

富邦產物保險股份有限公司 內部控制制度聲明書

本公司 113 年 1 月 1 日至 113 年 12 月 31 日之內部控制制度，依據自行檢查之結果，謹聲明如下：

- 一、本公司確知建立、實施和管理內部控制制度係董事會及管理階層之責任，本公司業已建立此一制度。內部控制制度之目的係在對營運、財務報導及法令遵循等目標之達成，提供合理之確保。營運之目標係在追求營運之效果及效率，包括獲利、績效及保障資產安全等目標；財務之報導目標係在追求對外之財務報導為可靠；法令遵循之目標則在追求相關法令之遵循。法令遵循制度係達成法令遵循目標內部控制制度之一部分；財務紀錄及報表係依保險法及相關規定編製、編製基礎前後一致，且係財務報導內部控制制度之部分成果。
- 二、內部控制制度有其先天限制，不論設計如何完善，有效之內部控制制度亦僅能對上述三項目標之達成提供合理之確保；而且，由於環境、情況之改變，內部控制制度之有效性可能隨之改變。惟本公司之內部控制制度設有自我監督之機制，缺失一經辨認，本公司即採取更正之行動。
- 三、本公司係依據金融監督管理委員會訂頒保險業內部控制及稽核制度實施辦法(以下簡稱「實施辦法」)之規定判斷本公司內部控制制度之設計及執行是否有效，上項判斷之作成亦依據「實施辦法」規定之內部控制制度有效性之判斷項目。內部控制制度劃分為五個組成要素：1. 控制環境，2. 風險評估，3. 控制作業，4. 資訊與溝通，及5. 監督作業。每個組成要素又包括若干判斷項目，前述項目請參見「實施辦法」之規定。
- 四、本公司業已採用上述內部控制制度判斷項目，檢查內部控制制度設計及執行之有效性。

- 五、本公司基於前項檢查結果，認為上開期間之內部控制制度(包括營運、財務報導、資訊安全整體執行情形及法令遵循)之設計及執行係屬有效，除附表所列事項外，能合理確保董事會及經理人業已知悉營運目標達成之程度、財務報導及法令遵循目標業已達成；亦認為財務紀錄及報表係依保險法及有關規定編製，編製基礎前後一致，其正確性係允當。
- 六、本聲明書將成為本公司年報及公開說明書之主要內容，上述公開之內容如有虛偽、隱匿等不法情事，將涉及證券交易法第二十條、第三十二條、第一百七十一條、第一百七十四條或保險法等相關規定之法律責任。
- 七、本聲明書業經本公司 114 年 3 月 12 日董事會通過。

此致

金融監督管理委員會

聲明人：富邦產物保險股份有限公司

董事長：許金泉



(簽章)

總經理：賴榮崇



(簽章)

總稽核：何俊霖



(簽章)

總機構法令遵循主管：李慧玲



(簽章)

資訊安全專責單位主管：王皓正



(簽章)

中 華 民 國 114 年 3 月 12 日

附表

富邦產物保險股份有限公司
內部控制制度應加強事項及改善計畫
(基準日：113 年 12 月 31 日)

應 加 強 事 項	改 善 措 施	改善執行情形
無		

「113 年資訊安全整體執行情形」說明

說明：

- 一、113 年資訊安全整體執行情形為依據「保險業內部控制及稽核制度實施辦法」第六條之一規定，保險業資訊安全專責單位負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情形，由資訊安全專責單位主管與第二十五條第一項人員聯名出具內部控制制度聲明書，提報董（理）事會通過。
- 二、富邦產險資訊部確實遵循「保險業內控制及稽核制度實施辦法」第六條、第六條之一規定，及同業公會所定資訊安全自律規範。經審慎評估後，113 年度資訊安全整體執行情形，摘述如下：
 - （一）強化資安教育訓練以及提昇員工資訊安全意識：
資安專責人員(共 5 員)分別於 113 年已接受超過 15 小時資安專業課程訓練；
另對於產險同仁每季配合聯合宣導進行資安教育訓練以及由人資部協辦四門線上資安教育訓練課程，累積時數 4 個小時已滿足規範要求 3 小時以上。
 - （二）辦理 113 年度電腦系統資訊安全評估，執行期間：113 年 8 月至 113 年 12 月，標的為第一類資訊系統，並於 113 年 12 月 26 日產出總結報告，後續將依「保險業電腦系統資訊安全評估作業原則」於 114 年 3 月底前上簽總經理核決。
 - （三）113 年行動 APP 資安檢測目標應完成第一類共 2 支行動應用程式(APP)檢測，已於 113 年 12 月前通過資安檢測。行動應用程式(APP)清單如下：
 1. 富邦產險(Android)
 2. 富邦產險(IOS)
 - （四）資訊安全事件演練：
 1. 配合風險管理部於 113 年 11 月 19 日完成 113 年惡意程式擴散攻擊事件暨個資外洩演練，並由總經理核決。
 2. DDoS 攻防演練於 113 年 9 月 19 日執行，由中孚科技擔任攻方、台灣大哥大擔任 DDoS 清洗系統(守方)、富邦產險 IT 單位為服務監控單位，演練期間所有攻擊皆能完整阻擋，且無影響服務，後續已由總經理核決。

3. 金控和產險於113年共執行4次電子郵件社交工程演練，針對不合格人員進行額外教育訓練及考試以達演練效果。
4. 由金控主辦之113年紅藍隊演練，其標的為各子公司外部網站或網路邊界等，以能取得資料庫資料(如個資)、帳號控制權等為目標期間從113年11月5日到114年1月7日止，演練結果針對產險部分之風險，已陸續進行修補。