突发事件应急制度

第一章 总则

1.1 制定目的

为有效预判、防范、处置零果直播平台运营过程中发生的技术安全突发事件、生产安全突发事件、内容安全突发事件，最大限度降低各类突发事故造成的人员、财产、舆情、合规损失，规范应急预警、分级响应、现场处置、事后复盘全流程工作，依据《网络安全法》《突发事件应对法》《互联网直播服务管理规定》等法律法规，结合我司网络表演业务实际，制定本突发事件应急管理制度。

1.2 应急组织架构

1.2.1 应急领导小组

组 长：田涵（公司法定代表人、总经理）

副组长：肖家松（技术总监、合规风控负责人）

成 员：运维、内容审核、主播运营、客服、行政财务部门负责人。

1.2.2 四大专项应急处置小组

技术安全应急小组：全体运维、技术研发人员，负责服务器故障、网络攻击、数据泄露、系统宕机等技术类突发事件排查、止损、修复处置；

内容安全应急小组：内容自审负责人、全体直播巡检审核人员，负责违规直播内容、舆情事件、群体性不良互动等内容类突发事件封堵、证据固定、处置上报；

生产安全应急小组：行政、人事、办公运维人员，负责线下办公场所消防、用电、人员人身安全、办公设备突发事故应急处置；

舆情与客服善后小组：客服、品牌运营人员，负责用户安抚、投诉集中处置、官方信息公示、监管部门材料报送。

1.3 突发事件分级标准

Ⅰ 级（特别重大突发事件）：全网平台瘫痪、大规模用户信息泄露、直播间出现涉政、恐怖、色情极端违规内容引发全网舆情、线下重大消防人身安全事故，需要立即上报属地文旅、网信、公安、应急管理部门。

Ⅱ 级（重大突发事件）：单区域服务器宕机、高频 DDoS 攻击、多名主播集中违规引发群体性投诉、办公场所火灾漏电等较大安全事故，由公司应急领导小组统筹处置，24 小时内向主管部门报备。

Ⅲ 级（一般突发事件）：单台直播间推流故障、单条违规弹幕 / 单次轻微主播违规、办公小型设备故障，由对应专项应急小组当场处置，事后台账记录归档。

第二章：技术安全突发事件预测及应急处置措施

2.1 技术安全突发事件类型预判

网络攻击类：DDoS 流量攻击、SQL 注入、恶意爬虫、勒索病毒入侵、后台暴力破解；

系统故障类：服务器硬件宕机、带宽满载断网、直播流媒体推流崩溃、数据库异常锁死、线上功能大面积 BUG；

数据安全类：用户实名数据、交易运营数据泄露、核心备份数据

误删除、第三方支付接口异常扣费；

账号风控类：大规模账号被盗、批量恶意注册薅羊毛、虚假刷单套取平台资产。

2.2 事前预警预防措施

搭建服务器、带宽、数据库全链路实时监控告警系统，设置负载、访问量、异常 IP 访问阈值，触发阈值自动向技术应急小组全员推送短信、企业微信告警，实现风险提前预判。

定期每月漏洞扫描、每半年第三方渗透测试，及时修复系统安全漏洞；全站 HTTPS 防护、WAF 防火墙常态化开启，异地多备份每日自动执行。

技术岗位实行 7×12 小时值班制度，节假日安排运维人员轮班值守，确保技术突发故障可第一时间响应处置。

提前配置备用服务器、备用带宽、数据库灾备恢复方案，定期每季度开展技术应急演练，模拟宕机、攻击、数据泄露场景演练切换恢复流程。

2.3 分级应急处置措施

2.3.1Ⅲ 级一般技术故障

技术人员 10 分钟内远程排查故障节点，重启服务、调整带宽参数快速修复；

故障期间安抚主播、直播间用户，故障修复后做好故障原因记录，优化程序 BUG；

2.3.2Ⅱ 级重大技术事件

应急小组 15 分钟内切断受攻击 IP、启用防火墙拉黑恶意访问地址，立即切换至备用服务器、备用带宽，恢复平台基础访问；

冻结异常批量账号，调取访问日志溯源攻击来源，固定网络攻击证据；

领导小组研判事件影响范围，24 小时内向网信、文旅部门书面报备事件情况、处置措施；

排查漏洞根源，全面加固安全防护策略，全平台推送故障致歉公告，妥善处理用户充值异常、观看权益受损引发的退费纠纷。

2.3.3Ⅰ 级特别重大技术事件

立即关停平台公网访问权限，防止泄露范围持续扩大，技术小组第一时间启动异地灾备备份恢复数据；

固定全部攻击日志、泄露数据范围证据，1 小时内上报属地公安网安、网信、文旅主管部门，同步留存所有涉案线索配合立案侦查；

舆情善后小组第一时间发布官方公告，告知用户风险防范措施，开通专项投诉退费通道；

全面溯源漏洞，全系统安全重构升级，经第三方安全检测合格后方可分批恢复平台线上服务；

事后开展全面复盘，追究安全管理失职人员责任，完善技术防护、值班巡检制度。

第三章：产安全突发事件预测及应急处置措施

3.1 生产安全突发事件类型预判

本平台生产安全主要为公司线下办公经营场所安全事件：办公区

域电气线路短路引发火灾、漏电触电事故；办公设备爆炸、消防设施故障；自然灾害导致办公场所受损；员工办公期间人身意外伤害、群体性公共卫生事件；档案机房涉密资料损毁、服务器机房断电失火等安全事故。

3.2 事前预警预防措施

行政部门每月开展办公场所消防安全排查，检查消防灭火器、应急通道、电气线路、机房稳压供电设备，杜绝私拉电线、大功率违规用电，堵塞消防通道等隐患；

办公区域、服务器机房张贴安全疏散示意图、消防应急联系方式，定期组织全员消防演练、触电应急救援培训；

服务器机房配置 UPS 不间断应急电源、气体灭火消防装置、温湿度监控系统，安排专人定期巡检，防止机房高温失火、断电数据丢失；

建立恶劣天气预警机制，收到暴雨、雷电等气象预警时，提前做好机房断电防护、重要纸质电子档案异地转移备份。

3.3 分级应急处置措施

3.3.1 Ⅲ 级一般生产安全事件

现场人员第一时间切断故障设备电源，使用就近消防器材处置初期险情，疏散周边办公人员；

行政安全负责人现场排查隐患，维修更换故障设备，做好安全事件记录，杜绝同类隐患重复发生。

3.3.2 Ⅱ 级重大生产安全事件

立即启动消防应急疏散，组织全员沿安全通道撤离至室外安全区域，拨打 119、120 急救电话；

技术人员第一时间启用 UPS 应急电源保护服务器数据，有序正常关机避免硬件损坏；

行政小组保护事故现场，配合消防、医护人员开展救援，统计人员受伤、财产损失情况，及时上报公司应急领导小组；

事故处置完毕后全面排查办公场所安全隐患，整改全部风险点，组织全员安全警示教育。

3.3.3Ⅰ 级特别重大生产安全事件

第一时间全员紧急疏散，拨打 119、120、110 报警，优先保障人员生命安全；

技术人员在安全前提下尽可能转移加密备份存储介质、核心业务数据硬盘，最大限度降低数据资产损失；

公司应急总指挥 1 小时内向属地应急管理、文旅主管部门上报重大安全事故；

配合政府部门开展事故调查、伤亡善后赔付工作，全面关停办公场所开展安全整改，整改验收合格后方可复工运营。

第四章：内容安全突发事件预测及应急处置措施

4.1 内容安全突发事件类型预判

单直播间主播出现涉政、色情、暴力、分裂、宗教极端等严重违法违规直播表演内容；

多个直播间集中出现同类违规内容、批量用户发布煽动性、造谣

类弹幕引发网络舆情；

主播网暴未成年人、公开泄露他人隐私引发全网负面舆论、大规模用户集体投诉；

直播内容被恶意剪辑断章取义在全网传播，引发针对平台的负面舆情危机；

未经审核的侵权、虚假宣传类直播内容大范围传播，引发版权纠纷、消费者维权群体性事件。

4.2 事前预警预防措施

严格落实“先审后播 + 7×24 小时实时双人巡检”制度，AI 敏感内容全量实时预警，违规内容毫秒级拦截；

建立内容舆情实时监测机制，专人全网监测短视频平台、社交论坛关于本平台直播内容的舆情信息，提前捕捉负面风险苗头；

定期开展审核人员重大违规内容处置应急培训，明确严重违规内容关停、证据固定、上报标准化流程；

建立主播重大违规黑名单库，对有严重违规前科人员永久限制入驻，从源头防范重大内容安全事件。

4.3 分级应急处置措施

4.3.1Ⅲ 级一般内容安全事件

巡检人员立即弹窗警告、删除违规评论，要求主播 3 分钟内现场整改，同步录入违规台账；

全程录屏留存违规片段，事后对主播开展合规警示教育，无需对外上报监管部门。

4.3.2Ⅱ 级重大内容安全事件

立即关停涉事直播间，固定直播回放、违规截图、音频全部证据，对涉事主播短期封禁、约谈处罚；

舆情小组全网排查同类违规内容，批量删除违规素材，针对网络负面言论及时发布官方澄清公告，引导正向舆论；

24 小时内向属地文化和旅游行政部门提交事件处置报告、违规证据、整改方案；

全面复盘审核漏审漏洞，升级敏感词库、加密重点直播间巡检频次，对全体主播开展专项合规警示教育。

4.3.3Ⅰ 级特别重大内容安全事件

巡检人员立即一键永久关停涉事直播间，切断直播推流，固定全部原始音视频、弹幕、主播实名证据，严禁删除、篡改任何涉案数据；

应急领导小组 1 小时内将事件情况、违规证据、初步处置措施书面上报属地文旅、网信、公安部门，主动配合执法调查；

舆情善后小组统一官方对外口径，及时发布事件处置公告，开通用户投诉专线，主动安抚公众情绪，杜绝谣言二次扩散；

全面暂停平台新主播开播申请，开展全平台内容合规专项自查整改，对所有在播直播间升级双人 24 小时值守巡检；

事件结案后开展全员深度复盘，追究审核、运营管理人员失职责任，完善内容自审、主播准入全链条管控机制，整改验收合格后方可恢复平台正常运营。

第五章：事后应急复盘、演练与档案管理

每一起突发事件处置完毕后 7 个工作日内，应急领导小组组织专项复盘会议，梳理事件诱因、处置短板，修订完善本应急预案、优化安全防控措施；

公司每半年至少组织一次综合性应急演练，分别针对技术攻击、重大内容违规、办公消防安全三类场景开展实战演练，留存演练方案、现场照片、演练总结报告；

所有突发事件受理材料、处置记录、证据文件、上报回执、复盘报告统一归档，档案保存期限不少于 5 年，随时接受监管部门核查。

第六章 附则

本制度由贵州零果科技有限公司应急管理领导小组负责解释，根据国家应急管理、网络安全法律法规适时修订。

本制度自发布之日起正式施行。