軒郁國際集團

個人資料檔案風險評鑑與管理程序

制訂單位	個資管理委員會
文件編號	01Q-3H07
版次編號	V0
生效日期	2023.06.30
文件類別	內部使用

文件制/修訂紀錄

項次	版次	頁數	制/修訂說明	生效日期
1	V 0	9	首次發行。	2023.06.30

第一條、目的

為建立本公司個人資料檔案風險評鑑與管理規範，提供共同遵行之風險評鑑標準，採取適當之對策或控制措施，以有效降低個人資料檔案遭受損害的風險，特訂定本程序。

第二條、參考依據

一、 個人資料保護法。

二、 BS10012 個人資訊管理標準。

第三條、適用範圍

一、 本程序適用範圍為本公司業務相關作業流程產生之個人資料檔案風險評鑑事宜。

二、 以個人資料檔案為風險評鑑標的。

三、 個人資料管理制度控制措施有效性量測。

第四條、權責

一、 個人資料保護管理委員會(以下簡稱個資管理委員會)-主管

（一） 視實際狀況決定個人資料檔案風險評鑑之時機與範圍。

（二） 監督個人資料檔案風險評鑑之執行。

（三） 個人資料檔案風險評鑑結果之審查及確認。

（四） 覆核個人資料檔案風險評鑑報告。

（五） 個人資料檔案風險處理計畫之審查。

（六） 有效性量測之審查及確認。

二、 各權責單位主管

負責所屬單位業務範圍之風險評鑑結果核准與確認作業。

三、 個資管理委員會-執行組

（一） 依據本程序書執行權責單位個人資料檔案之風險評鑑與處理。

（二） 指派專人彙總權責單位執行風險評鑑彙整表並記錄於「個人資料盤點清單暨風險評鑑彙總」。

（三） 指派專人彙總權責單位「個人資料檔案風險處理計畫」並提報審核。

（四） 權責單位個人資料檔案清冊之管理與維護。

（五） 擬定、執行權責單位個人資料檔案風險處理計畫，並評估風險處理計畫執行成效。

（六） 擬定、執行權責單位有效性量測作業。

（七） 依據個人資料風險評鑑結果建議可接受風險值。

（八） 統籌彙整本公司各單位個資流程鑑別、個資清查、風險評估與風險管理等資料，並撰擬風險評估報告。

（九） 分案及管制相關權責單位執行風險處理計畫。

第五條、定義

一、 可接受風險值：個資資產之最低風險容忍度。

二、 殘餘風險(RESIDUAL RISK)：在採用相關控制措施之後剩餘的風險。

三、 隱私衝擊分析(PRIVACY IMPACT ASSESSMENT，PIA)：用以識別各個人資料檔案其隱私或個人資料於收集、使用和揭露過程中可能產生之衝擊程度。

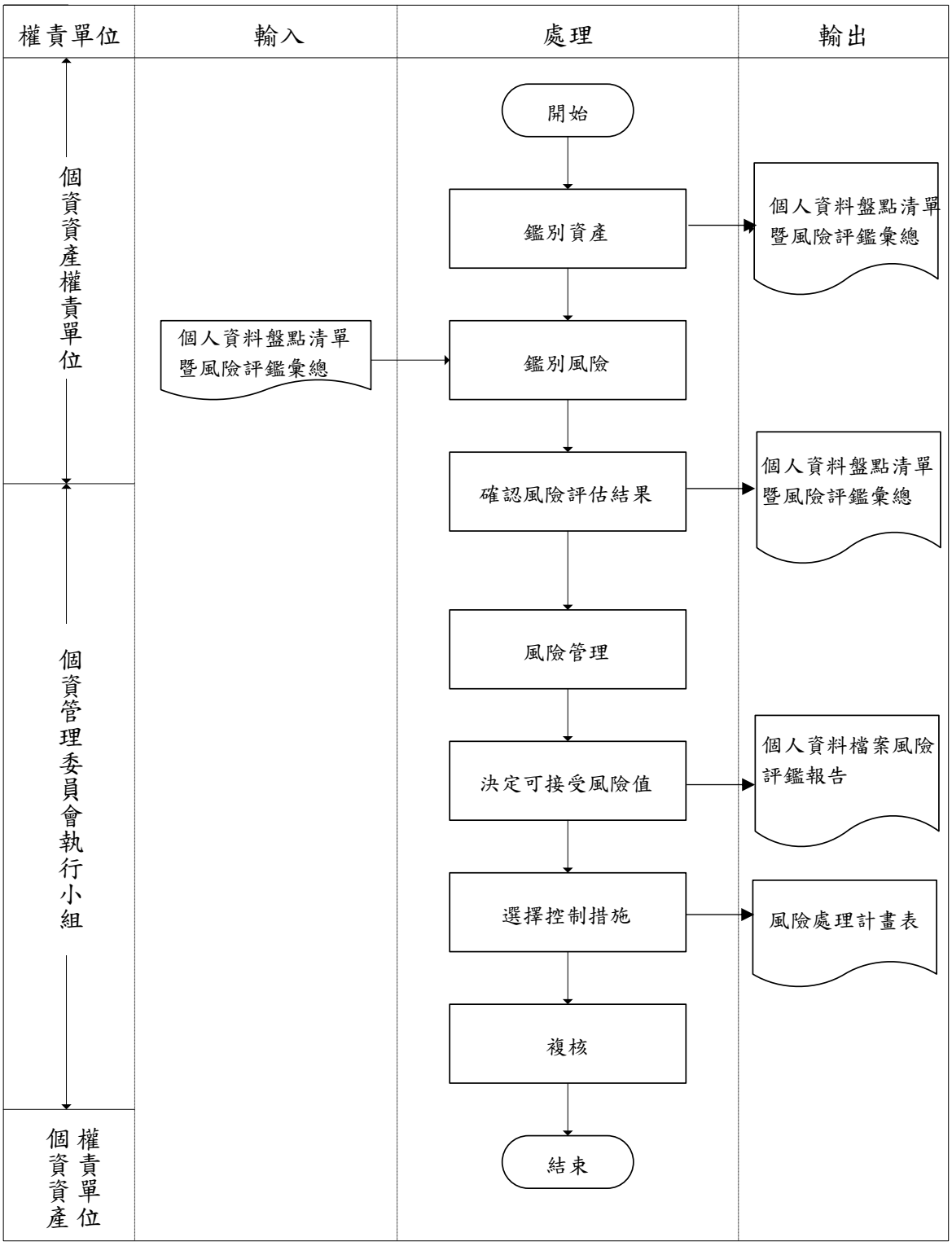
四、 風險(RISK)：可能對團體或組織的個資資產發生損失或傷害的潛在威脅，通常用產生之影響來衡量。

五、 風險擁有者(Risk Owner)：權責單位內針對各項個資資產流程風險管理具備核准與確認者，由各權責單位主管擔任。

六、 個人資料：泛指自然人之姓名、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資料。

第六條、作業說明

一、 個人資料風險管理作業流程圖



二、 個人資料資產分類

本公司個人資料資產分為電子與紙本兩類別，其分類說明如下：

（一） 電子資料：係指儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔案。

（二） 紙本資料：係指以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫、文件等紙本資料。

三、 個人資料檔案鑑別

（一） 各單位個人資料保護專責人員(聯絡窗口)應進行組織業務個資盤點作業，並視實際狀況進行內容調整。

（二） 依據作業流程分析結果，執行個人資料檔案鑑別作業，並建立「個人資料檔案清冊」。

（三） 本公司除每年執行一次個人資料檔案鑑別作業外，亦應於下列情形發生時，針對變動範圍內的作業程序與個人資料檔案進行個人資料檔案鑑別作業：

1、營運組織變更。 2、作業流程改變。

四、 評估項目

個人資料檔案風險評估下列幾個項目：

（一） 資產價值：個人資料檔案所含之個人資料範圍程度。

（二） 衝擊構面：為當個人資料檔案發生外洩等事故時，可能對各方面所產生的衝擊影響。

（三） 可能性構面：為該個人資料檔案發生外洩等事故的可能性高低。

五、 評估說明：

（一） 資產價值構面

個人資料檔案的資產價值，依據「個人資料盤點清單暨風險評鑑彙總」的結果填入，每個檔案所含資產價值的等級分別給予：低(1)、中(2)、高(3)與極高(4)，四個等級評估。

資產價值	個人資料範圍
低(1)	不含自然人之姓名及國民身分證統一編號（或護照號碼）。
中(2)	1.含自然人之姓名或國民身分證統一編號（或護照號碼），但不包含特種資料。 2.含自然人之姓名及員工編號（或學號），但不含特種個人資料。
高(3)	1.含自然人之姓名及國民身分證統一編號（或護照號碼），但不含特種個人資料。 2.含自然人之姓名或國民身分證統一編號（或護照號碼）及財務情況（如：薪資、局帳號），但不含特種個人資料。
極高(4)	自然人之姓名或國民身分證統一編號（或護照號碼）及特種個人資料。

（二）衝擊構面

為當個人資料檔案被竊取、竄改、毀損、滅失或洩漏等事故發生時，可能對各方面所產生的衝擊影響，包含「對當事人損害程度」、「對公司財務影響程度」

等 2 個構面，依其可能的衝擊嚴重程度，給予低(1)、中(2)、高(3)與極高(4)等四個等級評估，取最高值。

項目／評估值	對當事人損害程度	消費者以外之個資 對公司財務影響程度	消費者個資 對公司財務影響程度
低(1)	個人資料檔案機敏等級低，資料外洩對不致影響個人權益或僅導致個人權益輕微受損。(如：資產價值「1」者)	個人資料檔案 10 筆以下，若發生損害賠償對公司財務影響範圍較小。	當月會員資料或訂單數量 10%以下，或可能賠償金占公司資產總額 5%以下。
中(2)	資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益部份受損。(如：含身分證號、財務資訊，資產價值「2」者)	個人資料檔案 10 筆 (含)以上 50 筆以下，若發生損害賠償對公司財務影響範圍較小。	當月會員資料或訂單數量 10%(含)~20%以下，或可能賠償金占公司資產總額 5%(含)~15%以下。
高(3)	資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益嚴重受損。(如：含身分證號、財務資訊，資產價值「3」)	個人資料檔案 50 筆(含)以上 100 筆以下，若發生損害賠償對財務影響範圍較大。	當月會員資料或訂單數量 20%(含)~40%以下，或可能賠償金占公司資產總額 15%(含)~20%以下。
極高(4)	資料外洩將造成個人身心受到危害、社會地位受到損害、或衍生財物損失，當事人個人權益非常嚴重受損。(如：含特種個資、特種身分、輔導紀錄等，資產價值「4」以上者)	所含個人資料檔案 100 筆(含)以上，若發生損害賠償對財務影響範圍非常大。	當月會員資料或訂單數量 40%(含)以上，或可能賠償金占公司資產總額 20%(含)以上。

（三）可能性構面

項目／評估值	教育訓練	內部監督稽核	個資安全通報紀錄	保管人數及保管處
低(1)	業務相關人員近一年接受 3 小時以上個資教育訓練課程。	單位已建立內部稽核或監督管理機制，單位於每年執行稽核，並確實執行持續改善。	近三年內未發生過個資安全通報紀錄。	檔案存放在少於三人(含)可獲取的地方
中(2)	業務相關人員近一年接受 3 小時以內個資教育訓練課程。	單位有建立內部稽核或監督管理機制，但單位並未每年執行稽核或監督管理機制。	近三年內曾發生個資安全二次以內（含二次）通報紀錄。	檔案存放在公司內部人員三人以上可獲取的地方。

高(3)	業務相關人員近一年未接受個資相關教育訓練。	單位未建立內部稽核或監督管理機制。	近三年內曾發生個資安全三次以上（含三次）通報紀錄。	資料存放在公司內部人員可獲取的地方。

為當個人資料檔案被竊取、竄改、毀損、滅失或洩漏等事故發生時的可能性高低，包含「教育訓練」、「內部監督稽核」、「個資安全通報紀錄」等 3 個構面，依其可能性高低，給予低(1)、中(2)、高(3)等三個等級評估，取最高值。

六、 個人資料檔案風險評鑑

（一） 完成「個人資料盤點清單暨風險評鑑彙總」資產價值評估後，接續對於所表列之清單進行風險評鑑作業。

（二） 鑑別個人資料檔案資產價值。

（三） 個人資料檔案風險評鑑作業應於每年內部稽核活動前執行，個資管理委員會執行組可視實際狀況，決定執行之時機與範圍。除每年執行一次外，亦應於下列情形發生時，針對變動範圍內的作業程序與個人資料檔案進行風險評鑑：

1、營運組織變更。 2、作業流程改變。

3、新增或變更個人資料檔案。 4、發生重大個資外洩事件。

（四） 風險評鑑因子：個人資料檔案風險評鑑，分別針對個資遭受竊取、竄改、毀損、滅失或洩漏等風險，藉由資產價值、衝擊構面與可能性構面等三個因素，來決定個人資料檔案的風險值。

（五） 個人資料檔案風險值計算

1、 依據資產價值、衝擊構面與可能性構面進行評估，以進行風險值計算。

2、 資產價值＝依所獲得之極高、高、中與低之評估值，轉換成對應分數 4、3、2 與 1 分。

3、 衝擊構面＝MAX (衝擊構面 1，衝擊構面 2)。

4、 可能性構面＝MAX (可能性構面 1，可能性構面 2，可能性構面 3)。

5、 風險值＝資產價值 * 衝擊程度 * 可能性

6、 計算範例：

資產價值	價值等級
評定	高(3)

衝擊構面	衝擊構面一： 對當事人損害程度	衝擊構面二： 對公司財務影響程度
評定	中(2)	低(1)

可能性構面	構面一： 教育訓練	構面二： 內部監督稽核	構面三： 個資安全通報紀錄
評定	低(1)	中(2)	低(1)

資產價值＝3

衝擊構面＝Max（2,1）＝2

可能性構面＝Max（1,2,1）＝2

風險值＝3 * 2 * 2＝12

（六）風險評鑑報告產出

1、 上述評估資料之風險值，由各單位個人資料保護專責人員彙整後記錄於「個人資料盤點清單暨風險評鑑彙總」，呈核個資管理委員會召集人。

2、 個資管理委員會執行組依據個人資料風險評鑑結果撰寫「個人資料檔案風險評鑑報告」，並建議可接受風險值，交由個資管理委員會討論決議。

七、 個人資料檔案風險管理

（一） 決定可接受風險值

1、 本公司個人資料檔案風險評鑑之可接受風險值，需經「個資管理委員會」開會決議，並記載於會議紀錄中。

2、 除決定可接受風險值外，亦可訂定風險處理之補償條件，篩選出可接受風險值以下，但仍須進行風險處理之個人資料檔案項目。

3、 「個資管理委員會」每年召開會議檢討可接受風險值。可接受風險值得考量本公司作業環境及安全控管現況，作適當調整。

（二） 個人資料檔案風險處理計畫作業

1、 依個人資料檔案風險評鑑結果及可接受風險值之決議，由各風險項目負責人針對需降低風險值之個人資料檔案擬訂「個人資料檔案風險處理計畫」，以期將風險降至可接受程度。

2、 個人資料檔案風險處理計畫之風險處理措施，應根據「第二條、參考依據」對各項個人資料保護之安全要求目標，擬訂適當之處理措施及相關執行資源之資訊。

3、 個人資料檔案風險處理計畫應經由風險擁有者核准後，提報「個資管理委員會」審查後執行，並列入追蹤管理。

4、 風險處理計畫之風險處理措施及說明、改善活動與其所需資源、預訂完成日期等規劃項目應記錄於「個人資料檔案風險處理計畫」之「風險處理進度」欄，並於預訂完成日期結束後，提報「個資管理委員會」審查。

5、 個人資料檔案風險處理計畫若為長期之專案計畫，則應於執行前進行風險評估，確認其預期效益可達到風險處理之目標，並於專案各階段驗收後，提報「個資管理委員會」討論執行之成效與進度。

（三） 風險處理計畫執行成效暨殘餘風險處理

1、 風險處理計畫於預訂完成日期結束後，須由個資管理委員會執行組(各單位聯絡窗口)執行風險再評鑑，以確認風險處理計畫執行達到風險減緩預期效益，並經由風險擁有者核准後，提報個資管理委員會。

2、 實施控制的風險，若處理結果已降至可接受風險值以下，應於個資管理委員會會議中提出討論，決定是否列入下次風險評鑑審查事項。

3、 若處理後之風險值無法降至可接受風險值以下，應於管理審查會議中提出討論，決定是否接受此風險或增加其他控制。

八、 個人資料檔案風險管理評估審查

（一） 監控控制措施的實施應視需要建立相對應之有效性量測，以反映出控制措施實施狀況及成效，以利管理階層及相關人員定期或不定期審視審

（二） 持續改善為維持本風險評鑑方法之有效性，「個資管理委員會」應：

1、 每年檢討可接受風險值與「個人資料盤點清單暨風險評鑑彙總」中風險評鑑彙總之衝擊構面與可能性構面項目。

2、 將發生個資事故或遭遇個資訴訟判決相關資訊，納入「個人資料盤點清單暨風險評鑑彙總」之衝擊構面與可能性構面，進行評估項目之檢討。

九、 風險評鑑頻率

（一） 每年應至少執行 1 次風險評鑑。

（二） 當管理階層指示、作業環境、作業流程變更或系統重大異動後一個月內，應執行風險評鑑。

第七條、相關表單

一、 01Q-3H07-T01 個人資料盤點清單暨風險評鑑彙總。

二、 01Q-3H07-T02 個人資料檔案風險評鑑報告。

三、 01Q-3H07-T03 個人資料檔案風險處理計畫。