

## 農漁會信用部行動支付業務符合「金融機構提供 QR Code 掃描支付應用安全控管規範」自評表

自評日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

農漁會名稱：

所屬資訊共用中心：

自評依據(請配合申辦行動支付時適用之「金融機構提供 QR Code 掃描支付應用安全控管規範(下稱控管規範)」，為必要之調整)：

■ 金融監督管理委員會 106 年 8 月 30 日同意備查，由中華民國銀行商業同業公會全國聯合會(下稱銀行公會)所訂定之控管規範

安全控管作業項目	本案作法說明	合規性評估
QR Code 掃描支付過程中，所存取之資訊應遵循該業務所需最小化原則。 【控管規範第 3 條】		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用
採用交易資訊類 QR Code 者，應用程式應以彈出式視窗或其他方式提供接收方檢視 QR Code 之資料內容，再由接收方處理後續事宜。【控管規範第 4 條】		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用
被掃模式採用交易指示類 QR Code 者，因係屬使用者產生授權資訊同意扣款性質，應設定 QR Code 合理使用時效，且在時效內以使用一次為限。【控管規範第 5 條】		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用
QR Code 受理終端所提交之 QR Code 訊息請求應確保傳輸過程中的資訊完整性及隱密性，並確保在傳輸過程中不被篡改及洩露。【控管規範第 6 條】		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用
QR Code 受理終端相關應用程式，應能針對所解析之 QR Code 進行格式檢查，確保資料格式合理性，預防程式碼注入。【控管規範第 7 條】		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用
QR Code 受理終端相關應用程式，應能針對所解析之交易指示類 QR Code 進行來源辨識性及完整性檢查，對於未		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用

安全控管作業項目	本案作法說明	合規性評估
驗證通過之 QR Code 應予明確提示並拒絕執行交易。【控管規範第 8 條】		
QR Code 受理終端相關應用程式，對所解析之 QR Code 產生網站連結，應採包括但不限於白名單或伺服器認證等機制進行網站合法性檢查，以預防連結惡意網站或執行惡意程式風險。【控管規範第 9 條】		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用
主掃模式及被掃模式等各類應用情境，所生成之交易指示類 QR Code 收付不得共用，以確保專碼專用。【控管規範第 10 條】		<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用

\_\_\_\_\_ 資訊共用中心（請蓋印信）：

負責人：