技术安全保障管理制度

第一章 总则

1.1 制定依据

依据《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》等法律法规，围绕网站安全、信息保密、用户个人信息安全三大维度，建立本技术安全保障管理制度，全面防范网络攻击、系统故障、信息泄露、数据篡改等安全风险，保障网络表演业务稳定、合规、安全运行。

1.2 适用范围

本制度适用于零果直播官方网站、直播流媒体后台、内容审核管理系统、用户支付结算系统、主播入驻管理系统；适用于公司技术研发部、运维部、运营部、客服部所有接触服务器、业务数据、用户信息、平台机密资料的全体工作人员；覆盖平台开发、上线、运维、存储、数据传输、第三方接口对接全流程安全管理工作。

1.3 管理目标

保障零果直播网站 7×24 小时稳定安全运行，防范服务器宕机、网络攻击、恶意入侵、系统漏洞引发的业务中断风险；

建立全流程信息保密机制，严防平台商业机密、运营数据、审核台账、技术源码外泄；

全维度保护用户实名信息、交易数据、隐私内容，落实个人信息收集、存储、使用、传输、销毁全生命周期安全管控，杜绝用户信息泄露、滥用、非法交易。

第二章：网站安全保障措施

2.1 网络架构安全防护措施

平台服务器部署于国内具备等保资质的合规云机房，采用防火墙 + WAFWeb 应用防火墙双重防护策略，拦截 DDoS 流量攻击、SQL 注入、XSS 跨站脚本、恶意爬虫、暴力破解等网络攻击行为，设置流量访问阈值，异常访问自动拉黑 IP 地址。

采用内外网隔离架构，用户前端访问仅可通过公网访问业务开放端口，数据库、服务器运维后台仅允许公司固定内网 IP 地址登录，禁止公网直接访问核心数据库。

全站强制部署 SSL/TLS 安全证书，所有前端网页、API 接口统一采用 HTTPS 加密传输协议，防止数据传输过程中被窃听、劫持、篡改。

2.2 服务器与系统安全管理措施

服务器操作系统、数据库定期更新安全补丁，每月开展一次漏洞扫描，每半年委托第三方专业机构开展一次渗透测试，对高危漏洞限期修复，留存漏洞检测、修复台账。

服务器采用最小权限账号策略，禁止使用超级管理员账号日常运维操作，运维人员独立分配操作账号，设置强密码策略，异地登录必须通过企业微信、短信二次身份核验。

搭建服务器运行实时监控告警系统，对 CPU、内存、带宽、磁盘负载、在线并发访问量设置预警阈值，出现负载过高、异常访问、服务进程崩溃时，自动向技术运维负责人推送短信、系统告警，确保故

障早发现、早处置。

建立异地多备份机制：平台业务数据、直播回放视频、用户交易日志、审核台账实行本地+异地双备份，每日凌晨自动全量备份，备份文件加密存储，备份数据最少留存 180 天，遭遇服务器硬件故障、勒索病毒攻击时可快速恢复业务数据。

2.3 业务系统安全管控措施

平台后台管理系统实行分级权限管控：超级管理员、内容审核、运营、客服、财务岗位分配最小必要操作权限，岗位之间权限隔离，客服仅可查询用户基础订单，无法查看用户完整身份证隐私信息、无法修改后台业务参数，权限变更需履行书面审批流程。

所有第三方支付、实名认证接口采用加密密钥对接，密钥由技术负责人专人保管，禁止明文存储密钥，接口调用日志全程记录留存，防止第三方接口被恶意盗用。

上线前安全测试机制：平台版本迭代、功能更新上线前，必须经过安全功能测试、漏洞检测，严禁未经安全测试的新版本直接线上发布；重大功能更新采取灰度发布模式，小范围试运行无安全风险后全量上线。

2.4 网站应急安全保障措施

搭建备用服务器、备用带宽线路，当主服务器遭受攻击宕机、主干网络中断时，技术人员 15 分钟内切换至备用服务节点，最大限度缩短直播业务中断时长。

建立网站安全事件分级处置流程：一般网络攻击、系统卡顿由运

维人员当场处置；重大勒索病毒、大规模数据泄露攻击立即启动公司突发事件应急预案，第一时间关停公网访问、固定证据，同步向网信、公安网安部门上报。

定期每季度组织一次网站安全应急演练，模拟服务器宕机、DDoS攻击、数据误删除等场景，检验运维团队故障处置、数据恢复能力，持续优化网站安全防护策略。

第三章：信息安全保密管理制度

3.1 保密信息范围界定

绝密级信息：平台技术源代码、数据库核心密钥、服务器运维最高权限账号密码、未公开的风控算法、企业财务交易流水；

机密级信息：内容审核台账、违规主播处置档案、平台运营用户数据统计、商业合作方案、主播签约合同、未上线产品迭代方案；

秘密级信息：内部培训资料、客服投诉详细档案、用户纠纷完整证据材料、内部安全漏洞报告。

3.2 人员保密管理措施

所有入职接触平台保密信息的技术、运营、审核、财务人员，入职须明确泄密违约责任；员工离职时，立即回收所有系统操作权限、办公设备涉密资料，签署离职保密承诺，涉密岗位员工约定竞业保密义务。

实行涉密岗位专人负责制，绝密级资料仅限指定核心技术负责人查阅，严禁私自复制、转发、截屏涉密文档；内部办公文件仅允许在公司内网办公设备处理，禁止使用个人微信、私人邮箱传输涉密数据。

定期每季度开展全员信息保密法律法规培训，讲解《数据安全法》相关追责条款，建立培训档案，强化员工保密意识。

3.3 涉密资料存储、传输、销毁管理

涉密电子文档统一存储于公司加密内网服务器，设置访问密码与操作日志，每次查阅、下载自动记录操作人员、操作时间；纸质涉密文件存放于保险柜，专人上锁保管，借阅必须履行书面审批登记手续。

涉密信息内部传输必须使用公司加密办公系统，禁止通过公共社交软件、网盘传输；对外需要报送监管部门的合规资料，脱敏处理后通过加密邮件报送。

过期涉密纸质资料统一粉碎销毁，电子涉密文件采用专业数据粉碎工具彻底删除，禁止直接丢弃、格式化处理，留存销毁登记台账。

3.4 泄密事件处置与追责机制

发生信息泄密事件，当事人必须第一时间上报公司保密管理负责人，立即采取权限冻结、文件撤回、IP 封禁等止损措施，同步固定泄密路径、泄露范围证据。

根据泄密等级追责：轻微无意泄密给予内部通报批评、经济处罚；故意泄露、倒卖平台涉密数据、用户信息的，立即解除劳动合同，依法追究民事赔偿责任，涉嫌刑事犯罪的移交公安机关立案侦查。

泄密事件处置完毕后，全面复盘漏洞，优化权限管控、数据传输保密措施，避免同类泄密事件重复发生。

第四章：用户信息安全管理制度

4.1 用户信息收集合规原则

遵循最小必要收集原则：平台仅收集开展网络表演直播服务必需的用户信息，注册仅收集手机号，主播开播、用户充值评论仅需要身份证实名四要素+人脸核验，不得强制收集住址、银行卡详细信息、通讯录、地理位置等非必要个人信息。

收集用户信息前，在《用户隐私政策》中清晰告知收集目的、使用范围、存储期限、共享对象，取得用户明确同意后方可收集；禁止超范围、超目的使用用户个人信息。

未成年人个人信息收集必须取得监护人明示同意，方可完成实名认证，平台不得诱导未成年人授权非必要个人信息权限。

4.2 用户信息存储安全管理

用户身份证、人脸实名等敏感个人信息采用国密加密算法加密存储，数据库仅脱敏展示部分字段，客服、普通运营人员无法查看完整身份证号码、人脸原图；仅风控合规负责人在纠纷核验、监管协查场景下可临时申请调取完整实名信息，全程留存调取审批、操作日志。

用户个人信息与业务运营数据物理隔离存储，禁止将用户实名数据导出至公网、私人设备；用户原始实名信息存储期限不超过业务必需期限，账号注销后 60 日内完成用户个人信息脱敏销毁。

严禁向任何第三方出售、出租、非法共享用户个人信息；仅在用户授权、司法机关依法调取两种情形下可对外提供脱敏后的用户信息，司法调取必须核验执法文书并留存归档。

4.3 用户个人信息使用、主体权利保障措施

用户信息仅限用于账号身份核验、风控反欺诈、交易结算、违规

行为追溯、用户维权纠纷处置、监管部门依法协查六大场景，不得用于个性化商业广告推送之外的其他用途。

平台在个人中心设置用户信息自主管理入口，用户可在线申请：查阅本人平台留存信息、更正错误实名信息、删除非必要授权信息、注销账号销毁个人隐私数据，平台收到申请后 15 个工作日内办结并书面反馈结果。

当发生用户信息泄露、篡改、丢失安全事件时，公司立即启动应急预案，采取封堵漏洞、冻结账号等补救措施，及时通过短信、站内信告知受影响用户，并向网信部门上报安全事件。

4.4 用户信息安全内部管控与追责

严格限制用户敏感信息内部访问权限，建立用户信息调取审批制度，任何岗位需要查询用户完整实名信息，须向负责人申请，注明使用事由、调取范围，经公司合规负责人审批后方可临时开放权限。

严禁内部员工私自截图、下载、倒卖用户手机号、身份证等隐私信息，一经查实立即开除并移交司法机关；因管理疏漏造成大规模用户信息泄露的，追究部门负责人管理责任。

第五章 附则

本制度由贵州零果科技有限公司技术部、风控合规部共同负责解释、定期修订。

本制度自零果直播平台正式上线运营之日起实施。