顺丰集团信息安全政策

顺丰集团（以下简称"顺丰"）坚信，在数字经济加速发展的时代，信息安全与数据保护是企业持续健康发展的坚实基础，遵守所有适用的国家法律法规及行业规范是顺丰一直秉持的核心理念。顺丰将信息安全与隐私保护的责任置于业务发展的首要位置，始终保持对信息安全风险的高度警觉，持续完善内部信息安全管理体系建设。

顺丰信息安全与隐私保护的工作目标是为客户提供安全可靠的数智物流服务，护航企业的持续、稳定、健康发展；通过建立并强化信息安全管理体系，最大程度保护客户信息和公司信息资产，维护客户与公司的合法利益；以开放和合作的方式与政府监管部门、行业组织、合作伙伴、供应商等共同应对信息安全与数据保护方面的挑战；确保各项业务活动的合规运营，依法处理客户、员工、合作伙伴的数据信息，成为"备受尊重、全球领先的数智物流解决方案服务商"。

1. 目的和适用范围

1.1 目的

为建立健全顺丰信息安全管理体系，提升整体信息安全防护能力，保证信息安全资产安全的同时为客户提供安全可靠的数智物流服务，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及行业最佳实践，结合顺丰业务实际，特制定本《信息安全政策》。

1.2 适用范围

本政策面向顺丰全体员工（下称“员工”）。因业务需要而聘用的短期用工人员（劳务工、实习生、第三方合作伙伴等）也应参照本政策执行。本政策是员工信息安全管理的基本守则。

2. 工作方针

顺丰以“两个保护、两个坚持”作为信息安全工作开展的方针：

保护客户利益：通过建立并强化信息安全管理体系，最大程度保护客户信息，维护客户合法利益。

保护信息资产：定期开展风险评估，明确信息安全责任，落实信息资产保护要求。

坚持合规理念：信息安全保护需符合法律法规要求，符合顺丰的合规理念、文化和机制。

坚持务实态度：坚持适度安全的原则，对公司信息安全管理体系进行监控、评审和改进。

3. 组织架构与制度管理

3.1 组织架构

顺丰建立了由决策层、管理层、执行层构成的三级信息安全与隐私保护管理架构，其中信息安全与隐私保护委员会作为信息安全最高决策机构，负责信息安全重大决策、战略规划及资源配置，确保安全工作得到有效落实。

3.2 制度管理

顺丰致力于建设符合业界最佳实践的信息安全管理体系，基于业界最佳治理实践建立了完善的制度体系，制度体系涵盖信息安全组织、物理与环境安全、人力资源安全、网络安全、数据安全、个人信息保护、内容安全、AI 应用安全等核心领域，旨在为各个环节的信息安全控制和保护提供系统性的策略指导。

4. 数据安全管理

4.1 数据分类分级

顺丰对业务经营活动中涉及的数据资产进行分类分级管理，根据数据敏感程度与最小必要原则，实施差异化的保护措施，确保数据安全。

4.2 全生命周期管理

依照数据全生命周期理论，顺丰在数据采集、传输、使用、存储等阶段，对数据进行加密、去标识化、访问控制和数据备份等保护举措，确保数据的完整性、保密性和可用性。

4.3 技术能力建设

顺丰持续加强数据安全技术能力建设，构建集权管理、加解密管理、日志管理等技术防护体系。

4.4 数据安全评估

顺丰定期开展数据安全评估，依据最新监管法规要求全面评估数据安全风险，并根据评估结果持续完善信息安全管理体系。

5. 供应链安全管理

5.1 准入管理

顺丰加强对第三方合作伙伴开展数据安全尽职调查，评估内容包括基础安全情况、数据及隐私保护、系统安全及 AI 安全合规等方面，确保合作伙伴符合公司安全标准。

5.2 协议管理

顺丰与第三方合作伙伴签订保密协议和数据安全协议，明确双方的安全责任与义务，确保数据处理活动符合法律法规及公司安全要求。

5.3 软件供应链安全

顺丰构建了深度融合 SDL 理念的软件供应链安全治理体系，通过践行“安全左移”与“内生安全”战略，依托资产管理、智能审计及全链路投毒防御闭环等核心能力，将安全管控标准化并无缝嵌入从需求设计到运维发布的研发全生命周期，以提升软件供应链的整体安全合规与风险响应能力。

6. **监测响应与威胁管理**

6.1 监测响应

顺丰建立常态化监测预警机制，对信息资产进行持续监测，开展威胁分析和态势研判并及时进行通报预警。制定并持续更新完善信息安全事件应急预案，发现或发生信息安全威胁或事件时可快速、有效地恢复业务和系统的正常运转。

6.2 漏洞管理

顺丰建立包括漏洞检测、漏洞验证、漏洞风险评估、处置和修复四个方面的漏洞管理闭环机制，实施全闭环漏洞管理以提升网络安全防护能力，以有效应对漏洞对网络安全的威胁。

6.3 攻防演习

顺丰定期组织开展网络安全实战化应急演习，通过模拟各种网络安全攻击场景，在演习过程中不断发现自身信息安全防御弱点并复盘改进，全面提升事件应急响应能力。

7. **合规管理**

顺丰持续开展 ISO27001、ISO27701、网络安全等级保护三级认证及数据安全风险评估，确保信息安全管理体系合规与风险控制水平保持行业领先。

8. 员工信息安全责任

顺丰建立信息安全投诉举报渠道，鼓励员工发现可疑安全事件时向信息安全部门上报，携手营造和维护信息安全良好氛围。同时建立必要的信息安全培训与奖惩管理制度，所有员工均需参与信息安全培训和教育，签订保密协议和信息安全承诺书，持续培育“人人有责”的信息安全意识和素养，并对于信息安全违规行为予以坚决处罚。

9. 解释与生效

本政策由顺丰信息安全与隐私保护委员会负责解释。本政策自发布之日起施行，原有相关制度与本政策不一致的，以本政策为准。