亞東技術學院

個人資料安全管理程序書

機密等級：一般

文件編號：PIMS-B-08

版　　次：1.0

發行日期：2019/11/01

個人資料安全管理程序書					
文件編號	PIMS-B-08	機密等級	一般	版次	1.0

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	2019.11.01		個資保護執行小組	初版

目錄

個人資料安全管理程序書					
文件編號	PIMS-B-08	機密等級	一般	版次	1.0

1 目的

制訂亞東技術學院（以下簡稱本校）個人資料安全管理制度之作業規範，依過程導向的管理循環，建立完善的個人資料管理框架，達成個人資料安全管理目標。

2 範圍

本校個人資料管理制度導入範圍內，與個人資料之蒐集、處理與利用等作業相關之單位、人員、業務流程與系統均適用。

3 權責

3.1 個人資料保護推動委員會

本校個人資料保護管理決策組織。

3.2 個資保護執行小組

本校資訊 PIMS 規劃、建立、實施、維護、審查與持續改善，並將個人資料管理制度相關議題於個人資料保護推動委員會提報。

4 名詞定義

4.1 個人資料保護目標

由本校各單位針對其所負責且與個人資料蒐集、處理與利用相關之業務，訂定各項改善目標，並且定期檢討與改善，以持續改善及維持個人資料管理制度之有效運作。

4.2 個人資料管理制度制度稽核

PIMS 之獨立資訊安全檢查，以決定各項活動及相關結果是否與計畫的安排相符及此等安排是否有效執行及達成目標。

4.3 矯正措施

為避免不符合 PIMS 之事件重複發生，所採取之措施。

4.4 預防措施

為預防潛在不符合 PIMS 要求之事件發生所採取之措施。

5 作業內容

5.1 組織全景與適用範圍

5.1.1 本校應決定與教育營運目的相關，且會影響 PIMS 預期成果之內部與外部議題，鑑別出與本校所提供服務相關之利害關係者，以及這些利害關係者對本校的需求與期望，用以客觀決定 PIMS 之範圍。

5.1.2 建立「組織全景評鑑表」，以系統化鑑別本校之核心業務、與核心業務相關之利害關係者以及這些利害關係者對本校核心業務之需求與期望，並判別若無法達到些需求與期望會對本校造成何種程度之衝擊，並將上述評估及分析結果供管理高層決策 PIMS 之導入及驗證範圍。

5.2 管理階層責任

5.2.1 成立個資保護管理架構，有效推動與辦理個資保護之各項工作，

規範其運作方式與工作職責，以展現管理階層對個資保護之重視及支持。

5.2.2 個資保護執行小組為支持 PIMS 建立、實施、維護、審查與持續改善，依據 PIMS 管理審查，週期進行審查，確認相關控制措施支援營運要求，並確保被指定責任的人員，有能力履行被要求之工作，並提供適當的教育訓練與控制。

5.3 個人資料保護目標管理

5.3.1 資料分析統計

個資保護執行小組應於每年蒐集各單位個人資料保護相關之管理數據與資料，並加以統計分析，以作為個人資料保護目標之設定及審核之參考依據。

5.3.2 訂定個人資料保護目標及審核

個資保護執行小組依據如下之重點，設定可衡量之個人資料保護目標，並填寫於「個人資料保護目標設定表」，陳「執行秘書」審核。

5.3.2.1 個人資料保護目標應考量各單位之特性及能力。

5.3.2.2 個人資料保護目標應配合個人資料管理政策。

5.3.2.3 將重要個人資料管理流程尋找適當監測點，列入個人資料保護目標持續監測。

5.3.3 公布實施

經「執行秘書」核定之「個人資料保護目標設定表」，由「個資保護執行小組」依個人資料保護目標之要求向各單位同仁公佈，並確實要求各單位同仁努力達成個人資料保護之目標。

5.3.4 目標檢討

「個資保護執行小組」每季應針對上一季之個人資料保護目標執行情形進行檢討，並將檢討的結果記錄於「個人資料保護目標檢討表」，陳「執行秘書」審核。

5.3.5 研擬及執行改善措施

5.3.5.1 若個人資料保護目標多次無法達成，「執行秘書」得視需要，依矯正預防及持續改善程序，要求相關單位研擬改善措施。

5.3.5.2 個人資料保護目標之修正

5.3.5.3「個資保護執行小組」每季定期檢討個人資料保護目標，若有發現個人資料保護目標不適當時，均得重新提出「個人資料保護目標設定表」，經「執行秘書」核定後，方得依新核定之目標執行及檢討。

5.4 個人資料安全管理制度內部稽核

5.4.1稽核頻率

每年至少辦理一次個人資料安全內部稽核作業，並視需要採取針對個人資料安全事件的重大變更等特定目的之不定期稽核。

5.4.2稽核人員要求

為確保稽核過程的客觀性與獨立性，避免稽核自身工作。稽核人員需有個人資料安全制度稽核的經驗或訓練。

5.4.3稽核計畫

應事前規劃並編製個人資料安全稽核計畫，以作為執行稽核指導綱要，內容應包括：稽核依據、範圍、程序、人員、項目、預定時程等。

5.4.4稽核準則

稽核檢查內容應紀錄於「內部稽核查檢表」，檢查內容應符合最新BS 10012之要求。

5.4.5稽核執行

5.4.5.1 稽核人員依稽核準則執行稽核，抽樣收集足夠之客觀證據，以研判該稽核項目是否符合管理制度要求，稽核時應保存適當的稽核軌跡與佐證資訊。

5.4.5.2 受稽核人員應尊重及支持稽核人員，並接受調閱有關紀錄、報告及文件。

5.4.6稽核報告

5.4.6.1 稽核人員應將稽核結果彙整後提出稽核報告。稽核報告格式可參考 PIMS 文件編號及撰寫格式標準。

5.4.6.2 受稽核組別於接獲稽核報告後，稽核計畫中所要求之時限內將該組之缺失分析原因及擬採行之矯正與預防措施填列於「矯正與預防處理單」，且經主管核准後回覆稽核人員，並進行後續追蹤。

5.4.6.3 稽核報告需連同相關稽核資料，呈送受稽單位之主管審核，於審核完成後列管。

5.5 管理制度管理審查

5.5.1 管理審查會議召開時程：

5.5.1.1 組織每年應至少召開一次管理審查會議，必要時得召開臨時會議，相關會議討論與決議事項，應依據權責層級向上呈報。

5.5.2 管理審查會議審查內容應包含：

5.5.2.1 先前管理審查措施的執行狀況；

5.5.2.2 與 PIMS 有關之外部與內部議題的變更；

5.5.2.3 PIMS 的績效資訊，及各方回饋意見。

5.5.2.4 個人資料管理（蒐集、處理、利用）風險，及其他可能風險變化。

5.5.2.5 各類稽核結果。

5.5.2.6 個人資料管理各項程序變更審查。

5.5.2.7 個人資料相關之管理系統或其他技術升級及/或更換的結果。

5.5.2.8 主管機關檢查結果及評估要求。

5.5.2.9 個人資料申訴抱怨事件及當事人權利行使結果。

5.5.2.10 已違反或已發生個人資料內外部個資事件及事件統計與處理情形。

5.5.2.11 個人資料管理矯正預防及改善情形與追蹤報告。

5.5.2.12 其他持續增進改善個人資料管理系統事項。

5.5.3 管理審查會議依據審查及討論事項之內容，應有相關審查及討論議題之結論，並將個人資料管理審查結果製作成會議紀錄，以利後續之改善追蹤：

5.5.3.1 執行之各項持續改進措施或決議。

5.5.3.2 針對個人資料保護制度技術是否需提昇或改善之變更。

5.6 個人資料保護制度矯正預防

5.6.1 矯正及預防執行時機

5.6.1.1 內部、外部稽核、自行發現之不符合或效能改善事項時，應提出矯正及預防措施，並填寫於「矯正與預防處

理單」。

5.6.1.2 處理權責組別應分析問題發生之原因及影響程度，決定優先順序與處理時限，評估措施時須考慮成本效益及可行性，提出矯正與預防措施時，得區分為暫時性對策及永久性對策。

5.6.1.3 矯正與預防措施之執行狀況，應由處理權責組別依據「矯正與預防處理單」確實執行，並留存追蹤紀錄。

5.7 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	組織全景評鑑表	文管中心	至少 5 年
2	個人資料保護目標設定表	文管中心	至少 3 年
3	個人資料保護目標檢討表	文管中心	至少 3 年
4	內部稽核查檢表	文管中心	至少 3 年
5	矯正與預防處理單	文管中心	至少 3 年

6 相關文件

無

7 使用表單

7.1 組織全景評鑑表(PIMS-B-08-D-01)

7.2 個人資料保護目標設定表(PIMS-B-08-D-02)

7.3 個人資料保護目標檢討表(PIMS-B-08-D-03)

7.4 內部稽核查檢表(PIMS-B-08-D-04)

7.5 矯正與預防處理單(PIMS-B-08-D-05)