致理科技大學

個人資料存取控制規範

機密等級：■一般 □敏感 □機密

編號：P-3-04

版本：1.0

發行日期：106 年 4 月 20 日

文件制／修訂紀錄頁

版次	發行日期	修訂摘要	修訂者	文管人員
1.0	106.4.20	初次發行	呂瑞茹	呂瑞茹

目錄

壹、 目的：

因資訊化作業已深植於本校日常作業中，為避免因日常作業之疏漏造成個人資料或機敏資料外洩，特訂定本規範以規定作業中應注意之控制事項，以減低資料外洩風險。

貳、 範圍：

於本校作業上使用之應用系統、公用程式、作業系統、可攜式裝置、遠端裝置、網際網路及電子郵件。

參、 名詞定義

一、 可攜式裝置：本規範中可攜式裝置指可攜帶之資訊處理設備，如筆記型電腦、平板電腦及智慧型手機等。

肆、 規範項目說明

一、 應用系統、公用程式及作業系統

（一） 個人資料及系統之存取權限應依同仁之業務需求，賦予帳號對應作業所需之權限，未經授權不得存取與個人業務無關之個人資料。

（二） 設定存取權限時，應以最少且需要為原則，避免配發過大或不必要的權限。

（三） 當同仁調整職務、調離現職或離職時，應立即進行帳號與使用權限之註銷或更新。

（四） 應定期審查系統中帳號權限設定是否適當，避免因錯誤設定增加資料外洩的風險。

（五） 密碼應每半年進行更換。

（六） 應將系統中帳號權限設定之異動記錄、機敏資料或個人資料檔案的存取記錄予以保存，並確保其不會被竄改，以供發生異常事件時作為追查及佐證之用。

（七） 單位應用系統管理同仁應定期審查前項之記錄，以確保無異常存取行為發生。

（八） 應定期進行應用系統、公用程式及作業系統的軟體更新或修補作業。

（九） 單位若自行開發應用系統，應避免使用真實資料進行測試。若有使用真實資料進行測試，測試過程中需有與正式系統相同之保護措施（如權限審查、密碼保護等），測試結束後亦應確認測試資料是否已完全刪除。

二、 可攜式裝置

（一） 設備於外地使用時應給予適當的保護，如上鎖、置於櫃中保管、加裝防毒軟體、設定螢幕密碼保護裝置、重要資料應設定存取密碼並定時備份，備份資料應適當保管避免被偷或遺失。

（二） 行動裝置於外地公共區域使用時不可處於無人看管狀態。

（三） 行動裝置須定期進行軟體更新或修補作業。

（四） 應避免使用未知的公開無線網路傳輸隱私性高或機敏資料。

三、 遠端裝置

（一） 遠端裝置所在地應有適當的保護措施（例如：安裝監視錄影設備、進出管制門禁刷卡或人員管控等安全控制機制），避免設備被偷、資料被偷、設備不當使用或透過遠端設備未經授權存取本校資源。

（二） 須先確認遠端裝置所在地的安全控管符合安全管理要求，才可啟用遠端裝置。

（三） 遠端裝置終止使用後相關的授權、存取權限應取消，設備應歸還。

（四） 除上列所述項目，其他對本校內設備的安控要求機制亦適用於此。

四、 網際網路

（一） 將瀏覽器的安全等級調為至少中等以上，以防範惡意可移動程式碼(Mobile Code)。

（二） 限制自行使用來源不明的可移動程式碼(Mobile Code)，例如 JavaScript 或 ActiveX。

（三） 下列行為是不被允許的：

1. 運用此系統進行個人兼職業務。
2. 造訪色情、系統破解或其他不適當之網站。
3. 下載未經授權之檔案，如軟體、音樂、圖片、影片等。

4. 入侵、攻擊或騷擾任何本校、機構或個人之網路資源。

5. 其他不合本校工作規範者。

五、 電子郵件

（一） 非經授權，不可使用他人的帳號來傳送電子郵件，亦不可存取他人之電子郵件。

（二） 機密性或專有資訊透過電子郵件傳送時，須遵循「個人資料處理作業指引」執行。

（三） 為防止社交工程攻擊，使用電子郵件應預設封鎖圖片及影音內容，郵件中附件及連結亦不可隨意點選。若無法確認郵件內容真偽，可以電話或其它方式與來信單位進行確認，或於開啟附件前以防毒軟體掃描檢查。

伍、 相關法規：

一、 行政院國家安通安全會報技術服務中心「行動裝置資通安全注意事項」。