個人資料保護管理辦法

文件類別：內控制度系統	文件編號：I-W-2-039	版本：1	頁次：1 of 7

第一條　依據

本辦法係依據「個人資料保護法」及「個人資料保護法施行細則」規定訂定，如有未盡事宜，悉依相關法令規定辦理。

第二條　適用範圍

本公司各部門執行所保有個人資料之管理與維護，應依本辦法之規定辦理。

第三條　總則

一、本公司應設置「個人資料保護管理委員會」(以下簡稱個資管理委員會)，以落實個人資料之保護與管理。

個資管理委員會應設置召集人及執行秘書各一人，由總經理指定之，委員由各部門指派專人一人擔任。其個資管理委員會任務如下：

(一)個人資料保護政策之擬議。

(二)個人資料管理制度之推展。

(三)個人資料隱私風險之評估及管理。

(四)各部門專人與職員工之個人資料保護意識提升及教育訓練計劃之擬議。

(五)個人資料管理制度基礎設施之評估。

(六)個人資料管理制度適法性與合宜性之檢視、審議及評估。

(七)其他個人資料保護、管理之規劃及執行事項。

二、個資管理委員會會議得視業務推動之需要，不定期召開，由召集人主持；召集人因故不能主持會議時，得指定委員代理之。個資管理委員會會議開會時，得邀請有關單位或學者專家出(列)席。

三、個人資料管理各部門應指定個資聯絡人辦理下列事項：

(一)依當事人之請求，就其蒐集之個人資料，應答覆其查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

1.防害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

2.妨害公務機關執行法定職務。

3.妨害該蒐集機關或第三人之重大利益。

(二)當事人之個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

(三)執行各部門員工之個人資料保護意識提升及教育訓練計劃之擬議。

(四)個人資料保護法令之諮詢。

(五)個人資料保護事項之協調聯繫。

(六)部門內個人資料損害預防及危機處理應變之通報。

(七)個人資料保護方針及政策之執行、部門內個人資料保護之自行查核。

(八)其他部門內個人資料保護管理之規劃及執行。

四、本公司由管理部門設置「個人資料保護聯絡窗口」，辦理下列事項，並將其連繫方式(如：電話、email)置於本公司網站，以便利當事人提出請求。

(一)與其他公司間個人資料保護業務之協調聯繫及緊急應變通報。
(二)非資訊面個人資料安全事件之通報。
(三)重大個人資料外洩之聯繫單一窗口。
(四)個人資料專人名冊之製作及更新。
(五)個人資料專人與職員工教育訓練名單及紀錄之彙整。

第四條　個人資料範圍

本辦法所稱個人資料係指自然人姓名、出生年月日、國民身份證統一號碼、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。

本公司蒐集、處理或利用個人資料之範圍、類別及特定目的，以本公司依適當方式公開者為限。有變更者，亦同。

本公司特定目的之項目如下：

一、002 人事行政管理。
二、090 消費者、客戶管理與服務。
三、107 採購與供應管理。

第五條　個人資料之蒐集、處理及利用

一、個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得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。遇有疑義者，應提請個資管理委員會研議。

二、有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限，惟應報請個資管理委員會同意後為之。
(一)法律明文規定。
(二)公務機關執行法定職務或非公務機關履行法定義務所必要,且有適當安全維護措施。
(三)當事人自行公開或其他已合法公開之個人資料。
(四)公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。

三、各部門蒐集當事人個人資料時，應明確告知當事人下列事項：
(一)公司名稱。
(二)蒐集之目的。
(三)個人資料之類別。
(四)個人資料利用之期間、地區、對象及方式。
(五)當事人就其個人資料行使下列權利，不得預先拋棄或以特約限制之：
1. 查詢或請求閱覽。
2. 請求製給複製本。
3. 請求補正或更正。
4. 請求停止蒐集、處理或利用。
5. 請求刪除。

(六)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。

有下列情形之一者，得免為前項之告知：

(一)依法律規定得免告知。

(二)個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

(三)告知將妨害公務機關執行法定職務。

(四)告知將妨害第三人之重大利益。

(五)當事人明知應告知之內容。

四、各部門蒐集非由當事人提供之個人資料。應於處理或利用前，得以書面、電話、傳真、電子文件或其他適當方式向當事人告知個人資料來源及第五條第三點第一款至第五款所列事項，且其得於首次對當事人為利用時併同為之。

有下列情形之一者，得免前項之告知：

(一)有第五條第三點第二項所列各款情形之一。

(二)當事人自行公開或其他已合法公開之個人資料。

(三)不能向當事人或其法定代理人為告知。

(四)基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

(五)大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

五、各部門對個人資料之蒐集、處理、利用時，應取得當事人之「個人資料使用同意書」（可依各部門需求修改，惟修改之內容需經「個資管理委員會」之委員審核通過），並交由「個資管理委員會」保管。

蒐集或處理者知悉或經當事人通知禁止對該資料之處理或利用時，應主動或依當事人之請求、刪除、停止處理或利用該個人資料，由申請人填寫「個資應用申請表」，並經資料蒐集部門主管簽核後，移由「個資管理委員會」更正或補充並保管之。

六、各部門對個人資料之蒐集、處理、利用時，應經審核後使得為之。

各部門對個人資料為特定目的外之利用，應取得當事人之「個人資料使用同意書」，並交由「個資管理委員會」保管。

對於個人資料之利用，不得為資料庫之恣意連結，且不得濫用。

七、本公司保管之個人資料有誤或缺漏時，，由申請人填寫「個資應用申請表」，並經資料蒐集部門主管簽核後，移由「個資管理委員會」更正或補充之，並留存相關紀錄。因可歸責於本公司之事由，未為更正或補充之個人資料，應於更正或補充後，由資料蒐集部門以通知書通知曾提供利用之對象。

八、本公司保管之個人資料正確性有爭議者，由申請人填寫「個資應用申請表」，經資料蒐集部門主管簽核後，移由「個資管理委員會」停止處理或利用該個人資料。但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限。

個人資料已停止處理或利用者，資料保管部門應確實記錄。

九、本公司保管個人資料蒐集之特定目的消失或期限屆滿時，由申請人填寫「個資應用申請表」，經由資料蒐部門主管簽核後，移由「個資管理委員會」刪除並停止處理或利用。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

十、各部門違反本辦法規定蒐集、處理或利用個人資料時，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，由申請人填寫「個資應用申請表」，經簽核後由「個資管理委員會」執行之。

個人資料已刪除、停止蒐集、處理或利用者，資料保管單位應確實記錄。

十一、本公司違反本辦法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，經查明後，應以下列流程處理：

(一)個人資料外洩（竊取、洩露、竄改或其他侵害事件）時，應立即通知「個人資料保護聯絡窗口」及「個資管理委員會」。

(二)個資外洩部門，應即時以書面、電話、傳真、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。

(三)個資外洩部門應於事件 36 小時內復原或完成損害管制，並填報「個資安全事件通報單」回覆「個人資料保護聯絡窗口」及「個資管理委員會」，並由「個資管理委員會」保管留存。

第六條　當事人行使權利之處理

一、當事人依下列情況之一向本公司為請求時，應填具「個資應用申請表」，並檢附相關證明文件。

(一)當事人請求就本公司蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。

(二)本公司應維護個人資料的正確性，並應主動或依當事人請求更正或補充之。

(三)個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。

(四)個人資料蒐集之特定目的的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

(五)違反本辦法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

前項書件內容，如有遺漏或欠缺，應通知限期補正。

申請案件有下列情形之一下，應以書面駁回其申請：

(一)申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未補正者。

(二)第三條第一點第一項但書各款情形之一者。

(三)第五條第八及九點但書所定情形者。

(四)與法令規定不符者。

二、當事人依第六條第一點第一款所定情形之一提出之請求，應於十五日內為准駁之決定。

前項之准駁決正，必要時得予延長，延長期間不得逾十五日，並應將其原因以書面通知請求人。

當事人閱覽其個人資料，應由承辦部門派員陪同為之。

三、當事人依第六條第一點第二款至第五款所定情形之一提出之請求，應於三十日內為准駁之決定。

前項之准駁決正，必要時得予延長，延長期間不得逾三十日，並應將其原因以書面通

知請求人。

四、當事人請求查詢、閱覽或製給個人資料複製本者，得按次酌收必要成本費用。

五、個人資料檔案，其性質特殊或法律另有規定不應公開者，得依其他法律規定，限制公開或不予提供。

第七條　個人資料檔案安全維護

一、處理個人資料檔案之資訊設備之安全維護

(一)處理個人資料檔案之資訊設備，需設置使用者代碼及通行碼。

(二)通行碼至少每六個月更換一次，通行碼長度應至少 8 碼，且包含文數字。

(三)禁止與他人共用電腦系統帳號。

(四)採取權限區隔，非專責處理特定個人資料者不得具有存取或查閱個人資料之權限。

(五)個人資料檔案應予以加密。

(六)至少每月備份資訊設備內個人資料檔案一次。

(七)個人資料檔案使用完畢後，應立即退出應用程式。

(八)資訊設備應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 15 分鐘以內。

(九)交換個人資料檔案時，應對資料檔案加密，亦或是透過加密通道傳送。

(十)個人資料禁止存放於網路芳鄰分享目錄，並停用 Guest 帳號。

(十一)禁止使用點對點(P2P)軟體及 Tunnel 相關工具下載或提供分享檔案。

(十二)存放個人資料之資訊設備應與外部網路隔絕（如：防火牆）。

(十三)存放個人資料之資訊設備應安裝防毒軟體，除至少每日更新病毒碼外，並應每周執行完整掃瞄。

(十四)存放個人資料之資訊設備應定期檢視、更新作業系統、應用程式漏洞（如：Windows 作業系統、Windows Office、Adobe Acrobat 等）。

(十五)以直接或間接方式蒐集之個人資料後，應填寫「個人資料新增表」，經部門主管簽核後交由「個資管理委員會」彙整留存，以更新及確保個資資訊清單的正確性及完整性。

(十六)各部門因作業需求提出使用個人資料時，應填寫「個人資料使用需求表」經部門主管簽核後，向「個資管理委員會」提出申請，經授權同意後始得進行，並於進行個人資料使用時，應填寫「個人資料使用登記表」。

(十七)每年至少進行一次個人資料清查直接或間接蒐集之可直接或間接識別個人資料的所有紙本文件及電子檔，並填寫「個人資料盤點表」後交回「個資管理委員會」彙整留存，以更新及確保個資資訊清單的正確性及完整性。

二、設備管理之安全維護

(一)應指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施等，並檢視、處理其錯誤或異常事件等訊息。

(二)儲存個人資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。

(三)儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。

(四)外部團體或個人更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。

(五)儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

三、人員管理之安全維護

(一)應對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練（內、外訓皆可），並定期於單位內宣導個資隱私保護之重要性。

(二)處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。

(三)處理個人資料檔案之人員，應簽訂「保密切結書」，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，且收繳其通行證及相關證件。

(四)每半年個人資料檔案之保管人員應填寫「個人資料保護檢核表」，以確保內部個人資料受到保護。

四、系統開發及委外管理之安全維護

(一)自行開發或委外處理個人資料檔案之資訊系統，應在系統開發生命週期之初始階段，將個人資料檔案的安全需求納入考量（如：邏輯測試）；系統之維護、更新、上線、及版本異動等作業，應予安全管制，避免危害個人資料安全。

(二)宜避免允許維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密通道進行（如：HTTPS、SSH 等）。

(三)自行開發或委外處理個人資料檔案之資訊系統，應保護及控制測試資料，且宜避免以真實個人資料進行測試；如需使用，應將可辨識之個人資料修改為無法辨識之模糊資訊（如：虛擬或錯置），並於完成測試作業後迅速移除。

(四)個人資料檔案若委外建檔，應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。

五、文件管理

(一)個資聯絡人協助管制、保管、維護、建檔稽核計畫內相關文件，應將其鎖在安全的儲櫃或其他安全場所列管。文件發送對象應以最低必要的人員為限。

(二)個資檔案及文件，並依使用者職稱賦予適當之文件存取權限，並於文件、表單上載明為「限閱文件」，且至少需保留三年，應特別控管以避免資料外洩及有心人士或非授權人員拿取。

(三)含個人資料之記錄紙本文件請相關法令或契約保存年限保管，不再使用時請銷毀或依相關法令規定妥善處理，個資文件保留以最小化為原則。

(四)使用影印機、印表機、傳真機、掃描機或多功能事務機後，應立即將紙本資料取走。

(五)個資文件廢止或銷毀時，應填寫「個人資料銷毀申請表」，經部門主管核後並交由「個資管理委員會」進行銷毀。

六、資料稽核之安全維護

每年至少辦理一次稽核，針對控管結果之不符合事項及潛在不符合之風險，應規劃改善措施及預防措施，並確保相關措施之執行。執行改善與預防措施時，應完成以下事項：

(一)確認不符合事項之內容及發生原因。

(二)提出改善及預防措施方案。

(三)訂定合理之執行期限。

(四)紀錄執行結果。

第八條　本辦法如有未盡事宜得隨時修正之；本辦法經董事會核定後施行，修正時亦同。