附件三、保險業運用新興科技作業原則

壹、為協助保險業適當管理運用新興科技之風險，並保障消費者權益，特訂定本作業原則。

貳、雲端服務安全控管

一、雲端服務安全名詞定義

(一)雲端服務：係指服務提供者以租借方式提供個人或企業得承租其網路、伺服器、儲存空間、基礎設施、資安設備、系統軟體、應用程式、分析與計算等資源，以達資源共享之服務。

(二)軟體即服務(SaaS)：雲端服務業者提供軟體使用，承租人能使用軟體，但並不掌控軟體、作業系統、硬體。

(三)平台即服務（PaaS)：雲端服務業者提供作業系統使用，承租人能於此作業系統操作其軟體，可掌控運作軟體的環境也擁有作業系統部分掌控權，但並不掌控作業系統、硬體。

(四)基礎設施即服務（IaaS)：雲端服務業者提供基礎運算資源（如處理能力、儲存空間、網路元件或中介軟體)，承租人能掌控作業系統、儲存空間、已部署的應用程式及網路元件（如防火牆、負載平衡器等)，但並不掌控雲端基礎運算資源。

二、本安全控管範圍不包含僅提供會員公司內部使用且不涉及客戶資料處理之服務。

三、應制定雲端服務管理政策，至少每年檢視一次。

四、若使用雲端服務涉及保險業作業委託他人處理應注意事項之範疇，應依據其規定辦理監督與查核、境外規定要求、緊急應變及營運持續計畫等機制。

五、採用 IaaS 或 Paas 雲端服務模式者，應符合下列規定：

(一)應評估雲端服務提供者之合格條件、服務水準、復原時間、備援機制、權責歸屬及資訊安全防護等項目。

(二)應評估雲端服務提供之平台、協定、介面、檔案格式等，以確保互通性與可移植性。

(三)應確保雲端服務提供者提供之資源與其他承租人所使用之資源各自獨立，互不影響（如防火牆區隔)。

(四)應與雲端服務提供者簽訂服務協議，維持所需之服務水準並定期提出報告與操作 紀錄（如服務水準報告、系統變更紀錄、作業系統映像檔存取紀錄等)。

(五)保險業應確保資料之刪除、銷毀或不可復原，並留存必要之佐證紀錄以供查驗。

六、應針對所傳輸或儲存之客戶資料或敏感資料，建置適當之保護設備或技術，採取適當之存取管制（如資料加密)。採用加密演算法者，應能妥善保護加

密金鑰（如使用硬體安全模組）；另應明訂客戶資料保存期限及應留存之相關重要軌跡紀錄。

七、應監控並建立資訊安全事件通報程序。遇事件發生時，相關單位及人員應依循前述通報程序辦理。

八、應於服務合約終止或轉移時，將使用之作業系統映像檔、儲存空間、快取空間、備份媒體、客戶資料或敏感資料等全數刪除或銷毀，並留存刪除或銷毀之紀錄，以供事後確認。

九、應遵循「個人資料保護法」，資料當事人如申請行使其權利，要求停止處理或利用其資料，應確保其資料皆從雲端刪除或提供相關佐證。

十、提供電子商務服務者，應符合「保險業經營電子商務自律規範」及「保險業電子商務身分驗證之資訊安全作業準則」規定。

參、社群媒體控管程序

一、社群媒體係指一交流平台，參與者透過與其他單一或多位參與者單向分享或雙向 互動，進行內容產出、知識分享、討論共創之平台。

二、本控管程序不包含會員公司內部使用或與個別客戶溝通使用之平台。

三、應制定社群媒體管理政策，至少每年檢視一次。

四、應制定社群媒體使用守則，明確列出可接受使用之社群媒體、功能及使用規則。

五、應制定會員公司發言規範，明確定義各角色被授予之發言權責，並避免非授權之公務言論發表。

六、應制定內容過濾與監視政策，其監視內容應至少包含防止客戶隱私及會員公司機 密外洩、非授權或偽冒身分發言及不可有攻擊或詆毀同業之情事。

七、應制定不當發言之緊急應變程序。

八、應制定社群媒體異常事件通報程序。

九、如有不當發言，應留存通聯紀錄，以供日後調查使用。

肆、自攜裝置安全控管

一、自攜裝置係指非屬公司資產、透過該裝置以無線或有線通訊方式連接至會員公司 內部網路，存取作業系統或檔案服務。

二、應制定自攜裝置管理政策，至少每年檢視一次。

三、應列出允許使用之自攜裝置類型、作業系統、應用系統或服務。

四、對自攜裝置所採取之相關措施，應先取得裝置持有者同意，以避免爭議。

五、應列冊管理使用人員與裝置，至少每年審閱一次。

六、應建置使用人員身分與裝置識別機制(如帳號密碼識別、裝置識別碼)。

七、應制定自攜裝置連網環境標準，如未符合標準(如作業系統疑似遭破解或提權、未 安裝病毒防護、重大漏洞未修復)，應限制其連網功能。

八、應建置自攜裝置資料保護措施(如資料加密或遮罩)，並採取適當之存取管制。

九、應制定自攜裝置遺失處理程序。

伍、生物特徵資料安全控管

一、用詞定義如下:

(一)原始生物特徵資料:是指透過感應器(如掃描器、照相機)所擷取的原始資料。

(二)假名標識符:是指用於生物特徵比對之資料，其內容不為原始生物特徵資料之一部份。

(三)輔助資料:是指一演算法或機制，用來將原始生物特徵資料分離產生假名標識符。

(四)生物特徵資料:指包含原始生物特徵資料、假名標識符及輔助資料。

(五)身分識別資料:為非生物特徵資料之個人資料(如身分證字號、出生日期等)。

(六)錯誤拒絕率:是指同一人卻因比對其留存之生物特徵資料誤認為不同特徵而拒絕的機率。

(七)錯誤接受率:是指不同人卻因比對其留存之生物特徵資料誤認為相同特徵而接受的機率。

二、運用生物特徵資料做為識別客戶身分時，其蒐集、處理及利用之行為，應納入個資管理機制。

三、應針對生物識別機制，建立其錯誤接受率及錯誤拒絕率之標準，並每年定期檢視。若不符合會員公司要求時，應建立補償措施。

四、應於蒐集生物特徵資料時，取得客戶同意，並讓客戶充份了解所蒐集之目的及方式。

五、生物特徵資料儲存於會員公司內部系統時，應將原始生物特徵資料去識別化使其難以還原、將原始生物特徵資料及假名標識符進行加密儲存、 將生物特徵資料分別儲存於不同之儲存媒體(如資料庫)。

六、應考量現行業務情況，必要時更新客戶之生物特徵資料，以確保生物特徵資料不會隨時間而失效(如人臉辨識、聲紋辨識等)。

七、當會員公司無法以生物特徵資料識別客戶時，應提供重新蒐集生物特徵資料之管道。

八、應確保生物特徵資料於傳輸過程中之訊息隱密性、完整性、不可重複性及來源辨識性。

九、應於首次使用生物辨識技術、每年定期及技術有重大變更時(如輔助資料、技術提供商)，經資訊部門檢視該技術足以有效識別客戶身分，其評估範圍包含但不限於模擬偽冒生物特徵資料、確認符合相關法規要求、確認生物辨識機制、作業流程及補償措施之風險控管。