本會106年7月27日第12屆第9次理監事聯席會議討論通過
金管會106 年8月31日金管銀外字第10600195490號函洽悉
本會109年3月12日第13屆第5次理監事聯席會議討論通過
金管會109年4月17日金管銀外字第1090134542號函洽悉

附件一

金融機構運用新興科技作業規範

第一條　　中華民國銀行商業同業公會全國聯合會（以下簡稱本會）為協助會員銀行適當管理運用新興科技之風險，以促進銀行業務健全經營，特定訂本規範。

第二條　　雲端服務安全控管

一、 用詞定義如下：

（一）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。

（二）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。

（三）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、 雲端服務係指雲端服務業者以租借方式提供個人或企業得承租其網路設備、伺服器、儲存空間、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。

三、 本安全控管範圍不包含僅提供銀行內部使用之服務。

四、 應制定雲端服務管理政策，至少每年檢視一次。

五、 應確保作業風險控管，充分評估雲端服務業者處理之風險，採取適當風險管控措施，確保作業品質，並應注意作業委託雲端服務業者之適度分散。

六、 對雲端服務業者負有最終監督義務，並應具有專業技術及資源監督雲端服務業者執行作業，並得視需要委託專業第三人以輔助其監督作業。

七、 應確保其本身、主管機關及中央銀行，或其指定之人能取得雲端服務業者執行作業之相關資訊，包括客戶資訊及相關系統之查核報告，及實地查核權力。

八、 得自行委託，或與委託同一雲端服務業者之其他金融機構聯合委託具資訊專業之獨立第三人查核，並應符合下

列規定：

（一）確認其查核範圍涵蓋雲端服務業者處理作業相關之重要系統及控制環節。

（二）應評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準。

（三）應針對金融機構所指定作業範圍進行查核並出具報告。

九、傳輸及儲存客戶資料或敏感資料至雲端服務業者，應採行資料加密或代碼化等有效保護措施及訂定妥適之加密金鑰管理機制（如租用硬體安全模組）。

十、對雲端服務業者處理之資料應保有完整所有權，除執行指定作業外，金融機構應確保雲端服務業者不得有存取客戶資料之權限，並不得為指定範圍以外之利用。

十一、委託雲端服務業者處理之客戶資料及其儲存地以位於我國境內為原則，如位於境外，應依下列規定辦理：

（一） 金融機構須保有其指定資料處理及儲存地之權力。

（二） 境外當地資料保護法規不得低於我國要求。

（三） 除經主管機關核准者外，客戶重要資料應在我國留存備份。

十二、應訂定妥適之緊急應變計畫，降低因雲端作業而可能有服務中斷之風險。金融機構終止或結束作業委託，應確保能順利移轉至另一雲端服務業者或移回自行處理，並確保原雲端服務業者留存資料(如作業系統映像檔、儲存空間、快取空間、備份媒體)全數刪除或銷毀，並留存刪除或銷毀之紀錄。

十三、採用 IaaS 或 PaaS 雲端服務模式者應符合下列規定：

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

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

（三）應確保雲端服務業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）應與雲端服務業者簽訂服務協議，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）如有設備定期維護更換時(如硬碟更換)，資料也須進行全數刪除或銷毀、並留存刪除或銷毀之紀錄。

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

十五、提供電子銀行服務者，應符合本會制定之「金融機構辦理電子銀行業務安全控管作業基準」規定。

第三條　社群媒體控管程序

一、 社群媒體係指一交流平台，參與者可代表銀行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、 本控管程序不包含銀行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、 應制定銀行發言規範，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銀行機密外洩、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。

第四條　　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銀行內部網路，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。

第五條　　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。

（八）直接驗證生物特徵技術：是指由金融機構驗證客戶之生物特徵，以確認其身分。

（九）間接驗證生物特徵技術：是指由第三方驗證客戶之

生物特徵，再將驗證結果傳送至金融機構，以確認其身分。

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、應針對直接驗證生物特徵技術，建立其錯誤接受率及錯誤拒絕率之標準，並於上線前與每年定期檢視。若不符合銀行要求時，應建立補償措施；針對間接驗證生物特徵技術，應每年定期檢視並蒐集資安威脅情資，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運用方式。

五、生物特徵資料儲存於銀行內部系統時，應將原始生物特徵資料及假名標識符進行加密儲存、並將生物特徵資料分別儲存於不同之儲存媒體；加密金鑰應儲存於符合 FIPS 140-2 Level 3 以上或其他相同安全強度認證之設備，以防止該私鑰被匯出或複製。

六、應考量現行業務情況，得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、當銀行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，相關控管應符合「金融機構辦理電子銀行業務安全控管作業基準」。

九、應於首次使用生物辨識技術、每年定期或技術有重大變更時（如輔助資料、技術提供商），由資訊單位檢視該技術應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，並彙整相關資料交由資安、法遵及風控等單位建立各部門間之連繫機制、確認相關作業符合本作業規範及相關定型化契約等相關法令規定，留存驗證軌跡及各部門建議事項追蹤控管機制即可辦理。

第六條　本規範經本會理事會通過並函報金融監督管理委員會核備後實施，修正時亦同。