

潤弘精密工程事業股份有限公司
個人資料檔案安全維護處理方法

111 年 3 月 31 日訂立

一、個人資料之範圍

- (一) 特定目的：經營綜合營造業事務、工程技術顧問事務、契約或類似契約或其他法律關係事務、職業安全衛生管理、人事管理。
- (二) 第三人個人資料：
本計畫所稱之第三人個人資料，除係指第三人姓名、出生年月日、國民身分證統一編號、婚姻、家庭、教育、職業、聯絡方式外，及其他得以直接或間接方式識別該個人之資料。
- (三) 員工個人資料：
指姓名、出生年月日、身分證統一編號、婚姻、家庭、職業、健康檢查、財產狀況、聯絡方式等，及其他得以直接或間接識別該個人之資料。

二、風險評估及管理機制

(一) 風險評估

- 1、配合個資管理政策，指派適當人員負責風險評估與管理工作。
- 2、依據法令法規對個人資料定義進行個資盤點，製作個資清冊。
- 3、針對個資清冊內容實施風險評鑑時應考量以下可能之外洩管道，以識別風險等級：
 - (1)、經由本公司電腦下載或外部網路入侵而外洩。
 - (2)、經由接觸書面契約書類而外洩。
 - (3)、員工故意竊取、毀損或洩漏。

(二) 管理機制

- 1、藉由使用者代碼、識別密碼設定及文件妥適保管。
- 2、定期進行網路資訊安全維護及控管。
- 3、電磁資料視實際需要以加密方式傳輸。
- 4、加強對員工之管制及設備之強化管理。

三、個人資料蒐集、處理及利用之內部管理措施

- (一) 直接向當事人蒐集個人資料時，應明確告知以下事項：
 - a.公司名稱。
 - b.蒐集目的。
 - c.個人資料之類別。
 - d.個人資料利用之期間、地區、對

象及方式。e.當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。

- (二) 所蒐集非由當事人提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項。
- (三) 與第三人簽訂文件時，如獲得第三人同意，方得進行個人資料蒐集、處理及利用。
- (四) 利用個人資料為行銷時，當事人表示拒絕行銷後，應立即停止利用其個人資料行銷。
- (五) 中央主管機關對本公司為限制國際傳輸個人資料之命令或處分時，通知所屬人員遵循辦理。所屬人員於個人資料進行國際傳輸時，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域對資料接收方為下列事項之監督：1.預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。2.當事人行使個資法第 3 條所定權利之相關事項。
- (六) 當事人表示拒絕行銷或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，應提供受理連絡窗口，並將聯絡窗口及電話等資料，揭示於本公司或公司網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。
- (七) 負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。
- (八) 本公司員工如因工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。
- (九) 由指定之管理人員定期查核、界定蒐集、處理及利用個人資料之範圍、執行各項個人資料檔案之安全管理措施。
- (十) 本公司要求所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合個資法第 19 條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合個資法第 20 條第 1 項但書情形。
- (十一) 經清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置。但因執行職務或業務所必須或經當事

人書面同意者，不在此限。

(十二) 本公司如有委他人（或他公司）蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。

(十三) 本公司因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

四、事故之預防、通報及應變機制

(一) 預防：

- 1、本公司員工如因工作執掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。
- 2、建立資訊安全管理機制加強控管，降低個資事件發生機率。
- 3、加強員工教育宣導，並嚴加管制。

(二) 通報及應變：

- 1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向本公司個資管理人員通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。
- 2、對於個人資料遭竊取之第三人，以書面通知使其知悉及本公司已採取之處理措施及諮詢服務專線。
- 3、個人資料事故發生後以書面通報臺北市政府都市發展局。遇有達1,000筆以上之重大個人資料事故時，於發現後72小時內，以書面通報臺北市政府都市發展局，並副知內政部。
- 4、針對事故發生原因研議改進措施。

五、資料安全管理、人員管理及設備安全管理

(一) 資料安全管理

1、電腦存取個人資料之管控：

- (1) 個人資料檔案儲存在電腦硬式磁碟機上者，應在個人電腦設置識別密碼、保護程式密碼及相關安全措施。
- (2) 本公司員工如因工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。
- (3) 個人資料檔案使用完畢應即退出，不得任其停留於電腦終端機

上。

(4) 定期進行電腦系統防毒、掃毒之必要措施。

(5) 重要個人資料應另加設管控密碼，非經陳報本公司單位主管核可，並取得密碼者，不得存取。

2、紙本資料之保管：

(1) 對於各類契約書件（含個人資料表）應存放於公文櫃內並上鎖，本公司員工非經權限主管同意不得任意複製或影印。

(2) 對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

3、因本公司所使用資通訊系統蒐集、處理或利用消費者個人資料達五千筆以上，爰針對該資通訊系統，採取下列資訊安全措施，並針對本目之(5)、(6)措施定期演練及檢討改善：

(1) 使用者身分確認及保護機制。

(2) 個人資料顯示之隱碼機制。

(3) 網際網路傳輸之安全加密機制。

(4) 個人資料檔案及資料庫之存取控制與保護監控措施。

(5) 防止外部網路入侵對策。

(6) 非法或異常使用行為之監控及因應機制。

(二) 人員管理

1、本公司依業務需求，得適度設定所屬人員不同之權限，以控管其個人資料之情形。

2、本公司員工每三個月應變更識別密碼 1 次，並於變更識別密碼後始可繼續使用電腦。

3、本公司員工離職與公司終止僱傭契約時，將立即取消其使用者代碼(帳號)及識別密碼。其所持有之個人資料應辦理交接，不得在外繼續使用。

4、本公司員工應妥善保管個人資料之儲存媒介物，執行業務時依個資法規定蒐集、處理及利用個人資料。

5、本公司員工所簽訂之相關勞務契約或承攬契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。

(三)、設備安全管理

1、建置個人資料之有關電腦設備，資料保有單位應定期保養維護，

於保養維護或更新設備時，並應注意資料之備份及相關安全措施。

- 2、建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。
- 3、本公司應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經本公司單位主管同意並作成紀錄不得攜帶外出或拷貝複製。
- 4、本公司之個人資料檔案應定期下載以作為備份。
- 5、重要個人資料備份應異地存放，並應置有防火設備及保險箱等防護設備，以防止個人資料減失或遭竊取。
- 6、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物需報廢汰換或轉作其他用途時，本公司單位主管應檢視該設備所儲存之個人資料是否確實刪除。委託他人執行者，當對受託者為適當之監督並與其明確約定相關監督事項。

六、資料安全稽核機制

(一) 本公司定期(每半年至少 1 次)辦理個人資料檔案安全維護稽核，查察本公司是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

- 1、確認不符合事項之內容及發生原因。
- 2、提出改善及預防措施方案。
- 3、紀錄查察情形及結果。

(二) 前項查察情形及結果應載入稽核報告，並向本公司負責人提出稽核報告，並留存相關紀錄，其保存期限至少五年。

七、使用記錄、軌跡資料及證據保存

本公司個人資料、資訊系統與設備之軌跡資料，以及其他相關之證據資料須加以保存於適當處所。

八、認知宣導及教育訓練

(一) 對於新進人員應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

九、個人資料安全維護之整體持續改善

(一) 本公司將隨時依據本計畫執行狀況，注意相關社會輿情、技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正，並於規定期限內報請所在地直轄市、縣（市）主管機關備查。

(二) 針對個資安全稽核結果不合法令之虞者，規劃改善與預防措施。

十、業務終止後之個人資料處理方法

本公司業務終止後，所保有之個人資料不得繼續使用，應依實際情形採下列方式處理，並留存相關紀錄，其保存期限至少五年：

(一) 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

(二) 移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

(三) 其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。