附件六

保險業網路身分驗證之資訊安全作業準則

一、 為協助保險業使用網路身分驗證時，可建立有效的安全驗證機制，以確保減少身分冒用及詐騙情事發生，降低保戶與各公司之機敏資料外洩之風險，特訂定本作業準則。

二、 用詞定義及說明：

（一） 網路身分認證：係指於網路應用程序系統通過特定的身分驗證機制，以確認是否為保戶本人。

（二） 多因子驗證(Multi-Factor Authentication, MFA) ：係指為強化帳號密碼管理，降低系統相關帳號密碼遭假冒或竊用之風險，提高系統整體安全性並使用二種以上因子驗證方式。

三、 多因子驗證可運用的因子包含帳號及密碼、一次性密碼(OTP)、智慧卡、憑證、生物特徵辯識、或符合 FIDO 標準的驗證方式（Fast Identity Online）及 Mobile ID 行動身分識別服務等，其相關說明如下：

（一） 帳號及密碼、一次性密碼(OTP)安全性設計，應參考「保險業網路投保註冊會員密碼之設計安全作業準則」執行。

（二） 智慧卡應設有密碼功能(Pin Code)，於晶片進行密碼驗證，晶片應符合共通準則(Common Criteria) EAL 4+以上或其他相同安全強度之認證。

（三） 憑證應由憑證機構依經濟部核定之憑證實務作業基準簽發，憑證應具有時效性，過期應立即失效，須重新簽發或展延期限。

（四） 生物特徵辯識應符合「保險業運用新興科技作業原則」之(伍、生物特徵資料安全控管)規範。

（五） FIDO 應遵循國際 FIDO 聯盟所訂定之產業技術標準，並符合我國金融行動身分識別聯盟所制訂之相關標準及規範。

（六） Mobile ID 行動身分識別服務應由提供手機門號之電信業者進行身分驗證。

四、 會員公司辦理網路身分認證，則系統或環境存取需建立身分驗證機制，相關規則如下：

（一） 建立身份驗證機制應防範自動化程式之登入或密碼更換嘗試。

（二） 當進行密碼重設機制時，應針對使用者重新身分確認，並發送一次性及具有時效性符記。

（三） 供應商或合作廠商之網路身分驗證，應依合作性質建立適當控管機制，如限制登入 IP 及加強進行登入身分核實。