裕同科技网络与信息安全政策

为保障网络、信息系统、数据及相关业务活动的安全、稳定、持续运行，维护客户、员工、供应商、合作伙伴及公司的合法权益，深圳市裕同包装科技股份有限公司（以下简称“裕同科技”或“公司”）依据适用的法律法规与内部管理要求，建立并持续完善网络与信息安全管理体系，推动信息安全治理、风险防控和持续改进。

本政策适用于裕同科技及纳入管理范围的分子公司、全体员工，以及因业务合作接触或处理公司网络、信息系统、数据资源的供应商、承包商、外部服务商及其他合作方。

一、管理承诺与治理原则

公司坚持“预防为主、防治结合、分级管理、持续改进”的原则推进网络与信息安全工作，将网络与信息安全纳入经营管理和风险管理体系，明确管理职责、管理流程和控制要求，保障网络基础设施、信息系统、数据资产与关键业务的安全性、完整性和可用性。

公司持续完善信息安全制度体系，覆盖网络安全、数据保护、权限管理、漏洞管理、应急响应、源代码和保密管理等重点领域；同时结合业务变化、技术发展、监管要求和安全事件复盘结果，定期评估并优化管理措施，持续提升信息安全管理成熟度。

公司重视数据完整性保护，通过访问控制、变更管理、日志审计、备份恢复、漏洞修复和安全检测等手段，降低未经授权访问、篡改、泄露、损毁或中断风险，保障信息和数据在收集、存储、传输、使用、共享及销毁全过程中的安全。

公司根据岗位职责和业务需要落实分级授权与最小权限原则，严格控制特权账户、核心系统、数据库及敏感信息访问，定期开展权限复核，确保相关授权合规、适当、可追溯。

二、风险管理与应急响应

公司建立信息安全风险识别、评估、处置与改进机制，结合数据分类分级、资产重要性、威胁情报、脆弱性情况和业务影响，对网络、系统、应用、数据及第三方合作场景开展持续风险管理。针对重要系统、关键设备和敏感数据，公司通过安全监测、日志审计、漏洞扫描、访问行为分析及定期巡检等方式，及时发现异常行为、已知漏洞和潜在风险。

公司对识别出的安全风险实行分级管理，并结合现有控制措施的有效性评估风险水平；对于高风险事项，制定整改和缓解计划，明确责任部门、整改措施和完成时限，并跟踪验证整改效果。公司视业务变化、重大系统调整、法规更新及事件发生情况，适时开展专项风险评估和复盘优化。

公司制定网络与数据安全事件应急预案，建立分级响应、快速处置、调查溯源、修复恢

复和总结改进机制。当发生网络攻击、病毒感染、系统中断、数据泄露、异常访问或其他安全事件时，公司将及时启动相应应急流程，采取隔离、阻断、修复、恢复、监测加固等措施，尽最大努力降低事件影响。

对于可能影响客户、员工、供应商、合作伙伴及其他相关方权益的重大安全事件，公司将在遵循法律法规及监管要求的前提下，依法依规开展报告、沟通与处置工作，并持续改进防范机制，降低同类事件再次发生的可能性。

公司定期组织备份恢复测试、灾难恢复演练和安全应急演练，验证关键系统、关键设备和重要数据的持续运营与恢复能力，增强组织整体安全韧性。

三、员工责任与安全意识

公司坚持“信息安全，人人有责”的理念。全体员工应遵守公司网络与信息安全相关制度、流程和操作规范，在各自岗位范围内承担相应的信息安全责任，妥善保护公司、客户、员工、供应商及合作伙伴的信息和数据。

员工应按照授权范围访问和使用信息系统、数据和设备，不得超范围查询、导出、复制、传播、篡改或删除信息，不得擅自共享账户、泄露密码、私接网络设备、安装未经授权的软件，或通过不安全渠道传输敏感信息。涉及敏感数据、关键系统、特权账户、开发测试环境及外部远程接入的操作，应遵守更严格的审批、控制和审计要求。

员工在发现疑似安全风险、异常行为、钓鱼邮件、病毒木马、账户异常、数据泄露或其他安全事件时，应及时上报并配合处置，不得迟报、漏报、瞒报。公司对违反信息安全制度、造成安全风险或损失的行为，将依据内部管理规定进行问责；涉嫌违法的，将依法追究责任。

公司通过新员工培训、定期宣导、专题培训和重点岗位专项培训等方式，持续提升员工的信息安全意识、合规意识和风险识别能力，推动安全要求融入日常经营和业务活动。

四、第三方信息安全管理

公司重视供应商、承包商、外部服务商及其他合作伙伴带来的信息安全风险，并将第三方安全管理纳入整体信息安全治理体系。对于可能接触公司网络、系统、代码、数据或其他信息资产的合作方，公司将根据合作内容和风险程度实施相应的安全准入、协议约束、权限控制、过程监督和退出管理。

公司要求相关第三方在合作过程中履行保密和信息安全义务，遵守适用法律法规及双方约定，不得超出授权范围访问、使用、复制、留存、披露或转移公司信息和数据。对涉及客户信息、员工信息、业务数据、系统接口、源代码或其他敏感信息的合作事项，公司可要求签署保密协议、数据保护协议或其他安全承诺文件，并明确安全责任、使用边

界、违约责任和终止后的返还或销毁要求。

对于第三方提供的系统、服务或开发活动，公司将结合实际需要开展安全评估、漏洞修复要求、配置与发布控制、账号权限管理及必要的审计监督。合作终止或授权到期后，公司将按要求回收账号权限，并要求第三方返还、删除或销毁相关信息和数据。

公司将持续推动与供应链伙伴共同提升信息安全管理水平，降低因第三方合作带来的网络与信息安全风险。

五、主要控制措施

为落实本政策，公司结合业务需要采取适当的组织和技术控制措施，包括但不限于网络边界防护、终端安全管理、身份认证与访问控制、最小权限管理、日志留存与审计、恶意代码防护、漏洞扫描与修复、补丁管理、数据加密、备份恢复、系统变更管理及开发安全管理等。

公司根据数据敏感程度和业务重要性，对信息和数据实施分类分级管理，并对重要数据、敏感数据和关键系统采取更严格的防护措施，以降低泄露、篡改、丢失、滥用和服务中断风险。

六、审计、培训与持续改进

公司通过内部检查、专项审计、管理评审、演练复盘和必要的第三方评估等方式，定期验证网络与信息安全控制措施的执行情况和有效性，识别不足并推动整改落实。

公司将持续开展面向员工及相关岗位人员的信息安全教育培训，强化密码安全、邮件安全、数据保护、设备使用、远程接入、第三方协作和事件报告等要求，提升组织整体安全意识和应对能力。

七、附则

本政策为裕同科技公开披露的网络与信息安全原则性文件，用于说明公司在网络与信息安全方面的管理承诺、基本要求与治理方向。公司将根据法律法规、监管要求、业务发展及风险变化情况，适时对本政策进行更新和完善。