南山人壽保險股份有限公司
資訊安全政策

中華民國 103 年 11 月 4 日訂定
中華民國 108 年 3 月 21 日修訂
中華民國 111 年 3 月 29 日董事會修訂
中華民國 114 年 8 月 28 日董事會修訂

第一條 目的

為確保本公司各項資訊資產於營運及服務提供流程中之機密性、完整性、可用性與適法性，避免遭受內、外部蓄意或意外之威脅，採用「規劃-落實-檢查-行動」的持續改善管理模式，建立符合相關法規要求之資訊安全管理，特訂定本政策。

第二條 適用範圍

適用於資訊使用者所執行之資訊作業活動。

第三條 名詞定義

本政策名詞定義如下：

一、 機密性：

使資訊不可用或不揭露給未經授權之個人，確保只有經授權之人員才可以存取資訊。

二、 完整性：

保護資訊的準確度和完整，確保使用之資訊正確無誤、未遭竄改。

三、 可用性：

經授權個人因應需求而需存取或使用資訊時，確保其得以取得資訊及相關服務。

四、 適法性：

各項資訊作業活動依據主管機關相關法令規定辦理。

五、 資訊資產：

包含資訊系統、軟體、硬體、環境、文件、通訊、資料、人員等。

六、 資訊使用者：

經授權使用或管理資訊資產之相關人員，包含但不限於本公司所屬職員、業務員、約聘僱用人員、供應商(如：建置維護廠商、資訊作業委外廠商、雲端服務提供者）等。

第四條 政策遵循

資訊使用者均應遵循本政策。

第五條 遵循事項

一、資訊安全政策聲明事項如下：

(一) 本公司依據主管機關相關規範，建構資訊安全管理制度，透過定期審查與內外部稽核機制，確保持續性改進並強化對本公司資訊資產(包含不限於資訊系統、軟體、硬體、環境、文件、通訊、資料....等)之安全控管。

(二) 資訊使用者應透過適當程序落實本政策之要求，負有維護資訊安全之責任，且應遵守相關之資訊安全管理規範。

(三) 資訊使用者使用本公司之各類資訊資產應盡保密之義務，並遵守本政策及相關程序之規定。

(四) 本公司與有業務往來之資訊作業供應商（如：資訊作業委外廠商、雲端服務提供者等）制定資訊安全標準與相關合約條款，透過進行資安審查或稽核，確保其遵循本公司資安政策，保障資訊安全供應鏈之完整性，供應商應遵循下列事項：

1. 應遵守保密責任與法令法規要求。
2. 應就提供給本公司之服務採取適當的安全維護必要措施。
3. 發生資訊安全事故造成本公司損害應負擔之賠償責任。
4. 服務中止時，應進行轉移、刪除及銷毀作業。

(五) 本公司採取嚴格措施保護個人資料、財務資訊及內部營運數據，避免未經授權之存取、變造或洩漏，並符合法令如《個人資料保護法》與金融監理規範。

(六) 本公司與供應商對潛在之資訊安全弱點或威脅，應隨時保持警戒，並依《資訊安全事件通報暨管理程序》，透過適當通報機制，回報所發現之資訊安全事件及相關弱點。

(七) 本公司若有發生資訊安全事件或屬重大偶發事件時，應依《資訊安全事件通報暨管理程序》與《南山人壽保險股份有限公司重大偶發事件之處理規定》規定辦理，並秉持資訊透明原則，適時向受影響之利害關係人說明事件狀況、處置作為與後續改善措施。事件處理完畢後，應進行全面檢討評估脆弱性，以強化防範機制、降低再發生的風險。公司並可視情節輕重對事件相關人員進行懲處及評量，或訴諸法律行動。

二、為落實資訊安全管理與資料生命週期之保護，本公司應採取以下資訊安全控制措施：

(一) 識別資料、資訊以及相關存取權限，建立適當之存取原則。

(二) 定期辦理資訊資產風險評估與管理。

(三) 落實重要資訊與紀錄備份與管理。

(四) 維護工作區域場所以及營運設備之安全，確保其免於損害致使組織的作業中斷。

(五) 確保正確及安全的操作資訊設備。

(六) 訂定業務持續運作計畫且定期演練，並配合業務發展與組織現況持續調整更新。

(七) 落實通訊安全之管理。

(八) 資訊系統之取得、開發與維護，須符合並遵循本公司相關規範。

(九) 落實對資訊服務供應商之管理。

(十) 遵循內外部相關法令規定，建立應有之管控程序，定期執行資訊安全查核作業。

(十一)定期實施資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

三、公司應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務，每年於董事會報告資安整體執行情形，且應設置具職權行使獨立性之資訊安全專責單位，並指派協理以上或職責相當之人擔任資訊安全專責單位主管，負責規劃、監控及執行資訊安全管理作業，並配置適當人力資源及設備。資訊安全專責單位人員負責執行資訊安全專責單位主管所指派之資訊安全管理作業任務。

四、本政策依據主管機關及法令對資訊安全之要求或科技之變動，定期(每年至少一次)檢視或視實務需要修訂，確保資訊安全管理運作之可行性與有效性。

五、本政策倘有未盡事宜，悉依相關法令及中華民國人壽保險商業同業公會發布之自律規範及本公司訂定之相關規範辦理。前開法令或自律規定如有就本政策所規範事項為修訂，雖本政策尚未配合修訂者，仍依最新法令或自律規範之規定辦理。

第六條 施行

本政策經董事會核准後發布施行，修訂時亦同。

文件版本修改紀錄

修訂序號	修改詳情	版本號	編訂者	修訂日期
1	初訂發行	1.0		103.11.04
2	本政策修訂需經董事會核准。	2.0		108.03.21
3	本公司指派副總經理以上或職責相當之人兼任資訊安全長	3.0		111.03.29
4	配合DJSI道瓊永續指數 / 企業永續評鑑 1.8.2 要求做調整	4.0		114.08.28