附件四、保險業使用物聯網設備作業準則

一、為確保保險業使用物聯網(Internet of Things, IoT)設備之安全性，以確保適當管理運用物聯網設備之風險，並保障消費者。

二、本作業準則所稱物聯網設備係指具實際連線於 Internet 或 Intranet 之辦公公用設備（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 等）、環境管控（包括但不限於環境感測器、網路攝影機）等實體裝置或設備。

三、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。

四、設備應具備安全性更新機制，以維持設備之整體安全性。

五、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。

六、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。

七、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或該物聯網設備不與公司內部網路介接。

八、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。

九、設備存在已知弱點且無法修補或更新，無法落實前述安全控管規範，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；並視需要訂定汰換期程。

十、採購物聯網設備時，應優先採購經濟部與國家通訊傳播委員會共同發布物聯網資安標章認驗證制度之具有安全標章之物聯網設備。

十一、應每年對物聯網設備使用及管理人員安排適當之資訊安全教育訓練。

十二、汰換物聯網設備時，應訂定汰除作業程序以避免儲存於物聯網設備資料外洩。

十三、針對不具備遠端操控介面功能之感測器，仍應遵循本作業準則三、七、八、九、十二之要求辦理。