全盈支付金融科技股份有限公司

資訊安全政策

目錄

第一條　目的

全盈支付金融科技股份有限公司(以下簡稱本公司)為專營電子支付之公司，鑑於電子支付機構應建立資訊安全政策、訂定資訊作業相關管理及操作規範、清點人員與設備資產、定義人員角色與責任並提供教育訓練，並為確保客戶個人之交易資料以及公司相關營運資料的機密性、完整性及可用性，依據 PCI DSS 及 ISO27001 最新版本為基準，特訂定本政策，作為本公司有關資訊安全管理最高指導準則。

第二條　適用範圍

本資訊安全政策執行之範圍為本公司電子支付系統服務之相關部門(如 IT、風控、客服及財務)，管理的標的包括歸屬於本公司的所有有形及無形資產，如：軟體、硬體設備、人員、書面及電子檔案、儲存媒體等。

第三條　權責

一、 電子支付系統服務之員工及其往來廠商之所屬員工，均需閱讀及遵守資訊安全政策內容。

二、 制定程序：本政策由總經理室資安官制(修)訂，由董事會通過後公告施行。

三、 本政策下之各項管理辦法及相關程序授權由總經理核定後公告施行。

第四條　名詞解釋

無。

第五條　內容

一、 本公司資訊安全政策

提供客戶安全便利之金融服務，確保金融科技服務之機密性、完整性及可用性，使客戶交易資料及個人資料之處理均獲得安全保障，進而維護客戶權益，確保公司永續經營。

二、 本公司資訊安全目標

依本公司資訊業務性質特訂定下列資訊安全目標：

（一）符合政府法令及主管機關的要求。

（二）確保交易資料與客戶個人資料之機密性、完整性及可用性。

（三）保護顧客個人、交易與電子商務資料之機密性、完整性及可用性。

（四）確保提供金融服務資料之正確性與完整性。

三、 資訊安全管理體系運作流程機制

（一）資訊安全管理體系運作 PDCA 循環機制

1、 規劃評估(Plan)

建置風險管理制度並對影響資訊資產安全之威脅、弱點及現行控管機制進行風險評估。

2、 設計建置(Do)

依據 ISO 27001 的控制要求，經風險評估產出結果及考量成本效益設計或修正並建置執行應有之控制機制。

3、 覆核稽查(Check)

定期或不定期實施資訊安全自行查核，以確保資訊安全管理之落實。

4、 檢討改善(Act)

根據覆核檢查之建議結果，執行矯正與預防措施，改善並執行應有之控管機制；另透過管理審查，達成相關人員實施資訊安全控管之落實。

（二）文件及記錄管理要求

資訊安全文件之核發、管制與變更均應有管制之方式，資訊安全管理制度運作所產生表單及紀錄，記錄保管單位應指派相關紀錄保存人員妥善保管，訂定保存期限與核定與閱覽之權限，以利追蹤制度執行狀況，維護制度有效運作。

（三）管理階層責任

管理階層應確保完成下列工作，以表示對資訊安全管理制度之充分支持：

1、 審查與訂定資訊安全管理制度相關規範。

2、 確保建立資訊安全指標。

3、 指派資訊安全之職掌與權責。

4、 宣導及遵守本注意事項與法令規定、達成資訊安全指標及持續改善之重要性。

5、 提供資訊安全管理制度各項作業所需之資源。

6、 決定風險可接受水準。

7、 執行資訊安全管理制度之管理審查作業。

8、 建立及維護資訊安全管理制度並維持其有效性。

9、 確認資訊安全管理規範與作業程序可符合本公司營運之需求。

10、確保參與資訊安全管理制度作業之人員均具備工作所需之相關職能。

（四）資訊安全制度查核

應定期或不定期進行資訊安全管理制度之評估或查核作業，以檢討控管目標、規範與作業程序是否合乎相關標準、法令規定或資訊安全需求，並依預期規劃有效執行與維持，以持續增進資訊安全管理制度的有效性。

（五）資訊安全管理體系之管理階層審查

管理審查制度之落實以確保資訊安全管理制度持續運作的適用性、適切性及有效性。資訊安全委員會應定期召開會議討論 ISO 27001 所要求之審查輸入項目及產生審查輸出項目。

（六）矯正預防措施

1、 矯正措施應採取適當的控管措施，以減少資訊安全管理制度建置與運作過程中所發現之不符合事項，並防止再度發生。

2、 預防措施應採取適當的控管措施，以預防不符合事項之發生。

四、 本政策應每年至少評估 1 次，或於重大環境變更時執行評估變更，以反映政府法令、資訊技術及公司業務等最新發展狀況，確保資訊安全實務作業之有效性。

五、 資訊安全目標應每年檢視其適切性，並應涵蓋機密性、完整性與可用性且呼應資訊安全政策要求。

第六條　內部控制原則

第七條　參考資料

一、 PCI DSS V3.2.1 版本。

二、 ISO 27001:2013 版本。

第八條　附件

無。

第九條　表單

無。