使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上者應採取之資訊安全措施相關說明

一、依據內政部指定地政類非公務機關個人資料檔案安全維護管理辦法第16條規定：「非公務機關使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上者，應採取下列資訊安全措施：一、使用者身分確認及保護機制。二、個人資料顯示之隱碼機制。三、網際網路傳輸之安全加密機制。四、個人資料檔案及資料庫之存取控制與保護監控措施。五、防止外部網路入侵對策。六、非法或異常使用行為之監控與因應機制。前項第五款及第六款所定措施，應定期演練及檢討改善。」是以，公司（商號）有使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上之情形者，該資通訊系統應至少有上開六項資訊安全措施。

二、為利實作，爰參考《資通安全責任等級分級辦法》（附表十）資通系統防護基準就上開6項資訊安全措施說明如下，以供公司（商號）之資訊人員，或資通訊系統之建置廠商參考：

資通系統防護基準實作說明

項目	資訊安全措施	實作說明
一	使用者身分確認及保護機制	系統應建立帳號管理機制，包含帳號申請、建立、修改、啟用、停用及刪除之程序，並執行身分驗證管理，如身分驗證資訊不以明文傳輸、密碼複雜度或帳號鎖定機制等。
二	個人資料顯示之隱碼機制	系統界面呈現個人資料時，應以適當且一致性之隱碼或遮罩處理，以避免過多且非必要之個人資料揭露，可參考 CNS 29191「資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項」國家標準。
三	網際網路傳輸之安全加密機制	個人資料傳輸時，應採用傳輸加密機制，如採用加密傳輸通道、使用公開、國際機構驗

		證且未遭破解之演算法。
四	個人資料檔案及資料庫之存取控制與保護監控措施	儲存於電子媒體及資料庫之個人資料，應適當加密保護，並提供使用者識別、鑑別及身分管理，並採用最小權限原則進行存取控制管理。
五	防止外部網路入侵對策	針對外部入侵之防禦，應採用適當資安控制措施建立防禦縱深，包括防毒軟體、防火牆、入侵偵測與防禦系統，及應用程式防火牆等。
六	非法或異常使用行為之監控與因應機制	針對系統或個人資料檔案之存取，應確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件，且應留存系統相關日誌紀錄並定期檢視，或設置適當監控及異常行為預警機制。