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

科技风险管理政策(摘要)

目的

本政策目的是为建立和健全科技风险管理体系，提高科技风险管理水平，促进安全、持续和稳健运行，增强核心竞争力和可持续发展能力。

科技风险管理原则

本集团对科技风险管理所关注的内容划分为资讯科技管治、资讯财产管理、加密应用、系统保安管理、物理保安和人员保安、系统发展及变更管控、资讯处理管理、通讯网络管理、服务供应商管理、网络安保等领域进行管理。

总体原则

- 科技风险管理应覆盖到本集团各部门、岗位、人员及其日常工作中，确保所有的科技风险能够被识别、评估、监测、控制和报告。
- 对本集团业务和科技的发展变化进行持续性调整，确保科技风险管理能满足业务发展和科技发展的需要。

资讯科技管治方面

- 确保全体员工知悉和遵守本集团各项科技风险管理政策、管理办法和相关规定。

资讯财产管理方面

- 制定资讯财产分级及对应保护要求。

加密应用方面

- 采用适当和有效的密码学以保护信息的机密性、真确性和完整性。

系统保安管理方面

- 资讯系统安全应实行分级管理。根据资讯系统的重要性及安全性要求，采取不同等级的安全防护及控制措施。

物理保安和人员保安方面

- 制定及实施安全措施，防止对本集团的工作场所、各种设备、网络及系统未经

授权的物理访问、破坏和干扰。

系统发展及变更管控方面

- 资讯系统包括基础设施、业务应用系统、现成的系统产品和服务。所有资讯系统均须遵守本集团的安全架构及系统开发标准,以确保安全和复原需求已在系统开发周期的适当阶段得到关注和解决。

资讯处理管理方面

- 制定完整的管控计划和合适的管理程序，以管理购置、开发、操作及维修保养电脑系统过程中所涉及的科技风险。定期进行维修及检修资讯科技设施与设备。

通讯网络管理方面

- 制定及执行有关使用网络及网络服务的程序;采取适当的措施以保障网络的安全性及可用性，以支持业务正常运作。

服务供应商管理方面

- 制定管理措施,确保服务供应商交付或提供的服务符合本集团的资讯安全要求,并建立持续的管理程序,对服务供应商及其服务进行监控、评估及测试。

网络安保方面

- 采取必要措施，防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行状态，并保障网络存储、传输、处理信息的完整性、保密性、可用性的能力。建立网络威胁情报处理机制，加强对网络威胁情报的收集、分析、共享及通报，并已采取适当措施缓释相关网络风险。