附件一

本會106年12月21日第12屆第13次理監事聯席會議討論通過
金管會107年7月2日金管銀國字第10702093510號函洽悉
本會109年12月24日第13屆第3次理事會議討論通過
金管會110年4月30日金管銀國字第1100201928號函洽悉

金融機構使用物聯網設備安全控管規範

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)為確保金融機構使用物聯網(Internet of Things, IoT)設備之安全性，降低相關作業風險，特訂定本規範。

第二條　本規範所稱物聯網設備係指具IP網路連線功能並實際連線於Internet或Intranet之辦公設備（包括但不限於事務機、網路電話機、傳真機及印表機）、門禁監控（包括但不限於門禁、DVR、錄音設備）、環境管控（包括但不限於環境感測器、網路攝影機），排除已有管控機制設備(如伺服器、個人電腦、平板電腦、網路設備、資安設備、儲存設備)及僅使用藍牙、RS-232、USB連接等裝置。

第三條　應建立物聯網設備管理清冊並至少每年更新一次，以識別設備用途、設備IP、存放位置與管理人員，評估適當之實體環境控管措施及存取權限管制。

第四條　設備應具備安全性更新機制，以維持設備之整體安全性。

第五條　為確保經授權之使用者始得進行資料存取、設備管理及安全性更新等操作，設備應具備身分驗證機制，並應進行初始密碼變更，密碼長度不應少於六位，建議採英數字混合使用，且宜包含大小寫英文字母或符號，並以最小權限原則針對不同的使用者身分進行授權。

第六條　設備以無線連接網路者，應採用具加密協定之無線存取點連接網路，並以網路卡卡號白名單等機制進行設備綁定。

第七條　設備應關閉不必要之網路連線及服務，限制其對網際網路不必要之網路連線；並避免使用對外公開之網際網路位置，如設備採用公開的網際網路位置，應於設備前端設置防火牆以防護，並採用白名單方式進行存取過濾。

第八條　應與設備供應商簽訂資訊安全相關協議，以明確約定相關責任。

第九條　設備無法落實本規範第四、五、六、七條之安全控管規範，應限制網際網路連線能力，加強存取控制或進行網路連線行為監控。

第十條　設備存在已知弱點且無法修補或更新，應依本規範第九條辦理，並視需要訂定汰換期程。

第十一條　設備於採購前應依據本規範進行評估及測試，若因業務發展需求選用無法滿足本規範要求之設備，應依本規範第九條辦理。

第十二條　針對不具備遠端操控介面功能之感測器，仍應遵循本規範第三、七、八、九、十、十一條之要求辦理。

第十三條　物聯網設備管理人員每年應接受至少 1 個小時之相關物聯網安全教育訓練課程；另每年定期辦理之資訊安全宣導課程應有半個小時與物聯網相關，以強化使用人員對物聯網設備資安防護意識與技能。

第十四條　依據「金融機構辦理電腦系統資訊安全評估辦法」第四條之分類期程，對物聯網設備辦理該辦法第五條資訊安全評估作業時，併依本規範第四、五、六、七條之安全控管規範進行評估。

第十五條　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。