朗新科技集团股份有限公司

网络信息安全和隐私保护政策

朗新科技集团股份有限公司（以下简称“本公司”或“朗新科技”）为保障网络信息安全和用户隐私权益，规范个人信息处理活动，落实《个人信息保护法》《数据安全法》《网络安全法》及相关国家安全标准，制定《网络信息安全和隐私保护政策》（以下简称“本政策”）。

一、适用范围

本政策覆盖朗新科技所有业务、产品、服务及供应商等第三方合作方。本公司所有员工，包括但不限于正式员工、实习生、外包员工、兼职人员及其他可能出现的各类人员，应知晓并理解公司对网络信息安全和隐私保护的管理要求。此外，本公司也要求公司的合作伙伴和供应商遵守这一政策，并鼓励其制定类似政策。

二、主要内容

本政策面向全体员工及相关人员，围绕管理架构与职责、安全管理体系制度、数据全生命周期管理、安全技术与管控措施、员工管理与培训、第三方与供应链管理、个人信息主体权利保障、安全合规监督和自查等方面做出规定，明确违反本政策将面临相应的处罚。本政策不仅是企业合规的“底线”，更是构建数据信任、防范风险、提升竞争力的核心战略。本公司通过系统化的管理框架、全员参与和持续改进，有效平衡数据利用与安全保护，实现企业与社会的协同发展，保障企业稳定运营和可持续发展。

三、管理架构与职责

1. 网络与信息安全暨隐私保护管理委员会

朗新董事会委员对公司网络安全管理工作总体负责。

主任：由朗新科技 CEO 担任，统筹网络安全与隐私保护战略。

委员：董事会成员、公司高级管理层、安全质量管理部、人力资源管理部、流程与系统部、业务部门负责人。

职责：作为网络与信息安全最高领导、统筹、决策机构，负责规划部署公司安全战略；对重大安全事件进行决策、指导。

2. 安全与隐私联合工作组

负责对本公司网络与信息安全治理领域进行整体管控；制定网络与信息安全方针、政策；负责本公司网络与信息安全工作的协同调度，确保安全体系有效执行。

3. 专职部门

安全质量管理部：负责安全合规体系建设，制定并监督执行数据安全和个人信息保护管理制度，开展风险评估、漏洞管理及应急预案管理、保障产品和服务安全等。

人力资源管理部：制定员工个人信息安全管理制度流程，保障员工隐私保护。

流程与系统部：实施技术防护措施，保障网络基础设施安全。

行政管理部：负责办公园区空间安全及相关软硬件设施安全。

法务部：负责法律合规审查、用户权利请求处理及监管沟通。

会计与内控部：负责个人信息保护合规审计工作。

四、安全管理体系制度

朗新科技根据国家和所在地区的法律法规、安全标准以及技术发展，建立健全公司网络与信息安全、数据安全及个人信息保护管理制度和相关操作规程。本公司将数据安全和隐私保护与公司整体风险管理体系结合，同时纳入公司风险评估流程和合规审计，定期开展个人信息保护影响评估工作和个人信息保护合规审计工作，确保公司个人信息治理框架和隐私政策与国内外法规的一致性。

五、数据全生命周期管理

1. 数据分类分级：建立全面的数据资产清单，根据数据敏感程度将数据分为四级，制定重要数据和敏感个人信息的处理规则，实施全流程分类分级管理和保护。
2. 数据采集：规范数据收集的要求，确保收集个人信息的准确性、完整性和合法性，收集个人信息遵循最小必要原则，并获得用户的明确同意。
3. 数据传输：按照数据敏感程度，采取适当的安全技术措施（包括加密、访问控制、完整性校验等手段），确保数据传输的保密性、完整性、可靠性和网络传输服务可用性等符合相应级别保护要求。针对跨境业务开展内部数据安全自评估，触发重要数据和个人信息出境申报条件的情况，需向国家网信部门申报数据出境安全评估。
4. 数据存储：核心级数据加密存储，重要级数据脱敏存储，存储期限不超过业务必需时间。做好数据备份和恢复管理，定期备份数据并验证备份的完整性和可用性。
5. 数据使用：明确数据使用目的限制，仅限授权人员在限定场景下使用，禁止超范围处理。规范个人信息加工使用要求，委托处理和共享转让及披露。
6. 数据删除：采用物理或逻辑擦除技术，确保数据不可恢复。同时，采用与第三方相关的数据信息销毁/处置约定和监督删除机制。

六、安全技术与管控措施

1. 在威胁监控方面，部署防火墙、入侵检测系统（IDS）、零信任架构、透明加密终端等技术手段，控制进出网络的数据流，防止未经授权的访问和数据泄露。引入新技术（如 AI 驱动的安全工具、自动化告警系统）优化防护措施，实时监控异常行为（如网络攻击、未授权访问、数据泄露迹象），确保与最新安全威胁和合规要求同步。
2. 定期进行渗透测试和漏洞扫描，确保系统的安全性。建立内部安全评估机制，分析系统的安全漏洞缺陷，制定改进计划，持续改进信息安全系统。

3. 数据处理全生命周期，采用数据加密技术保护数据的存储和传输，使用哈希校验、数字签名等技术嵌入完整性校验机制，确保数据完整性与保护。
4. 实施基于角色的访问控制（RBAC），确保只有授权人员可以访问重要敏感数据。记录重要敏感数据操作日志，设置数据操作的审批流程，确保所有操作都经过适当的授权。
5. 定期开展安全演练与复盘工作，模拟安全事件演练，定期分析事件原因并优化技术措施和管控流程。

七、员工管理与培训

1. 为确保全体员工了解信息安全管理责任与保密责任，所有员工入职需签署安全保密协议和网络信息安全承诺书，重要岗位签署数据安全责任书，明确岗位涉及的数据安全责任。此外，员工离职或调岗时需完成数据交接并注销相关权限。
2. 制定并发布《网络与信息安全管理办法》《数据安全管理办法》《个人信息保护管理办法》《员工安全行为指南》《网络与信息安全十五不准》等系列规章制度，规范员工日常工作行为，落实内部监督工作和问责机制。
3. 本公司每年定期组织员工开展安全意识培训与考核，并将安全培训作为新员工入职必修课程，要求安全考试必须满分通过。具体安排包括：每年至少开展 2 次全员安全意识宣贯培训、1 次全员数据安全与个人信息保护专题培训。同时，本公司建立考核机制，将信息安全纳入部门和员工的绩效考核指标。

八、第三方与供应链管理

1. 第三方供应商等合作方需符合 ISO 27001 等安全认证或同等资质，认证范围需覆盖相应的服务内容，确保其安全能力与业务需求匹配。

2. 签署项目合同和数据安全保护协议，明确第三方供应商等合作方的数据保护义务，包括信息安全、数据保护、合规性等方面的要求，确保其与公司的安全政策和标准保持一致。合作方违反协议导致安全事件或数据泄露的，承担连带赔偿责任。
3. 严格执行公司《第三方供应商安全管理规范》，明确第三方人员的网络和数据安全行为管理原则，强化安全风险管控和运营。对第三方技术服务过程中的安全事件和违规行为进行调查和处理，确保及时纠正和改进。
4. 每年复审第三方供应商网络安全和数据安全能力，对于关键供应商定期执行核心项抽查。针对第三方供应商及其工作人员的活动进行评估和审查，评估其是否符合合同约定的安全要求和标准，未达标者终止合作。

九、个人信息主体权利保障

1. 收集员工和客户的个人信息遵循合法、正当、必要原则，仅收集与业务相关的信息，且明确告知收集目的和用途，并获得用户明确的同意。未经个人信息主体同意，不得用于其他用途或向第三方披露。
2. 收集的用户个人信息仅用于公司正常业务开展，禁止将用户数据擅自用于次要或无关目的。业务停止运营后停止收集并删除个人信息，确保个人信息存储时间最小化。
3. 对收集的个人信息进行去标识化处理和采取必要的安全措施后再存储。制定个人信息分类分级标准，根据个人信息不同级别和不同类别，采取适当的技术措施和管控流程。内部员工访问他人信息需经过审批才能获得相应权限，且仅限工作所需。
4. 针对公司开发建设或运营的 APP 或小程序等线上渠道的隐私政策开展内部安全检查，重要系统平台引入第三方合规审计，确保个人信息处理合法合规。

5. 公司制定发布《个人信息保护影响评估制度》《个人信息主体权利响应机制》等内部规章和操作规程，制定完整的个人信息主体权利响应的流程，明确各环节的职责分工，并建立个人信息主体行使权利的申请受理和处理机制，以及投诉管理机制。
6. 公司的隐私政策确保向个人提供其行使权利的方式和途径，明确个人信息主体权利的内容，包括个人信息的撤回同意、访问、复制、转移、更正补充、删除及约束系统自动决策等，并对各个权利的适用情形和例外情形进行规定。

十、安全合规监督与自查

1. 定期开展安全合规自查工作，结合自身业务模式、相关产品形态，开展合规自查和重点问题整改。检查和监控网络环境、信息系统、员工操作行为、数据信息、第三方供应链等方面是否存在安全风险隐患，持续加强公司网络安全保障体系和能力建设。
2. 根据法律、法规和标准的要求，定期开展个人信息保护影响评估工作，分析个人信息处理活动全生命周期对个人权益可能产生的影响，并据此采用适当的个人信息安全控制措施，有效加强对个人信息主体权益的保护。
3. 将隐私政策与公司整体风险管理体系结合，制定整体审计工作计划，定期检查隐私政策与国内外法规（如《个人信息保护法》、GDPR）的一致性。成立独立内审组开展个人信息保护合规审计工作，通过人员访谈，管理制度、策略和机制等文档查验和技术核查等方式，监督检查公司各个业务板块是否存在侵害个人信息主体权益的风险。
4. 对于提供重要互联网平台服务、用户数量巨大、业务类型复杂的业务板块，开展外部审计或委托外部第三方进行合规审计。

十一、违规处理（零容忍政策）

1. 公司对数据泄露、违规处理个人信息、侵犯隐私和个人信息权益、违反授权访问、超范围使用、擅自共享披露、规避审计或未按要求报告安全事件等行为采取零容忍态度。
2. 公司制定安全事件响应流程和违规行为处理流程。任何数据泄露、隐私侵权、个人信息违规处理或疑似安全事件，应在发现后 24 小时内按照公司流程上报，并由相关责任部门开展评估、处置、调查、纠正和复盘。 同时，公司对受安全事件影响的利益相关方保持透明度，积极向他们通报事件调查进展。
3. 员工违规：经核实存在违反本政策、法律法规或公司信息安全与个人信息保护制度的行为，公司将依据情节轻重采取警告、通报批评、绩效扣减、调岗、降职、解除劳动合同等处罚；造成损失的，公司保留追偿权。
4. 管理层失职：对未履行监督管理职责、隐瞒不报、处置不当或导致风险扩大的直接责任人和主管领导，公司将依法依规追究管理责任。
5. 第三方违规：供应商、合作伙伴、外包人员或其他第三方违反合同约定或公司隐私保护要求的，公司可采取警告、限期整改、暂停合作、追责赔偿、终止合作等措施，并将相关表现纳入供应商评价。
6. 法律追责：构成违法犯罪或依法需要监管报告的，公司将按照法律法规要求及时处理，必要时移送司法机关或配合监管调查。

十二、附则

安全管理办公室负责编写本政策，经朗新科技网络与信息安全暨隐私保护管理委员会批准后执行。之前已执行的相关政策内容与本政策不符的，一律按本政策执行。

安全管理办公室负责监督本政策的执行情况，并对其有最终解释权。