保險業經營電子商務自律規範

中華民國一百十二年八月二十四日金融監督管理委員會金管保綜字第1120144706 號函同意備查修正第 7、8、12 條條文

第一條（目的）

本自律規範之目的在於發展保險電子商務，建立活絡有序之電子商業環境，經由本規範之確立，以確保消費者權益，並增進保險業之服務效能。

第二條（遵循宣示）

保險業經營保險電子商務，除本自律規範規定外，並應遵守保險法、公平交易法、消費者保護法、金融消費者保護法、個人資料保護法、電子簽章法、洗錢防制法、資恐防制法、金融機構防制洗錢辦法、保險公司與辦理簡易人壽保險業務之郵政機構及其他經金融監督管理委員會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法、保險業招攬及核保理賠辦法、保險業辦理電子商務應注意事項、保險業保險代理人保險經紀人與異業合作推廣附屬性保險商品業務應注意事項（以下簡稱異業合作應注意事項）、保險業申請業務試辦作業要點等相關法令之規定。

本規範內容應揭示於保險業之網頁，保險業應宣示遵守本自律規範；並提供與主管機關網頁超連結，方便消費者查閱相關監理資訊。

保險業經營電子商務，應經由保險公司建置網站專區、網頁或保險公司設置之行動應用程式（APP）投保平台，且其所屬業務員不得自行建置。

保險業依異業合作應注意事項與異業合作辦理網路投保業務及網路保險服務，該異業建置網站專區、網頁或行動應用程式（APP）投保平台，應由保險業負責管理維護並揭露相關資訊。

本自律規範所稱保險電子商務包含網路投保業務及網路保險服務。

前項所稱網路投保業務，係指要保人得經由網路與保險公司電腦連線或親臨保險公司之方式，完成首次註冊及身分驗證程序後，於網頁輸入要保資料並完成投保及身分驗證程序，直接與保險公司締結保險契約者（要保人以自然人為限）。

第五項所稱網路保險服務，係指保戶經由網路與保險公司電腦連線或親臨保險公司方式，完成註冊及身分驗證程序後，於網路上辦理除網路投保以外之各項保險服務；另團體保險網路保險服務係指要保單位經由書面申請，並指定授權人員及被保險人，經保險公司完成授權驗證後於網路上辦理，但經主管機關核准或保險業申請業務試辦獲准者，不在此限。

第三條（廣告與宣傳之規範）

保險業從事保險電子商務應尊重及維護消費者權利，並採行下列公平之商業、廣告及行銷活動：

一、應確保其廣告內容之真實性，其對消費者所負之義務不得低於廣告之內容。應承諾不刊登色情、暴力或違法之廣告。

二、網頁廣告內容應具體、明確、禁止誇大或過於抽象。

三、應對其他保險同業廣告之創意予以尊重，並承諾不侵害智慧財產權，同時杜絕抄襲行為。

四、承諾拒絕以不實之攻擊做為廣告內容，同時不利用廣告遂行不公平競爭。

五、在寄送電子廣告郵件時，為尊重消費者之自主選擇權，應明白向消費者揭示中止方式；一旦消費者要求停止寄送時，即應立即中止電子廣告郵件之寄發。

第四條（保險業資料之提供）

保險業應於網站揭露各項營業資料，以利消費者辨認，進而建立交易安全信心。保險業揭露之各項營業資料，至少應包括：公司組織結構、部門職掌及各部門負責人姓名、總公司、分公司（經辦郵局）、通訊處等其他分支機構設立時間、地址、電話、傳真、免費申訴專線電話、公司網站之網址、電子郵件信箱及其他依法或主管機關規定應向消費者揭露之事項。外國保險業並應記載其總公司所在地、設立時間及資本額。

第四條之一（主管機關指定平台辦理網路投保業務之規範）

保險業辦理保障型保險商品平台之網路投保業務，其連結至各公司之專屬網頁應

符合下列規定：

一、與該公司原網路投保網頁區隔，不得有連結至該公司官方網頁、原網路投保網頁及其他非保障型保險商品平台相關網頁之情事。

二、應建立導回該平台入口網頁之連結。

三、依本自律規範應於網頁(網站)揭示(揭露)之事項，除第二條第二項規定之主管機關網頁外，均不得以超連結方式呈現。

第五條（完整提供交易條件資訊）

保險業辦理網路投保業務時，應於網頁完整提供消費者交易條件相關資訊，其揭示應以明顯且消費者易於取得之方式辦理。

保險業提供之交易條件資訊至少應包括下列項目：

一、所提供商品或服務之參考價格、種類及性質。

二、消費者應支出之費用項目與金額。

三、要約與承諾之傳送方式、生效時間、要約有效期間、契約成立時點。

四、付款時間及方式。

五、服務提供之內容、方式與時間。

六、消費者得終止或撤銷契約之時間、方式與限制，及雙方之權利義務。

七、網路上之目錄提供或線上服務如需付費，需明白向消費者揭示。

八、消費者抱怨及申訴管道，例如：電子郵件、傳真、電話或線上諮詢服務台。

九、可選擇之付款方式及安全交易機制。

十、隱私權保護政策。

十一、消費者確認購買保險商品時，於保險費繳付後保險業應賦予序號以資連繫查詢；惟保險業仍保有保險契約核保權利。

其他依法或主管機關規定應揭露之事項。

第六條（保險業辦理網路投保業務之義務與責任）

保險業辦理網路投保業務，應確實履行下列事項：

一、契約成立或變更後，應對消費者發送確認之訊息。

二、提供符合契約內容要求之保險商品及服務。

三、交付方式：

對消費者所簽訂之保險契約及相關文件應選擇安全、適當及迅速之交付方式。

四、審閱期間或撤銷契約機制：

(一) 承諾提供消費者保險契約約定之審閱期間或契約撤銷權及申請契約撤銷之作業流程說明。

(二) 消費者得於收受保險契約之翌日起，十日內申請契約撤銷。但保險期間二年以內之短期險不在此限。

五、應確實履行所提供之服務內容。

六、應依公司規定保存期限保存交易資料。

七、對消費者合理要求應迅速給予回應。

八、應承擔交易風險之責任，並建立電子交易風險內部管控機制。

第七條（網路投保之首次註冊及身分驗證作業應遵守之事項）

具行為能力之消費者得經由網路與保險公司電腦連線、親臨保險公司或經主管機關核准之方式，完成首次註冊及身分驗證作業而取得帳號密碼後，始得進行網路投保作業。

保險業辦理前項作業，除主管機關另有核准外，應遵守下列事項：

一、消費者以網路方式申請者：

(一) 於保險公司或異業建置網站專區、網頁或行動應用程式（APP）投保平台載明法定相關告知事項（包括但不限於同意網路投保聲明事項、履行個人資料保護法告知義務內容、網路保險服務定型化契約等）提供消費者閱覽、點選告知事項已讀及網路投保同意後，始得進行首次註冊及身分驗證作業。

(二) 確認消費者已填寫足資驗證其身分之個人基本資料。但經消費者同意，得以下列方式之一辦理：

1、以網路銀行帳戶（以銀行臨櫃辦理者為限），或數位存款帳戶（適用電子轉帳交易指示類高風險交易之第一類帳戶）進行註冊及身分驗證作業。

2、以該異業之會員帳戶進行註冊及身分驗證作業。

(三)發送一次性密碼（以下簡稱 OTP）、生物辨識、行動身分識別(Mobile ID)或金融行動身分識別(金融 FidO)等方式，確認消費者身分，並引導消費者完成身分確認。

二、消費者以親臨保險公司（含其分支機構）營業處所方式申請者：

(一) 要求消費者應親臨保險公司（含其分支機構）營業處所申請辦理。

(二) 以書面或其他日後可資證明之方式提供法定相關告知事項(包括但不限於同意網路投保聲明事項、履行個人資料保護法告知義務內容、網路保險服務定型化契約等)提供消費者閱覽，消費者須簽名同意，以完成首次註冊及身分驗證作業。

(三) 要求消費者提供足資驗證其身分之個人基本資料。

三、消費者以數位憑證方式申辦者：

(一) 消費者如為首次註冊者，保險業應於網站專區、網頁或保險公司設置之行動應用程式（APP）投保平台載明法定相關告知事項（包括但不限於同意網路投保聲明事項、履行個人資料保護法告知義務內容、網路保險服務定型化契約等）提供消費者閱覽、點選後，始得以數位憑證完成首次註冊及身分驗證作業。

(二) 應確認消費者已填寫足資驗證其身分之個人基本資料。

(三) 應引導消費者於網頁選取欲使用數位憑證之發證公司及數位憑證以執行數位簽章，保險業應以電子訊息傳送數位簽章至憑證機構驗章。由憑證機構即時回覆驗章成功或失敗訊息給保險業。保險業確認驗章成功後，即完成首次註冊及身分驗證作業。

消費者經完成前項身分驗證作業而取得帳號密碼後，如消費者於申請完成後五年之期間內並未再與該保險業辦理網路投保業務者，消費者非經重新完成前項身分驗證作業，不得再利用該帳號密碼進行網路投保作業。

第八條（網路保險服務之首次註冊及身分驗證作業應遵守之事項）

保險業辦理網路保險服務應提供具行為能力之既有保戶依經主管機關核准之方式或下列方式擇一辦理註冊或身分驗證作業：

一、以網路方式：

(一) 保險業應於網站專區、網頁或保險公司設置之行動應用程式（APP）投保平

台載明法定相關告知事項，包括但不限於同意網路保險服務聲明事項、履行個人資料保護法告知義務內容等，提供保戶閱覽、點選告知事項已讀及網路保險服務同意後，始得進行首次註冊及身分驗證作業。

(二) 既有保戶得於線上約定並經由身分驗證程序或數位憑證方式取得帳號。但經既有保戶同意，得以網路銀行帳戶(以銀行臨櫃辦理者為限)或數位存款帳戶(適用電子轉帳交易指示類高風險交易之第一類帳戶)進行註冊及身分驗證作業。

(三) 既有保戶完成網路註冊及身分驗證作業後，保險業應以 OTP、生物辨識、行動身分識別(Mobile ID)或金融行動身分識別(金融 FidO)等方式確認保戶身分，並應引導保戶完成身分確認。

(四) 如保戶已依前條完成註冊及身分驗證者，得沿用該帳號進行網路保險服務。

二、以親臨保險業(含其分支機構)營業處所申請方式辦理，並進行身分驗證程序後，提供保戶帳號密碼。保險業應以書面或其他日後可資證明之方式提供法定相關告知事項，包括但不限於同意網路保險服務聲明事項、履行個人資料保護法告知義務內容等，提供保戶閱覽，保戶須簽名同意以完成首次註冊及身分驗證作業。

保戶經完成前項身分驗證作業而取得帳號密碼者，如於申請完成後五年之期間內並未再與該保險業辦理網路保險服務者，保戶非經重新完成前述身分驗證，不得再利用該帳號密碼辦理網路保險服務。

申辦強制汽車責任保險電子式投保證明及查詢汽車保險繳費作業，得以被保險人國民身分證統一編號(或營利事業統一編號或財稅機關編發之統一編號)及汽車牌照號碼辦理查詢，免辦理前項註冊或身分驗證作業。

第九條(團體保險網路保險服務之首次註冊及身分驗證作業應遵守之事項)

保險業辦理團體保險網路保險服務，應依下列流程申請辦理註冊及授權驗證作業：

一、保險業應以書面方式提供法定相關告知事項，包括但不限於同意網路保險服務聲明事項、履行個人資料保護法告知義務內容等，經要保單位簽章同意約定註冊網路保險服務，並指定授權人員辦理網路保險服務。

二、要保單位書面指定授權人員，經保險公司核對申請文件與要保單位原留印鑑相符後完成授權驗證，應寄送帳號密碼至要保單位辦理本項業務指定之電子郵件信箱。

三、要保單位書面申請授權各被保險人辦理網路保險服務。經保險公司核對申請文件與要保單位原留印鑑相符後完成授權驗證。保險公司應檢核被保險人所屬要保單位已完成前述申請程序後，始得進行首次註冊及身分驗證作業，以辦理網路保險服務。

要保單位經完成授權驗證作業而取得帳號密碼者，保險業應訂定帳號密碼有效使用期限。

第十條（投保作業應遵守之事項）

保險業辦理網路投保業務之投保作業，應遵守下列事項：

一、於保險公司或異業建置網站專區、網頁或行動應用程式（APP）投保平台提供可進行網路投保之所有保險商品之商品說明、保單條款等，以利要保人隨時瀏覽參閱。

二、於要保人輸入相關投保資料及選擇欲投保之保險商品後，保險業應於保險公司或異業建置網站專區、網頁或行動應用程式（APP）投保平台上顯示該保險商品之保單條款全文或連結及保險商品重要內容說明（投保須知），以提供要保人閱覽並點選同意。

三、於要保人送出確認投保前，保險業應以 OTP、生物辨識、行動身分識別(Mobile ID)或金融行動身分識別(金融 FidO)等方式，確認要保人身分，並引導要保人完成身分確認，始得完成投保作業；要保人如以數位憑證方式辦理投保者，於其送出確認投保前，保險業應透過數位憑證進行身分驗證作業，於確認要保人身分後始得完成投保作業。

四、於要保人輸入投保資料後，如屬於財產保險商品中之車體險或竊盜險而需勘車者，財產保險業應確認要保人同意進行勘車作業。

五、如屬依法令規定應提供審閱期間之保險商品，並應依法令規定辦理。

六、保險業受理要保人與被保險人不同人，以網路投保人身商品時，限以自然人

憑證註冊或要保人為其七歲以下未成年子女投保旅行平安保險。如採自然人憑證註冊，要保人以自然人憑證註冊後，被保險人限以自然人憑證為意思表示。保險業並應於保險公司或異業建置網站專區、網頁或行動應用程式（APP）投保平台以醒目標示提示消費者有關要/被保險人之關係須符合保險法第十六條規定之範圍。

人身保險商品如屬投資型年金保險，保險公司於網站專區、網頁或保險公司設置之行動應用程式（APP）投保平台，應建立以下控管與配套作業：

一、提醒告知商品特性及相關風險；另於申請投保時，確認瞭解商品風險及投保意願。

二、應揭露完整商品內容，包括但不限於以下事項：

(一)保單運作流程。

(二)保險給付項目。

(三)投資標的簡介。

(四)保單相關費用。

(五)投保規定(年齡、保險費等限制)。

(六)銷售文件(條款、商品說明書等)下載連結。

(七)投資相關風險。

(八)保險費繳交與轉入投資配置時間點不同之相關提醒。

三、申請投保過程中，應確認保戶已完整審閱商品重要銷售文件(如條款、商品說明書等)，及逐項確認瞭解商品重要內容及投資風險。

四、應清楚揭露各項作業流程，前述作業項目包括但不限於以下事項：

(一)保險費繳交。

(二)核保。

(三)電話訪問。

(四)保單發放。

(五)不承保或契撤之退還保險費。

五、保險業應按要保人指定之方式，以紙本或電子文件方式交付商品說明書及保險單。保險業以電子文件方式提供商品說明書及保險單者，須經要保人表示同意，

且不得有誘導要保人之情形。另如與保戶約定採電子文件方式提供保單，應建立保戶未於時限內點閱或下載並簽收保單之提醒輔助機制及因應機制，且就保戶所點閱或下載及簽收之紀錄，留存相關軌跡。

六、須即時連線保險業通報作業資訊系統，檢核同業累積保險費不得超過「保險業辦理電子商務應注意事項」附件一之規定。

第二項第四款作業流程之揭露需輔以時間軸方式呈現各項作業相關時間點。另應就保費繳交與轉入投資配置時間點不同，向保戶清楚揭露。

第二項第五款所稱因應機制係指保戶如於保險公司寄送保單後三十日內未點閱或下載並簽收保單，保險公司應改以紙本保單方式供保戶審閱並簽收。

第十一條（核保作業應遵守之事項）

保險業對於以網路方式投保財產保險商品之核保作業，應遵守下列事項：

一、投保強制汽車責任保險：

強制汽車責任保險之保險費試算系統，應即時連線財團法人保險事業發展中心之強制汽車責任保險資訊作業中心平台，查詢承保及理賠紀錄，避免試算保險費錯誤與重複投保。

二、投保任意汽車保險：

任意汽車保險之保險費試算系統，應即時連線關貿網路股份有限公司之任意汽車保險共用平台，查詢承保及理賠紀錄，避免保險費錯誤，並提供要保人於保險費試算後，仍得修改投保相關內容之服務。

三、投保住宅火災及地震基本保險、住（居）家綜合保險：

(一) 住宅火災及地震基本保險及住（居）家綜合保險之保險費試算系統，應參考中華民國產物保險商業同業公會台灣地區住宅類建築造價參考表，並提供要保人於保險費試算後，仍得修改投保相關內容之服務。

(二) 於要保人確認投保後，應即時連線財團法人住宅地震保險基金之住宅地震保險複保險查詢平台，以進行複保險檢核避免重複投保。

保險業對於以網路方式投保人身保險商品之核保作業，應遵守下列事項：

一、於送出繳款資料並取得信用卡或轉帳銀行授權碼後即時連線辦理收件通報，

並應於扣款完成後且保險契約成立時二十四小時內，立即辦理承保通報。

二、須檢核承保公司內部有無異常投保或理賠紀錄，且單一公司保險金額不得超過保險業辦理電子商務應注意事項規定之限額。

三、須即時連線保險業通報作業資訊系統，檢核同業累積保險金額不得超過保險業辦理電子商務應注意事項規定之限額。

四、保險業應依各投保險種及投保金額所應遵循之核保規範進行網路投保核保作業。除現行線上無法直接承保之機制外，如有包含但不限需體檢、財務核保或不符合承保公司內部訂立之網路投保篩選標準或其他情形者，得自行評估並依保險業核保規範辦理該件轉人工核保作業，並自同意承保後，依本自律規範第十二條規定完成線上繳費作業。

第十二條（繳費作業及身分輔助驗證機制應遵守之事項）

保險業對於以網路方式投保之繳費作業及身分輔助驗證機制，應遵守下列事項：

一、要保人於保險公司或異業建置網站專區、網頁或行動應用程式（APP）投保平台以網路方式首次註冊及身分驗證者，於進行網路投保時，保險業僅得接受以要保人本人之信用卡、要保人本人存款帳戶或電子支付帳戶(限第一類或第二類)轉帳方式繳交保險費。

二、消費者投保人身保險商品，並以本人信用卡或本人存款帳戶繳費者，保險業應與財團法人聯合信用卡處理中心、財金資訊股份有限公司或其他合作銀行或電子支付機構建立身分輔助驗證機制。

三、採數位憑證或親臨保險公司方式申請帳號密碼客戶，保險業亦得提供自動櫃員機（ATM）、銀行臨櫃、連鎖便利商店業及其他經主管機關核准之繳費方式供要保人選擇。

四、保險業應發送簡訊或電子郵件通知要保人已完成扣款及投保作業，並寄發紙本保單或電子保單予要保人。

第十三條（辦理電子商務之審核及通知程序）

保險業辦理保險電子商務業務，應依相關法令及內部核保、保全、理賠內部控制

作業進行審核，且於完成審核時通知保戶辦理結果。

前項通知得以與保戶所約定之電子文件為之。

第十四條（發單前之確認作業）

為確認以網路方式投保之要保人之投保意願，除要保人單獨投保強制汽車責任保險、旅行平安保險、旅行綜合保險及投保財產保險之既有保戶，於保單屆期前，於網路完成投保且承保內容、保險金額與前一年度相同者外，保險業應執行以下確認程序：

一、屬於新保戶者，寄發保單予要保人前，應抽樣百分之十進行電話訪問，以確認投保。如經確認要保人並未投保者即不予承保。（採數位憑證或親臨保險公司除外，但列為第二款抽樣母數）。

二、屬於既有保戶者，於保單寄發要保人前應抽樣百分之五進行電話訪問，以確認投保。如經確認要保人並未投保者即不予承保。

三、投保投資型年金保險者，寄發保單予要保人前，須百分之百進行電話訪問，以確保要保人明確瞭解投資型年金保險的商品內容、相關投資風險及投保意願；如電話訪問未成者，即不予承保。另保險業應通知並確認要保人知悉保險契約是否成立。

前項情形，如電話聯繫要保人未成或拒訪者，保險業應補寄信件、簡訊或電子郵件提醒相關投保權益。

要保人為聽語障人士者，其確認投保意願之方式得以簡訊、電子郵件或足資辨識之方式替代電話訪問。

第一項之電話訪問過程應經要保人同意全程錄音，並備份存檔。

第十五條（消費者個人資料及隱私權之保護）

保險業應遵守個人資料保護法令及下列消費者隱私權保護原則：

一、告知義務：保險業在蒐集消費者資料前，應明白告知其隱私權保護政策，包括資料蒐集之內容及其使用目的。

二、蒐集及使用限制：資料之蒐集應經由合法及公平之方法，並應取得消費者之

同意。除消費者同意或法令另有規定外，使用上不得逾原先所告知消費者之使用目的。

三、參與：消費者得查詢及閱覽其個人資料，保險業並應提供增刪及修正機制。

四、資料保護：對消費者之資料應依法定保存期限為妥當之保護，避免遺失或未經授權之使用、銷燬、修改、再處理或公開。個人資料已無保存必要時，應確實銷燬。

五、責任：保險業如未能遵守上述原則或未能遵守其在隱私權保護政策中所承諾之措施時，則應負法律責任。

第十六條（安全之交易環境）

保險業應採取適當之措施保障交易安全，以保護於網路上傳輸及儲存於保險經營者處之付款及個人資料。

保險業應提供消費者其所使用之網路交易安全或相關電子憑證技術資訊，讓消費者瞭解該安全控管系統之風險。

保險業應鼓勵消費者以安全方式提供個人機密資料。

保險業應參酌相關之安控標準適時更新所使用之安全及憑證技術，以保持或提升交易安全等級。

第十七條（安全之付款機制）

保險業應提供消費者易於使用且安全之付款機制。

保險業應提供下列付款資訊：

一、單一或可供選擇之付款方式。

二、各種付款方式之安全性。

三、如何正確且有效使用該付款方式。

四、對各種付款方式之安全性應設風險警語。

保險業應協調合作之金融機構採取適當措施，協助消費者解決與保險業間因未授權交易或其他有瑕疵交易所產生之消費爭議。未經消費者授權之交易，除消費者有故意或重大過失者外，消費者不須負擔責任。

第十八條（應保存之交易紀錄項目）

保險業經營電子商務者，應至少保存下列項目之紀錄：

一、網路投保業務之消費者身分驗證作業之申請、審核及啟用紀錄。

二、與消費者間之相關往來紀錄。

第十九條（儲存媒體及備份資料之要求）

保險業以電子簽章、加密等技術保存現有和已歸檔之交易資料紀錄時，應使用加密之特定媒體儲存或委託公信第三者保存，並定期製作備份資料。

第二十條（歸檔資料之保存期限）

保險業對已歸檔儲存之交易資料紀錄（以下簡稱歸檔資料），其保存期限為保險契約期滿後或通知要保人不同意承保後至少五年；用以處理歸檔資料之應用程式保存期限亦同。

第二十一條（歸檔資料之控管原則）

保險業管理電子商務之歸檔資料，應依下列原則控管：

一、不得新增、修改或刪除歸檔資料。

二、必要時得將歸檔資料移至另一儲存媒體儲存，但應提供適當的保護，且保護等級應不低於原保護等級。

三、歸檔資料應存放於安全處所。

四、歸檔資料之管理應訂定相關作業程序。

五、應對歸檔資料之歸檔時間加以紀錄及管理。

六、欲取得歸檔資料者，除法令另有規定外，須以書面提出申請並經允許後始得為之。歸檔資料之調閱如涉及個人資料者，應依個人資料保護法相關規定辦理，未涉及個人資料者，則依內部調閱程序辦理。

第二十二條（電腦網路設備安全之防護要求）

保險業對於電腦網路設備安全之防護，應符合下列條件：

一、所有網路硬體設備應安置於安全地點。

二、安置網路硬體設備之地點應加裝不斷電系統或備用發電機，並依法令規定設置必要及合格之消防安全設施。

三、安置網路硬體設備之地點應建立安全維護及人員進出之控管機制。

第二十三條（網路管理之緊急事故應變與災害復原應訂定之程序）

保險業經營電子商務者，應就網路管理之緊急事故應變與災害復原處理訂定下列程序：

一、緊急事故通報程序。

二、緊急事故應變程序。

三、災害復原程序。

四、測試程序。

第二十四條（網路安全規劃管理作業應涵括之項目）

為確保電子商務資訊安全，保險業應訂定網路安全規劃與管理作業，以達成整體網路作業之安全管理。

前項網路安全規劃與管理作業應包括下列項目：

一、網路安全政策。

二、網路安全服務管理。

三、網路安全連結。

四、主機與消費者端設備安全防護。

五、身分識別和驗證。

六、網域劃分與安全控制。

七、防火牆安全管理。

八、遠端連線控制。

九、網路安全監控。

十、監控處理程序。

十一、事件安全記錄。

十二、入侵偵測檢視。

十三、防範電腦病毒及惡意軟體之攻擊。

第二十五條（作業人員之管理）

保險業應依下列原則管理負責電子商務作業之人員：

一、就資訊系統與人員之管理及權責分工訂定相關作業辦法，並與員工簽署書面約定及定期宣導，以提醒員工注意。

二、訂定人員違反資訊安全規定之處理程序，並明訂交易資料授權處理層級。

三、作業人員應定期接受有關資訊安全之訓練，並作成紀錄。

第二十六條（委外處理電子商務應注意之原則）

保險業辦理電子商務，如有依據保險業作業委託他人處理應注意事項辦理時，應遵循下列原則：

一、事先研擬委外服務計畫書。

二、慎選具有足夠安全管理能力及經驗之廠商作為委辦對象。

三、事前審慎評估可能潛在之各項風險。

四、與委外廠商簽訂適當的資訊安全協定及課予相關安全管理責任，並納入契約條款。

五、逐年檢討評估委外廠商之履約情形，如有未履行或未達約定之服務水準者，應要求檢討改進，必要時得終止部分或全部契約，並依法追究其責任。

第二十七條（安全稽核應包含之項目）

保險業之電子商務安全稽核，應至少包含下列項目：

一、是否留有足供安全稽核之記錄資訊。

二、是否已建立防範不法入侵之機制。

三、是否已建立安全修復機制。

四、是否有定期更新修補程式。

五、　　是否已建立警示系統，對於安全違例事件的發生能立即採取有效防範措施。

第二十八條（客戶申訴與抱怨處理）

保險業應依第五條第二項第八款設置專人處理消費者申訴與抱怨，且對消費者之申訴與抱怨應積極進行處理，並在適當時日內迅速給予消費者妥適回覆。

保險消費爭議或糾紛發生時，保險業應妥適處理。

第二十九條（保險犯罪通報）

保險業經營保險電子商務，若發現有疑似保險犯罪情事，應即通報財團法人保險犯罪防制中心。

第三十條（定期調整修正事項）

為因應網路之發展與進步，保險業應定期審視本自律規範內容進行調整修正，以維護消費者信心，健全保險電子商務發展。

第三十一條（納入內控內稽事項）

各會員公司辦理保險電子商務，應將本自律規範內容納入內部控制及內部稽核項目，並依據保險業內部控制及稽核制度實施辦法規定辦理。

第三十二條（施行程序）

本自律規範由中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會共同訂定，經各該公會理事會通過，並報請主管機關備查後施行；修正時亦同。