明新學校財團法人明新科技大學個人資料檔案安全維護計畫

104 年 9 月 14 日個人資料保護推動委員會會議訂定

113 年 11 月 8 日個人資料保護推動委員會會議修正

一、目的

明新學校財團法人明新科技大學（以下簡稱本校）為落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損或洩漏，與業務終止後個人資料處理方法等相關個人資料管理事項，特訂定本校個人資料檔案安全維護計畫（以下簡稱本計畫）。

二、依據

(一) 個人資料保護法

(二) 個人資料保護法施行細則

(三) 個人資料保護法之特定目的及個人資料之類別

(四) 本校個人資料保護推動委員會設置要點

(五) BS10012 國際標準

(六) 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

三、適用範圍

本校之個人資料管理範圍涵蓋全校。包括基於特定目的範圍內所有之教育或訓練行政、學生資料管理、人事管理、內部控制事項，及所有教職員工與學生之個人資料蒐集、處理、利用及國際傳輸。

四、權責

(一) 個人資料保護推動委員會

1. 本校個人資料保護政策之擬議與推動。
2. 本校教職員工生個人資料保護意識之提升及教育訓練計畫之研議。
3. 本校個人資料隱私風險之評估及管理。
4. 本校個人資料管理制度適法性與合宜性之檢視、審議及評估。
5. 其他本校個人資料保護、管理之規劃及執行事項。

(二) 個資推動小組

1. 協助各單位進行個資盤點與彙整。
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. 負責規劃個人資訊管理制度之維運工作及文件之制（修）定作業。

(三) 緊急事故處理小組

1. 評估個人資料安全事件的影響範圍，啟動緊急應變機制並進行事件損害控制。
2. 個資事故發生時，辦理對外說明或記者會。

(四) 個資稽核小組

1. 擬定稽核計畫。
2. 辦理個資管理稽核作業。
3. 複查稽核報告不符合事項之矯正措施。

(五) 本校所有同仁

1. 落實個人資料保護相關作業規範。
2. 執行本校於各項個人資料保護之決策及交辦事項。

五、名詞定義

(一) 特種個資：個資法第 6 條有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

(二) 國際傳輸：指將個人資料作跨國（境）之處理或利用。

(三) 有關個人資料名詞定義，請查閱「個人資料文件名詞解釋彙整表」。

六、作業內容

(一) 個人資料保護管理組織

1. 本校為落實個人資料之保護及管理，設置「個人資料保護推動委員會」並由校長指派之副校長一人擔任召集人，並於「個人資料保護推動委員會」下共設置個資推動小組、緊急事故處理小組與個資稽核小組等 3 個組。有關「個人資料保護推動委員會」之組成、任務與權責，依「個人資料保護推動委員會設置要點」之規定。
2. 本校之個人資料保護官由執行秘書擔任。
3. 有關個人資料稽核小組與個人資料保護管理執行小組之組成、任務與權責，另訂「個人資料保護推行組織與責任分工程序書」規範之。

(二) 個人資料檔案盤點、風險評鑑及風險管理

1. 本校各單位個資管理專人需依據實際作業，執行個人資料檔案鑑別作業，盤點出本校各單位關於各項業務或特定目的所涉及的作業，並於彙整後填於個人資料檔案清冊中。
2. 個資管理部門除每年一次執行個資檔案鑑別作業，並應於營運組織變更、作業流程改變發生時，針對變動範圍內之作業程序與個資檔案進行個資檔案鑑別作業。
3. 用於進行清查之個人資料檔案清冊，應至少包括個人資料檔案名稱、檔案類型、保有依據、特定目的、類別、鑑別蒐集處理與利用流程及參與單位。用於發行或供本校各單位查詢之個人資料檔案清冊，由個人資料保護管理執行小組規劃適當之格式與內容，並採取必要保護措施，以避免個人資料檔案清冊遭未經授權之修改或誤用個人資料檔案清冊版本。
4. 個資管理部門針對個人資料檔案清冊內容，依據風險評估分析構面表進行風險分析，並將結果應呈現彙整於「風險評估表」。
5. 本校每年應至少執行一次風險評鑑。
6. 本校依個資檔案風險評鑑結果及可接受風險值之決議，各風險項目由個資

管理部門業務承辦人針對需降低風險值之個資檔案綜整單位「個人資料風險處理計畫」，以期將風險降至可接受程度。

7. 有關個人資料檔案清冊之清查、彙整與風險評鑑、風險管理之實施方式，另訂「個人資料檔案清查暨風險管理程序書」規範之。

(三) 個人資料事故之預防、通報及應變機制

1. 當本校保有之個人資料檔案遭受不可抗力之天然災害或人為破壞（損毀、竊取、洩漏、竄改、違法利用、設備破壞），或違法蒐集個資，遭媒體揭露、當事人提起訴訟，或造成本校聲譽受損時，應依本程序立即辦理通報作業。
2. 當發生個資事件時，由事件發現人員向秘書處通報，並由秘書處填寫「個資安全事件通報處理紀錄表」，通知個資管理單位評估事件影響範圍、可能造成之損失，及預定採取之應變處理措施，並判斷個資安全事件等級。若研判需召開會議由執行組或緊急事故處理小組召集相關委員及事件相關處理單位（含廠商）召開會議，討論事件影響與衝擊程度，並決定危害初步控管（終止或減緩個資事件持續擴大）應變措施及復原機制啟動時機、相關作業處理單位及協調聯繫方式、媒體因應作為、是否通報主管機關、當事人及通報方式等。
3. 有關個人資料安全事故之通報與處理方式，另訂「個人資料事件之預防、通報及應變程序書」規範之。

(四) 當事人權利行使

1. 本校個人資料檔案清冊中所列之各項個人資料檔案，依法接受個人資料當事人行使當事人權利包括：請求查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除。
2. 當事人應填具「個人資料權利行使申請表」或依本校相關業務申請辦法辦理申請，如為代理人申請則另需檢附委託書及出示相關身分證明文件，若確認非當事人或無法確認是否為當事人委託，則應於申請表中註明後直接駁回申請並歸檔。
3. 本校各單位於受理個人資料當事人行使當事人權利案件處理期限如下：查詢或請求閱覽、請求製給複製本應於十五日內，為准駁之決定，必要時，得予延長十五日內並以書面通知請求人。請求補充或更正、請求停止蒐集、處理或利用、請求刪除應於三十日內，為准駁之決定，必要時，得予延長三十日內並以書面通知請求人。
4. 本校各單位應依據業務職掌，對於經常性之個人資料查詢或請求閱覽、請求製給複製本個人資料，規劃受理當事人申請行使上述各項權利之適當管道，並提供申請方式與收取費用之說明。
5. 本校網站設置個資申訴案件投訴信箱或網頁，由本校個資保護聯絡窗口為對外單一窗口，接受當事人申訴案件。
6. 有關個資保護聯絡窗口受理各項案件之處理方式，請查閱「當事人權利行使作業說明書」。

(五) 個人資料蒐集、處理及利用

1. 本校各單位應於業務執行、服務提供或透過資訊系統蒐集個資前，應依個資法第 8 條規定告知當事人蒐集之目的與範圍，並且遵循適當、相關且符合資料最小化原則，避免取得無關或超過蒐集目的之個人資料，並請當事人填寫「個人資料蒐集聲明暨同意書」取得同意。若當事人未滿 18 歲，依民法規定應取得法定代理人之同意。
2. 本校保有個人資料之處理，應依據個資法第 15 條規定應有特定目的並符合特定情形，並依個人資料檔案分類之結果進行保護，若委託其他機關代為處理保有之個人資料，應依個資法施行細則第 8 條之要求進行適當之監督。
3. 本校同仁因履行法定義務而進行個人資料之利用，應依相關法令法規辦理，且於利用前應先確認利用的目的是否和原先蒐集的特定目的相同。
4. 本校個資涉及國際傳輸時，須遵循輸入、輸出國家之相關個資法令法規之規定；或藉由契約與行政協議形式確保個人資料保護之責任。
5. 有關個人資料蒐集、處理及利用之作業管制詳細規定，另訂「個人資料蒐集、處理及利用程序書」規範之。

(六) 資料與設備安全管理

1. 本校對所有保管個人資料、管理個人資料儲存媒體，以及可以存取個人資料之人員依本校資訊安全相關規定進行必要之權限管理，各類權限之授予以最小且滿足業務所需為限。
2. 本校人員應妥善保管個人帳號及密碼，不得供予他人使用（密碼長度 8 碼以上，同時需為英文字母、數字或特殊字元的組合），並定期更換密碼，同一密碼使用期限最長應不超過 6 個月，儘量避免重複或循環使用舊的密碼。
3. 本校個人電腦應設定螢幕保護程式（不應超過 10 分鐘），並安裝防毒軟體及定期更新病毒碼。
4. 本校機敏性等級之個人資料檔案於個人電腦宜加密儲存，以保護其機密性。
5. 未使用或下班時，個人資料書面文件及可攜式資訊設備或儲存媒體，應遵守桌面淨空政策，放置於抽屜或櫃子上鎖，以避免個資外洩。
6. 有關資料、設備與實體環境安全之詳細規定，請查閱「個人資料安全作業說明書」。

(七) 人員管理及教育訓練

1. 本校教職員生、約聘僱人員、外包廠商皆應遵守本校個人資料保護政策及個資管理制度相關文件之規範。
2. 本校人員於到職時，應簽署「個人保密切結書」，並克盡保密之責。
3. 本校每年應訂定或辦理一般人員教育訓練計畫及課程，並依要求人員每年需達 3 小時以上時數。
4. 本校人員離職應於規定時間內關閉該人員所使用之各類權限以及通行證件，並依規定列冊移交相關儲存媒體及資料，由主管實施監交作業。
5. 針對違規人員之懲處建議，並依情節輕重移送相關單位辦理懲處。

6. 有關人員管理及教育訓練之實施方式，另訂「人員管理及教育訓練程序書」規範之。

(八) 委外管理

1. 供應商與作業人員應遵守本校個資安全管理制度及資訊安全管理制度之規定。
2. 供應商作業人員到點服務除需依規定簽署供應商保密切結書外，請購單位應告知作業項目及場所相關安全管理規定。
3. 除非相關法律有特別之規定，受委託廠商應於履約完成後進行個人資料載體之返還，以儲存方式而持有之個人資料需安全的刪除，並提供確切之證據，請購單位得對於有疑慮之項目進行實地之查核。
4. 有關對於受委託之監督管理實施方式，請查閱「個人資料業務委外監督管理作業說明書」。

(九) 個人資料內部稽核管理

1. 本校內部稽核，由個資稽核小組針對本校之個資管理制度、個資清查、風險評估與風險管理、個資事故應變措施、演練等作業及適法性，進行定期查核，以確保其成效。
2. 本校外部稽核，由本校以外單位所進行的個資業務稽核，如主管機關個資業務檢查等。
3. 有關個人資料檔案安全稽核機制之實施方式，另訂「個人資料保護內部稽核程序書」規範之。

(十) 個人資料使用紀錄、軌跡資料及證據保存

1. 本校個人資料相關文件或紀錄，依單位需求訂定保存期限，屆滿保存期限之紀錄由各單位個資管理專人編造銷毀清冊，辦理銷毀後，銷毀清冊副本交付文件管制人員留存。
2. 有關個人資料使用紀錄管理之細部規定，另訂「個人資料文件及紀錄管理程序書」規範之。

(十一) 個人資料安全維護之整體持續改善

1. 本校各單位於個人資料安全維護推行過程，應接受稽核，並針對稽核發現之缺失檢討其根本原因，提出消除已知缺失事項之改正措施與消除其根本原因防止再發之矯正措施。
2. 有關改正措施與矯正措施之實施與追蹤方式，另訂「個人資料保護持續改善程序書」規範之。

(十二) 業務終止資料處理方法

本校業務終止後個人資料處理方法，應依下列規定辦理，並留存相關紀錄：

1. 銷毀：除法律另有規定不得銷毀之外，本校應依據個別個人資料載體或媒介物之性質，以適當的方式於適當的處所進行銷毀，並作成相關紀錄，供日後存查。
2. 移轉：如個人資料檔案有移轉之必要，應依據個人資料檔案清冊，辦理個

人資料檔案移交手續並製作移交清冊；移交清冊至少應包含移轉之原因、對象、方法、時間、地點及移轉對象得保有該項個人資料檔案之合法依據與證明等。

3. 刪除、停止處理或利用：除法律另有規定不得刪除、停止處理或利用之外，本校會應依據個別個人資料載體或媒介物之性質，以適當的方式於適當的處所進行刪除，或停止處理或利用，並作成相關紀錄，供日後存查。

七、參考文件

(一) 個人資料保護政策
(二) 個人資料保護推行組織與責任分工程序書
(三) 個人資料文件及紀錄管理程序書
(四) 個人資料檔案清查暨風險管理程序書
(五) 個人資料蒐集、處理及利用程序書
(六) 個人資料事件之預防、通報及應變程序書
(七) 人員管理及教育訓練程序書
(八) 個人資料保護內部稽核程序書
(九) 個人資料保護持續改善程序書
(十) 當事人權利行使作業說明書
(十一) 個人資料業務委外監督管理作業說明書
(十二) 個人資料安全作業說明書

八、本計畫經個人資料保護推動委員會會議通過，陳請校長核定後發布實施，修正時亦同。