# 倉佑實業股份有限公司

## 114 年度個人資料保護政策及執行情形

本公司重視「客戶隱私權保護」，遵循《個人資料保護法》，訂定《個人資料保護管理流程及政策》，及嚴謹的個資隱私安全管理與防護措施，並建構資料治理制度，制定資料標準與分級，落實資料存取權限管控及資料擁有者之覆核機制，確保資料的存取與共享受到妥善治理與保護，以及資料的可用性、完整性及保密性。適用範圍涵蓋所有分公司、營運據點、子公司、客戶及供應商。針對營運過程中所涉及之個資隱私之蒐集、處理、利用及保護，除遵循政府相關法令規章，在法令規定之範圍內使用，不會提供、出租或以其他變相之方式，將個資揭露予第三人，且會依循公司所定之《個人資料保護管理流程及政策》落實執行，致力維護客戶的資料安全及隱私權利。本公司《個人資料保護管理流程及政策》如下：

一、流程說明：

1. 目的：為規範個人資料之蒐集、處理及利用，依行政院公布之「個人資料保護法」( 以下簡稱個資法 )，特訂定本管理流程，以提升對個人及客戶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。
2. 定義：所謂個人資料，係指依個資法第 2 條第 1 款所稱個人資料以及個資法第 2 條第 2 款所稱之個人資料檔案。泛指自然人之一般個資(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、聯絡方式、財務情況、社會活動)，與特種個資(醫療、基因、性生活、健康檢查、犯罪前科)，以及其他可以直接或間接識別出個人的資料或各種型式檔案(包括備份檔案)。
3. 範圍：凡本公司對個人資料保護之資源配置、風險評估與管理機制、蒐集、處理及利用程序、資料安全管理、事故預防及緊急應變程序、稽查及持續改善等悉依本流程規範執行之。
4. 權責：
   - 4.1 資安委員會：負責推動、協調及督導本公司個資保護及資訊安全管理業務。由總經理或其指定代理人擔任主任委員，並指派相關人員執行組織任務。
   - 4.2 個資管理單位：凡為所屬業務與因業務執行而進行個人資料之蒐集、處理、利用資料之業務執行單位，均應善盡管理及保護之責。
   - 4.3 資訊安全管理單位:資訊單位應確保公司內外部傳輸之電子資料(含個資)及資訊系統內資料檔案已為適當之安全維護。
   - 4.4 個資使用者：各單位主管或人員若因執行工作需求，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。

二、人員及資源配置

1. 為落實公司整體資訊安全(包含個人資料)之保護與管理，本公司設置資安委員會，此委員會之組織：
   1.1 主任委員：由總經理或其指定代理人擔任。
   1.2 執行秘書：由資訊主管擔任。
   1.3 委員(管理人員)：由副總經理、個資管理單位主管以及經營階層指派之人員擔任。
   1.4 監督人員:由稽核室督導並評核資訊安全(包含個人資料)保護管理程序運作及安全措施執行之成效。
2. 資安委員會之職掌：
   2.1 本公司資訊安全(含個人資料保護)政策之擬議。
   2.2 本公司資訊安全(含個人資料保護)管理制度之推展。
   2.3 本公司資訊安全(含個人資料隱私)風險之評估及管理。
   2.4 本公司各單位職員工之資訊安全(含個人資料保護)意識提升及教育訓練計畫之擬議。
   2.5 本公司資訊安全(含個人資料保護)管理制度基礎設施之適當性評估。
   2.6 本公司資訊安全及個人資料管理制度適法性與合宜性之檢視、審議及評估。
   2.7 本公司資訊安全事件審查及監視的結果，並針對資訊安全事件提出適當的行動方案。
   2.8 其他本公司資訊安全(含個人資料保護)管理之規劃及執行事項。
3. 資安委員會之運作：
   視業務推動之需要，不定期召開會議。執行秘書需負責會議之召集，由主任委員擔任主席，主任委員因故不能主持會議時，得指定委員會委員代理之。

三、個人資料盤點、風險評估與風險管理機制

1. 個人資料盤點：
   為界定個人資料範圍，應由資安委員會之執行秘書召集各個資管理單位，共同規劃個人資料盤點作業並建立「個人資料檔案清冊」，於管理單位新增業務以及業務變更終止時亦須進行更新，以確實掌握公司內部所保有之個人資料，並據以進行風險評估及管理，達成個人資料保護與管理之目標。
2. 風險評估：
   為掌握本公司個人資料之蒐集、處理或利用等作業活動之安全風險，個資管理單位應於盤點後依「個人資料風險評估表」，評估個人資料所可能發生的風險，並依據評估結果，採取適當的因應，透過事先鑑別方式，作為個資保護措施之規畫依據。
   個人資料之盤點結果、檔案清冊及風險評估結果應繳交給資安委員會之執行秘書或指定窗口進行彙整，並將彙整結果呈報資安委員會進行討論，以利訂定可承受風險之等級，並展開各項管理制度或管理方案的檢討與個人資料安全維護之整體持續改善。

四、個人資料之蒐集、處理、利用或其他管理程序

【個人資料蒐集、處理及利用程序】

1. 各單位應確保對個人資料之蒐集、處理、利用或傳輸，係以誠信方式進行，出於最小且不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。
2. 有關醫療、基因、性生活、健康檢查及犯罪前科之「特種個資」，除法律有明文規定或因履行法定義務所必要，且有適當之安全維護措施外，不得蒐集、處理或利用，若有疑義應報請資安委員會同意後為之，並應於當次使用完畢或使用期限屆滿後，將資料和電子媒體應儘速銷毀。
3. 各單位於蒐集或處理「一般個資」應有特定目的，並符合下列情形之一：
   (1)法律明文規定。
   (2)與當事人有契約或類似契約之關係。
   (3)當事人自行公開或其他已合法公開之個人資料。
   (4)經當事人書面同意。
   (5)與公共利益有關。
   (6)個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
4. 各管理單位依前條向當事人蒐集個人資料時，除有個資法第 8 條第二款之免告知義務外，應以『個人資料授權使用同意書』明確告知當事人下列事項：
   (1)公司名稱。
   (2)蒐集之目的。
   (3)個人資料之類別。
   (4)個人資料利用之期間、地區、對象及方式。
   (5)當事人依第三條規定得行使之權利及方式。
   (6)當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
5. 各單位蒐集非由當事人提供(間接取得)之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條所列應告知事項。但符合個資法第九條第二項規定情形之一者，得免告知。
6. 對個人資料之「利用」應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，始得為特定目的外之利用：
   (1)法律明文規定。
   (2)為增進公共利益。
   (3)為免除當事人之生命、身體、自由或財產上之危險。
   (4)為防止他人權益之重大危害。
   (5)經當事人書面同意。
   (6)有利於當事人權益。

7. 若因業務需要，個資管理單位人員於提供個人資料予當事人，及當事人部門主管以外之需求者前，應充分確認需求原因符合特定目的，且已獲需求單位之部門主管同意後後始得提供。若有疑義應報備個資管理單位主管後為之，提供時亦應以書面或電子郵件照會個資管理單位、需求單位及被提供人之單位主管，以留下記錄。

【委外監督作業程序】

1. 若因業務需要，委託他人蒐集、處理或利用個人資料時，委託單位應慎選受託對象，並對受託者進行適當之監督，以確保委託處理個人資料之安全管理。
2. 委託關係終止或解除時，應要求受託者依約定方式確實刪除、銷燬或返還因執行受託業務所保有之個人資料，並提供刪除、銷燬或返還個人資料之時間、方式、地點等紀錄；必要時，得進行實地查訪。

【當事人行使權益之處理】

1. 當事人就其個人資料請求查詢、閱覽、複製、補充、更正，應填具『個人資料申請書』向個資管理單位提出；若委託代辦申請，須另附提委託授權書及受託人身份證明文件。申請案件有下列情形之一者，個資管理單位得駁回其申請：
   (1)申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未補正者。
   (2)妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
   (3)與法令規定不符。
   (4)妨害公司或第三人之重大利益。
2. 對於個人資料要求查詢、閱覽或複製的請求，公司須在 15 天內決定是否同意，若要拒絕得書面行文當事人說明理由，得最多可再延長 15 天。對於個人資料要求補充或更正，公司得在 30 天內答覆，最多再延長 30 天。
3. 個資管理單位應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。
4. 申請查詢或請求閱覽個人資料或製給複製本者，公司得酌收必要成本費用。

五、個人資料保護之安全措施

1. 為防止個人資料被竊取、竄改、毀損或洩露，個人資料之管理單位應指派專人負責個資的管理和維護，並進行下列防護措施：
   1.1 書面資料應上鎖保管。
   1.2 電子檔資料應加以密碼鎖定。
   1.3 凡負責管理個人資料人員因職務異動時，應將所保管之電子媒體及文件資料列冊移交。
2. 存放於公司網路上之個人資料，由資訊單位進行下列防護措施：
   2.1 資訊單位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軌跡資料。

2.2 聘用外部專人更新或維修公司電腦設備時，設備使用者應通知資訊人員到場，以防止個人資料被竊取、竄改、毀損或外洩。

2.3 電腦設備報廢或移轉使用，資訊人員應確實刪除電腦設備中儲存有關個人資料之檔案。

3. 實施稽核人員得調閱有關保護個人資料之措施作法和查看硬體設施。
4. 其他電子文件作業之保護安全措施，參照「電子資料安全作業細則(IS-001)」規範辦理。

六、事故之預防、通報及應變作業程序

1. 為使所屬人員了解個資保護之重要性，以提高蒐集、處理、利用個人資料之適法性及安全性意識，並妥善保護個人資料，人資及資訊單位應規劃個資法令、個人資料保護管理制度或資訊安全維護之相關教育訓練或宣導。
2. 各單位若發現個人資料被竊取、洩漏、竄改、毀損或其他侵害者，經初步確認屬個資外洩之危機事件後，應立即通報權責主管及資安委員會之執行秘書，由其通報主任委員並進行事故分析及研擬應變處理措施，以避免事故擴大。於事故查明後，應由個資管理單位以適當方式通知當事人被侵害之事實以及已採取之措施。
3. 事故之調查結果應提報至資安委員會中進行審查，並針對資訊安全事件提出適當的行動方案。

七、稽查及持續改善

1. 稽核單位應定期稽核個資保護管理制度之實際執行狀況，藉以瞭解相關缺失，持續進行改善，使個資保護管理制度能夠更加完善。
2. 資安委員會之執行秘書，遇下列情形之一並認為有必要時，應呈報召集人召開資安檢討會議，並應做成會議記錄以利持續改善：
   (1)法令修正時。
   (2)重大個資外洩事故。
   (3)有重大稽核缺失時。
   (4)其他重大事由。

八、客戶資料目的外利用

本公司致力於保護客戶的隱私權，因此不會將蒐集到的客戶資訊於本攻策所列目的以外進行利用。

九、聯絡方式

如對本隱私權政策有任何疑問，請依以下方式和我們聯絡：

地址：嘉義縣民雄工業區中山路 18 號

電話：+886 05-2200888 分機 1260

您也可利用網站「聯絡我們」功能，或寄電子郵件至 chun@tsangyow.com.tw。

本公司就「員工個資保護培訓課程」、「供應鏈與合作夥伴管理」、「內部管理與技術防護」及「事件回應與風險管理」四大面向，揭露114 年度投入個資保護政策相關量化數據及管理指標如下：

- 員工個資保護培訓課程

  114 年度共完成 344 人次資訊安全教育訓練與測驗，

  訓練內容涵蓋營業秘密保護、智慧財產權保護及個人資料保護等，

  受訓員工佔全體比例 100%

  完訓後測驗及格率皆為 100%

- 供應鏈與合作夥伴管理

  100%合格供應商名冊採購合約書制訂保密相關要求

  114年度執行共12家供應商稽核

- 內部管理與技術防護

  114年度執行61家(每年/次)已交易客戶信用檢核作業

- 事件回應與風險管理

  0%個資申訴案件，若發生案件應於1天內回覆處理，

  114年度發生0起違反『個人資料保護管理流程』事件，

  行為不當的員工皆依情節輕重受到包含職務調整、解雇在內不同程度懲處。