

電子支付機構資訊系統標準及安全控管作業基準 辦法總說明

為確保電子支付機構之交易資訊安全及業務健全運作，避免因資訊系統運作、傳輸或處理錯誤，影響服務之穩定與安全，並衍生相關糾紛，電子支付機構管理條例(以下簡稱本條例)第二十九條第一項、第三項、第三十九條及第四十條準用第二十九條第一項、第三項規定，電子支付機構應確保交易資料之隱密性及安全性，並維持資料傳輸、交換或處理之正確性；電子支付機構就電子支付機構業務，利用行動電話或其他可攜式設備於實體通路提供服務，其作業應符合主管機關所定安全控管作業基準規定，並於開辦前經主管機關核准。

為明確規範電子支付機構之資訊系統標準及安全控管作業基準，以利相關業者遵循及主管機關執行法令，爰依第二十九條第二項、第三十九條及第四十條準用第二十九條第二項授權，並參酌 CNS 27001「資訊技術-安全技術-資訊安全管理系統—要求事項」國家標準、金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法及中華民國銀行商業同業公會全國聯合會「金融機構資訊系統安全基準」、「金融機構辦理電子銀行業務安全控管作業基準」等規範，訂定本辦法計二十四條，其要點如下：

- 一、本辦法之適用範圍及用詞定義。(第二條及第三條)
- 二、使用者註冊時身分確認、登入帳號與固定密碼、交易類型與限額及各網路型態之交易安全設計。(第四條至第九條)
- 三、電子支付平臺之設計原則。(第十條)
- 四、電子支付機構應訂定組織、人員及設備安全之相關管理措施；其提供之電子支付平臺應就機房、營運、網路、金鑰、系統生命週期、資安事故及營運持續管理等資訊系統標準，採取相關資訊安全維護措施。(第十一條至第二十二條)
- 五、電子支付機構除應盤點與資訊安全相關法令，定期檢核落實程度外，並應於業務申請時及其後每年四月底前，由會計師進行檢視，提出資訊系統及安全控管作業評估報告。(第二十三條)
- 六、本辦法之施行日期。(第二十四條)