上海卓拉网络科技有限公司信息安全管理策略（V1.0）
文件编号：IS-2026-001
生效日期：2026 年 05 月 20 日
审批人：李志勇
适用范围：公司全体员工、外包人员及所有业务系统、办公终端、数据资产

一、目的与范围

1. 目的：为规范公司信息安全管理，防范网络攻击、数据泄露、系统故障等安全风险，保障公司业务数据、客户个人数据及系统资产的安全，符合监管法规及合作平台合规要求，特制定本策略。
2. 适用范围：本策略适用于公司所有部门、全体在职员工及外包服务人员，覆盖办公终端、业务系统、网络环境、数据资产全场景。
3. 基本原则：遵循“谁主管谁负责、最小权限、预防为主、持续改进”的原则，将信息安全要求融入日常业务运营全流程。

二、组织与职责

1. 信息安全负责人
   由公司技术/运维负责人担任，统筹全公司信息安全管理工作，负责本策略的审批、发布与更新，牵头安全事件处置与对外合规对接。
2. 各部门负责人
   负责本策略在部门内的落地执行，监督本部门员工遵守安全规范，配合开展安全检查与整改工作。
3. 全体员工
   严格遵守本策略各项要求，规范使用办公设备与系统账号，发现安全风险及时上报信息安全负责人。

三、核心安全要求

1. 终端安全管理
- 所有办公电脑、服务器终端必须安装正版杀毒软件，开启实时防护功能，病毒库保持自动更新；每月开展一次全盘安全扫描，留存扫描记录。
- 办公终端统一设置安全基线：15 分钟无操作自动锁屏，解锁需身份验证；禁止私自卸载安全软件、关闭防护功能。
- 禁止在办公终端私自安装来源不明的软件，禁止使用办公设备从事违规网络活动。

2. 网络安全管理
- 对办公网络、生产业务网络实行分区隔离，通过防火墙/安全组配置访问控制规则，禁止非授权跨域访问核心数据系统。
- 部署网络边界防护与流量监控措施，实时监测异常访问、外部入侵等网络威胁，发现风险即时处置。
- 禁止私接无线路由器、私自搭建网络环境，禁止使用公共网络直接访问核心业务系统。

3. 数据安全管理
- 公司数据按敏感程度分级管理，客户个人数据、业务核心数据列为敏感数据，实行重点保护。
- 敏感数据静态存储采用 AES-256 及以上强度加密；数据对外传输、跨网络传输必须使用 TLS v1.2 及以上加密协议，严禁明文传输敏感数据。
- 禁止私自复制、导出、传播敏感数据，禁止将敏感数据存储于个人设备或非授权云盘。

4. 访问控制与账号管理
- 严格遵循"最小权限、按需分配"原则，系统账号与数据访问权限仅授予完成岗位职责所需的最小范围。
- 权限开通需经部门负责人与信息安全负责人双审批；员工岗位变动、离职时，即时回收所有系统权限。
- 密码必须满足复杂度要求：长度≥8 位，包含大小写字母、数字与特殊字符，每 90 天更换一次，禁止复用历史密码。
- 所有管理员账号、核心业务系统账号必须启用多因素身份验证（MFA）。
- 系统访问操作日志全量留存，留存周期不少于 180 天；每年开展一次全量权限复盘清理。

5. 漏洞与风险管理
- 定期对核心业务系统、服务器开展漏洞扫描，每年至少开展一次全面安全检测；对发现的漏洞按风险等级分级处置，高危漏洞 72 小时内完成修复。
- 持续关注行业安全威胁情报，对新型漏洞、攻击手段及时预警并采取防范措施。
- 所有漏洞扫描、修复记录统一归档留存。

6. 安全事件响应
- 建立安全事件应急响应机制，明确事件分级、处置流程与各岗位责任，设立内部安全告警上报渠道。
- 发生数据泄露、系统入侵等安全事件时，须第一时间上报信息安全负责人，按流程开展处置、溯源与整改工作。
- 若事件涉及合作方数据，须按约定时限与渠道向合作方同步事件情况、影响范围与处置进展。
- 每年至少组织一次安全事件应急演练，验证响应流程有效性。

四、策略评审与更新

1. 本策略每年至少开展 1 次全面评审，根据监管要求、业务变化与技术发展进行修订更新。
2. 遇公司业务架构重大调整、相关法规标准更新时，即时启动策略修订工作。
3. 策略更新后须重新审批发布，并同步至全体员工。

五、附则

1. 全体员工须严格遵守本策略，违反规定造成安全风险或损失的，公司将按相关制度追责。
2. 本策略由公司信息安全负责人负责解释。