一、目的：

為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本管理作業。

二、風險：

未遵循相關個人資料保護之法令規定，致公司遭受巨額罰則及刑責。

三、作業程序：

（一）用詞定義：

1. 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。
2. 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料集合。
3. 蒐集：指以任何方式取得個人資料。
4. 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
5. 利用：指將蒐集之個人資料為處理以外之使用。
6. 國際傳輸：指將個人資料作跨國（境）之處理或利用。

(二)設置個人資料保護執行小組：

個資小組由最高管理階層指派管理代表、管理小組、內評小組。

1. 個資小組任務：

(1)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等相關事項。

(2)訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

(3)定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員責任範圍及個人資料保護事項之方法或管理措施。

2. 個資小組會議視業務推動之需要，不定期召開，由管理代表主持。
3. 執行小組設置聯絡窗口，辦理下列事項：

(1)採取適當之應變措施，以控制事故對當事人之損害，並通報有關單位。

(2)查明事故之狀況並以適當方式通知當事人。

(3)研議預防機制，避免類似事故再次發生。

(三)個人資料之蒐集、處理及利用

1. 各單位應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。
2. 各單位對於個人資料之蒐集、處理或利用，應確實依本法第五條規定為之。遇有疑義者，應提請個資小組研議。
3. 依個資法第六條第一項但書規定蒐集、處理或利用有關醫療、基因、性生活、

健康檢查及犯罪前科之個人資料，應報請個資小組同意後為之。

4. 各單位蒐集當事人個人資料時，應明確告知當事人下列事項。
   （1）機關或單位名稱。
   （2）蒐集之目的。
   （3）個人資料之類別。
   （4）個人資料利用之期間、地區、對象及方式。
   （5）當事人依個資法第三條規定得行使之權利及方式。
   （6）當事人得自由選擇提供個人資料時，不提供對其權益之影響。
5. 各單位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上款所列事項。
6. 各單位依個資法第十九條第五款及第二十條但書第六款規定經當事人書面同意者，應取得當事人同意書。
7. 各單位依個資法第十九條或第二十條規定對個人資料之蒐集、處理、利用時，應詳為審核並簽奉核定後為之。
8. 本公司保有之個人資料有誤或缺漏時，應由資料蒐集單位簽奉核定後，移由資料保有單位更正或補充之，並留存相關紀錄。
9. 本公司保有之個人資料正確性有爭議者，應由資料蒐集單位簽奉核定後，移由資料保有單位停止處理或利用該個人資料。個人資料已停止處理或利用者，資料保有單位應確實記錄。
10. 本公司保有個人資料蒐集之特定目的消失或期限屆滿時，應由資料蒐集單位簽奉核定後，移由資料保有單位刪除並停止處理或利用。個人資料已刪除、停止處理或利用者，資料保有單位應確實記錄。
11. 各單位依本法第十一條第四項規定應主動或依當事人之請求刪除、停止蒐集、處理或利用個人資料者，應簽奉核定後移由資料保有單位為之。個人資料已刪除、停止蒐集、處理或利用者，資料保有單位應確實記錄。
12. 各單位遇有個資法第十二條所定個人資料被竊取、洩漏、竄改或其他侵害情事者，須依通報程序進行通報，經查明後，應由資料外洩單位依本公司相關訊息發布程序進行訊息之發布並以適當方式儘速通知當事人。

(四)當事人行使權利之處理：

1. 當事人依本法第十條或第十一條第一項至第四項規定向本公司為請求時，應填具個人資料申請單，並檢附相關證明文件。
2. 當事人依個資法第十條及第十一條規定提出之請求之准駁、延長，應依個資法第十三條規定期間內辦理，並應將其原因以書面通知請求人。
3. 當事人閱覽其個人資料，應由各單位個人資料保護業務窗口陪同為之，並依本公司相關檔案文件調閱程序辦理。
4. 個人資料檔案，其性質特殊或法律另有規定不應公開其檔案名稱者，得依政府資訊公開法或其他法律規定，限制公開或不予提供。

(五)個人資料檔案安全維護

1. 確保系統安全

   存取個資系統的人員，應具備唯一的識別碼(ID)，針對不同的職務角色，應完成權限控管；存取個人資料的相關作業(新增、異動、刪除、傳輸)應留有記錄。

2. 強化實體安全

和個資有關的資訊設備機房應設有門禁管理，針對主機和儲存媒體，應有良好的安全防護措施，場所應作好天然災害和意外災害的防護、備份媒體以防火或上鎖設備異地存放。

3. 災害防護演練

萬一發生天然災害或個資發生遭人惡意破壞毀損事件、作業不慎等危安事件，或有駭客攻擊等非法入侵情事，應變處理進行損害控制、系統備援、災害復原和通知當事人等。若是人為惡意的損害，應保存證據、要求損害賠償的措施。

四、控制重點：

1. 是否設置個人資料保護執行小組
2. 個人資料保護執行小組是否確實依規範運作
3. 是否定期對所屬人員施以基礎認知宣導或專業教育訓練
4. 個人資料之蒐集、處理及利用是否依規辦理
5. 當事人行使權利之處理是否依規辦理
6. 個人資料檔案是否安全維護

五、依據資料

1. 個人資料保護法

六、使用表單

1. 個人資料運用同意書

七、增(修)紀錄:

訂定:103 年 12 月 30 日董事會會通過。