



康和綜合證券股份有限公司

個人資料管理目標與政策

文件編號:PIMS-L1-001

管轄單位：法令遵循部

核定層級：董事會

制定 修正 廢止 施行日期：113年01月30日

版次：第4版



# 康和綜合證券股份有限公司

## 個人資料管理目標與政策

### 一、目的

康和綜合證券股份有限公司(以下簡稱本公司)為落實個人資料保護、管理及遵循《個人資料保護法》所述之相關要求及保障個人資料當事人之權利，降低任何個人資料受侵害之事件所可能帶來的衝擊，並依據「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」，特訂定本個人資料管理目標與政策(以下簡稱本政策)。

### 二、範圍

- (一) 本政策描述本公司之個人資料管理體系之架構與建置方法，闡明本公司同仁應遵循的個人資料保護目標與政策，以及在個人資料管理的工作規劃、實踐與持續改進過程中所應扮演的角色與權責。
- (二) 本公司所有人員均適用本政策。
- (三) 個人資料管理體系之驗證範圍為：本公司個人資料管理相關之活動。

### 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) 所有人員  
涵蓋本公司所有員工(包含但不限於委任或僱傭關係)、臨時雇員、承包商(委外廠商)及顧問。
- (三) 個人資料侵害事件  
未經個人資料當事人授權使用或不當蒐集、存取及揭露個人資料而超乎預期使用狀況皆屬之。
- (四) 管理階層  
本公司個人資料管理之管理階層，包含董事長、總經理及各部室主管等。

#### 四、相關文件

無。

#### 五、權責

本公司所有人員，皆應瞭解並確實遵守本政策。

#### 六、內容

##### (一) 個人資料管理目標

本公司個人資料管理目標如下：

1. 符合我國個人資料保護之法令法規、主管機關命令以及客戶契約或專業職責等要求；
2. 維護個人資料當事人之人格權，提供其個人資料的完全自主權；
3. 對個人資料之蒐集、處理及利用過程，於特定目的範圍內以誠實信用方法為之，並應與蒐集之目的具有正當合理之關聯；
4. 提供個人資料檔案適當之安全措施，以確保本公司得以盡良善管理之注意義務；
5. 訂定個人資料保護之可接受的風險程度與因應措施；
6. 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。

##### (二) 個人資料管理政策

1. 本公司個人資料管理政策如下：

- (1) 遵守我國個人資料保護相關之法令規定。
- (2) 本公司只會基於合法、正當合理的特定目的，在確實必要的範圍內蒐集個人資料；
- (3) 基於合法、正當合理的特定目的蒐集最少的必要個人資料，且不會處理多餘的個人資料；
- (4) 本公司會清楚告知當事人，其個人資料將如何被使用及被誰使用；
- (5) 已蒐集的客戶資料只會作適當且相關的處理；
- (6) 公平合法地處理個人資料；
- (7) 維持一份本公司處理的個人資料類別清單；
- (8) 確保個人資料的正確性，並於必要時進行更新；
- (9) 已蒐集的個人資料將會依法或在合法的特定目的下保存；
- (10) 尊重當事人對其個人資料所能行使之權利，包含查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、

處理或利用及請求刪除等；

- (11) 以適當安全之水準技術保護其所蒐集、處理、利用之個人資料，確保所有個人資料的安全；
- (12) 只有在確實並受適當充分保護的狀況下，本公司才會將個人資料進行國際傳輸；
- (13) 當個人資料應用於《個人資料保護法》所允許之例外情形時，應確保其適當性與合法性；
- (14) 建立與實施個人資料管理制度並持續維運，讓個人資料保護政策落實，以確保個人資料檔案之安全；
- (15) 鑑別內外部利害關係者及其參與個人資料管理制度治理與運作的程度；
- (16) 於個人資料管理制度運行中，明確界定員工之責任與義務。
- (17) 規劃緊急應變程序以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。
- (18) 如有委託蒐集、處理及利用個人資料時，妥善監督受託機關。
- (19) 設置聯絡窗口，供當事人行使關於個人資料之權利或提出相關之申訴與諮詢。

2. 為宣達本公司個人資料管理政策，亦以「個人資料管理政策聲明」(PIMS-L1-001-01) 進行公告。

### (三) 個人資料管理組織

本公司為落實個人資料之保護及管理，將明定個人資料管理體系內相關人員之權限及責任，以確實推行及監督個人資料保護機制。

### (四) 個人資料管理體系

本公司個人資料管理體系採用「Plan-Do-Check-Act (PDCA)」之循環運作模式，說明如下：

#### 1. 規劃與建立(Plan)

依據本公司整體策略與目標，藉由成立個人資料管理組織，控制潛在之威脅及漏洞，規劃風險評估與安全控管機制，以建立個人資料管理體系。

#### 2. 實施與運作(Do)

依據評估規劃之結果，建立或修正應有之個人資料管控機制。

#### 3. 監督與查核(Check)

監督個人資料管理體系各項作業之落實執行，並查核其有效性。本政策係與本公司現行稽核制度併行，定期實施個人資料保護內部稽核作業，以確保個人資料管理之落實。

#### 4. 維護與改進(Act)

根據監督查核之結果與建議，執行矯正與預防措施，改善並執行應有之控管機制，以持續維護個人資料管理體系之運作。

#### (五) 管理階層責任

對於本公司個人資料管理體系之規劃、建立、實施、運作、監督、查核、維護與改進各項作業，管理階層應訂定並遵循下列事項：

##### 1. 管理階層承諾

管理階層應確保完成下列工作，表示對個人資料管理發展及增進的充分支持：

- (1) 訂定個人資料管理之角色與職責；
- (2) 提供個人資料管理體系各項作業所需之資源；
- (3) 決定風險可接受水準；
- (4) 執行個人資料管理體系之管理審查作業；
- (5) 依本政策要求督導建立和實行個人資料管理體系。

##### 2. 組織文化的深植

- (1) 確認所有人員均具備工作所需相關職能；
- (2) 評估職能訓練與相關措施之有效性；
- (3) 建立並維護教育訓練、技能、經驗與資格之相關紀錄；
- (4) 宣導遵守本政策與法令規章。

#### (六) 個人資料管理體系自行評估與查核

管理階層應確保定期或不定期進行個人資料管理體系的自行評估或查核作業，以檢討管制目標、管控措施與程序是否合乎相關標準、法令規章或個人資料管理需求，並依預期規劃有效執行與維持，以持續增進個人資料管理體系的有效性。

#### (七) 個人資料管理體系管理階層審查

管理階層應定期或在發生重大變化時執行管理審查，以確保個人資料管理體系運作之適切性、充足性及有效性。

#### (八) 個人資料管理體系之持續改進

本公司可藉由稽核查核結果、矯正及預防措施及管理階層審查，以持續改進個人資料管理體系之有效性。

#### (九) 政策指導與覆核

本政策應每年至少評估一次，以反映政府法令、資訊技術及公司業務等最新發展狀況，確保個人資料管理實務作業之有效性。

#### (十) 政策與法令之遵循

所有人員均應遵循本政策，違反者須依本公司相關規定予以處分。如涉有相關民事賠償、刑事責任、行政裁罰者，本公司得終止其委任或僱傭關係並衡酌情節追訴其法律責任。員工對於本公司之個人資料保護義務於雙方終止委任或僱傭關係後仍繼續有效。

(十一) 個人資料檔案安全維護計畫及業務終止後個人資料處理方法相關規範之規劃、訂定、修正與執行

(十二) 本公司應衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行個人資料檔案安全維護計畫及業務終止後個人資料處理方法相關規範，其訂定、修正與自我評估報告授權由董事長核定。

#### 七、表單／附件

個人資料管理政策聲明(PIMS-L1-001-01)。

#### 八、核准權限

本政策經董事會通過後實施，修訂時亦同。