遠雄人壽保險事業股份有限公司

資訊安全管理政策

管轄單位：資訊室
民國 104 年 8 月 21 日董事長核准新訂定
管轄單位：資訊管理部
民國 107 年 8 月 31 日董事長核准修正
民國 109 年 11 月 20 日董事長核准修正
民國 110 年 10 月 28 日董事會審議通過修正
民國 112 年 9 月 21 日董事會審議通過修正

第一條 遠雄人壽保險事業(股)公司(下稱本公司)基於「客戶滿意、公司獲利、員工忠誠、股東認同、社會肯定」的企業責任，並確保本公司資訊及通訊系統、設備及資訊資產之安全，提升同仁對資訊安全之認知，保障客戶權益，並達成「永續經營」的企業精神，特訂定本政策。

資訊安全整體目標在確保資訊資產之機密性、完整性及可用性，防範本公司營運受到資訊安全事件之衝擊。

第二條 本政策用詞，定義如下：

- 一、 資訊系統(Information and communication system)：係指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統，泛指具備資訊或通訊處理能力之系統。
- 二、 資訊資產：係指與本公司資訊作業相關的有價值的資訊系統及其所含的資訊資產(如軟體、硬體、文件、資料、服務及人員等)。
- 三、 核心業務：指包含但不限於核保出單、保全(批改)、理賠、保費相關之業務種類。
- 四、 核心資訊系統：指支持核心業務持續運作必要之資訊系統。
- 五、 資訊安全：指防止資訊資產遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
- 六、 資訊安全事件：指資訊系統、服務或網路狀態經鑑別而顯示可能違反本政策或保護措施失效狀態的發生，並影響資訊系統運作，構成本政策之威脅。
- 七、 機密性(Confidentiality)：確保只有經授權的人才可以存取資訊資產。
- 八、 完整性(Integrity)：確保資訊資產的內容與處理方法是正確且完整的。
- 九、 可用性(Availability)：確保經授權的使用者在需要時，可以存取資訊資產。

第三條 適用範圍包含本公司各項資訊資產、全體員工(含約聘雇人員、工讀生)、及受本公司委託處理資訊業務之廠商(含其受僱人、使用人或代理人等)皆應遵守，且應以適當方式告知。

辦理資訊系統建置、維運或資訊服務提供前，需求單位會將資訊安全相關因素或風險納入評估，如有委外廠商，亦會明定其資訊安全責任、保密協議，並納入合約，俾利廠商遵循。

- 第四條 資訊安全之整體目標在確保資訊資產之機密性、完整性及可用性，防範本公司營運受到資訊安全事件之衝擊，降低營運風險。
- 第五條 應落實資訊資產之盤點，依其重要性予以分類(級)和風險評估等作業，並針對該作業結果訂定安全管控機制適用性。
- 第六條 為維護資訊系統持續營運，本公司建立資訊系統持續營運計畫及資訊安全事件應變機制，並定期辦理核心資訊系統資訊安全事件演練。
如遇資訊安全事件發生，本公司人員應依相關規定進行通報及應變處理。
- 第七條 本公司依員工角色及職能為基礎，依人員業務類別辦理妥適資訊安全教育訓練或宣導，使各人員瞭解資訊安全重要性，俾利提高資訊安全意識並熟悉相關職責。
- 第八條 本公司應導入至少涵蓋以下領域的資訊安全管理制度，並視需要通過第三方驗證。
一、 資訊安全權責及分工推動組織(含諮詢小組)
二、 人員安全管理
三、 資訊資產盤點及安全管理
四、 網路及通訊安全管理
五、 存取權限控制安全管理
六、 系統開發及維運安全管理
七、 實體及環境安全管理
八、 營運持續運作安全管理
九、 供應商關係安全管理
十、 資訊安全相關規範遵循性管理
前開各項管理機制之評估、回應與監控等，由資訊管理部訂定相關適用性說明(含資安管理目標、管控措施原則等)，並由各部門依其經營的資訊系統特性，自行研擬資訊資產安全管控準則或執行規範，做為執行資訊安全之依據。
- 第九條 為強化本公司資安監理相關事宜，應遴聘「具資安背景之董事、顧問」或設置「資訊安全諮詢小組」，以提供本公司各單位資訊安全管理相關作業執行情形，或內外外部議題之建議或諮詢，帶動本公司重視資安的組織文化。
- 第十條 本公司應確實遵守包括但不限於「個人資料保護法」、「著作權法」等相關法令(規)及本公司資訊安全相關規定，以確保適當使用本公司資訊系統及資訊資產。
- 第十一條 資訊管理部每年檢視本政策，或於發生重大變動時重新檢視，以符合資訊安全相關法令、技術、組織及營運之最新發展趨勢，並於每年第一季提報前一年度本公司資訊安全整體執行情形於董事會審議。
- 第十二條 本政策經董事長核准，並提報董事會同意後實施，修正時亦同。