案安全維護計畫

113 年 8 月 5 日智財權暨個資保護委員會會議通過

壹、依據

德明財經科技大學（以下簡稱本校）依據行政院之「個人資料保護法」(以下簡稱個資法）以及教育部之「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」，落實個人資料保護及管理，特訂定本校「個人資料檔案安全維護計畫」(以下簡稱本計畫)。

貳、目的

為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校所屬人員應依本計畫辦理個人資料檔案安全管理維護。

參、適用範圍

本校承辦相關個人資料作業均適用之。

肆、個資保護規劃及權責

一、智慧財產權暨個人資料保護委員會(以下簡稱智財暨個資委員會)

(一)個人資料保護管理政策之訂定與管理制度之審查。

(二)訂定及執行本計畫，包括業務終止後之個人資料處理方法。

(三)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。

(四)對所採用之技術、方法及程序之研議及評估。

(五)個人資料保護相關事件之檢討及監督。

二、智財暨個資委員會推動小組

(一)協助各單位進行個資盤點與彙整。

(二)協助各單位個人資料管理、保護及維護等事項。

三、智財暨個資委員會稽核小組

(一)協同本校內部稽核小組執行全校個資保護作業稽核。

(二)協助鑑別潛在之風險、追蹤矯正預防措施之處理與完成情形。

四、智財暨個資委員會緊急事件處理小組

協同本校校安中心負責於重大個資事件發生時，緊急處理、通報並恢復原狀。

五、各單位個人資料保護聯絡窗口暨承辦人

(一)進行單位內個資盤點與彙整。

(二)單位內接獲個人資料抱怨申訴、個資事件處理、個人權利行使處理作業。

六、本校所有同仁

(一)落實個人資料保護相關作業規範。

(二)執行本校於各項個人資料保護之決策及交辦事項。

伍、作業內容

一、作業管理措施

(一)個資檔案資料庫應定期備份。

(二)處理個資檔案相關之資訊系統或應用程式使用完畢後，應立即登出。

(三)內部傳遞或與其他機關交換個資時，應選擇可靠且具備保密機制之傳遞方式，如實體文件封袋並加以彌封，或對資料檔案壓縮加密。

(四)進行個人資料國際傳輸，應符合相關法規並制訂作業規範。

(五)儲存個資檔案之電腦或相關設備如需報廢或移轉他用時，檔案應確實刪除。

(六)報廢之設備若有儲存個資檔案，應避免資料不當外洩，並採取下列銷毀措施：

1.硬碟或隨身碟利用檔案資料清除軟體或以物理方式破壞，清除檔案資料內容。

2.無法清除檔案資料內容之儲存媒體如光碟片，應以物理方式破壞，使其無法繼續使用。

(七)紙本個資文件，不得回收再利用，應用碎紙機或依其他核可之方式進行銷毀；電子檔案須確實刪除並清空資源回收筒。

(八)可攜式儲存媒體使用規範：

1.可攜式儲存媒體如需連接本校電腦設備或網路時，應先進行病毒掃描。

2.具個資之資料應避免長期存放於可攜式儲存媒體，如有儲存之必要時，應考量使用加密技術。

3.可攜式儲存媒體如為機關內共同使用，使用者切記在使用完畢後將所有個資文件刪除，以避免個資資料不當外洩。

(九)個資委外作業

1.個資若委外建檔，應於委外合約中載明所處理之個資保密義務、資訊安全相關責任及違反之罰則。

2.與委外廠商所簽訂正式書面協議或契約中，應明確陳述契約終止或解除時，相關個人資料之銷毀或交還程序。

二、物理環境措施

(一)儲存個資之資訊設備應置於實體安全區域（如門禁控管之辦公區域或機房），或與外部網路隔絕（如防火牆），設置門禁或監視錄

影設備，避免有心人士或非授權人員存取。

(二)儲存個資檔案之磁碟、磁帶及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如上鎖之保管箱、書櫃或檔案室），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。

三、技術管理措施

(一)使用個人電腦、相關設備或系統處理個資檔案，應設置使用者登入帳號及密碼，帳號不得與他人共用，密碼則須符合安全之密碼複雜度原則且定期更新。

(二)儲存個資之資訊設備應安裝防毒軟體，並設定自動更新病毒碼及定期執行排程掃描。

(三)儲存個資之資訊設備應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定一定時間內。

(四)個資檔案禁止存放於網路分享，或設定存取權限至指定之目錄。

(五)儲存個資之資訊設備應定期檢視、更新作業系統與應用程式漏洞。

(六)使用資通系統處理特種個人資料時，應採取下列資訊安全措施：

1.使用者身分確認及保護機制。

2.個人資料顯示之隱碼機制。

3.網際網路傳輸之安全加密機制。

4.應用系統於開發、上線、維護等各階段軟體驗證及確認程序。

5.個人資料檔案與資料庫之存取控制及保護監控措施。

6.防止外部網路入侵對策，並定期演練檢討改善。

7.非法或異常使用行為之監控及因應機制，並定期演練檢討改善。

四、事故之預防、通報及應變機制

本校應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，確實記錄通報與處理情形，並追蹤應變措施之有效性，執行重點：

(一)採取適當之措施，控制事故對當事人造成之損害。

(二)查明事故發生原因及損害狀況，並以適當方式通知當事人。

(三)研議改進措施，避免事故再度發生。

(四)發生個人資料被竊取、 洩露、竄改、或其他侵害事故發生時起七十二小時內，填具個人資料侵害事故通報與紀錄單，通報主管機關，若未依時限通報，應附理由，並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。

五、認知宣導及教育訓練

(一)本校應對處理個資之專人施予資訊安全與個資保護之教育訓練，並不定期宣導個資保護之重要性。

(二)本校應對教職員生實施個資保護法認知宣導。

六、紀錄機制

本校執行安全維護計畫各項程序及措施，應保存下列紀錄：

(一)個人資料之維護、修正、刪除、銷毀及轉移。

(二)提供當事人行使之權利。

(三)存取個人資料系統之紀錄。

(四)因應事故發生所採取之措施。

(五)定期檢查處理個人資料之資訊系統。

(六)教育訓練。

(七)業務終止後處理紀錄。

七、業務終止處理作業

業務終止後，其保有之個人資料之處理方式及留存紀錄如下：

(一)銷毀：可使用碎紙機、物理破壞或其他不可逆之實體破壞方法，經審核奉准後，於時限內實施，進行前項個人資料銷毀處理時，應記載處理之時間、地點，並以照相或錄影方式留存相關紀錄。

(二)移轉：業務移轉經審核奉准，於時限內實施移轉作業，並記錄移轉之文件、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

(三)刪除、停止處理或利用個人資料：業務終止後經審核奉准，於時限內實施資料刪除、停止處理或利用作業，並留存時間或地點等記錄。

陸、其他

本計畫經智慧財產權暨個人資料保護委員會會議通過，陳請校長核定後發布實施，修正時亦同。