缺失態樣

客戶資料之安全維護有未臻妥適之情形。

缺失情節

- 對個資外洩之應變演練，尚未就外部網路入侵及非法或異常使用行為所致之個資外洩情境，研擬演練計畫並定期演練及檢討改善。
- 員工使用電子郵件傳遞資料，尚未建立檢核所傳送之資料檔是否含有個人資料之控管機制，或過濾篩選原則不含帳號、電子郵件，有欠周延。
- 核心主機系統存有大量個資檔案，惟存取權限設定過於寬鬆，不利個資保護。
- 資料檔案之存出或寫入均使用「非加密註冊型隨身碟」，不利機敏資料檔案之管控。

改善作法

- 應依規辦理個資外洩之應變演練，設計合宜妥適之情境，並定期演練及檢討。
- 對員工使用電子郵件傳遞資料，應利用程式或工具軟體進行檢查及偵測是否含有個人資料，且過濾原則應具有完整性，以防範客戶個人資料遭不當使用。
- 應檢討存取權限設定之妥適性，以維個人資料安全。
- 應使用加密型隨身碟，並建立可攜式儲存媒體使用管理機制，每日產製使用紀錄之控管報表及建立覆核機制。

缺失態樣

個人資料透過網際網路或電子郵件傳遞，未建置完善之加密通訊保護機制。

缺失情節

- 對外提供服務網站之網頁，有蒐集、處理個人姓名、性別及聯絡方式等個資，惟於網際網路傳輸時未妥善加密處理，易致個資外洩。
- 以電子郵件傳送個人資料，未加密處理，易致個資外洩。
- 已建置電子郵件稽核系統管理對外寄送含一定筆數個資之電子郵件資料偵測作業，惟對未達所設定之數量或無法判讀之加密檔、圖檔等，則未加以檢核或採取其他補強措施，逕予以寄送。
- 將正式作業主機之個資檔案及資料庫複製至開發測試主機作業，未將個資資料予以去識別化。

改善作法

- 對以網路或電子郵件傳送個資檔案至外部單位，應建立加密通訊保護機制，強化檔案傳輸之安全性，俾確保個人資料之安全防護。
- 應對含有個人資料之外寄電子郵件，設定妥適過濾原則及安全控管政策，建立定期檢視機制，確實將個人資料完整納入系統設定之過濾原則，針對附件為加密檔、圖形檔等無法辨識過濾之電子郵件，建立事前審核檔案傳輸之管控機制。
- 應重新檢視複製正式主機檔案及資料庫至測試主機去識別化作業程序之妥適性，避免將客戶真實資料複製至測試環境作業，如確有須將未去識別化個資複製至測試環境之業務需求，除應建立申請、刪除、留存完整稽核軌跡之控管機制外，並應嚴格管理該等資料檔案之存取權限。