國立陽明交通大學個人資料保護實施細則

110 年 9 月 28 日本校 110 學年度第 1 次資通安全暨個人資料保護推動委員會議通過

一、國立陽明交通大學（以下簡稱本校）為規範個人資料之蒐集、處理、利用，並促進個人資料之合理使用，防止個人資料被竊取、竄改、毀損、滅失或洩漏，並依據國立陽明交通大學資通安全暨個資保護管理要點特訂定本個人資料保護實施細則，以為遵循。

二、名詞定義如下：

1. 個人資料：自然人之姓名、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。
2. 個人資料檔案：包含紙本與電子檔案，電子檔案包含個人電腦內存放之檔案、資訊系統之資料庫檔案等。

三、各單位應指派人員擔任個人資料保護窗口，負責管理與彙整各單位個人資料檔案清查內容，並接受稽核。

四、個人資料檔案清查內容：

1. 依據資訊中心提供之個人資料清查表範本，各單位至少每年定期進行一次個人資料檔案清查填報及更新作業、風險評鑑作業。
2. 個人資料檔案清查應鑑別單位高處理風險之個人資料，可能包含：
   (1)「個人資料保護法」所明定之特種個資。
   (2)個人財務資訊。
   (3)身分證字號。
   (4)弱勢資訊。
   (5)個人特徵的詳細說明。
   (6)對個人將產生負面影響的資訊。
3. 個人資料檔案清查作業應包含資料使用目的、資料流向。
4. 個人資料檔案風險評鑑為參考資料重要性，檢視與評估個人資料檔案目前存在的資料安全風險與違法風險。

五、蒐集、處理或利用個人資料，除法律明文規定外，應採取適當之告知方式。於特定目的外利用個人資料時，應檢視是否符合當事人書面同意、或為增進公共利益、或有利於當事人權益之特定目的外利用條件。告知當事人的資訊包含：

1. 學校、機構名稱。
2. 蒐集之目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人依「個人資料保護法」第三條規定得行使之權利及方式。
6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

六、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不得蒐集處理，但在徵得當事人同意或法令明定之情況下除外。如作為學術利用時，應對其揭露方式作適當處理，使其無從識別特定之當事人。

七、各單位為行政目的使用資通系統或雲端資通服務（如 Google 表單、Microsoft Forms 等問卷調查服務）涉及蒐集個人資料者，應注意下列事項：

1. 資料蒐集最小化：僅蒐集適當、相關且限於處理目的所必要之個人資料，處理及利用時，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。
2. 存取控制：應注意檔案存取權限設定，應採最小權限原則，僅允許使用者依目的，指派任務所需之最小授權存取。
3. 使用雲端資通服務者，應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，並應注意避免設定允許顯示其他使用者作答內容（如 Google 表單不應勾選「顯示摘要圖表和其他作答內容」），避免使用者能瀏覽其他使用者資料，造成個人資料外洩。公佈前應確實做好相關設定檢查，並實際操作測試，確認無誤後再行發布。
4. 傳輸之機密性：網路傳輸應採用網站安全傳輸通訊協定（HTTPS）加密傳輸，並使用 TLS 1.2 以上版本傳輸。
5. 資料儲存安全：如涉及蒐集個人資料保護法第 6 條之個人資料或其他敏感個人資料，應以加密方式儲存。
6. 應訂定個人資料保存期限，並於期限或業務終止後將蒐集之個人資料予以刪除或銷毀，避免個人資料外洩。

八、各單位提供共用之電腦或自動化機器設備內之資料，應指定專人進行個人資料管理及維護工作。

九、單位非例行業務或首次業務需跨單位資料流通時，應填寫「資料調用申請表」。

十、針對所保有之個人資料內容，儲存、傳輸及備份之狀況，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。擬提供予當事人知悉之資料，應注意檢查檔案是否包含當事人以外之其他個人資料，並確認資料收受者之正確性，避免因疏失傳送洩漏與業務無關之人員知悉。

十一、 各單位行文及網站公告，如有涉及國民身分證統一編號之登載者統一隱碼欄位為身分證編號後 4 碼。

十二、 個人資料檔案處理人員應使用本校提供之電子郵件系統傳輸個人資料檔案，並應對檔案加密，禁止使用非本校提供之工具進行個人資料檔案傳輸或公開(如:即時通訊軟體、外部網頁式電子郵件(Webmail)、點對點(P2P)軟體、Tunnel 相關工具、雲端儲存工具(如 dropbox 等)、社群網站、部落格、公開論壇或其他利用網際網路形式等）。

十三、 個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，嗣該媒介物於報廢或轉作其他用途時，應確實銷毀，並填寫「個資銷毀紀錄單」或「個資移轉終止紀錄單」。

十四、 委託廠商蒐集、處理及利用個人資料時，應於採購契約明訂監督條款、資安條款、保密條款及違約之處置條款，且廠商應管理相關委外專案人員及外部人員之各項資訊資產存取權限，導入個人資料管理流程。委託結束後，廠商應返還本校之個人資料，並簽具「個人資料歸還與銷毀切結書」。

十五、 對於業務受託人蒐集、處理及利用個人資料，應採取適當監督措施：

1. 對於受託人之蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
2. 受託人之適當安全維護措施。
3. 受託人有複委託時，其約定之受託人。
4. 違反個人資料保護法或委託契約條款時，受託人應向委託人通知之事項及採行之補救措施。
5. 委託人對受託人保留指示之事項。

6. 委託關係終止或解除時，受託人就個人資料載體之返還，及儲存於受託人持有個人資料之刪除。

十六、 技術管理措施：

1. 電腦、相關設備或系統上應設定帳號密碼等認證機制，密碼應至少包括英文大小寫與數字，長度為 8 碼以上，並須定期更換密碼，及定期測試權限機制之有效性。
2. 電腦須安裝防毒軟體與即時更新病毒碼。
3. 電腦應維持作業系統修補更新，並評估必要的應用軟體更新。
4. 電腦應設定 15 分鐘內啟動螢幕保護並以密碼鎖定。
5. 具備存取權限之電腦不得安裝檔案分享軟體。
6. 定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。
7. 各單位應針對不同之作業內容、作業環境及個人資料之種類與數量，實施必要之門禁管理，以適當方式或場所保管個人資料之儲存媒體。

十七、 執行保護個人資料，應保存下列紀錄以供查驗：

1. 個人資料交付、傳輸之紀錄。
2. 確認個人資料正確性及更正之紀錄。
3. 提供當事人行使權利之紀錄。
4. 所屬人員權限新增、變動及刪除之紀錄。
5. 個人資料刪除、銷毀或移轉紀錄。
6. 個人資料保護事件預防、通報及處理程序之紀錄。
7. 備份及還原測試之紀錄。

十八、 各單位應配合內部稽核的時程，填寫個人資料管理內部稽核查檢表。

十九、 各單位人員每年應接受主管機關要求的教育訓練時數。

二十、 本細則經資通安全暨個人資料保護推動委員會會議通過後實施，修正時亦同。