

# 耀勝電子股份有限公司

## 個人資料保護及管理程序

### 1. 目的：

為規範個人資料之蒐集、處理及利用，提升對個人資料之保護與管理能力，降低公司營運風險，並創造可信賴之保護個資和隱私環境。

本公司所屬人員應依本程序辦理個人資料檔案安全維護及業務終止後個人資料處理事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏，若有員工違反本程序，本公司將依內部規範進行懲戒。

### 2. 範圍：

本程序適用範圍涵蓋所有分公司、營運據點、子公司、客戶及供應商，凡涉及個人資料的蒐集、處理與利用之行為皆適用。

本公司有權修訂本程序，並於修訂後，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件(包括以前述方式告知提供詳載本告知書內容之網站連結)或其他足以使當事人知悉或可得知悉之方式告知當事人修訂要點。

本公司客戶或供應商為推廣業務，非自本公司蒐集第三人之個人資料者，應遵循個人資料保護法規定(如踐行告知義務)，並妥善保存所保有個人資料；若因不當蒐集、處理、利用他人個人資料涉有違反法令規定情事者，本公司可視情節輕重依契約所定條款予以懲處。

### 3 權責：

3.1 各單位：本公司各單位因為其負責業務或執行任務，對該個人資料檔案負有管理的權利與責任，為個人資料檔案最後保存與負責銷毀單位，其權責如下：

#### 3.1.1 資料蒐集：

3.1.1.1 確認蒐集目的與範圍，並明確告知當事人。若非法律明文規定或與當事人有契約或類似契約關係時，需取得當事人書面同意。

3.1.1.2 個人資料的更正或補充，通知曾提供利用個人資料的第三方。

3.1.1.3 個人資料的更正或補充，當因可規則於本公司時，應主動通知當事人。

3.1.1.4 個人資料盤點登記與維持最新的個人資料檔案清冊。

3.1.1.5 機密與極機密個人資料檔案保留處理紀錄。

#### 3.1.2 資料處理：

3.1.2.1 第一次行銷或研究時，提供當事人拒絕機制。

3.1.2.2 逾越原特定目的，再取得當事人書面同意。

3.1.2.3 第三方提供之個人資料，於首次對當事人利用時告知法定事項。

3.1.2.4 依個人保存期限，進行個人資料檔案的銷毀。

3.1.2.5 保留個人資料超過保存期限時，應載明正當之理由。

#### 3.2 資訊部：

3.2.1 資訊部應依本公司業務規模及特性，衡酌經營資源之合理分配，配置管理人員及相當資源，負責個人資料保護管理政策之訂定及修正以及安全維護計畫之訂定、修正及執行，並應適時宣導予員工，以免員工不知情或疏漏，造成公司巨額損失。

- 3.2.2 本公司資訊部應評估個人資料風險及管理機制，並擬訂對事故之預防、通報及應變機制，且針對個人資料安全維護之整體持續改善。
- 3.2.3 資訊部應視事實需要召開會議，針對最新法令規定和公司被當事人請求事項，檢視現行處理程序是否妥當並酌情增修相關管控程序。
- 3.2.4 儲存個人資料之電子媒體，由資訊部負責管理和維護使用記錄、軌跡資料及證據保存，並建立定期備份和緊急復原制度。
- 3.2.5 公司遇有侵害個人資料保護之情事、或可能情事時，資訊部應召集緊急應變小組召開會議，擬訂因應對策，以維護公司之權益。

#### 4. 定義：

個人資料泛指自然人姓名、出生年月日、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，以及其他可以直接或間接識別出個人的資料或數位形式都屬於個人資料之保護範圍，其來源包括：當事人提供資訊給本公司時、基於雙方間的法律關係而取得之資訊、當事人自行公開之個人資料、當事人造訪本公司的網站、當事人向本公司任何一個網站註冊以使用本公司的網站、產品或服務、當事人和本公司網站上的第三方內容或廣告進行互動。另外，本公司也可由第三方獲得當事人的個人資料。

#### 5. 內容：

##### 5.1 個人資料之蒐集

- 5.1.1 公司蒐集個資時，應向當事人告知公司名稱、處理使用目的、利用時機、對象與方式，並取得當事人書面同意文件。公司針對醫療、基因、性生活、健康檢查、犯罪前科等特種個人資料，原則上不得主動蒐集、處理、利用。若因間接或例外因素蒐集、處理或利用特種個人資料時，於當次使用完畢後將資料和電子媒體應儘速銷毀。
- 5.1.2 公司應注意對個人資料之蒐集、處理、利用或傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。公司各部門因執行工作需求，接觸員工和家屬之個人資料時，應善盡管理責任，防止個人資料被竊取、竄改、毀損或洩露。人資部門因職務異動時，應將所保管之電子媒體及文件資料列冊移交。
- 5.1.3 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。
- 5.1.4 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，告知式得以書面、電話、傳真、電子文件或其他適當方式為之。

##### 5.2 資料安全管理

- 5.2.1 本公司所屬人員禁止使用私人可攜式設備（例如 USB 隨身碟、外接硬碟、筆記型電腦、手機、記憶卡等）儲存本公司所保有個人資料檔案。
- 5.2.2 本公司所保有個人資料檔案應以加密方式儲存，僅經授權之所屬人員得開啟處理、利用。以網際網路傳輸個人資料時，亦應以加密方式為之。
- 5.2.3 本公司所保有個人資料檔案應定期備份，以防止資料受損，備份資料之保護比照原件辦理。
- 5.2.4 本公司所保有之個人資料存在於紙本者，於保存期限屆滿時，應以碎紙、委外焚化等方式銷毀。本公司所保有之個人資料存在於磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物者，該媒介物於報廢時應採取消磁、剪斷、敲擊等破壞措施，以免由該媒介物洩漏個人資料。
- 5.2.5 本公司委託他事業執行紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物銷毀時，應與受委託事業簽定個人資料保護條款規範，並派員監督處理程序及留存相關事證。

##### 5.3 設備安全管理

- 5.3.1 本公司所保有個人資料存在於紙本者，應儲存於上鎖之保管箱或檔案室內，僅業務主管有開啟調閱權限。

- 5.3.2 本公司所保有個人資料存在之電腦主機應置放於機房，並設門禁管制，僅業務主管及資訊人員得刷卡進入。
- 5.3.3 其他所屬人員因業務需要而須調閱個人資料者，應事前提出申請，經業務主管人員同意後調閱。
- 5.3.4 本公司所屬員工應妥善保管個人電腦存取資料之硬體，並設定登入及螢幕保護程式密碼。
- 5.3.5 本公司所屬員工於下班前應關閉電腦電源，並將所保有其他個人資料之媒介物置於個人抽屜內上鎖保管。
- 5.3.6 儲存個人資料紙本之保管箱或檔案室內，應設置防火裝置及防竊措施。儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。前項主機置放之機房應設置門禁、監視錄影及防火設備。
- 5.3.7 資訊部應加強資訊流通安全檢查及防護機制，建置防火牆、防毒軟體、密碼存取控制、資料加密..等功能，以防範外部侵入並留存執行 log 記錄。
- 5.3.8 聘用外部專人更新或維修公司電腦設備時，應指定專人在場，防止個人資料被竊取、竄改、毀損或外洩。
- 5.3.9 電腦設備報廢或移轉使用，應確實刪除電腦設備中儲存有關個人資料之檔案，並依「固定資產管理辦法」之流程執行之。

#### 5.4 人員管理措施

- 5.4.1 本公司所屬人員使用電腦設備蒐集、處理、利用個人資料，應以專屬帳號密碼登入電腦系統，存取個人資料檔案權限應與所職掌業務相符。
- 5.4.2 因業務需要而須利用非權限範圍之特定個人資料者，應事前提出申請，經業務主管人員同意後開放權限利用。
- 5.4.3 本公司所屬人員均應簽署保密協定，就於本公司任職期間因業務所接觸個人資料均負保密義務。

#### 5.5 資料銷毀

- 5.5.1 超過保存期限或不再需要使用之個人資料檔，經權責單位主管核准後，進行資料銷毀。但若有正當事由並經審核同意後得延長保留期限。
- 5.5.2 因結束業務經營、交易完成、特定目的消失、契約或法令規定期限屆滿等，所保有之紙本個人資料應以碎紙、委外焚化等方式銷毀紙本，個人資料儲存於磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物者，應以消磁、剪斷、敲擊等破壞措施銷毀。本公司進行前項個人資料銷毀處理時，應記載處理之時間、地點，並以照相或錄影方式留存紀錄。
- 5.5.2.1 紙本若屬大量銷毀應指定專業廠商有相關安全控管措施(如:人員全程陪同或全程錄影監控)。
- 5.5.2.2 紙本若少量則應以碎紙機銷毀。若為電子檔案，應依規範辦理刪除。
- 5.5.2.3 若為資料庫檔案，權責單位提出單位主管核准文件後，由資料庫管理人員進行刪除，並留下紀錄。
- 5.5.3 「機密」等級之個人資料檔案，資料銷毀時應有相關人員陪同，並於銷毀後填寫「個人資料檔案銷毀紀錄表」。
- 5.5.4 磁性媒介需報廢或不堪再使用時，依媒介性質則由個人或資訊處人員以實體破壞或使用其他應用程式或工具清除資料或銷毀該媒介。

6. 附件：無

7. 修改與實施：本辦法呈總經理通過後實施，修正時亦同。