中銀香港(控股)有限公司
BOC HONG KONG (HOLDINGS) LIMITED

科技風險管理政策(摘要)

目的

本政策目的是為建立和健全科技風險管理體系，提高科技風險管理水平，促進安全、持續和穩健運行，增强核心競爭力和可持續發展能力。

科技風險管理原則

本集團對科技風險管理所關注的內容劃分為資訊科技管治、資訊財產管理、加密應用、系統保安管理、物理保安和人員保安、系統發展及變更管控、資訊處理管理、通訊網絡管理、服務供應商管理、網絡安保等領域進行管理。

總體原則

- 科技風險管理應覆蓋到本集團各部門、崗位、人員及其日常工作中，確保所有的科技風險能夠被識別、評估、監測、控制和報告。
- 對本集團業務和科技的發展變化進行持續性調整，確保科技風險管理能滿足業務發展和科技發展的需要。

資訊科技管治方面

- 確保全體員工知悉和遵守本集團各項科技風險管理政策、管理辦法和相關規定。

資訊財產管理方面

- 制定資訊財產分級及對應保護要求。

加密應用方面

- 採用適當和有效的密碼學以保護信息的機密性、真確性和完整性。

系統保安管理方面

- 資訊系統安全應實行分級管理。根據資訊系統的重要性及安全性要求，採取不同等級的安全防護及控制措施。

物理保安和人員保安方面

- 制定及實施安全措施，防止對本集團的工作場所、各種設備、網絡及系統未經

授權的物理訪問、破壞和干擾。

系統發展及變更管控方面

- 資訊系統包括基礎設施、業務應用系統、現成的系統產品和服務。所有資訊系統均須遵守本集團的安全架構及系統開發標準，以確保安全和復原需求已在系統開發週期的適當階段得到關注和解決。

資訊處理管理方面

- 制定完整的管控計劃和合適的管理程序，以管理購置、開發、操作及維修保養電腦系統過程中所涉及的科技風險。定期進行維修及檢修資訊科技設施與設備。

通訊網絡管理方面

- 制定及執行有關使用網絡及網絡服務的程序；採取適當的措施以保障網絡的安全性及可用性，以支持業務正常運作。

服務供應商管理方面

- 制定管理措施，確保服務供應商交付或提供的服務符合本集團的資訊安全要求，並建立持續的管理程序，對服務供應商及其服務進行監控、評估及測試。

網絡安保方面

- 採取必要措施，防範對網絡的攻擊、入侵、干擾、破壞和非法使用以及意外事故，使網絡處於穩定可靠運行狀態，並保障網絡存儲、傳輸、處理信息的完整性、保密性、可用性的能力。建立網絡威脅情報處理機制，加强對網絡威脅情報的收集、分析、共享及通報，並已採取適當措施緩釋相關網絡風險。