台灣樂天信用卡(股)公司內部控制制度聲明書

TRC Internal Control Statement

謹代表台灣樂天信用卡股份有限公司聲明本公司於 113 年 1 月 1 日至 113 年 12 月 31 日確實遵循「信用卡業務機構內部控制及稽核制度應注意事項」，建立內部控制制度，實施風險管理，並由超然獨立之稽核部門執行查核，定期陳報董事會及監察人。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。

On behalf of Taiwan Rakuten Credit Card Co., Ltd., it is stated that the company has strictly adhered the "Implementation Rules of the Internal Audit and Internal Control System of Credit Card Business Organizations" from January 1, 2024 to December 31, 2024 to establish an internal control mechanism to ensure risk is managed and independently conduct audits and periodical report to BOD and the Supervisor. After prudent evaluation, the internal control and compliance of each unit in this year can be effectively and effectively executed except for the items listed in the attached table.

謹 致 To FSC

金融監督管理委員會

聲明人

董事長：前川龍一 （簽章）

總經理： （簽章）

稽核主管： （簽章）

法令遵循主管： （簽章）

中 華 民 國 114 年 3 月 17 日

台灣樂天信用卡(股)公司內部控制制度應加強事項及改善計畫

（基準日：113 年 12 月 31 日）

應加強事項 The status of Improvement action to address the issue were identified from FSC's 2024 punishment official letter	改善措施 Corrective action plan	預定完成改善時間 Target Completion Date of Corrective Action Plan
主管機關懲處案件: 金管會就本公司遭駭客入侵資安事件及員工竊取客戶個人資料所涉缺失事項： 一、未建立主機與伺服器等重要資訊設備的本機外日誌保存機制及網路通訊設備的軟硬體更新規範。 The local system log for important information system equipment such as hosts and server's preservation mechanism and the specifications for the software and hardware updates of network communication equipment have not been established for important information equipment, such as the host server.	一、系統部已修訂網路安全管理程序準則，定義日誌 (包含主機、伺服器) 保存期間及存取權限、收集機制、並執行定期日誌備份及覆核；另就網路設備預訂於 2025 年 7 月 31 日開始每月執行軟體狀態檢查和更新。 The system dept. revised Cybersecurity Management Procedure Guidelines, define log storage period, access rights, collection mechanism, and perform regular log backups and reviews. in addition, monthly software status checking and updates will be implemented for network equipment scheduled to begin on July 31, 2025.	一、持續辦理中，預計於 2025 年 7 月 31 日
二、未能就遭駭客攻擊一事進行緊急應變。 Failed to implement the emergency response measures to hacker attacks incident.	二、本公司已成立 CSIRT (電腦資安事件應變團隊)，導入 EDR (端點偵測及回應工具)，惟就導入 SOC (安全運營中心) 監控網路系統攻擊，尚進行相關評估中，預訂於 2025 年 5 月開始啟用。 TRC has established a CSIRT (Computer Security Incident Response Team) and introduced EDR (Endpoint Detection and Response Tool). However, the introduction of a SOC (Security Operations Center) to monitor network system attacks is still under review and is scheduled to be launched in May 2025.	二、持續辦理中，預計於 2025 年 5 月

應加強事項 The status of Improvement action to address the issue were identified from FSC's 2024 punishment official letter	改善措施 Corrective action plan	預定完成改善時間 Target Completion Date of Corrective Action Plan
三、未完善建立個資存取管理機制。 Insufficient establishment of the management control mechanism for personal data access.	三、系統部已修訂機密資料傳遞作業準則，對含有個資之機敏資訊檔案加密保護且須經授權取得密碼，始得存取檔案，並自 2024 年 10 月起每月執行文件伺服器的帳號審查。 已於 2024 年度個人資料盤點作業時納入應用系統、資料庫、伺服器、檔案、個人電腦及對外部單位資料收送之電子檔。 System dept. has revised "transfer of confidential information policy", need to authorize and passwords to access encryption sensitive personal information files and monthly review file server account from Oct 2024. Completed the 2024 PI data inventory has including APP, DB, server, file, PC, and external transfer file.	三、已於 2024 年 12 月完成
四、未落實執行對防毒軟體告警訊息監測與處置的內部程序。 The procedure for monitoring detecting and handling anti-virus software alarm messages has not been properly implemented. Failure to effectively execute internal procedures for monitoring and addressing antivirus software alerts.	四、系統部已設置電腦資安事件與應變團隊政策準則規範，建立預警機制，並藉由導入 24 小時系統運作中心進行監控，惟就導入 SOC (安全運營中心)偵測網路病毒預防，尚進行相關評估中，預訂於 2025 年 5 月 31 日前開始啟用。 TRC has established "Computer Security Incident and Response Team Policy", and implemented monitoring through the introduction of a 24-hour system operation center. However, the introduction of the SOC (Security Operations Center) to detect network viruses is scheduled to be activated before May 31, 2025.	四、持續辦理中，預計於 2025 年 5 月

應加強事項 The status of Improvement action to address the issue were identified from FSC's 2024 punishment official letter	改善措施 Corrective action plan	預定完成改善時間 Target Completion Date of Corrective Action Plan
五、未落實執行高權限帳號控管的內部規範。 特權帳戶的集中管理不足。 Ineffective controls of the Privilege Accounts with the highest authority, Inadequacy centralized controls over Privilege Accounts management.	五、系統部已修訂帳號密碼使用準則， 1. 已就 AD 最高權限帳號，導入 LAPS (本機管理員密碼解決方案) ，並導入特權帳號管理系統(CyberArk)以利建立申請審核及操作後審查機制；2. 另預訂於 2025 年 3 月 31 日前對各系統帳號權限全面清查完成；3. 針對網際網路伺服器及 AD 伺服器評估導入雙因子認證之解決方案，，預訂於 2025 年 4 月 30 日前完成。 System dept. has revised "Account and password usage policy". (1) For the control of AD Privilege Accounts was implemented LAPS , and the privileged account management system (CyberArk) has been introduced to facilitate the establishment of an application authorization and post-operation review mechanism; (2) Will conduct inventory of the account permissions of all system is scheduled to be completed by March 31,. (3) Planning to introduce 2FA for internet server and AD server, and review by CyberArk before end of Apr 2025.	五、持續辦理中，預計於 2025 年 4 月底
六、未按內部規範所定時程執行電子郵件查核作業。 Control execution Lapse of periodic email review tasks in accordance with the designated schedule set by internal	六、本公司已依郵件管理作業準則執行覆核每週寄送至外部之電子郵件，並啟用對外發送郵件需經CEO/CFO核准後寄送之功能；另訂於2025年12月底前轉換為Microsoft系統；將加強以電子郵件宣導密碼原則外，並提高密	六、持續辦理中，預計於 2025 年 12 月底

應加強事項 The status of Improvement action to address the issue were identified from FSC's 2024 punishment official letter	改善措施 Corrective action plan	預定完成改善時間 Target Completion Date of Corrective Action Plan
standards. 以上經金管會核處新臺幣250萬元罰鍰【金管銀票字第11302038731號】	碼複雜度及鎖定原則以防止暴力破解及字典攻擊。 TRC has follow "Email management policy", weekly check the outgoing mail, and has enabled the function that external emails must be approved by the CEO/CFO before being sent. Plans to convert to Microsoft system by the end of Dec 2025. in addition to strengthening the promotion of password principles through email, it will also increase password complexity and locking principles to prevent brute force cracking and dictionary attacks.	