附件五

保險業網路投保註冊會員密碼之設計安全作業準則

會員公司若辦理網路投保業務，則網路投保註冊會員時應以靜態密碼或使用一次性密碼(OTP)自行設定，使用規則如下：

一、 靜態密碼:

1. 應至少 8 位數。
2. 應採英數字混合使用，且宜包含大小寫英文字母或符號。
3. 不得使用客戶之統一編號及身分證字號等顯性資料作為密碼。
4. 不應訂為相同的英數字、連續英文字或連號數字，預設密碼不在此限。
5. 密碼與代號/帳號不應相同。
6. 密碼連續錯誤達五次，各公司應做妥善處理。
7. 變更密碼不得與前一次相同。
8. 首次登入時，應強制變更預設密碼。
9. 密碼超過一年未變更，各公司應做妥善處理。
10. 應採用下列一項密碼儲存管控機制：
    (1)密碼於儲存時應先進行不可逆運算（如雜湊演算法），雜湊值應進行加密保護或加入不可得知的資料運算。
    (2)採用加密演算法者，其金鑰應儲存於經第三方認證（如 FIPS 140-2 Level 3 以上）之硬體安全模組內並限制明文匯出功能等。

二、 一次性密碼(OTP)：

1. 應至少 6 位數。
2. 密碼與帳號不應相同。
3. 輸入密碼連續錯誤達五次，該密碼即失效。
4. 每次密碼有效性不得超過 5 分鐘，超過時即需重新申請發給新密碼。