資訊安全風險管理架構

<資訊安全政策>

基於第一產物保險股份有限公司（以下簡稱本公司）的業務特性，為維護客戶、股東及公司之權益，本公司及全體同仁有責任和義務，共同建立及維護一個安全的資訊與通訊作業環境，讓資訊安全成為企業文化的一環，本公司已成立資訊安全委員會並訂定資訊安全政策以明確定義安全目標與安全要求，以資遵循。

為落實資安防護作業，提升人員資安防護意識及資安專業技能，每年於董事會報告資安整體執行情形;本公司資安專責單位主管已於 110 年 3 月 26 日董事會提出 109 年資訊安全整體執行情形聲明書，並已針對應加強事項辦理改善措施。

<組織與分工>

本資訊安全管理委員會由資源群最高主管擔任召集人,管理部最高主管擔任副召集 人，並指派一名執行祕書，負責資訊安全管理委員會各項協調工作。各險部與資訊 安全相關部門均應指派代表加入資訊安全管理委員會，並將人員名冊列在資訊安全 組織名冊。

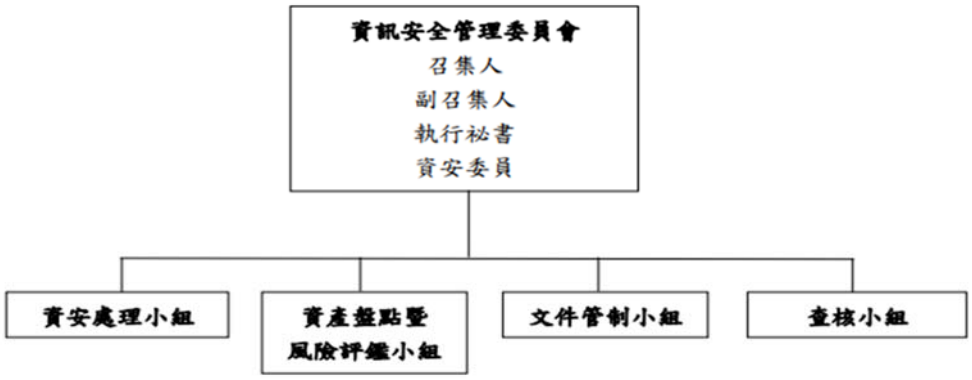

圖 1：資訊安全組織架構圖

<執行資訊安全管理機制>

訂定控制措施，包括負責人員、程序、步驟以及紀錄之留存，發行並實施控制措施。

(一)人力資源安全管理

人力資源安全管理請參照「人力資源安全管理程序書(ISMS-L2-07)」相關規定辦理。

(二)實體與環境安全管理

實體與環境安全管理請參照「實體安全作業說明書(ISMS-L3-01)」相關規定辦理。

(三)通訊與作業安全管理

系統與網路安全管理請參照「系統與網路安全作業說明書(ISMS-L3-03)」相關規定辦理。

(四)存取控制安全管理

資訊系統存取控制安全管理請參照「存取控制作業說明書(ISMS-L3-02)」相關規定辦理。

(五)系統開發及維護安全管理

系統開發及維護安全管理請參照「系統開發與維護作業說明書(ISMS-L3-04)」相關規定辦理。

(六)委外管理

有辦理資訊委外業務，應於規劃時，參考「資訊系統委外作業說明書(ISMS-L3-08)」納入合約執行。

(七)資訊安全事件處理機制

資訊安全事件處理機制請參照「資安事件通報管理程序書(ISMS-L2-09)」相關規定辦理。

(八)營運持續管理

營運持續管理請參照「營運持續管理程序書(ISMS-L2-08)」相關規定辦理。

(九)溝通及傳輸

為使本公司之需求、目標能有效地傳遞到與本公司業務相關之關注方(如：民眾、上級單位、其他連結機關、本公司同仁及廠商)，本公司利用媒體、函文、會議、官網、電子郵件等途徑，進行彼此關注議題討論、溝通，於必要時邀請雙方主管參與，並保留討論、溝通之議題、地點、時間、參與人員、決議方式與結果等紀錄做為後續之依據。

(十)專案管理之資訊安全

為避免專案運行過程中不當的設計、規劃、操作影響到本公司資訊資產之機密性、完整性及可用性。應於專案活動中納入資訊安全考量，防範發生危害資訊安全之情況。專案活動參與執行的對象可分為內部人員與外部人員：

1.內部人員：

本公司內部人員於執行各項專案活動時應遵循資訊安全管理制度，避免影響到本公司資訊資產之機密性、完整性及可用性。

2.外部人員：

委外廠商、駐點人員皆屬外部人員。應於合約中要求遵守本公司「資訊系統委外作業說明書(ISMS-L3-08)」之規定。