



瑞銀證券投資信託股份有限公司 持續核心營運系統及設備營運資源說明

一、 持續核心營運系統及設備營運所需之資源

瑞銀證券投資信託股份有限公司(以下簡稱"本公司")持續關注關鍵的網路和資訊安全能力，並投入資源和投資。我們的首要任務是保護客戶及其資產和數據的安全。瑞銀集團有專業的資訊團隊，以保護您的數據、商業資訊和金融資產。我們的網路和內部系統通過強大的技術控制和安全協議進行保護，並進行持續監控。瑞銀的資訊安全控制、員工培訓和溝通以及網路威脅監控計劃提供了強大的網路防禦，以幫助防止我們的運營受到網路安全事件的重大影響。我們繼續增強我們的網路能力，跟上不斷變化的威脅。

瑞銀集團的網路和資訊安全計劃由集團資訊安全官(CISO)領導，向集團運營和技術官以及集團合規和治理官彙報。網路和資訊安全計劃旨在識別、預防、檢測和應對網路和資訊安全事件，以維護我們的技術基礎設施的完整性和可用性，以及瑞銀資訊的機密性和完整性。瑞銀的集團 CISO、集團運營和技術高級管理人員以及負責監督網路和資訊安全計劃的管理人員都具有豐富的網路和資訊安全領域的相關專業知識。我們的網路和資訊安全計劃包括以下要素：威脅情報、預防和檢測控制、網路防禦和事件回應能力、教育和培訓、第三方風險以及監測和測試。瑞銀集團在網路安全框架中所往來之所有外部合作夥伴都必須符合瑞銀的網路安全標準。

瑞銀集團利用市場上最優秀公司的服務，為其客戶提供最創新和無縫的體驗。瑞銀集團通過其網路安全框架和第三方風險管理框架管理其對全球外部合作夥伴的依賴。這些合作夥伴必須遵守瑞銀集團的網路安全和風險管理框架，包括合同要求遵守瑞銀集團設定的網路安全標準，並在發生可能對瑞銀集團構成威脅的網路安全事件時立即通知瑞銀集團。

本公司資訊部門在集團的領導下，執行本公司資訊安全防護及有關事項之落實，綜理本公司資訊系統及持續營運相關作業。本公司核心營運系統皆訂有持續營運計畫以降低本公司營運中斷風險，並定期備份營運所需資料，以確保面臨偶發事件仍能持續營運。

二、 預算

資訊設備及系統之建置或維運預算由瑞銀集團 CISO 每年視集團短中長期計畫統一編列並分配。

三、 教育訓練計畫

本公司負責資訊安全之主管及人員，每年應至少接受十五小時以上資訊安全專業課程訓練或職能訓練，其他使用資訊系統之人員每年應至少接受三小時以上資訊安全宣導課程，及每季對全公司員工辦理資訊安全宣導。資訊安全教育訓練也是全公司員工每年必要性線上訓練課程的一部分。本公司每年至少辦理一次“電子郵件社會工程演習”（通常稱為釣魚演習）。

四、 災害復原演練

本公司每年至少辦理一次「災害復原演練」以確保偶發事件發生本公司具有即時應變能力。