台灣樂天信用卡(股)公司內部控制制度聲明書

謹代表台灣樂天信用卡股份有限公司聲明本公司於 112 年 1 月 1 日至 112 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。

謹 致

金融監督管理委員會

聲明人

董事長：（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　　113　　年　　7　　月　　7　　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：112 年 12 月 31 日）

應加強事項	改善措施	預定完成改善時間
一、無線網路尚未有身分驗證機制，僅用密碼進行控管 現行允許特定筆電使用無線網路連接至網際網路，使用無線網路前需填寫申請單經主管同意後方可使用，惟現行無線網路尚未有身分驗證機制，僅有密碼登入機制。	Set up identity authentication (e.g. AD authentication) by March 2024.	持續辦理中，預計於 113/3/31 前完成。
二、端末設備 IP 配發機制未臻完善 端末設備 IP 配發採用 DHCP，未針對可連線的端末設備進行管控機制，故非公司之設備可透過 RJ45 網路孔即可獲得 IP 並存取內部網路。	Apply binding of IP and MAC addresses as advised by Mar 2024.	持續辦理中，預計於 113/3/31 前完成。
三、磁帶備份機制未臻完善 每日執行主機備份作業將其資料備份至伺服器硬碟及磁帶設備，惟現行磁帶設備故障故未進行磁帶備份作業。	The tape backup system will be improved in order to perform daily tape backup operation by December 2023. Enhance daily check task by Mar. 2024.	持續辦理中，預計於 113/3/31 前完成。
四、高權限帳號控管作業未臻完善 現行針對網路設備、防火牆設備、入侵防禦設備、與伺服器皆使用高權限帳號進行日常營運管理，使用高權限帳號時無需申請也無使用後覆核機制，且存在多位負責人員皆使用同一組高權限帳號之情事。	By February 2024, create individual privilege accounts for each user in Internal and External firewalls, Core Switch, Type 1 system, and AD Server, and apply for permissions for each use. Starting April 2024, change privilege account passwords every 90 days, perform account inventory, and review usage logs. By June 2024, conduct monthly reviews of usage logs and evaluate the PAM solution for account password management.	持續辦理中，預計於 113/6/30 前完成。

五、設備存取紀錄及帳號權限，未有識別異常紀錄與確認警示機制 現行針對網路設備、防火牆設備、入侵防禦設備、伺服器及物聯網設備之存取紀錄及帳號權限，未有識別異常紀錄與確認警示機制。	● Review the usage log of the core system privilege account when using by April 2024. ● Monthly review the usage log of the privilege account for Internal and External firewalls 、 Core Switch 、 Type 1 system (including OS、AP、DB) and AD Server by June 2024. ● The possibility of using SIEM or SOC will be evaluated by June 2024.	持續辦理中，預計於 113/6/30 前完成。
六、網路釣魚偵測機制未臻完善 現行未有網路釣魚偵測機制。	● Manual detection for fake Taiwan Rakuten Card APP and Official website detection is already in place. The take down process will be followed if it is necessary. ● Consider using a vendor for fake Taiwan Rakuten Card APP and Official website detection and take down process by June 2024.	持續辦理中，預計於 113/6/30 前完成。
七、弱點修補議題 CTI 系統委由外部廠商進行維護作業，惟其合約內容未包含弱點修補之雙方權責區分。	Review and Modify of security agreement from CTI contract by March 2024.	持續辦理中，預計於 113/3/31 前完成。
八、資料庫監控機制未臻完善 現行尚未針對資料庫之不安全例外處理及不安全資料庫查詢命令進行監控與告警作業。	Apply DB monitoring mechanism, including defining DB abnormal event pattern 、 DB abnormal event notification and saving DB monitoring records by March 2024.	持續辦理中，預計於 113/3/31 前完成。
九、硬體設備或軟體版本 EOS 議題 現行使用之 Cisco ASA 5515-K9 防火牆，為已不受原廠支援之 EOS 設備。	Replace it by Apr. 2024.	持續辦理中，預計於 113/4/30 前完成。

十、用戶代號在同一時間內能登入一個以上連線 樂天信用卡公司官方網站(e-Navi)之會員服務，採使用者帳號、使用者密碼及身分證字號進行唯一驗證登入，惟同一用戶代號在同一時間內能登入一個以上連線(session)，核與「金融機構辦理電子銀行業務安全控管作業基準」第七條 第七款 第二項身分驗證規定不符。	The change of the application setting will be finished by June 2024.	持續辦理中，預計於 113/6/30 前完成。
十一、網頁逾時中斷機制未臻完善 樂天信用卡官方網站(e-Navi)之會員服務，客戶登入會員後超過 25 分鐘未使用才中斷其連線，核與「金融機構辦理電子銀行業務安全控管作業基準」第九條 第一款 第二項 應設計連線(Session)控制及網頁逾時(TimeOut)中斷機制，客戶超過十分鐘未使用應中斷其連線或採取其他保護措施不符。	The change of the application setting will be finished by June 2024.	持續辦理中，預計於 113/6/30 前完成。
十二、模擬瀏覽器控管機制未臻完善 尚未採用適當保護機制，防止攻擊者以模擬瀏覽器(如 WebView、WebBrowser 等)方式竊取客戶身分核驗資訊或機敏資訊。	The change of the application setting will be finished by June 2024.	持續辦理中，預計於 113/6/30 前完成。
十三、物聯網供應商未簽訂資訊安全協議及約定相關責任 未與物聯網設備供應商簽訂資訊安全協議，且未明定設備安全性更新相關責任。	Review and Modify the contract of IOT vendors or isolating IOT devices from office networks by June 2024.	持續辦理中，預計於 113/6/30 前完成。
十四、網際網路服務伺服器及 AD 主機雙因子認證議題	Implement GW server to comply with 2FA authentication by April 2024.	持續辦理中，預計於 113/4/30 前完成。

針對提供網際網路服務之伺服器及 AD(網域服務)主機，尚未對最高權限帳號及特殊功能權限帳號，採用雙因子認證。		
十五、對外系統之網頁與程式異動監控未臻完善 尚未針對提供網際網路服務之系統，監控其網頁與程式異動，並於記錄通知相關人員處理。	Apply automated tools to monitor changes in web pages and web programs in external systems, and enable real-time notification mechanisms by March 2024.	持續辦理中，預計於 113/3/31 前完成。 2024/3/31