機密等級：內部文件

農業部
桃園區農業改良場

處理資訊紀錄及個人資料之人員及設備安全管理指引

第 1.0 版

113 年　8　月　22　日　　頒行

目錄

壹、目的

各項資料、資訊系統與設備是本場重要資產，適當之使用有助於業務推展與執行，本場各單位執行之業務涉及個人資料者，均應遵守共同規範，因此透過本指引訂定使用規定，各級主管應確保同仁具有充分認知並確實遵守，進而達成個人資料保護。違反使用規範，經查屬實，將依相關規定進行懲處。

貳、適用範圍

一、組織與業務

本指引適用於本場涉及個人資料蒐集、處理、利用、傳輸、銷毀之相關業務與系統。

二、個人資料檔案

涵蓋資訊紀錄、資訊系統其型式可為電子檔案、系統化資料庫、紙本等，如下列參考類別與項目(但不限於下表所列項目)：

資產類別	個資檔案**範例**(不限於本表所列項目)	
資訊紀錄	●人事資料庫、資料檔 ●保險資料 ●考試分發人員基本資料 ●同仁在離職證明書/服務證明書 ●廠商通訊錄 ●研討會/教育訓練報名表	●約聘僱人員契約書 ●公務人員派免令 ●甄審、進修暨考績甄審委員會委員名單 ●公務人員訓練、進修資料 ●保密切結書 ●學員/農友名冊
資訊系統	●人事管理資訊系統 ●政府歲計會計資訊管理系統	●土壤肥力與作物營養診斷服務查詢系統

參、名詞定義

一、個人資料

依個人資料保護法之定義。

二、個人資料檔案

依個人資料保護法之定義。

肆、權責

一、個人資料保護管理執行小組(以下簡稱本小組)

(一) 審核本指引。

(二) 提供資源使人員與設備安全管理活動能順利進行。

二、本小組執行秘書

(一) 督導各單位遵守本指引。

(二) 執行成果陳報個人資料保護管理執行小組。

三、 本小組委員

(一) 督導該單位遵守本指引。

(二) 審核與授權使用相關紀錄與軌跡資料。

四、 各單位個人資料保護專責人員

(一) 宣導個資與資安防護相關規定。

(二) 發生個資事件，協助處理與調查。

五、 各單位個資業務承辦

(一) 產生、蒐集與保存各項使用紀錄與軌跡資料。

(二) 發生個資事件時，負責處理與調查。

六、 資訊/個資專責單位

(一) 電腦主機與個人電腦安全控管、作業系統及檔案管理。

(二) 電腦主機及各週邊設備運轉之管理。

(三) 資料輸出/輸入設備使用管制作業。

(四) 提供儲存設備，保存並備份資料。

(五) 發生個資事件時，提供必要之諮詢與協助。

伍、設備安全管理程序

一、 資料檔案之安全控制

(一) 資訊管理單位之統籌控制

1. 主機部份：定期備份資料。
2. 重要性等級 3(含)以上之系統，均應備份。
3. 定期將所備份之資料，進行資料還原測試並留下紀錄。

(二) 使用單位對檔案之存取

1. 具個人資料之備份儲存媒體除資訊管理單位與承辦單位外，不得調借其他單位。若業務需要，須經申請經授權後，始得為之。
2. 為確保資料機密性與完整性，資訊管理單位應設定權限控管，禁止非經核准之檔案存取。
3. 為避免檔案資料遭病毒毀損，資訊管理單位定期自動偵測病毒，並訓練所有人員使用偵測病毒軟體，以偵測外來儲存媒體之病毒。

二、 設備之安全控制

為確保系統運作順暢、安全，資訊管理單位對各項電腦設備詳加規劃與管理，茲將設備分成電腦設備、網路通訊、支援、電源設備四種，其使用之安全控制管理分述如下：

(一) 電腦設備管理：包含電腦主機、儲存設備、終端機、印表機等：

1. 凡機器設備於購入時，資訊管理單位會同使用單位驗收，並依實際需求與廠商簽訂維護合約，定期檢查或清理機器設備，保持機器之乾淨。
2. 電腦系統之弱點防護依「硬體設備及系統監控管理指引」辦理。

(二) 網路通訊設備管理

1. 通信網路保持機密性，防止資料被他人截取。
2. 若設備線路發生故障時，資訊管理單位派員立即檢查，以了解線路故障原因，通知廠商或電信局進行維修。若有重要資料需立即處理時，應報請主管同意，改以人工作業代替之。
3. 應確認網路線於集線架之擺放位置，網路管理人員與網路線製作廠商實地勘察確認網路線製作之規格、長度、網路標籤識別規則。
4. 設備應適當防護，未經授權人員不得接近，且附近不可放置易燃或危險物品。

(三) 支援設備管理

1. 備有自動火警設備，以警示有火災訊息。
2. 備有自動滅火設備並同時設置手動開關，以防止偵測系統失效時，能及時啟動。
3. 於明顯及重要地點設置滅火器，以便火災時滅火用。
4. 滅火器應定期更換，並有專人負責消防系統之定期檢查與維修。

(四) 電源設備管理

1. 重要設備應裝設有不斷電設備(UPS)及電源供應器以防止較長時間的停電。
2. 應安裝自動電壓穩定裝置。
3. 使用的電源要具有電磁式開關及地線接地，以保護電腦設備。

三、 電腦機房之管制

(一) 機房內設置獨立之空調設備，以維持機房溫度之適當性。

(二) 人員進出應予以管制。

(三) 機房設有刷卡進出管制，資訊管理單位人員進入機房，應予刷卡，非授權人員因公務須進入機房，則應填寫機房進出紀錄，並經資訊管理單位人員陪同方可進入，嚴禁未經許可擅入機房。

(四) 操作管理

1. 操作人員應填寫「資訊服務申請單」，紀錄操作機器狀況。
2. 機房中所有機器設備操作人員，依操作文件規定啟動及操作。
3. 系統之控制台所留下之紀錄，需加以保留。
4. 「資訊服務申請單」至少需保留一年。

(五) 工作守則

詳見「實體與環境安全管理指引」。

四、 硬體設備維護紀錄

(一) 資訊管理單位所有硬體設備的運轉情況、故障送修情形及定期維護保養，均需加以紀錄其日期、原因及廠商名稱，並由相關同仁核閱。其維護紀錄需保留一年。

(二) 本機關所有之硬體設備，其型號應紀錄於「資訊設備清冊」，以利維護作業。

(三) 重要設備應由廠商定期辦理預防性維護措施，做成紀錄，並訂定書面契約，以確定維護內容，於做完維護時，需有專人會同檢收。

陸、人員安全規定

本場同仁於服務期間應遵守「公務員服務法」及「個人資料保護法」等相關規定及下列各項守則。

一、 資安及個資相關規定：

(一) 本場各單位凡因業務需要而涉及個人資料之蒐集、處理及利用等作業，均應遵循「個人資料保護法」等相關規定，審慎保管，以避免個資外洩，影響當事人權益

(二) 新進員工均應接受資訊安全及個人資料保護宣導，及本場同仁應每年接受資訊安全、個人資料保護相關之教育訓練或宣導。

(三) 為尊重智慧財產權，不得自行安裝非法軟體於個人電腦。

(四) 不得以任何手段蓄意干擾或妨害網路系統的正常運作。

(五) 禁止利用本場網路資源從事個人網站營利及不法之情事。

(六) 不宜隨意打開來路不明的電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞；如有任何異常中毒跡象，應立即通知權責單位處理。

(七) 個人電腦存取密碼必須定期更換，且不得洩露他人。

(八) 不得冒用他人的帳號及密碼登入電腦操作系統。

(九) 員工未經授權許可不得進入管制區(機房)，未經授權人員進入須由授權人員陪同且須填寫登記表。

(十) 所有個人電腦含筆記型電腦在經過 15 分鐘的閒置後，必須啟動設有密碼的螢幕保護程式。

(十一) 於工作區域內，必須配戴識別卡或門禁卡。

二、 懲處規定

(一) 違反規定情節輕微

本場員工(職員、約聘僱人員、技工、工友、駕駛、駐警、臨時人員、工讀生等)違反資通安全相關規定情節輕微者，由所屬單位主管予以口頭告誡，如屢犯仍未配合改善者，列入平時考核之參考。

(二) 違反規定情節重大

1. 懲處規定：

(1) 本場員工違反資通安全相關規定情節重大，各依現行法令適用「公務員服務法」、「公務人員考績法」、「公務人員考績法施行細則」、「行政院及所屬各級行政機關學校公務人員獎懲案件處理要點」等相關規定辦理。

(2) 如為臨時人員與工讀生，則逕行予以解僱；若涉及法律責任，依相關規定辦理。

(三) 懲處作業程序

1. 提交考績委員會審議。
2. 應不分主、從機關(單位)一併討論責任歸屬，覈實議處。
3. 稽核小組提報資安懲處案件，應引據法條，詳述具體事由及建議懲度。
4. 情節重大者，人事室應將懲處事由通知被懲處人，被懲處人得提出書面說明，如有必要考績委員會得同意被懲處人至本場說明。

(四) 外包人員(計畫人員)相關懲處

承包商派駐本場人員，須依照契約之規範遵守本場資通安全相關規定，如有違反經查證屬實者，本場得要求承包商主管議處。

三、 保密規定

(一) 本場正式員工應遵守「公務員服務法」。

(二) 聘用員工必須簽訂相關聘用契約書，以維護本場資通安全。

(三) 委外廠商因提供服務而接觸本場相關敏感業務資料之人員，應依本場規定接受身家調查，並由廠商簽訂保密協議，切結保證所屬人員之保密責任。

(四) 為確保本場資通安全，與委外廠商、承包商簽訂契約時，須加入資通安全相關規範，規範內容參考「契約文件之資通安全規範參考條文」。

(五) 委外廠商人員應與本場簽訂「委外廠商人員保密切結書」。