

太平洋建設股份有限公司

個資保護政策運作情形

114 年度

本公司重視「客戶隱私權保護」，遵循《個人資料保護法》，訂定《個人資料檔案安全維計畫或業務終止後個人資料處理方法》，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。適用範圍涵蓋分公司、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《個人資料檔案安全維計畫或業務終止後個人資料處理方法》落實執行，致力維護客戶的資料安全及隱私權利。此外，本公司為更有效管理隱私相關風險，由資訊部負責執行與監督《個人資料檔案安全維計畫或業務終止後個人資料處理方法》的遵循情形。每年定期舉辦相關課程宣導，建立跨單位個資法遵循溝通平台，並提供個資保護工作所需的支援。本公司個人資料檔案安全維計畫或業務終止後個人資料處理方法內容請參閱附檔。

本公司為更有效管理隱私相關風險，持續不間斷取得 ISO 27001 國際資訊安全管理認證，及落實隱私與個資保護宣導等，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總完訓人數為 25 人，課程總時數達 75 小時受訓員工佔全體比例 34% 完訓後測驗及格率皆為 100% 另稽核室業依辦法執行查核程序，核核結果皆依規定辦理無差異性，因執行情形良好 114 年度本公司無個資申訴案件發生。



太平洋建設股份有限公司

個人資料檔案安全維護計畫或業務終止後個人資料處理方法

壹、組織、規模及特性

一、行業特性：

- | | |
|---|---|
| <input checked="" type="checkbox"/> 營造業 | <input type="checkbox"/> 不動產開發業 |
| <input type="checkbox"/> 建築師事務所 | <input type="checkbox"/> 公寓大廈管理維護公司 |
| <input type="checkbox"/> 都市更新業務財團法人 | <input type="checkbox"/> 其他經中央主管機關公告指定者 |

二、組織型態：股份有限公司

三、資本額：新台幣參拾捌億柒仟萬元整

四、處所地址：台北市信義區光復南路495號

五、代表人（負責人）：柳逸義

六、員工人數：70~90人

貳、個人資料檔案之安全維護管理措施(計畫內容)

一、管理人員及資源

(一) 管理人員：

1、配置人數：1人。

2、職責：負責規劃、訂定、修正與執行個人資料檔案安全維護計畫或業務終止後個人資料處理方法(以下簡稱本計畫或處理方法)等相關事項，並向負責人提出報告。

(二) 預算：每一年新台幣貳拾伍萬元整。

(三) 個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、篡改、毀損、滅失或洩漏。

(四) 本公司依部門業務將聯絡資訊分別揭示於本公司網頁，以提供當事人(或客戶)表示拒絕接受行銷、個人資料事故諮詢服務及行使個人資料保護法第三條之權利聯絡使用。

二、個人資料之範圍

(一) 特定目的：行政管理、不動產開發服務、建築管理都市更新、國民住宅事務、契約或類似契約或其他法律關係事務、信託業務、消費者、客戶管理與服務、人事管理、住宅行政。

(二) 個人資料：

1、本計畫之個人資料類型，不以消費者為限。

2、個人資料係指自然人之姓名、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。

(三) 依個資法第51條第1項規定，以下個人資料排除於本計畫之外：

- 1、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
- 2、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

三、風險評估及管理機制

(一) 風險評估：

- 1、經由本公司電腦下載或外部網路入侵而外洩。
- 2、員工及第三人故意竊取、毀損或洩漏。
- 3、設備送修、遺失或被竊。
- 4、業務終止後個人資料未銷毀。

(二) 管理機制：

- 1、定期進行網路資訊安全維護及控管。
- 2、落實教育訓練及管理稽核，並監督其業務之執行。
- 3、設備送修前或保存，應先備份或加密，避免非授權存取。
- 4、個資檔案使用期限已結束應銷毀。

四、個人資料蒐集、處理及利用之內部管理措施

(一) 告知義務：

- 1、直接向當事人(或客戶)蒐集個人資料時，應明確告知當事人(或客戶)下列事項：(1)本公司名稱。(2)蒐集目的。(3)個人資料類別。(4)個人資料利用之期間、地區、對象及方式。(5)當事人(或客戶)得查詢或請求閱覽、製給複製本、補充或更正、刪除、停止蒐集、處理或利用其個人資料之權利及申請程序。(6)當事人(或客戶)得自由選擇提供個人資料時，不提供將對其權益之影響。
- 2、所蒐集非由當事人(或客戶)提供之個人資料，應於處理或利用前，向當事人(或客戶)告知下列事項：(1)個人資料來源。(2)本公司名稱。(3)蒐集目的。(4)個人資料類別。(5)個人資料利用之期間、地區、對象及方式。(6)當事人(或客戶)得查詢或請求閱覽、製給複製本、補充或更正、刪除、停止蒐集、處理或利用其個人資料之權利及申請程序。

(二) 於告知當事人(或客戶)上述應告知事項後，並獲得其書面同意，始得進行個人資料之合法蒐集、處理及利用。

(三) 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。

(四) 本公司於首次行銷時，應提供當事人(或客戶)表示拒絕接受行銷之方式，



並支付所需費用。當事人（或客戶）表示拒絕接受行銷時，本公司應立即停止利用其個人資料行銷，並將拒絕情形通報（公司）彙整後再周知所屬各部門。

- (五) 內政部對本公司所屬行業為限制國際傳輸個人資料之命令或處分時，本公司應通知所屬人員遵循辦理。所屬人員於國際傳輸個人資料時，應檢視未受上開限制，及無個人資料保護法第21條4種例外情形，始得合法進行國際傳輸，並告知當事人（或客戶）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（或客戶）行使本法第3條所定權利之相關事項。
- (六) 當事人（或客戶）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，本公司應告知當事人（或客戶）行使上述權利之申請程序。受理申請時應確認申請人身份，申請文件有遺漏或欠缺，應通知申請人限期補正。如認有拒絕當事人（或客戶）行使上述權利之事由，應附理由通知當事人（或客戶）。當事人（或客戶）請求答覆查詢、提供閱覽個人資料或製給複製本時，如有收取必要成本費用者，應主動告知收費基準。上述申請程序，應依個資法第13條規定於處理期限內辦理完成。
- (七) 本公司於蒐集、處理或利用過程中，應維護個人資料之正確，有不正確時，應主動或依當事人（或客戶）之請求更正或補充之。
- (八) 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，除因執行職務或業務所必須或經當事人（或客戶）書面同意者外，應予刪除、停止蒐集、處理或利用該個人資料之處置，並留存記錄。
- (九) 本公司如有委託他人（或他公司）蒐集、處理或利用個人資料時，應與受託者明確約定相關監督事項，至少應包含個資法施行明細第8條第2項所規定之各款事項，並定期確認其執行狀況。

五、事故之預防、通報及應變機制

(一) 預防：

- 1、本公司員工或所屬之建築師如因其工作執掌而須輸出、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、非承辦之建築師或員工參閱契約書類時，應得公司負責人或經指定之管理人員之同意。
- 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、滅失或洩漏即向公司負責人通報，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當事人（或客戶），於事故查明後即時以書面通知使其知悉被侵害之事實、本公司已採取之處理措施及諮詢服務專線。
- 3、遇有達1,000筆以上之個人資料事故時，於發現後72小時內，以書面（格式如附件）通報公司所在地之縣市政府或財團法人主管機關。
- 4、針對事故發生原因研議改進措施，避免類似個人資料事故再次發生。
- 5、個人資料事故相關紀錄文件應妥善留存。

六、資料安全管理、資通訊系統、人員管理、環境及實體設備

（一）資料安全管理

- 1、訂定各類設備或儲存媒體之使用規範：
 - (1) 個人資料檔案儲存在個人電腦者，應設置識別密碼、保護程式密碼及相關安全措施。
 - (2) 定期進行電腦系統防毒、掃毒之必要措施。
 - (3) 對於各類委託書、契約書件（含個人資料表）應存放於公文櫃內並上鎖，員工或所屬人員非經公司負責人或營業處所主管同意不得任意複製或影印。
- 2、設備送修前應備份或加密，避免設備送修或遺失被非授權取得個人資料。
- 3、設備或紙本，於報廢、汰換或轉作其他用途時，應採取適當防範措施，避免個人資料銷毀、轉移程序不當而洩漏個人資料。

（二）人員管理

- 1、適度設定所屬人員使用個人資料之工作權限，並控管其接觸個人資料之情形，並依工作職務或人員異動調整工作權限。
- 2、各個資業務流程應指定管理人員，負責定期管理稽核各項個人資料檔案之安全管理措施。
- 3、本公司員工及所屬人員應妥善保管儲存個人資料之媒介物，並要求遵守個人資料內容之保密義務（含契約終止後）。（註：媒介物指存有個人資料之紙本、磁碟、光碟片等物品。）
- 4、職務異動或所屬人員與公司終止僱傭或委任契約時，其所持有之個人資料應辦理交接，並簽訂保密切結書。

（三）環境及實體設備安全

- 1、個人資料之資訊設備或紙本應置放於安全區域（如：門禁控制區域、機房、檔案室），並設有監控設備（如：監視器、防盜系統）。相關進出管制簽名記錄、門禁記錄、影像攝影等記錄應妥善保管並嚴禁修改。
對於各類委託書、契約書件（含個人資料表）應存放於公文櫃內並上鎖，未經申請程序不得任意複製或影印。
- 2、資訊設備之攜入（例如新購硬碟）、攜出（例如送修、報廢），應透過申請程序經單位主管同意，並作成紀錄。
- 3、保存個人資料有安全之環境控管（溫、濕度管制、遠離火源、不斷電系統）。



七、資料安全稽核機制

(一)本公司定期(每半年至少一次)辦理個人資料檔案安全維護稽核，查察是否落實本計畫或處理方法各事項，針對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中，由公司負責人簽名確認。

八、使用記錄、軌跡資料及證據保存

所有個人資料之使用紀錄、軌跡資料及證據，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。

本公司就書面文件依相關法令規定依序保存，置放檔案室專人管理，電腦檔內資料則有密碼管控，非經辦人無法接觸，若有需要時得由主管核准方可取得。資料至少保存五年以上，依相關法令規定屆期時專人銷毀。

九、認知宣導及教育訓練

- (一)本公司每年進行個人資料保護法基礎教育宣導及教育訓練至少1次，使員工或所屬人員知悉應遵守之規定。前述教育宣導及訓練應留存紀錄。
- (二)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。

十、個人資料安全維護之整體持續改善

本公司隨時依據業務與本計畫及處理方法之執行狀況，注意相關社會輿情、技術發展及相關法規訂修等事項，檢討所定本計畫及處理方法是否合宜，必要時予以修正；如修正，應於15日內將修正後之本計畫及處理方法報請公司所在地之縣市政府或財團法人主管機關備查。

十一、業務終止後之個人資料處理方法

針對個人資料之銷毀、移轉或刪除、停止處理或利用等作業，應規範其處理方式及應記載事項，並留存相關紀錄；委託他人執行者，亦應遵守本項規定辦理。

- (一)進行個人資料銷毀時，應記錄其銷毀個人資料之方法、時間、地點及證明銷毀之方式等欄位。
- (二)進行個人資料移轉時，應記錄其移轉個人資料之原因、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等欄位。
- (三)進行個人資料刪除停止時，應記錄其刪除、停止處理或利用之方法、時間或地點等欄位。

十二、附則

未盡事項另以公告補充之，本方法由總經理奉核公布後實施，修訂時亦同。



附件 個人資料事故通報及紀錄表

非公務機關名稱 <hr/>	通報時間： 年 月 日 時 分 通報人： 職稱： 電話： Email： 地址：	
通報機關 <hr/>		
發生時間		
發生種類	<input type="checkbox"/> 竊取 <input type="checkbox"/> 竄改 <input type="checkbox"/> 毀損 <input type="checkbox"/> 滅失 <input type="checkbox"/> 洩漏 <input type="checkbox"/> 其他侵害情形	個人資料侵害之總筆數(大約)： <input type="checkbox"/> 一般個人資料: _____ 筆 <input type="checkbox"/> 特種個人資料: _____ 筆
發生原因及摘要		
損害狀況		
個人資料侵害可能結果		
擬採取之因應措施		
擬通知當事人之時間及方式		
是否於發現個人資料外洩後七十二小時內通報	<input type="checkbox"/> 是 <input type="checkbox"/> 否，理由 :	

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。

說明：配合內政部指定營建類非公務機關個人資料檔案安全維護管理辦法第九條規定非公務機關發生重大個人資料事故之情事者，應於七十二小時內將相關事項以書面通報各該主管機關，爰擬定「個人資料外洩通報表」之統一格式俾利非公務機關填報。