

--	--	--	--

財團法人台灣兒童暨家庭扶助基金會資訊安全與個人資料保護管理辦法

104 年度第 33 次(104.09.24)行政主管會議通過實施

壹、資訊安全政策

一、目的

為建立安全及可信賴的資訊環境，以確保資訊資產的機密性、可用性與完整性，採取適當的控制措施，確保資訊的適當安置及資訊安全實務作業的可行性與有效性。

二、目標

為維護本會資訊資產之機密性、完整性與可用性，保障使用者資料隱私之安全。期藉由共同努力以達成下列目標：

- (一)、保護本會業務服務之安全，機密性資料須確保需經授權人員才可存取資訊，以確保其機密性。
- (二)、保護本會業務服務之安全，避免未經授權之修改，以確保其正確性與完整性。
- (三)、確保本會各項業務服務之執行須符合相關法令或法規之要求。

三、責任

- (一)、管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序以實施本政策。
- (二)、本會之內部人員、委外服務廠商與訪客等應遵守本政策。
- (三)、本會之內部人員、委外服務廠商與訪客等有責任透過適當通報機制，通報資訊安全事件或弱點。
- (四)、任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本會之相關規定進行議處。

四、資訊安全管理範圍

本政策適用範圍為本會之內部人員、委外服務廠商與訪客等。

資訊安全管理範疇涵蓋八項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本會造成各種可能之風險及危害，各領域分述如下：

- (一)、個人電腦資訊安全守則
- (二)、伺服器資訊安全管理
- (三)、資產(個資)盤點及業務流程
- (四)、個人資料保護管理
- (五)、文件管理
- (六)、通訊與作業管理
- (七)、實體與環境安全控管
- (八)、委外廠商管理

貳、資訊安全與個人資料保護辦法

一、個人電腦使用安全守則

個人電腦定義：含桌上型電腦、共用之公共電腦、可攜式電腦、伺服器 etc。

(一)、個人電腦使用原則：

1. 時常檢查電腦是否有不明程式啟動執行。
2. 不要開啟無法確定及不必要的服務，如.exe, .scr, .vbs...等，避免遭受植入木馬程式。
3. 不得瀏覽不知名或不安全的網站，且不得下載或使用非公務用之圖片、影音、免費軟體、遊戲。
4. 外部網頁瀏覽權限由各單位主管自行決定，主要以公務處理、業務需求為原則。
5. 定期檢視更新系統安全修補、防毒軟體及防毒碼，保持更新至最新狀態，勿自行關閉系統自動更新程式，以維持系統正常運作。
6. 公務電腦設備不可任意架站或做私人、營利用途。
7. 電腦設備應隨時保持清潔，避免髒污、灰塵造成設備損壞或公共危安，下班前，不需使用之設備應先行關機始得離去，電腦關機應依正常程序操作。
8. 電腦附近應避免放置茶水、飲料、細小文具用品等物品，以免造成電腦設備損壞。
9. 桌面勿放置 IP、序號、帳號、密碼及個資等文件，長時間離開座位時重要資料及可攜式媒體請置放於安全場所。
10. IE、Chrome、Firefox 等相關瀏覽器之安全等級需遵守本會相關系統之設定。
11. 電子郵件軟體應關閉收信預覽功能，請勿任意開啟不明來源及具聳動標題之電子郵件，為避免惡意連結及圖片危害可使用文字模式閱讀信件。

12. 對於郵件主旨、內容有疑慮者之電子郵件，須向發信者確認後再開啟。
13. 須定期整理與備份電子郵件，確定不要的郵件須將郵件徹底刪除。
14. 個人電腦不使用時，需採用密碼保護、鎖定或登出離線等安全措施。
15. 電腦應採用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 10 分鐘以內。
16. 非公務必要使用時，請勿開啟網路芳鄰分享目錄與檔案，並停用 Guest 帳號。
17. 檔案分享時，不得將整個磁碟分享及分享給未經授權使用的第三人。
18. 公務用筆記型電腦攜離辦公室使用時，請確保設備妥善管理、資訊安全及病毒防護。
19. 傳輸檔案時，應事先掃毒並遵照資訊安全規範。
20. 不得將作業系統內建之個人防火牆功能關閉。
21. 使用文書處理軟體(包括 Word、Excel、PowerPoint 等)應將巨集安全性設定為高級或更高，若執行特殊程式時如須降低安全性，請先執行安全性評估作業。
22. 禁止使用點對點(P2P)互連之相關工具或任何有危害單位網路、設備及造成網路壅塞佔用頻寬等軟體及架站軟體(FTP)作私人用途。
23. 使用個人電腦設備儲存、處理、傳輸機密資料（含個人資料）時，應作加密機制處理。
24. 應定期備份個人電腦設備內重要文件及資訊，各種備份工具（如軟碟、磁帶、抽取式硬碟等），需存放於安全之地點。
25. 個人電腦請關閉插入可攜式儲存媒體或光碟時之自動執行功能（Autorun）。

26. 應避免使用非本會防護範圍內(本會各辦公室)之網路及電腦設施辦理公務，若確有其必要使用外部(如住家、公共場所)資訊環境，請確認資訊使用環境是否具備下列防護措施：
- (1). 儲存於攜帶式儲存媒體(如行動碟)之公務相關電子檔案應予加密。
 - (2). 使用之連網電腦設備應安裝防毒軟體(含最新版之病毒碼更新)及防火牆，並應保持啟動運作狀態。
 - (3). 處理公務之電腦設備以不連上網路為原則(使用本會網路應用系統除外)，同時於處理完畢後應將公務相關電子檔案移除，且避免存放於主機。
27. 應隨時清理個人電腦的資源回收筒，確保已經刪除的重要資料不會因遺留在資源回收筒未清理，而遭未經授權之使用。
28. 未經書面授權不得將任何非本會資產之電子媒體攜帶至辦公室使用。
29. 微軟公司自 103 年 4 月 8 日起終止 XP 作業系統之支援服務, 為避免滋生資安漏洞，請依行政院國家資通安全會報技術服務中心提出的「因應微軟公司 Windows XP 作業系統終止支援服務之防護措施建議」，預為規劃並管制落實相關防護措施。

(二)、密碼設定原則：

1. 電腦設備應設定帳號密碼並定期檢查，密碼建議每 6 個月更新一次。
2. 密碼設定原則密碼建議長度至少 8 個字元，且包含英文數字及特殊符號等。建議可採用包含大寫及小寫字母、數字、標點符號、特殊字元之組合以增加複雜度。
3. 密碼之設定不得與帳號相同。
4. 妥善保管帳號及密碼，不隨意透漏或提供給他人使用；勿將密碼記載在他人垂手可得之地方，如：貼在螢幕上。
5. 懷疑密碼洩洩，立即變更密碼。

(三)、軟體使用安全：

1. 請勿下載、安裝或使用來路不明、未經授權或影響電腦網路環境安全之電腦軟體。
2. 進行下載、複製、使用軟體或不明來源檔案前，應先完成掃描檢查是否具有惡意軟體，確認檔案安全無虞，嚴禁任意移除或關閉防毒軟體。
3. 移除電腦設備中非法或未經受授權軟體、音樂、影片檔等。
4. 公務用電腦設備安裝軟體時，注意下列事項：
 - (1). 禁止使用無授權及非法軟體，以落實使用合法軟體。
 - (2). 使用軟體時，請注意其授權數量、範圍、使用期限，與取得合法授權證明或相關佐證(授權序號或授權資料網頁)，以確認所使用軟體之合法性。
5. 會內許可安裝之軟體類別有：本會專業系統、電腦作業系統、辦公室應用軟體、防毒軟體、美工設計、影音編輯、統計分析、解壓縮、檔案傳輸軟體(不包含 P2P 軟體)、文書編輯軟體、翻譯軟體。上述軟體如經取得合法授權或為免費軟體即可安裝，其餘軟體需提出申請由電腦室審核。

二、伺服器資訊安全管理

- (一)、各單位提供之伺服器，須有專人負責維護並進行相關資訊安全作業。
- (二)、設定防火牆以控管外界與單位內網路間之資料傳輸與資源存取，並關閉不使用的通訊埠，以避免病毒感染及駭客攻擊。
- (三)、開放外界連線作業之伺服器主機，應避免外界直接進入資訊系統或資料庫存取資料。
- (四)、伺服器主機管理之安全性，應視需要之使用情況，加密通道（如 VPN、SSH）等各種安全控管技術。
- (五)、各單位開發之系統及網站(含委外開發)，應於完成後，先執行弱點掃描與完成修補風險弱點始可上線；運作中網站亦請定期進行必要的系統及網站弱點掃描。
- (六)、每次掃描完成後應產出弱點掃描報告與進行相關漏洞修補。
- (七)、重要系統設定檔、網頁資料、伺服器檔案、資料庫及機密性檔案資料均應訂定備份週期。
- (八)、伺服器管理員需定期備份重要的資料檔案至第二、三媒體。
- (九)、資訊設備使用如有立即危及安全之疑慮，應立即處置。
- (十)、伺服器結束遠端系統維護作業後，應關閉應用系統及網路連線，並清除螢幕上的資訊，將作業系統登出。
- (十一)、檢視各設備中系統之時間是否一致，並進行校正及同步作業。
- (十二)、檔案伺服器使用管理：
 - 1. 各單位請依照現有部門、組別、專案或特定職務屬性建立專屬之資料夾，並依存取層級個別設定人員權限，勿讓所有人員皆可隨意存取所有資料夾之檔案。

2. 具有機密性之檔案請存放於專屬之資料夾，並設定可存取人員之權限，如：個案資料、認養人資料…等機密性檔案，切勿存放於公用資料夾裡。
3. 所有資料夾，包括：部門資料夾、公用資料夾…等，切勿存放非工作所需之檔案(如：電影影片、MP3、盜版軟體)；及大型備份檔案(如：.gho 檔案)。
4. 單位資訊人員需定期檢視檔案伺服器的容量，以評估是否增加空間和刪除不必要之檔案或移除已備份之不常使用之檔案。
5. 資訊人員至少每周需針對檔案伺服器進行一次完整備份。

三、資產(個資)盤點及業務流程

(一)、各單位應鑑別所管轄設備，含已申請報廢仍繼續使用之資訊資產，並建立資訊資產清單。

(二)、每年至少進行一次資產盤點與資訊資產清單覆核，以更新及確保資訊資產清單的正確性及完整性。

(三)、資訊資產分類規則：

資訊資產依其性質不同，分為三類：軟體、硬體、個人資料。

1. 軟體 (Software)：作業系統、應用系統程式、套裝軟體等。
2. 硬體 (Hardware)：相關硬體設施，如：網路設備、伺服器、個人電腦、公共電腦、筆記型電腦、智慧型裝置及其他電子數位產品等。
3. 個人資料(Personal Information)：儲存於硬碟、磁帶、光碟等儲存媒介或以紙本形式存在之文書資料、報表等紙本文件，含直接或間接蒐集之可直接或間接方式識別個人之資料。

(四)、資訊資產盤點說明

1. 軟、硬體

清查各單位之全部電腦設備(含網路設備、伺服器、個人電腦、公共電腦、筆記型電腦、智慧型裝置及其他電子數位產品…等)及軟體，逐一編碼記錄於資訊資產清單。另將該電腦設備之 IP 位址及安裝軟體名稱(含作業系統、應用系統程式、套裝軟體)一併列入清單中。

2. 個人資料

清查直接或間接蒐集之可直接或間接識別該個人資料的所有紙本文件及電子檔。

(五)、資訊資產之報廢（或銷毀）採取適當之方式進行銷毀，如：硬碟報廢丟棄前需先將硬碟內之資料完全清除並加以完整格式化後，才能丟棄。

(六)、資訊設備資產應設置於安全、穩定、適切之環境，並列冊本會財產帳目，以利管理。資訊設備管理由資訊業務主管單位，依各項設備不同之產品特性規定之。

四、個人資料保護管理規範

(一)、個人資料使用管理：

1. 蒐集個人資料時，明確告知當事人機關名稱、蒐集目的、個人資料之類別、利用期間、地區、對象及方式、當事人行使之權利事項及方式等，及當當事人不提供個人資料時會對其權益所造成之影響。
2. 蒐集個人資料應符合特定之目的，並確保資料之正確性、完整性和時效性。
3. 當事人可以行使之權利及方式，例如當事人可請求查詢、閱覽、製給複製本、補充、更正、刪除、停止蒐集、處理或利用。
4. 向當事人說明可自行判斷是否提供個人資料，若為本會提供服務時所必須之資訊，因而造成無法提供該服務情形時，當讓當事人瞭解對其個人權益之影響。
5. 蒐集個人資料時，需經適當之授權與監督並僅就所需之必要欄位進行搜集。經授權同意交換個人資料時，電子類文件需對資料檔案加密或透過加密通道傳送、紙本類文件以彌封或其他安全方式進行傳遞交換工作。
6. 個人資料若非經資料當事人之書面同意或經法令規定許可，不得任意揭露、販售或用於蒐集時的特定目的以外之用途。
7. 非由當事人提供之個人資料，得於處理或利用前向當事人補行告知義務，告知方式得以書面、電話、傳真、電子文件或其他適當方式為之。
8. 個人資料之處理行為需經單位主管核准，宜釐定使用範圍及調閱或存取權限。個資存取時應視需要考量採取權限區隔、資料加密機制，或相關核准程序加以控管，並留存可識別之發送紀錄需及個資使用者身分以供事後稽查。
9. 使用者經正式授權存取個人資料檔案時，其帳號必須為唯一，避免共用帳號。

10. 以電腦處理個人資料時，需核對個人資料之輸入、輸出、編輯或更正是否與原件相符。個人資料提供利用時，對資料相符與否如有疑義，應調閱原始檔案查核。
11. 針對有備份必要之個人資料，除有必要時採取加密機制，存放重要機密資料之備份媒體亦應以適當方式保管，且定期執行資料回復測試，以確認備份資料之可用性。
12. 禁止使用即時通訊軟體、私人外部信箱（如奇摩信箱、Gmail、Hotmail等）傳輸及存取個人資料檔案。若因公務需求而欲使用通訊軟體傳輸公務資料時，請針對檔案進行加密保護。
13. 各單位管理之網站或網頁內容，於確有必要公布個人資料時，需經單位主管核准，且依相關法律及規範處理，始得公布。

（二）、個資處理人員管理：

1. 處理接觸機密資料人員，應克盡保密之責，需依「工作規則合約中之保密約款」規定之，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。
2. 因業務需要所保管之資訊、資料與系統，未經授權不得提供外界使用，亦不得作為私人用途。
3. 禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人與會內資料。
4. 資訊系統與設備管理者如因職務異動而成為非授權使用者時，相關單位應主動通知資訊業務單位與網路系統管理人員變更該使用者之帳號權限。
5. 離(退)職人員，需依據本會人員離(退)職處理流程辦理，並確實交接業務範圍內之相關資料，離職流程中應將資訊業務單位列為必經之程序，並由資訊業務單位停用該帳號後，始完成離(退)職程序。

- (三)、為了落實適當之安全性防護措施，本會會採取使用紀錄、軌跡資料及證據保存的機制。
- (四)、員工因執行業務需要而需調閱資訊記錄者，應提出書面申請，並經單位主管核准，情節重大者由最高主管裁示。
- (五)、個人資料外洩(竊取、洩露、竄改或其他侵害事件)處理流程：
1. 立即通知該單位主管。
 2. 個資外洩單位以最速件級別專簽會行政處辦理。
 3. 發生個資外洩事件，即時以書面、電話、傳真、電子文件或其他足以使當事人知悉或可得知悉的方式，通知個人資料受侵害項目、產生之影響及已採取之因應措施。
- (六)、蒐集、利用及處理個人資料時，請務必遵守「個人資料保護法」，確實妥善保管所取得之個人敏感性資料。個人資料管理人若違反個人資料保護法規定者，將受法律制裁；其他未盡事宜，悉依個人資料保護法之規定辦理。
- (七)、員工若違反「工作規則合約中之保密約款」或「個人資料保護法」之規定，經查明屬實，將立即停止使用資訊設備之權利，並依本會「人事管理規則」議處。其他未盡事宜，將呈請人事委員會討論議處。若情節重大已達違反法律者，將依法處理，並配合司法機關調查。

五、文件管理

- (一)、文件處理需符合本會文件管理辦法之規定。
- (二)、資安與個資聯絡人協助管制、保管、維護、建檔稽核計畫內相關文件，將其鎖在安全的儲櫃或其他安全場所。文件發送對象應以最低必要的人員為限。
- (三)、文件須分類歸檔，並依使用者職權賦予適當之文件存取權限，對於具機密性資料及文件，應特別控管以避免資料外洩。
- (四)、表單或紀錄至少需保留一年，且考慮單位或法律上資料保存期限之要求。
- (五)、單位承辦人保有之個人資料之紙本文件，不需使用時應置放於上鎖之安全儲櫃或其他安全場所內，避免有心人士或非授權人員拿取。
- (六)、使用影印機、印表機、傳真機、掃描機或多功能事務機後，應立即將紙本資料取走。
- (七)、含個人資料之紀錄紙本文件請依相關法令規定或契約保存年限保管，不再使用時請銷毀或依相關法令規定妥善處理，個資文件保留以最小化為原則。
- (八)、文件之報廢（或銷毀）應依相關規定，採取適當之方式進行銷毀。

六、通訊與作業管理

(一)、儲存管理：

1. 電腦儲存設備、可攜式資訊媒體若需連接資訊媒體設備或網路時，應先進行電腦病毒掃描，確認無問題後始可使用。
2. 電腦儲存設備、可攜式資訊媒體如為單位內共同使用，使用者切記在使用完畢後將所有的資料文件移除，以免資料遭他人誤用。
3. 機密性資料若儲存於電腦儲存設備、可攜式資訊媒體，應考量使用加密技術或其他技術加強安全控管。
4. 重要之儲存媒體(含機密性資料之電腦儲存設備)、可攜式資訊媒體，不使用時應置放於實體安全區域及環境(如：門禁控管辦公區域內之上鎖之防潮箱、書櫃)或由專人管理，僅經授權或簽署保密協議後方可使用。
5. 非公務需求不得將載有機密性資料之可攜式資訊媒體攜出辦公場所。
6. 電腦儲存設備、可攜式資訊媒體所使用之密碼或編碼技術不應透露予與業務無關之人員。
7. 電腦儲存設備、可攜式資訊媒體遞送前應加以妥善包裝保護，避免發生實體損壞。
8. 當發現資訊設備有異常現象，請立刻連絡資訊人員處理。
9. 資訊設備發生損壞，原因為不當操作或違反使用規定所造成，設備使用者須自負維修復原之責。
10. 外部團體或個人更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。

(二)、存取管理：

1. 使用者職務異動或離職時，應即時通知相關單位調整或終止使用者之存取權限。並將其所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。
2. 會內應用系統之使用，僅限業務相關之授權使用者，並應適當控制。例如新增、刪除或執行等。
3. 會內應用系統特殊權限之授權管理，須依執行業務別需求，賦予系統存取特殊權限的授權，並以執行業務及職務所需之最低資源存取授權為限。
4. 使用者經正式授權存取業務相關之系統資料時，其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。
5. 重要資訊系統及特殊權限之存取帳號之密碼變更期間應較一般權限之帳號頻繁。
6. 使用者或委外廠商之人員如因作業需求，需對系統進行存取，需經主管授權或允許執行存取作業。並針對需求內容、所需權限、帳號有效時間，由系統管理者依照所需權限及帳號有效時間，建立必要之帳號供使用。

七、實體與環境安全控管

(一)、安全管理：

1. 機房平時需要關門上鎖。
2. 為確保相關設施之安全，非單位指定之人員不得擅自進入機房或使用相關資訊設備。
3. 於單位安全區域與辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關單位進行處理。
4. 若外部人員或單位內部未具機房或管制場所進出權限之人員，因執行業務需求進入該場所時，應指派人員隨行方可進出。

(二)、報廢管理：

1. 報廢後移作他用之電腦設備，請移除所有軟體(含作業系統與應用軟體等)並清除儲存之資料內容。
2. 儲存機敏性資料檔案之電腦或相關設備，於報廢或移轉他用時，應利用資料清除軟體工具，清除儲存之內容，確認所儲存之資料已清除且無法還原閱讀其內容。
3. 軟、硬體資訊資產報廢時，應更新修改「資訊資產清單」，經單位主管審核並確認資料、軟體清除後，方可進行資訊資產報廢程序。
4. 機密性文件廢止時，請依相關法令規定妥善處理。
5. 機密紙本文件不再使用時，嚴禁擲為廢紙回收再使用，應以碎紙機進行破壞使其無法閱讀識別，並刪除電子檔。

八、委外廠商管理

- (一)、 委外廠商於支援執行業務時，處理之個人資料或獲知機密等級(含)以上資訊，應遵守「個人資料保護法」及本會之相關規定，不得對外透露、任意複製或攜出機密性之業務資料，為確保前述事項之落實，要求廠商及其人員簽署「保密切結書」，更換廠商或人員時亦同。
- (二)、 針對涉及個資的委外作業，委外廠商視同委託機關，屬個資法適用範圍內。應重新審閱委外合約，於委外合約中載明所處理之個人資料的保密義務，同時委外廠商也負有管控資訊安全的相關責任及違反之罰則。
- (三)、 於專案期間，本會可透過稽核等方式監督委外廠商之個人資料管理作法，如個資蒐集、處理、利用、傳輸與銷毀之管理情形。
- (四)、 與委外廠商所簽訂正式書面協議或契約中，應明確陳述契約終止時，相關個人資料的銷毀或交還程序。
- (五)、 自行開發或委外處理個人資料檔案之資訊系統，避免以真實個人資料進行測試，如需使用，完成測試作業後立即移除，或將可辨識之個人資料修改為無法辨識之模糊資訊。
- (六)、 宜避免允許維護人員或系統服務廠商以遠端登入方式進行牽涉機密性資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密通道進行（如：HTTPS、SSH 等），及權限控管及留存稽核紀錄。
- (七)、 委外廠商履行合約應提供其使用之軟體，且均須為合法軟體，並不得違反智慧財產權之規定，如有違反事情發生，委外廠商須承擔所有法律責任。
- (八)、 委外廠商所使用之工具軟體、處理作業之執行紀錄及異常處理記錄應留存，本會有權進行稽核，廠商不得異議。

- (九)、 委外廠商人員對於系統帳號應善盡保管之責，系統帳號不得任意交由非作業相關人員使用。
- (十)、 委外廠商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及終止作業權限。
- (十一)、 委外廠商人員，於進行開發或維護軟硬體作業時，需視處理程序中之可能風險，採取適當的安全控制措施，並條列安全規定於正式合約中。
- (十二)、 委外廠商需針對交付之系統，應保證系統內不含後門程式、隱密通道及特洛伊木馬程式。