上海商業儲蓄銀行資訊安全政策

資訊安全處擬定
107.11.10 訂定

第一條、**目的**

上海商業儲蓄銀行(以下簡稱本行)配合政府政策，提供社會大眾金融服務。為確保資訊資產之機密性、完整性、可用性及適法性，避免遭受內、外部蓄意或意外之威脅，爰導入國際資訊安全管理系統(ISO 27001)並參酌相關法令，根據本行之業務需求訂定本政策，以為執行之依據。

第二條、**權責**

本行全體員工、與本行有業務往來之供應商、資訊安全利害關係人等，皆應遵循本政策。如因違反本政策而導致本行權益受損需負相關責任。

第三條、**資訊安全治理目標**

一、確保本行資訊資產之機密性，落實安全存取公司資訊，資訊需經授權人員方可存取。

二、確保本行資訊作業處理方法之完整性，落實資料修改正確性，資訊需經授權人員方可修改。

三、確保本行資訊資產之可用性，維持本行資訊系統之持續運作，資訊安全需由裡到外全面防護。

四、確保本行資訊作業安全之作為符合相關法令規定要求，落實專業資安管理，保障安全的數位營運。

五、確保本行資訊安全環境符合國際金融資安評級，資訊安全需以風險為本持續優化。

第四條、**資訊安全治理策略**

為強化資訊安全治理目標，本行訂定以下之資訊安全防護基準相關控制措施，資訊安全處負責規劃、評估與監控政策及控制措施之執行成效：

一、成立資訊安全委員會，以督導及規劃全行資訊安全控制措施之執行。所有當責單位與人員之資訊安全責任應明確定義及分工並與相關單位、資訊安全利害關係人保持適當之溝通管道。

二、應實施符合主管機關要求之資訊安全教育訓練及宣導，確保員工均瞭解自身之資安責任，且能踐行其所擔任之角色。

三、應依資訊資產其價值、相關法令要求與對組織之重要性建立全行資訊資產清單；儲存媒體在傳遞過程中應受保護，以避免未經授權的存取、誤用或毀損。

四、應規範資訊與其處理設備、系統及應用程式的使用權限，以防未經授權的存取。

五、應建立密碼控制措施，維持適當且有效的密碼，以保護數位資訊之機密性、鑑別性及完整性。

六、應預防資訊本身及其處理設施遭未經授權的實體存取、破壞及干擾而造成企業營運中斷，所有設備報廢或再利用前應作檢查，確保任何的敏感資料及授權軟體均已被移除。

七、應將作業程序加以文件化，對開發、測試及營運環境進行分隔；建立對惡意軟體之偵測、預防、復原等控制措施，依循備份程序，定期進行各項資訊的備份與測試，隨時監控、調配各項資源的使用與系統技術弱點資訊，採取適當改善措施以降低風險。

八、應依使用者業務將網路加以區隔，以維護使用網路的系統與應用程式的資訊安全，建立資訊交換控制措施，維護行內與外部資訊交換的安全性。

九、系統開發或變更於開發週期內應受變更、測試程序控管，並

考量納入新興科技運用資訊安全相關要求，保護交易資訊，以防止不完整的傳輸、錯誤路由(mis-routing)、未經授權的訊息修改、揭露或複製；於測試階段應小心選擇、保護及管制測試資料以確保測試資料的安全性。

十、有關第三方存取、處理、儲存、通信或提供本行資訊處理基礎設施組成元件等資訊，應符合資訊安全要求，以確保第三方存取本行資產的安全性；並定期檢視、審查與稽核第三方交付的服務報告，若有服務變更情事，均依專案程序加以管理，並考量所涉及之時程、預算需重新評估，以維本行權益。

十一、應明訂管理責任與實施程序以確保對資訊安全事故做出迅速、有效的回應及通報，並識別、收集、取得及保存可用來作為證據的資訊，分析與解決以降低未來事故發生的可能性或影響。

十二、應確保資訊持續營運計畫應被包含在行方的持續營運管理體系中，以確保提供足夠的備援機制；定期驗證並實作資訊持續營運計畫，以確保其有效性。

十三、應定期查核資訊作業是否遵循組織資訊安全政策與標準，避免違反相關法令、法規或合約。

第五條、**評估週期**

本政策應考量政府法令規定、資訊技術及業務等最新發展現況，每年至少評估檢討一次，確保資訊安全作業之有效性。

第六條、**核定層級**

本政策經董事會核定後實施，修正時亦同。