保誠人壽保險股份有限公司資訊公開說明文件

項　　目：資通安全管理

更新日期：115/03/27

更新週期：年度終了三個月

維護單位：資訊安全暨營運持續風險

PCA Life Assurance Co., Ltd. 8/F, No.1 Songzhi Rd., Taipei 11047, Taiwan (R.O.C.)
保誠人壽保險股份有限公司 11047台北市信義區松智路1號8樓
Tel (02)8786-9955 www.pcalife.com.tw 0809-0809-68

保誠人壽保險股份有限公司資訊公開申報表

表4-26 資通安全管理

申報年度 114

項目	申報內容
敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。	1.資通安全風險管理架構： 本公司依據董事會核准之「保誠人壽風險管理政策(PCALT Risk Framework)」推動風險管理，涵蓋「資訊安全政策」以指導並要求資訊安全相關事務。組織面設有資訊安全暨營運持續管理委員會，由風控長擔任主席綜理資訊安全政策推動、督導及資源調度等事務，並設置資訊安全專責單位與主管(資訊安全暨營運持續風險部，編制含專責主管1人與單位人員6人)，負責規劃、監控及執行資訊安全管理作業，資訊科技轄下部門負責資安作業之規劃、執行及資安技術作業。每年將前一年度資訊安全整體執行情形，由董事長、總經理、總稽核、總機構法令遵循主管及資訊安全專責單位主管聯名出具內部控制制度聲明書，提報董事會通過。 2.資通安全政策： 本公司已訂定「資訊安全政策」，為確保資訊安全之有效管理，以符合法規、集團等相關要求，除依據資訊安全政策授權訂定之「資訊安全暨營運持續管理委員會組織章程」設有跨部門成員代表參與之委員會，負責決策、指導、監督及推動全公司資安事務，同時依循國際資訊安全標準建立完整之管理制度體系，包含風險管理、教育訓練、法令遵循、事件與事故、矯正與改善及涵蓋各控制領域等管理規範，以供全公司遵循、落實相關規定並達成整體資安治理之目的。 3.具體管理方案及投入資通安全管理之資源： (1)資安治理 本公司藉由領導、規劃及控制組織之資訊安全流程，確保與各階層人員進行有效溝通，遵循與維繫「規劃（Plan）、執行（Do）、檢查（Check）、行動（Act）」之運作與持續改善模式，深化公司資訊安全管理制度作業。辦理包含至少每年一次資訊安全暨營運持續管理委員會會議、持續通過國際標準認證、資訊資產盤點作業、風險評鑑作業、資安內部查核作業、資安制度與規章修訂等各項活動，並參考「金融業導入零信任架構參考指引」，研討零信任網路導入評估與規劃，持續辦理相關作業。 (2)第三方獨立認證、評估及檢測作業 本公司每年委由外部第三方獨立機構，協助進行下列各項認證、評估及檢測作業： a.已導入國際資訊安全管理系統(ISO 27001)與個人資料管理系統(BS 10012)雙認證，並辦理第三方驗證作業，持續維持有效之國際證書。 b.完成電腦系統資訊安全評估作業，藉由外部評估建議及執行改善作業，確保資安制度與防護之完整度與有效性。 c.公司行動裝置應用程式(APP)通過安全檢測，符合經濟部工業局「行動應用App基本資安檢測基準」規範之安全要求。 (3)系統復原與資安防護演練 a.辦理年度資訊系統災害復原演練(IT DR Drill)，驗證重大災變情境下，各主要關鍵系統之復原結果。 b.辦理年度阻斷服務攻擊(DDoS)演練，於遭受一定程度攻擊時可維持對外網站可用性。 (4)認知與教育訓練 a.辦理年度社交工程詐騙郵件演練，持續透過定期演練與宣導提高同仁警覺。 b.採用線上訓練辦理全公司資安宣導課程，資安專責人員亦完成專業訓練課程，強化全公司安全意識與累積專業能量。 (5)持續建構並強化資安技術面防護 a.導入並更新靜態程式碼掃描工具，強化軟體開發生命週期之安全測試機制。 b.導入與強化電子郵件網域驗證及偵測處理機制，降低公司電子郵件網域遭盜用寄送偽冒電子郵件之相關風險。 c.強化網際網路應用程式介面(API)安全防護機制，提升API運作安全，降低資料外洩與被攻擊風險。
列明最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實及原因。	114年度未發生重大資通安全事件，公司持續強化前述各項資通安全防護機制，以降低重大資通安全事件發生機率與風險。
資通安全風險對公司財務業務之影響及因應措施。	近年來金融業偶有遭遇重大駭客攻擊或發生資料外洩事故，如：金融機構遭DDoS攻擊、保險業資訊服務或商業服務相關供應鏈遭勒索軟體或駭客攻擊等資安事件，在社會上與業界造成廣泛的討論與檢討。現今消費者、政府機關及企業均甚為重視資訊安全威脅，如若公司因遭受資安攻擊而導致外洩1,000筆客戶資料之重大資安事件，除造成客戶的權益受損與本公司商譽損失外，若客戶提起訴訟，可能之財務損失影響約為新台幣2,000萬元(依據個人資料保護法，當事人不能證明其實際損害額時，以每人每一事件新臺幣二萬元以下計算；單一案件賠償上限為新台幣二億元)及主管機關裁罰等。故為了降低資通安全風險，本公司持續強化防護機制，並與外部資安顧問專家合作，由內、外部檢視並優化資訊安全管理與個資保護機制等，同時定期實施各項資安測試、人員訓練及演練，以加強整體資訊安全防護及應變能力。

申報頻率

除主管機關另有規定外，應於年度終了後三個月內更新。

附註一

本表單係配合111年5月25日發布修正之「財產保險業辦理訊公開管理辦法」及「人身保險業辦理資訊公開管理辦法」第8條第3項第2款規定而新增，自111年終了後三個月內開始申報。