ICS 03.080.01
CCS A10

DB43

湖 南 省 地 方 标 准

DB 43/T 2740—2023

公共资源交易服务安全与应急管理规范

Specification for safety and emergency management of public resource transaction services

2023－08－10 发布　　2023－11－10 实施

湖南省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由湖南省公共资源交易中心提出并归口。

本文件起草单位：湖南省公共资源交易中心、国泰新点软件股份有限公司、广联达科技股份有限公司、湖南省标准化协会。

本文件主要起草人：刘定文、韩伟、欧益清、胡雄鸽、刘欢、李中华、高阳、桂丹妮、于权、李青松、丁盛、唐国伟、白冰彦。

公共资源交易服务安全与应急管理规范

1 范围

本文件规定了公共资源交易平台服务机构在服务过程中的安全与应急管理工作的总体要求、安全要求和应急管理要求。

本文件适用于公共资源交易平台服务机构在服务过程中的安全与应急管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2893.1 图形符号 安全色和安全标志 第1部分：安全标志和安全标记的设计原则

GB/T 2894 安全标志及其使用导则

GB/T 9361 计算机场地安全要求

GB/T 10001.1 公共信息图形符号 第1部分：通用符号

GB 14934 食品安全国家标准 消毒餐（饮）具

GB 17859 计算机信息系统安全保护等级划分准则

GB/T 18894 电子文件归档与电子档案管理规范

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20270 信息安全技术 网络基础安全技术要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 20275 信息安全技术 网络入侵检测系统技术要求和测试评价方法

GB/T 20281 信息安全技术 防火墙安全技术要求和测试评价方法

GB/T 21061 国家电子政务网络技术和运行管理规范

GB/T 22081 信息技术 安全技术 信息安全控制实践指南

GB/T 25068.1 信息技术 安全技术网络安全 第1部分：综述和概念

GB 50016 建筑设计防火规范

GB 50166 火灾自动报警系统施工及验收标准

GB 50222 建筑内部装修设计防火规范

GB 50325 民用建筑工程室内环境污染控制规范

GB 50348 安全防范工程技术标准

GB 50354 建筑内部装修防火施工及验收规范

GA/T 367 视频安防监控系统技术要求

GM/T 0115 信息系统密码应用测评要求

GM/T 0116 信息系统密码应用测评过程指南

DB43/T 2427 公共资源交易网上开标服务规范

DB43/T 2733.1 公共资源交易专家抽取服务规范 第1部分：综合评标专家

DB43/T 2734 公共资源交易电子评标（审）服务规范

3 术语和定义

DB43/T 2427界定的以及下列术语和定义适用于本文件。

3.1

交易场所 trading places

公共资源交易平台服务机构为公共资源交易相关交易主体、社会公众、行政监督管理部门等提供从事公共资源交易活动的场地。

4 总体要求

4.1 应设立应急管理领导小组（以下简称“领导小组”），主要负责人为第一责任人，领导小组下设办公室，并设置工作组负责对应的安全与应急管理工作。

4.2 应建立交易场所安全、公共安全、信息系统安全、交易服务安全等应急管理制度。

4.3 应配备具有专业知识的工作人员负责安全管理。

4.4 应定期开展安全宣传教育或应急技能培训及与岗位相关的职业道德培训。

4.5 应对交易场所潜在风险进行辨识和评估，根据对潜在风险的评估结果制定应急处置预案。

4.6 应定期或不定期开展安全与应急演练，加强各部门、人员之间的沟通与协调，提高应急救援人员的救援熟练程度和技术水平，并对演练中发现的问题进行分析、整改。

4.7 安全与应急管理过程应形成记录并予以保存。

5 安全要求

5.1 交易场所安全

5.1.1 消防安全

5.1.1.1 应设置消防控制室（值班室），并配备电话、警铃等联络通讯装置。

5.1.1.2 应配置各类消防设施，如消防栓、灭火器、防毒面具、火灾自动报警系统等设备设施，并符合 GB 50166 的要求，定期对消防设施设备进行维护检修。

5.1.1.3 应在交易场所醒目位置采用适当方式设置楼层导向图、功能分区平面图、安全疏散路线图，疏散距离、安全出口位置、疏散通道宽度设计等应符合 GB 50016 的相关要求。

5.1.1.4 应保持疏散通道、安全出口畅通。疏散通道、安全出口疏散门设置的电子门锁、门禁应可在灾警时自动解锁和解禁。

5.1.1.5 应定期或不定期组织消防检查和消防演练，开展火灾隐患整改工作。

5.1.2 设备设施安全

5.1.2.1 应设置清晰、易于识别的导向标识、门牌标识、禁止标识、安全标识、疏散指示标识以及不同人员通道的标识标志，且标识标志符合 GB/T 2893.1、GB/T 2894、GB/T 10001.1 的要求。

5.1.2.2 应将设备安全操作规程、登记标志、警示标志、安全注意事项、应急救援电话号码置于操作场所醒目位置，并保持完好。

5.1.2.3 应对在用设备如电梯等特种设备和发电机、门禁、音视频、网络监控等日常设备使用情况进行日常巡检，发现安全问题要及时上报处理，并做好相关记录。

5.1.2.4 对设备设施的安装、改造、重大修理，应由具有相关许可资质的专业机构按照安全技术规范的要求进行。

5.1.2.5　应建立设备设施安全档案，并安排工作人员负责相关档案的保管。
5.1.2.6　应配备应急照明和备用电源系统，在电网出现故障发生短时间停电时，维持电力的正常供应。
5.1.2.7　定期检查水电气暖线路、管道，保证正常运行。
5.1.2.8　未取得相关产权单位或组织管理单位的同意，不应擅自改装、拆除、迁移井盖、阀门和仪表等水电气暖设施，应在取得允许的情况下进行检修改造，并做好安全防护。

5.1.3　建筑工程安全

5.1.3.1　应按照国家及地方有关法律法规取得交易场所新建、扩建、改建等建设工程的建设行政许可。交易场所建设工程的设计、施工、验收、移交应符合国家、行业及地方工程建设标准的规定。
5.1.3.2　交易场所装饰装修改造不应改动原有的建筑承重结构。
5.1.3.3　交易场所建筑室内装修防火应符合 GB 50016、GB 50222、GB 50354 的规定。
5.1.3.4　交易场所室内装修装饰使用的工程材料应符合 GB 50325 的要求。

5.2　信息化系统安全

5.2.1　内部网络信息系统安全

5.2.1.1　网络安全应符合 GB/T 20270、GB/T 21061、GB/T 25068.1 的有关要求。
5.2.1.2　信息安全应符合 GB/T 22081、GB/T 20269、GB/T 20271 相关要求。
5.2.1.3　宜对使用商用密码进行保护的关键信息基础设施、信息系统，每年开展不少于一次的商用密码应用与安全性评估工作，测评工作符合 GM/T 0115、GM/T 0116 的要求，发现问题及时组织整改。
5.2.1.4　涉及的各业务系统应符合信息安全等级保护要求，并采取身份识别、权限控制、防计算机病毒、防木马及防攻击等技术措施。
5.2.1.5　应制定分级、分类的不同系统权限管理和身份认证制度，包括不限于人员权限、操作规范和安全防护等。
5.2.1.6　应提供多层次安全控制手段，局域网与互联网的接口应建立安全隔离区，可采用防火墙、信息过滤、入侵检测、防病毒网关等安全措施，防止内部敏感信息的外泄和外部网络攻击。
5.2.1.7　应定期做好所有系统网络杀毒、防火墙升级等工作，及时查找、修复系统漏洞，提升网络安全防护能力。
5.2.1.8　应对重要数据进行异地容灾备份。
5.2.1.9　应对电子交易系统、电子服务系统、网络安全审计的监督行为以及各级系统管理员的操作行为和日常运维情况进行详细记录，记录保存时间应符合相关法律法规规定且不少于 6 个月，并提供统计、审计与分析功能。

5.2.2　外部系统接入安全

5.2.2.1　互联网接入应符合 GB/T 20281、GB/T 20275 的安全要求。
5.2.2.2　接入的第三方系统应遵循以下安全要求：

——应制定服务终端软件的操作规程，并要求工作人员按操作规程执行服务终端软件管理操作；
——应根据各部门连接范围的不同和承载信息系统的安全等级的不同，划分不同的子网，并根据等级保护要求，为各子网分配 IP 地址段，实施不同强度的安全保护；
——应设置终端准入控制策略，通过物理接入点或办公终端 MAC 地址等物理因素，外部访问终端接入到指定的物理子网或逻辑子网中；
——应提供并启用用户鉴别信息复杂度检查功能，并采用国家规定的加密算法传输用户的账号信息，保证身份鉴别信息不易被冒用；

——应限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问；
——应设置登录策略，具备防范账户暴力破解攻击措施的能力，如限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定。所有用户的登录密码要求长度至少 8 位，数字、小写字母、大写字母和特殊符号至少包含三种；
——应设置并启用重要软件日志审计策略，对软件增加、修改、删除等软件变更情况进行审计，审计信息应包括日期、时间、来源、用户、操作、结果等要素，审计数据保存在独立于被保护的客户端；
——当用户和业务系统的通信双方中的一方在一段时间内未作任何响应，另一方应能自动结束会话；
——应限制用户在信息发布、交易过程中上传文件的大小、类型及路径，并关闭 web 服务器对上传目录的脚本执行权限与文件可执行权限；
——应保持技术中立，为电子标书制作、造价、电子辅助评标等各类第三方工具软件开放数据标准接口，不应限制符合技术规范的工具软件与其对接，不应捆绑第三方工具软件。

5.2.2.3　应建立信息安全保障体系，充分利用网络隔离闸、身份认证、电子签章、数据加密等技术措施。

5.2.2.4　接入的第三方系统的运营商（企业）应符合 GB 17859 规定，将系统定为三级（或三级以上），并按要求每年开展不少于一次测评，发现问题及时组织整改。

5.2.3　网络设备安全

5.2.3.1　应根据系统业务应用需求，对数据库服务器等关键应用服务器进行异地备份，实现主机故障切换，保证系统连续可用性和安全可靠性。

5.2.3.2　对网络设备进行维护时，应安排技术人员现场全程监督，对设备进行验收、病毒检测和登记核查。

5.2.3.3　机房应采取措施防止产生水、火和易燃、易爆物品等安全隐患，且符合 GB/T 9361 要求。

5.2.3.4　对网络服务设备的防毁、防电磁辐射泄漏、抗电磁干扰及电源保护等采取技术保护措施，传输线路的抗干扰和防电磁骚扰应符合 GB 50348 的相关要求，电磁辐射防护应符合 GA/T 367 的相关要求。

5.2.4　数据安全

5.2.4.1　按照“谁采集、谁负责；谁产生、谁负责；谁提供、谁负责”的原则对交易过程中所需使用的数据根据数据标准规范进行采集汇聚运用，建立数据存储、容灾备份、访问控制、数据审计、日志追溯、定期巡查、应急演练等数据安全措施。

5.2.4.2　根据数据传输要求，采用适当的加密保护措施，保障传输通道、传输节点和传输数据的安全，防止传输过程中的数据泄露。

5.2.4.3　应对重要数据进行安全监测，定期对系统后台打开记录、数据拷贝记录等进行检测。

5.2.4.4　应与运维服务单位签订保密协议，保障系统数据安全。

5.2.4.5　数据出现问题时，应由技术部门提供现场技术支持，恢复后，进行验证、确认。

5.2.4.6　备份数据应根据备份要求进行定期保存或永久保存，并确保可以随时使用，数据清理实施应避开业务高峰期，避免对联机业务运行造成影响。

5.2.4.7　数据的转存和查询使用应在介质有效期内进行，通过有效的查询、使用方法保证数据的完整性和可用性，同时做好详细记录。

5.2.4.8　数据使用及存放数据介质的调拨、转让、废弃或销毁应按照程序进行逐级审批后，方可处理。

5.2.4.9　按照“一项目一档”的要求，将交易服务过程中产生的电子文档、音视频等数据资料按规定统一归档，保证档案的安全、保密，归档案卷需齐全、完整、目录清晰。

5.2.4.10　电子档案的采集、整理、归档、管理应遵循统一标准，通过技术手段，确保电子档案客观、真实、完整地反映交易活动的全过程。

5.2.4.11　电子档案管理应符合 GB/T 18894 及以下要求：

——归档载体应作防写入处理，避免擦、划、触摸记录涂层；

——单片载体应装盒，竖立存放，且避免挤压；

——存放时应远离强磁场、强热源，并与有害气体隔离；

——超过保管期限的电子档案的鉴定和销毁应按规定流程审批后，方可处理。

5.2.4.12　查阅和借阅档案数据时，应履行审批登记手续和权限分级，用毕立即归还，并办理注销手续，不应转借。

5.3　公共安全

5.3.1　重大疫情防控

5.3.1.1　应按疫情防控政策制定防控应急方案，做好宣传告知、人员防护、卫生消毒、应急处置工作。

5.3.1.2　应配备具有基本防控知识的防控工作人员。

5.3.1.3　应配备相应的防护物资，并做好应急物资储备和调度。

5.3.1.4　应按防疫管理要求对进入交易场所的人员进行防疫检查，做好信息登记工作，必要时按防控要求进行限流、劝返、隔离等防护措施。

5.3.1.5　应对交易场所进行卫生清洁、消毒，保持环境清洁，通风换气。

5.3.1.6　交易场所现场工作人员及现场交易主体人员应执行疫情管理要求，主动做好个人健康监测。

5.3.1.7　应开通电话预约、不见面开标等网上办事的渠道，引导交易主体网上办理。

5.3.2　治安防控

5.3.2.1　应组织工作人员对各公共区域开展日常巡查、安防工作。

5.3.2.2　应配备必要的防护、防暴、救生、通讯等器材，设置公共区域的监控系统，实施 24 小时不间断监控。

5.3.2.3　应保存公共区域视频监控数据，便于事后调查取证。

5.3.2.4　若发生案件，应注意保护现场，禁止无关人员破坏现场，配合公安部门开展调查、取证。

5.4　交易现场安全

5.4.1　交易现场

5.4.1.1　公共资源交易场所应配置自动体外除颤器、急救包等医疗急救物资，并进行检查、维护、保养，及时更新，确保其完好。

5.4.1.2　应按现场管理要求，引导交易主体及进入交易场所的人员遵守现场纪律，对进入交易现场封闭区域的人员应发放工作牌或其他身份识别标识，并要求规范佩戴。

5.4.1.3　应提供物理隔离的评标（评审）封闭空间和具录音功能的语音呼叫系统，确保评审过程保密。评标专家管理应符合 DB43/T 2734 相关要求。

5.4.1.4　专家中途需要退出评标或在评标过程中因突发身体原因无法继续评标的，应按本文件 6.1.3 的应急处置流程处理。

5.4.2　业务中断

5.4.2.1　应引导交易主体按业务流程和交易系统提示进行操作。应通知相关部门进行处置，并及时向交易主体说明处置情况。

注：业务流程主要包括业务咨询、项目登记、场地安排、公告和公示信息公开、交易过程保障、资料归档、数据统计与综合利用、档案查询等。

5.4.2.2　因停电、设备运行、网络通信、电子交易系统故障或人员操作失误导致交易活动无法开展或中断的，应查明原因，排除故障，并记录故障处理情况。

5.4.2.3　短时间可排除故障的，故障排除后继续交易活动。

5.4.2.4　短时间内无法排除故障的，应协助交易主体做好资料封存和情况记录，待故障排除后再重新预约场地恢复交易活动。

5.4.2.5　依法暂停或终（中）止交易的，应通过信息发布渠道发布公告通知交易主体，并向行业监管部门报告。

6　应急管理

6.1　预防与处置

6.1.1　监测预警

6.1.1.1　应对交易场所的公共环境、配套的设施设备、公共资源电子交易系统等日常运行情况进行监测，辨识潜在风险，对风险隐患进行调查和评估分析，制定风险防范措施和应急处置预案，及时防范风险发生，排除风险隐患。

6.1.1.2　应定期收集、更新国家及本地发布的安全及应急有关的法律法规、政策文件，评估现有安全及应急工作的适用性。

6.1.2　信息报送

6.1.2.1　突发事件发生后，现场工作人员应立即报告领导小组，领导小组负责有关突发事件信息的核实、上报，并决定是否启动应急处置预案。

6.1.2.2　根据突发事件的紧急程度，采用电话、书面等报告形式，报送内容包括并不限于突发事件的时间、地点、规模、涉及人员、破坏程度、伤亡等事项，并根据事态的发展状况及时续报信息。

6.1.3　应急处置

6.1.3.1　应依据风险评估结果制定风险防范措施和应急处置预案。应急处置预案中应明确应急响应责任人、风险隐患监测、信息报告、预警响应、应急处置流程、人员疏散撤离组织和路线、可调用或可请求援助的应急资源情况及如何实施等，应急处置流程宜包括以下：

——信息化系统安全事件应急处置流程，见附录A；

——公共安全事件应急处置流程，见附录B；

——消防安全事件应急处置流程，见附录C；

——重大疫情防控应急处置流程按照国家相关防控要求；

——交易服务安全事件应急处置流程按DB43/T 2733.1、DB43/T 2734相关要求。

6.1.3.2　突发事件发生后，应及时对突发事件具体情况进行分析，按照相应的应急管理预案进行处置。

6.1.3.3　突发事件造成的威胁和危害得到控制或基本消除，应急处置工作即告结束，由领导小组宣布应急处置工作解除。

6.2　事后管理

6.2.1　应成立事件调查组，协助相关部门对突发事件的起因、过程、性质、人员伤亡、财产损失等情况进行调查、分析，形成调查报告，提出处理意见和防范类似事件发生的建议，报领导小组。采取必要的措施，恢复正常运行秩序。

6.2.2　事故原因查清后，应总结事件处理过程中的经验，并对原突发事件应急预案进行评估和完善。

6.2.3　应根据事件处置情况做好后续发布工作，按照信息公开相关要求及时发布事件原因、责任及处理结果等信息。

6.2.4　应对突发事件中应急处置过程情况进行全面整理、统计和登记，收集收发的信息、现场录像、图片等见证材料整理归档，形成应急管理档案。

6.2.5　应建立异常情况登记台账，每月对异常情况进行分析研判，总结交易现场异常情况多发重点环节、高发人群行为，分析异常情况出现原因，制定改进措施，进一步规范交易现场服务工作，确保各类交易活动正常开展，建立健全交易现场异常情况防控的长效机制。

6.3　评价与改进

6.3.1　应定期组织开展安全与应急检查和评价，内容包括但不限于：

——安全与应急管理制度执行的有效性；

——安全与应急管理方案或应急演练实施情况；

——安全与应急措施的适宜性、有效性。

6.3.2　应针对发现的问题制定整改计划，采取纠正措施，并督促相关部门和人员落实整改计划，持续改进。

附 录 A
（资料性）
信息化系统安全事件应急处置流程

A.1 电源断电事件处置流程

发生断电事故时，应按以下流程处置：
——启动UPS供电系统，并检查UPS是否正常供电；
——查明故障原因；
——备份服务器数据、交换机配置；
——必要时主动关闭服务器、交换机、存储等设备，以免设备损坏或数据损失；
——通知相关部门进行电源维修，评估供电恢复时间；
——及时上报，做好事件记录。

A.2 局域网中断事件处置流程

发生断网时，应按以下流程处置：
——信息技术人员判断故障节点，查明故障原因；
——若是线路故障，重新安装线路；
——若是路由器、交换机等设备故障，应立即从指定位置将备用设备取出接上，并调试畅通；
——若是路由器、交换机等配置文件损坏，应迅速按照要求重新配置，并调试畅通；
——及时上报，做好事件记录。

A.3 核心交换机故障事件处置流程

发生核心交换机故障时，应按以下流程处置：
——检查、备份核心交换机日志；
——启用备用核心交换机，检查接管情况；
——备份核心交换机配置信息；
——将服务器接入备用核心交换机，检查服务器运行情况，将楼层交换机、接入备用核心交换机，检查各交换机运行情况；
——联系供应商维修核心交换机；
——及时上报，做好事件记录。

A.4 光缆线路故障事件处置流程

发生光缆线路故障时，应按以下流程处置：
——立即联系技术人员携带辅助材料，及时熔接连通；
——检查并做好备用光缆或备用芯的跳线工作，随时切换到备用网络；
——及时上报，做好事件记录。

A.5 计算机病毒爆发事件处置流程

发生计算机中毒事故时，应按以下流程处置：
——关闭计算机病毒段上的端口；
——隔离中病毒计算机；

——关闭中病毒计算机上联端口；
——根据病毒特征使用专用工具进行查杀；
——系统损坏的计算机在备份其数据后，进行重装；
——通过专用工具对网络进行清查；
——及时上报，做好事件记录。

A.6 服务器设备故障事件处置流程

发生服务器故障时，应按以下流程处置：
——主要服务器应做多个数据备份；
——如能自行恢复，则立即用备件替换受损部件，如：电源损坏更换备用电源，硬盘损坏更换备用硬盘，网卡、主板损坏启用备用服务器；
——若数据库崩溃应启用备用系统，并检查备用服务器启用情况；
——对主机系统进行维修并做数据恢复；
——如不能恢复，立即联系设备供应商安排技术人员前来维修；
——及时上报，做好事件记录。

A.7 网络攻击事件处置流程

发生黑客等不明网络攻击时，应按以下流程处置：
——若通过入侵监测系统发现有黑客进行攻击，立即通知信息技术人员处理；
——将被攻击的服务器等设备从网络中隔离出来；
——及时恢复重建被攻击或被破坏的系统；
——查看被攻击服务器硬件、软件配置参数、审计记录等方面进行调查取证，通过备份等方式收集攻击者证据；
——及时上报领导小组，若事态严重，联系公安部门报警，做好事件记录。

A.8 机房设备设施异常事件处置流程

对于机房电源断电、空调报警、网络设备监测异常时，应按以下流程处置：
——立即判断故障节点，查明故障原因；
——备份服务器数据、交换机配置，并通知维修人员进行维修；
——若造成路由器、交换机等配置文件损坏，应迅速按照要求重新配置，并调试畅通；
——必要时应上报请示，主动关闭服务器、交换机、存储等设备，以免设备损坏或数据损失；
——做好事故记录。

A.9 云数据库安全事件处置流程

发生云端数据库故障时，应按以下流程处置：
——应对云数据库系统做多个备份；
——发生数据库数据丢失、受损、篡改、泄露等安全事件时，信息技术人员应查明原因，按照情况采取相应措施，如更改数据库密码，修复错误受损数据；
——如果数据库崩溃，信息技术人员应启用备用系统，并向信息技术部门报告，在备用系统运行期间，信息技术人员对主机系统进行维修并作数据恢复；
——及时上报，做好事件记录。

A.10 数据信息泄密突发事件处置流程

在发生数据信息泄密事件时，应按以下流程处理：

——应在发现交易数据泄密的第一时间保护现场并向领导小组报告泄密事件发生的地点、时间和简要过程，研究处置方案；

——查明被泄密信息的主要内容、密级、数量及载体形式，以及可能造成的危害程度，事件的重要情节和有关责任人；

——调查泄密原因并进行搜索查找，尽快找到或锁定范围，必要时向公安部门报警处理；

——在事件未调查清楚前，应同相关部门进行协作预防媒体或网络上对泄密信息的报道或炒作；

——对出现在公共网络、出版物、广播、电视等媒体上的泄密信息，协调相关职能部门，责令有关单位立即删除、收缴、停播、销售,并收缴有关涉密载体；

——根据调查结果，由事件发生部门对相关责任人做出处理，需追究法律责任的,移交司法机关依法追究其责任。

A.11　信息内容安全突发事件处置流程

在发生信息内容安全事件时（利用信息网络发布、传播危害国家安全、社会稳定和公共利益的等不良信息内容事件），应按以下流程处理：

——应在发现信息内容安全事件的第一时间向领导小组报告事件发生的主要内容、数量及载体形式以及可能造成的危害程度，研究处置方案；

——调查信息内容安全事件发生原因并进行搜索查找，锁定范围，隔离网络，清除不良信息，必要时向公安部门报警处理；

——对出现在公共网络上的不良信息内容，协调相关职能部门，立即进行删除，消除不良影响；

——根据调查结果，由事件发生部门对相关责任人做出处理，需追究法律责任的,移交司法机关依法追究其责任。

附 录 B
（资料性）
公共安全事件应急处置流程

B.1 治安突发事件处置流程

发生打架斗殴、醉酒滋事、盗窃、外来暴力侵害等治安事件时，应立即向领导小组报告并向公安机关报警，并按以下程序处理：

——保持冷静，尽量避免人体冲撞，以保护人身安全为重；

——如有人员受伤，应立即拨打120求救；

——保护现场，及相关当事人的遗留物品，不应自行处理，要避免破坏指纹痕迹，配合交公安部门处理；

——做好相关事件记录。

B.2 停水、停电突发事件处置流程

B.2.1 接到计划性停水通知后，应立即将停水原因、停水时间通知各部门，提前采取应对措施。

B.2.2 发生突发停水事故时，应按以下程序处理：

——发现人员应立即通知相关部门组织人员进行抢修并通报全体人员停水原因、时间，尽快恢复供水，并将恢复过程相继汇报给领导小组；

——给水系统或消防系统出现故障，主管道或阀门发生破裂时，发现人员应立即通知相关部门，针对特殊事故可关闭阀门和电源，防止其他次生事故，马上组织人员实施抢修；

——故障结束后就事故情况、处理过程、处理结果及时上报领导小组。

B.2.3 在接到计划性停电通知时，应及时通知各部门停电原因和时间，并适当调整工作安排，做好重要设备的应急供电保障。

B.2.4 发生突然停电事故时，应按以下程序处理：

——立即启用备用电源或发电机；

——逐一检查电梯内有无被困人员并关注平台呼救报警信息，发现有人被困时，立即施救；

——立即检查供电系统，属外部供电故障的，与供电部门联系，问询停电原因，了解何时恢复供电；

——现场内部电路出现突发事故，应立即组织人员抢修，并将突发事故情况及时报告受影响部门，并告知预判的恢复供电时间，以便做出工作调整；

——提供照明灯具，加强巡视，维持现场秩序，如安全原因需安排人员离场时，应手动开启门禁，保证应急通道畅通；

——恢复正常供电后，相关部门应立即组织维修人员检查各相关设备，确保各系统正常运行；

——及时上报，做好相关事件记录。

B.3 可疑物品及其他危险物品事件处置流程

工作区域发现可疑爆炸物及其他危险物品时，应按以下程序处理：

——现场工作人员应立即上报，并向公安机关报警；

——设置隔离带，在保证安全的情况下对可疑物进行检查判断（但不应挪动可疑物），在不能确定可疑物危险程度时，不应擅自对可疑物采取任何处置行动；

——稳定现场人员情绪，做好人员疏散，必要时，可封闭交易现场，等候公安人员到场处置；

——当发生爆炸、毒气泄漏等事件时：

- 立即关闭现场中央空调或盘管空调风机，防止有毒气体通过空调系统扩散；
- 应立即启动排烟机组并开启现场窗户通风，排除有毒气体快速输送新风；
- 尽快指挥人员撤离现场；
- 有人员受伤时，应及时拨打 120 求救。

B.4 群体突发事件处置流程

发生公众聚集等群体事件时，应按以下程序处理：

——应立即向领导小组报告，维护好现场秩序，发生暴力行为时，应拨打110、120请求援助；

——现场工作人员应冷静处置，稳定人员情绪，及时做好疏导工作，防止事态激化；

——应在人员情绪相对稳定后，安排人员接待了解事由，做好记录，并根据事由通知相关部门处置；

——应密切关注事态的发展和处置情况，情况严重时，立即通知公安机关。

附 录 C
（资料性）
消防安全应急处置流程

C.1 用电事故突发事件处置流程

发生电气失火时，应按以下流程处置：

——立即切断事发地电源，利用附近的干粉灭火器等专用灭火器采取有效措施进行先期处置，报告领导小组，迅速组织人员参与灭火；

——发现有人触电，同时用绝缘工具帮助触电者脱离电源，视情况现场施救或送就近医疗机构急救；

——火情继续扩大的，迅速拨打119报警，如有人员受伤应首先抢救伤员，并拨打120救助；

——火灾无法控制时，领导小组应立即采取措施疏散人员，关闭供电系统，同时疏通消防通道，指定专人引导消防人员进入现场。

C.2 火灾突发事件处置流程

发现火灾时，应采取如下措施：

——立即按下火灾报警按钮，切断事发地电源，采取最快捷方式通知消防控制室操作人员、单位值班人员并上报；

——对火势较小，应立即组织人员使用消防设施、器材，扑救初起火灾，并在保障安全的同时，疏散群众、抢救着火物资；

——对较大火势，应稳定群众情绪，畅通消防通道，引导消防人员进入现场，组织引导人员疏散；

——应协助120抢救、护送受伤人员；

——现场警戒组阻止无关人员进入火场，维持现场秩序。