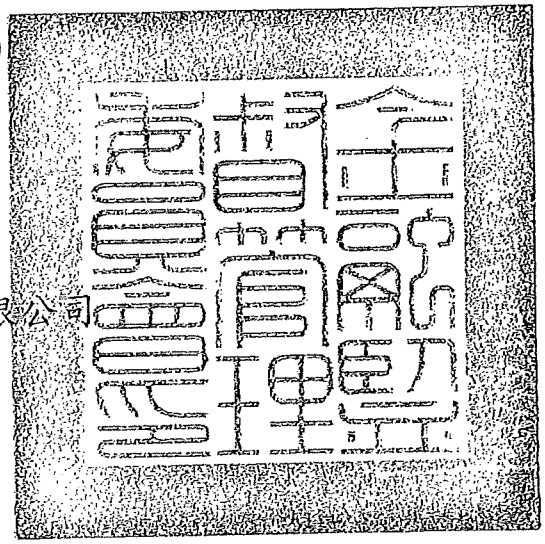
正本

檔　　號：
保存年限：

金融監督管理委員會　處分書

受文者：合作金庫人壽保險股份有限公司(代表人杜振遠先生)



發文日期：中華民國108年8月30日
發文字號：金管保壽字第10804949372號
速別：普通件
密等及解密條件或保密期限：密(發文後解密)
附件：

裝

相對人：合作金庫人壽保險股份有限公司
公司代表人：杜振遠先生
出生年月日：民國43年7月25日
性別：男
身分證統一號碼：F10370****
地址：臺北市大安區忠孝東路四段325號10樓

主旨：有關本會對貴公司電子商務專案檢查報告(編號：107F140)所列缺失事項，查貴公司有違反保險法相關規定之情事，應依保險法第149條第1項規定予以7項糾正。

訂

事實及理由：

一、檢查意見二、(三)，貴公司所訂「硬體及系統軟體之購置、使用及維護之控制作業手冊」規定「1.屬高風險弱點一個月完成。2.屬中風險網路及網頁滲透測試弱點掃描於三個月內完成。」，惟查有未落實依內規辦理者，如：依委託APAC每月辦理對外網站之弱點掃描作業追蹤紀錄表，有編號150161、150162、150022及150124等分別於106.11-107.4發現之中風險弱點均已逾3個月，惟迄107年10月仍未修補；107年1月發現伺服器之1項高風險弱點(IBM WebSphere Java Object Deserialization RCE)迄107.6始完成改善，不利電腦系統安全，核有礙健全經營之虞。

線

二、檢查意見二、(五)，貴公司部分伺服器最高權限帳號有未收回納管之情形，如：合庫人壽官方網站系統、電銷系統

(Telemaster)、IT需求單處理系統(ITRMS)等，與所訂「資訊資產保護注意事項」中「...最高權限密碼函應指定專人負責製作，彌封緊急密碼函中保管，並保管於上鎖設備裏。」，核有礙健全經營之虞。

三、檢查意見二、(六)貴公司電子商務系統及XO壽險核心系統相關伺服器主機安全設定作業，有下列事項欠妥，核有礙健全經營之虞，如：

(一)部分伺服器各項稽核原則均設定為「沒有稽核」，致未留存相關稽核紀錄，不利系統安全，如：電子商務系統WEB、OTP、DB主機及XO壽險核心系統資料庫主機等。

(二)未設定最小密碼長度及不得與前幾次密碼相同，與所訂「密碼設定、傳遞與變更原則」中「密碼長度至少6碼，不得與前3次相同。」規定不符，如：電子商務系統OTP、DB主機及XO壽險核心系統資料庫主機。

(三)帳號密碼設定為永久有效，與所訂「資訊安全管理規範」中「使用者須經常更改密碼(以最少每三個月更改一次為原則，最長不宜超過六個月)」規定不符，如：電子商務系統WEB主機、OTP主機及DB主機帳號等。

(四)有使用者帳號已無業務需求仍未刪除或設定多餘之本機登入功能，易致增加作業風險者，如：電子商務系統WEB主機帳號pwsadmin(僅為排程指定帳號以控管執行時權限)及PWS_FTP(僅供FTP傳檔用)無須本機登入功能；電子商務OTP主機帳號OTPAdmin無人使用；電子商務AP主機帳號apdebuguser1無人使用、pwsadmin(僅為排程指定帳號以控管執行時權限)無需本機登入功能；XO壽險核心系統資料庫帳號ALVIN，VOICE、SPOTLIGT等無使用者。

(五)電子商務及XO壽險核心等系統相關主機中具管理者權

限之帳號tcbit，為系統開發及硬體維護之經辦人員共用，辦理日常維護作業，除違反最小授權原則，且與所訂「系統帳號及權限管理作業手冊」中「禁止使用通用帳號，每一個帳號都必須對應到一位指定人員」規定不符。

四、檢查意見二、(七)貴公司Oracle資料庫參數設定，有資料庫存取授權未符合最小授權原則，不利資訊安全，核有礙健全經營之虞，如：壽險核心系統資料庫(TPES075TP002及TPES075TP027)資料庫管理員日常登入使用帳號(TCB_HANKHUANG)擁有EXP_FULL_DATABASE(匯出資料庫)、IMP_FULL_DATABASE(匯入資料庫)等高權限；電子商務資料庫(TPES075TP028)資料庫管理員日常登入係使用系統最高權限帳號SYS；對非資料庫管理員之使用者帳號TCB_GEORGECHANGCHIEN授予XO壽險核心系統資料庫(TPES075TP002及TPES075TP027)及電子商務資料庫(TPES075TP028)最高權限等。

五、檢查意見三、(一)貴公司對存放客戶個資檔案之共用檔案伺服器，有將存有客戶個資(包含姓名及身分證字號，且有財務或聯絡資料等欄位)之檔案，設定為全部網域使用者代號均可讀取之情形，如：\sms\JV TA_PEP List_20170605、\xo\Personal\Share\All\TM\201803\812\Tmr_daily_data_detail及\joda_ftps\From PMC\KHT\Rita\Offshore_income_data_main等，且未設計留存對共用檔案伺服器之存取稽核軌跡，不利個資安全，核有礙健全經營之虞。

六、檢查意見四、(二)貴公司辦理資料異動相關作業，有下列事項欠妥，核有礙健全經營之虞，如：

(一)貴公司所訂「資料處理作業程序」僅規範「資料進行變更，須建立控管程序並經權責主管授權核准後方可執

行，資料變更前視需要適度備份，應留有變更紀錄或軌跡，並檢視異常狀況進行追蹤與矯正，以確保資料的正確性與完整性。」，未明定相關權責分工、測試程序、必要檢附檔案文件、留存軌跡及覆核機制等事項，不利作業遵循。

(二)貴公司辦理資料異動係系統維護人員輸入正式環境帳號及密碼後，交由程式人員進行後續資料異動，不符分工牽制原則。

(三)貴公司辦理資料異動係以人工方式啟動側錄工具，對操作行為進行側錄，致有側錄缺漏、資料異動留存軌跡不完整之情形，如：依ITRMS需求管理系統查詢統計107年1月至10月，約有完成450筆資料異動需求單，惟系統僅留存23筆側錄資料，有缺漏之情形。

(四)貴公司資料庫稽核軌跡留存不完整，如：有權限異動核心資料庫之帳號未納入監控範圍；107.2.9至107.11.16稽核軌跡異常，無帳號維護監控紀錄；另未產生相關管控報表供主管覆核。

七、檢查意見四、(四)貴公司網路投保系統、網路保險服務系統及「合作金庫人壽」行動裝置應用程式之功能及安全性設計，有下列事項欠妥，核有礙健全經營之虞，如：「合作金庫人壽」行動裝置應用程式未建立可信任憑證清單及驗證完整憑證鏈，亦未建置偵測行動裝置疑似遭破解(root或jail- break)，並提示使用者系統遭破解可能面臨風險之功能，安全性欠妥。

法令依據：

一、上述事實一，違失事實明確，依保險法第149條第1項規定，予以糾正。

二、上述事實二，違失事實明確，依保險法第149條第1項規定，予以糾正。

三、上述事實三，違失事實明確，依保險法第149條第1項規定，予以糾正。

四、上述事實四，違失事實明確，依保險法第149條第1項規定，予以糾正。

五、上述事實五，違失事實明確，依保險法第149條第1項規定，予以糾正。

六、上述事實六，違失事實明確，依保險法第149條第1項規定，予以糾正。

七、上述事實七，違失事實明確，依保險法第149條第1項規定，予以糾正。

正本：合作金庫人壽保險股份有限公司(代表人杜振遠先生)
副本：金融監督管理委員會檢查局、保險局

主任委員　顧　立　雄

授權單位主管決行