璟德電子工業股份有限公司
個人資料安全保護辦法

1 目的：符合個人資料保護法與相關法令規範，就個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本規則辦法。

2 範圍：為防止個資保護清冊表(表單編號：T-H00-X039)所載的個人資料被竊取、竄改、毀損、滅失或洩漏，所採取之技術上及組織上之措施。

3 名詞定義：

3.1 個人資料：指自然人之姓名、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。

3.2 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

3.3 蒐集：指以任何方式取得個人資料。

3.4 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

3.5 利用：指將蒐集之個人資料為處理以外之使用。

3.6 公務機關：指依法行使公權力之中央或地方機關或行政法人。

3.7 當事人：指個人資料之本人。

4 權責：

4.1 稽核室：稽核相關程序是否完備，防範個人資料被盜用。

4.2 各部門：使用相關部門所提供涉及到個人資料資訊時之合法性並做必要的教導與提醒。

4.3 資訊部：相關硬體設備安全防護之措施。

4.4 人資部：確保個人資料蒐集、處理與利用之合法程序。

5 作業程序：

5.1 應於法律允許之範圍內提供資料當事人下列權利：

5.1.1 查詢、閱覽、提供複本、補充、更正。

5.1.2 請求停止蒐集、處理、利用或刪除。

5.1.3 當事人權利行使，應採取下列管理措施：

5.1.3.1 當事人身分之確認。

5.1.3.2 告知所需支付之費用及應釋明之事項。

5.1.3.3 對當事人請求之審查方式，遵守個資法處理期限之規定。

5.1.3.4 有個資法所定得拒絕當事人行使權利之事由者，應將理由通知當事人。

5.2 資料管理者對於個人資料基本應用原則：

5.2.1 經當事人書面同意或於具有其他法律所允許之事由時，以合法、公正手段於適當場所蒐集、揭露或用於蒐集時的特定目的以外之用途。

5.2.2 符合蒐集個人資料特定目的，並確保資料之正確性、完整性和時效性。

5.2.3 應於蒐集個人資料之當時即向當事人明確闡述蒐集的目的，或依法令另為告知，不得另作他用。

5.2.4 調閱個人資料：

5.2.4.1 限於被調閱員工資料的主管可申請調閱，填寫紙本個人資料調閱申請表(表單編號：T-H00-X040)，經部門主管核准。

5.2.4.2 公務機關發文正式函文。

5.2.4.3 經個人資料保管的主管審查申請原因的合理性後核准，文件才可以提供。

5.2.5 進行個人資料國際傳輸前，檢視是否受主管機關限制並遵循之。

5.2.6 檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應主動或依當事人之請求，刪除、停止處理或利用。

5.3 個人資料保護及安全原則：

5.3.1 系統安全：

5.3.1.1 處理個人資料檔案之資訊設備，需設置帳號及密碼，密碼應定期更換一次。

5.3.1.2 禁止與他人共用系統帳號。

5.3.1.3 個人資料輸入、輸出、列印、存取、更新、更正或註銷等處理行為，宜釐定使用範圍及調閱或存取權限。

5.3.1.4 應定期備份個人資料之主機一次，以防止個人資料被竊取、竄改、毀損、滅失或洩露。

5.3.1.5 個人資料檔案使用完畢後，應即退出應用程式，不得留置於電腦螢幕。

5.3.1.6 傳遞處理個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案加密。

5.3.1.7 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問，應調閱原檔案查核。

5.3.1.8 存放個人資料之主機設備不可對外連網。

5.3.1.9 存放個人資料之主機設備應安裝防毒軟體，應定期更新病毒碼及程式，並排程掃瞄。

5.3.1.10 存放個人資料之資訊設備應定期檢視、更新作業系統、應用程式漏洞。

5.4 設備管理注意事項：

5.4.1 應指定專人負責管理儲存個人資料檔案之主機設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息。

5.4.2 儲存個人資料之主機設備應置放於門禁控管之辦公區域、機房，以保護主機安全。

5.4.3 儲存個人資料檔案、紙本等相關儲存媒體，應指定專人管理，保存於安全環境，以防止資料損壞、遺失或遭竊取。

5.4.4 外部人員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。

5.4.5 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

5.5 個人資料管理人員應注意事項：

5.5.1 應對處理個人資料檔案之員工施予資訊安全與個資隱私保護之教育訓練，並定期於公司內宣導個資隱私保護之重要性。

5.5.2 處理個人資料檔案之員工，應簽訂保密切結書，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員應重設密碼，必要時更換使用者帳號。

5.5.3 處理個人資料檔案之員工須確認於離職時或合約終止時，取消或停用其使用者帳號，且收繳其通行證及相關證件。

5.5.4 禁止員工在社群網站、部落格、公開論壇或其他利用網際網路形式、使用任何即時通訊軟體、外部網頁式電子郵件(Webmail)、WebHD、P2P 軟體或其它相關工具，公開、下載、傳輸或分享(Share)於公司內所取得之檔案或個人資料。

5.6 系統開發及委外管理注意事項：

5.6.1 個人資料檔案之資訊系統，維護、更新、上線、及版本異動等作業，應由專人管制。

5.6.2 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個人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、VPN 等）。

5.6.3 開發處理個人資料檔案之資訊系統，應將個人資料(包含測試用個人資料)施予妥善之保護與控管。

5.6.4 應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。

5.7 通報、應變及預防處理機制

5.7.1 員工發現有資料洩漏或違反本辦法及個人資料保護法法規等事件時，應迅速通報單位主管或人資部門處理。

5.7.2 個人資料發生竊取、竄改、毀損、滅失或洩漏等安全事故，應採取下列措施：

5.7.2.1 控制當事人損害。

5.7.2.2 必要時，於查明事故後通知當事人事故事實、所為因應措施及諮詢專線。

5.7.2.3 進行矯正預防措施。

5.7.3 資料洩漏者之行為若觸犯法律規定，由人資部門與資訊部門進行查處。

5.8 安全稽核、紀錄保存及持續改善機制

5.8.1 為確保本辦法之落實，應依其業務規模及特性，衡酌經營資源之合理分配，訂定適當之個人資料安全稽核機制，並列入內部控制及稽核項目。

5.8.2 執行各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。

5.8.2.1 依規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

5.8.2.1.1 刪除、停止處理或利用之方法、時間。

5.8.2.1.2 將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

5.8.2.2 前項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

5.8.3 為持續改善個人資料安全維護，其所屬個人資料管理單位或人員，應定期提出相關自我評估報告，並執行下列機制：

5.8.3.1 檢視、修訂本作業相關個人資料保護事項。

5.8.3.2 針對評估報告中有違反法令之虞者，規劃、執行改善及預防措施。