

凱撒衛浴股份有限公司 個人資料管理辦法

一、目的

因應個人資料保護法的施行，為遵守個人資料之蒐集、處理及利用之生命週期規範，以避免人格權受侵害，促進個人資料之合理使用。

規範所有人員應遵循的個人資料保護目標，保障客戶個資及員工個資使用，降低本公司與員工可能的法律風險，保障客戶權益及維護本公司信譽。

二、適用對象與範圍

本公司所有人員、與本公司有業務往來之廠商或顧問（包含其員工或臨時雇員），均屬本政策涵蓋之對象。

三、名詞定義

（一）個人資料管理體系

以營運風險導向為基礎，用以建立、實作、運作、監視、審查、維持及改進個人資料管理。

（二）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。

（三）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。特種個人資料(以下簡稱「特種個資」)之定義及範圍如日後因應主管機關或法規變動配合修訂時，以修訂後的定義及範圍為準。

（四）個資管理負責人

指負責個人資料保護管理之各單位執行人員，並負責落實管理程序。

（五）個人資料保護管理執行組織

由個資管理負責人組成，並由授權主管督導執行本公司個資法相關遵循事務。

四、管理範圍

由管理階層指派授權主管負責本政策之擬訂及推展，並建立個資管理組織。進行個人資料管理體系之規劃、實施、運作、監督、查核、維護與改善作

業。並定期或在重大變化時執行管理審查個人資料管理體系，確保運作之有效性。管理範疇包含以下項目：

(一) 建立個人資料保護管理程序

公司應透過作業流程識別、個人資料盤點、風險評鑑及風險處理等程序，改善個人資料之風險管理與保護管理措施。

(二) 規範個人資料蒐集、處理及利用原則，基於合法之特定目的在確實必要的範圍內處理個人資料。

1. 向當事人蒐集個人資料時，除法律明文規定外，需經當事人同意並明確告知蒐集目的、個人資料之類別、利用期間、地區、對象及方式。
2. 蒐集個人應符合特定之目的，並確保資料之正確性、完整性和時效性。
3. 蒐集個人資料時，需經適當之授權與監督並僅就所需之必要欄位進行收集。經授權同意交換個人資料時，電子類文件需對資料檔案加密或透過加密通道傳送、紙本類文件以彌封或其他安全方式進行傳遞交換工作。
4. 當個人資料蒐集範圍逾法律、法規命令，應依個資法規定取得當事人之書面同意。
5. 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。
6. 非由當事人提供之個人資料，應於處理或利用前向當事人補行告知義務，告知方式得以書面、電話、傳真、電子文件或其他適當方式為之。
7. 個人資料之處理行為需經單位主管核准，宜釐定使用範圍及調閱或存取權限。個資存取時應視需要考量採取權限區隔、資料加密機制，或相關核准程序加以控管，並留存可識別之發送紀錄需及個資使用者身分以供事後稽查。
8. 使用者經正式授權存取個人資料檔案時，其帳號必須為唯一，避免共用帳號。
9. 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義，應調閱原始檔案查核。
10. 禁止使用即時通訊軟體、外部信箱（如 Gmail、Hotmail…等）傳輸及存取個人資料檔案，利用公司內部信箱（webmail）傳輸個人資

料時請加密保護與留存追查紀錄。

(三)貫徹個人資料檔案安全維護措施

以適當之技術保護個人資料，提供個人資料檔案適當之安全管理措施，保護其所蒐集、處理或利用之個人資料。

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）私自儲存本公司所保有個人資料檔案。
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。
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。
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。
5. 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。
6. 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。
7. 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。
8. 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。
9. 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。
10. 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。
11. 業務終止後個人資料處理方法：本公司因交易完成、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，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。

(四)落實個人資料管理事件事故之預防、鑑識、通報及應變管理

1. 建立個人資料保護之可接受的風險程度與因應措施，當個資事件發生導致利害關係人權益受損時，進行適當地回應與處理。
2. 設置處理申訴及諮詢的管道，供當事人行使關於個人資料的相關權

利。

(五)持續維運個人資料保護管理的相關程序

1. 進行相關個人資料管理程序、個人資料管理體系及個人資料管理指標的評估及查核作業，以確保本辦法及相關程序之有效性，並檢查落實執行。
2. 如有未落實執行或規範變更時，協助改善相關的程序及管理措施，以持續增進個人資料管理系統的有效性。

(六)個資處理人員管理規範

1. 處理接觸機密資料人員，應簽署「保密切結書」，克盡保密之責，並確認於離職時或合約終止時取消或停用其使用者識別帳號。
2. 禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。
3. 以電腦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列冊移交，接辦人員應另行設定密碼，以利管理。

(七)個人資料外洩(竊取、洩露、竄改或其他侵害事件)處理流程：

1. 追查外洩發生主要管道與原因。立即回報公司內部權責單位主管個資外洩單位以最快方式通知相關部門辦理。
2. 發生個資外洩事件，即時以書面、電話、電子文件或其他足以使當事人知悉或可得知悉的方式，通知個人資料受侵害項目、產生之影響及已採取之因應措施。

五、權責單位：

(一)本公司所有會接觸與使用個資人員，皆應瞭解並確實遵守本辦法。

(二)個資管理負責人之直屬主管，應就本公司個人資料管理制度之運作，負監督管理權限之責，並管理、指揮該部門之個資運作與稽查，執行落實遵循個資法。

(三)主要個資管理單位：

1. 管理部：處理公司同仁人事資料檔案管理與維護控管
2. 客戶服務部：處理公司維修客戶服務之個資料檔案管理與維護控管
3. 營業管理處：處理公司客戶等個資料檔案管理與維護控管

六、違反責任及罰則：

(一)本公司同仁均應遵循本辦法，違反者須依本公司相關規定予以處分。

- (二)如涉有相關民事賠償、刑事責任、行政裁罰者，本公司得終止其僱用關係並衡酌情節追訴其法律責任。
- (三)員工對於公司之個人資料保護義務於雙方終止僱用關係後仍繼續有效。

七、其他管理要點：

- (一)本公司各單位的個資管理人員應接受公司統一之個資法與個資管控基本認知訓練。有利全體個資管理人員落實法規與公司管理要求，嚴防個資外洩事件。
- (二)公司行政管理單位每年針對法規更新重點或當年度重大個資事件進行內部宣導或訓練，以利確保公司經手個資的相關單位維持個資管控管理品質。防範發生任何個資外洩風險。
- (三)公司權責單位應定期進行個人資料安全管理之稽核作業。
- (四)公司行政管理單位持續維護及改善已建置之個人資料保護管理制度。

八、本辦法經由董事會核准後公告實施;修改、廢止時亦同。

九、本辦法訂定於中華民國一〇二年七月三十日

本辦法第一次修訂於中華民國一一三年二月二十六日