歐付寶內部控制制度聲明書

謹代表歐付寶電子支付股份有限公司聲明本公司於106年1月1日至106年12月31日確實遵循「電子支付機構內部控制及稽核制度實施辦法」，建立內部控制制度，實施風險管理，並由超然獨立之稽核單位執行查核，定期陳報董事會及監察人或審計委員會。經審慎評估，本年度各單位內部控制及法規遵循情形，除附表所列事項外，均能確實有效執行。

謹 致

金融監督管理委員會

聲明人

董事長：林一泓 （簽章）

總經理：許維洲 （簽章）

稽核主管：藍曉萍 （簽章）

法令遵循主管：林延壽 （簽章）

中　華　民　國　107　年　3　月　22　日

歐付寶電子支付股份有限公司

內部控制制度應加強事項及改善計畫

（基準日：106 年 12 月 31 日）

應加強事項	改善措施	預定完成改善時間
伺服器與資安設備的管理員以及日誌檔案管理主機的管理員應由不同人員擔任。	已調整由不同人員擔任以及加強監控措施作業。	已改善完成
資安及個資管理委員會應每年定期或視需要時召開會議。	已於 106 年第二季完成召開資安及個資管理審查會議。	已改善完成
伺服器及資安設備的管理員具有異動系統的權限，其使用時未取得權責主管同意，故有未經授權即使用最高權限帳號進行操作之風險。	已於 106 年第二季起增加由資安人員定期檢核伺服器及資安設備的管理員存取使用紀錄，確認其異動作業皆經權責主管核准後辦理，資安人員檢核記錄亦呈送其主管核准。	已改善完成
盤點稽核軌跡紀錄，規劃管理機制後設計告警及報表機制。對於系統異動或資料庫存取等行為，應設計審核及覆核操作紀錄機制。	1. 已修訂「伺服器管理辦法」、「網路管理辦法」並明確增訂系統異常紀錄程序，並已依其辦理記錄異常處理並進行分析，並呈權責主管核准。 2. 建立系統日誌管理系統與其例行檢核作業記錄，並呈權責主管核准。	已改善完成
清查盤點個人資料製作清冊為，再依據盤點結果進行風險評估及規劃控管機制。為持續改善個人資料安全維護，其所屬個人資料管理單位或人員，應定期提出相關自我評估報告。	已於 106 年第二季盤點完成電子支付作業環境進行個人資料清冊，並已於董事會報告個人資料風險評估報告。	已改善完成
建立個人資料資料外洩防護機制。	1. 已啟用監控措施，如信用卡資料、限制網路空間及免費信箱使用。 2. 導入使用者端管制監控軟體，並建立報表檢核機制作業。	已改善完成
設置硬體安全模組管理辦法，訂定相關管理及操作規範。	已訂定「HSM 加密金鑰管理辦法」。	已改善完成
進出電腦機房應遵循內部管理規範，確實填具「電腦機房進出登記表」。	人員於進出電腦機房，已確實填寫其進出登記表，並加強內部宣導。	已改善完成

應加強事項	改善措施	預定完成改善時間
非業務相關的網站應進行控管。	已啟用非業務相關網站限制。	已改善完成
每年進行應進行乙次社交工程演練。	106 年第一季～第二季已完成電子郵件社交工程演練，並已請點擊信件者加強教育訓練。	已改善完成
禁止內部人員透過內部無線網路連線至電子支付作業環境。	已禁止內部無線網路連線至電子支付作業環境，並已修訂「網路管理辦法」明確規範之。	已改善完成
進行營運衝擊分析，並以業務內容及範圍來規劃及建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應的資源、系統回復程序和處理機制。	已完成營運衝擊分析決定並最大可中斷時間，並已訂定系統緊急應變處理 SOP 文件及修訂「資訊事故通報作業及管理辦法」。	已改善完成