ICS 03.160
CCS A 00

DB51

四 川 省 地 方 标 准

DB51/T 1718—2024
代替 DB51/T 1718—2013

公共资源交易（服务）中心安全与应急规范

2024－05－08 发布　　2024－06－08 实施

四川省市场监督管理局　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。

本文件代替DB51/T 1718-2013《公共资源交易（服务）中心安全与应急规范》，与DB51/T 1718-2013相比，除结构性调整和编辑性修改外，主要技术内容变化如下：

a) 增加了规范性引用文件有关内容“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 13495.1 消防安全标志　第1部分：标志、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、GM/T 0115　信息系统密码应用测评要求、DB51/T 2775-2021 公共场所新冠肺炎疫情防控技术规范 ”　（见第2章）；

b) 增加了“网络信息安全要求”中的“信息安全”相关内容。（见5.1.1）

c) 增加了“网络设备安全”（见5.1.2）；

d) 增加了“数据安全”（见5.1.3）；

e) 增加了交易场所的“设施设备安全”（见5.2.2）；

f) 增加了“重大疫情防控”相关内容（见5.2.4）；

g) 增加了“重大疫情”应急处置要求（见6.2.7）；

h) 增加了“重大疫情防控应急处置”（见附录B.5）。

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专利的责任。

本文件由四川省政府政务服务和公共资源交易服务中心提出、归口并解释。

本文件起草单位：四川省政府政务服务和公共资源交易服务中心、四川省公共资源交易协会。

本文件主要起草人：吕芙蓉、张敬陆、舒新华、姚素英、龚太平、陈卫东、陈书、易雄、邹华娟、文满昌、佟巍、程红丽。

本文件及其所代替文件的历次版本发布情况为：

——DB51/T 1718，2013年首次发布；

——本次为第一次修订。

公共资源交易（服务）中心
安全与应急规范

1 范围

本文件规定了公共资源交易服务中心安全与应急管理的一般要求、安全要求以及应急处置要求。

本文件适用于四川省、市（州）、县（市、区）公共资源交易中心（含公共资源交易服务中心、政务服务和公共资源交易服务中心 ）。

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 13495.1 消防安全标志 第1部分：标志

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 22239 信息安全技术 网络安全等级保护基本要求

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/T 38315火灾应急预案

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

GB 55037 建筑防火通用规范

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

DB51/T 2775-2021 公共场所新冠肺炎疫情防控技术规范

3 术语和定义

本文件没有需要界定的术语和定义。

4 一般要求

4.1 设立安全应急管理领导小组，并设置工作组负责对应的安全与应急管理工作。
4.2 配备具有专业知识的工作人员负责安全管理。
4.3 建立信息安全制度、交易场所安全与应急管理制度，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。

5 安全要求

5.1 信息安全

5.1.1 网络及信息安全

5.1.1.1 网络安全应符合 GB/T 20270、GB/T 21061、GB/T 25068.1 的有关要求。
5.1.1.2 信息安全应符合 GB/T 22081、GB/T 20269、GB/T 20271 相关要求。
5.1.1.3 应对使用商用密码进行保护的信息系统适时开展风险评估（每年不少于一次），测评工作符合 GM/T 0115、GM/T 0116 的要求。
5.1.1.4 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。
5.1.1.5 网络安全专业技术岗位人员应获得网络安全专业资质。
5.1.1.6 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。
5.1.1.7 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。
5.1.1.8 应定期做好所有系统网络杀毒、防火墙升级等工作，及时对系统漏洞、包括中间件和插件等第三方服务漏洞进行修复升级，提升网络安全防护能力。
5.1.1.9 建立异地容灾备份系统，对重要数据进行备份。
5.1.1.10 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并保存，并提供统计、审计与分析功能。

5.1.2 网络设备安全

5.1.2.1 应根据公共资源交易系统业务应用需求，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。
5.1.2.2 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。
5.1.2.3 机房应符合 GB/T 9361 要求，应防止产生水、火和易燃、易爆物品等安全隐患。

5.1.2.4　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。

5.1.3　数据安全

5.1.3.1　公共资源交易数据安全管理坚持“谁采集、谁负责；谁产生、谁负责；谁提供、谁负责”的原则。

5.1.3.2　应对交易过程中使用、产生的数据，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。

5.1.3.3　数据存储，应采用数据加密、隐私计算和身份认证等技术手段，对数据实施分类分级保护。

5.1.3.4　数据传输，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。

5.1.3.5　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。

5.1.3.6　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。

5.1.3.7　数据的转存和查询应在介质有效期内进行，转存、查询应保证数据的完整性和可用性，做好转存、查询记录。

5.1.3.8　数据使用及存放数据介质的调拨、转让应按照权限进行审批。

5.1.3.9　数据及存放数据介质的废弃或销毁应履行审批权限。

5.1.3.10　应按照“一项目一档”的要求，将交易服务过程中产生的电子文档、音视频等数据资料统一归档，归档案卷需齐全、完整、目录清晰，档案的移送、保存应安全、保密。

5.1.3.11　电子档案的采集、整理、归档、管理应遵循统一标准，客观、真实、完地反映交易活动全过程；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。

5.1.3.12　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。

5.2　交易场所安全

5.2.1　消防安全

5.2.1.1　建立消防安全制度、消防安全操作规程，制定灭火和应急疏散预案。

5.2.1.2　按照国家标准、行业标准配置消防设施、器材。按 GB 50140 规定，结合场所的火灾类别和危险级别配置灭火器；火灾自动报警系统、自动喷水灭火系统、防排烟设施、防火分隔设施、消防电梯等建筑自动消防设施的设置应符合 GB 50016 和 GB 55037 的要求，并按 GB 25201 的要求进行日常维护保养。

5.2.1.3　按照 GB 13495.1 要求，设置消防安全标志。交易场所内外应设置清晰、易于识别的导向标识、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，疏散指示标志应醒目、无遮拦。

5.2.1.4　交易场所的疏散通道、疏散楼梯、安全出口和消防车通道应保持通畅，保证防火防烟分区、防火间距符合消防技术标准；常闭式防火门应保持常闭状态；公共区域的外窗不应设置障碍物。

5.2.1.5　定期组织对消防设施、消防安全标志和疏散通道等进行防火检查，并建立巡查记录，及时消除火灾隐患。
5.2.1.6　对职工进行岗前消防安全培训，定期组织消防安全培训和消防演练，对演练中发现的问题进行整改。
5.2.1.7　建立消防档案，确定消防安全重点部位，实行严格管理。

5.2.2　设备设施安全

5.2.2.1　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，保持完好。
5.2.2.2　应对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，发现问题及时上报处理，并做好记录。
5.2.2.3　对消防、燃气、电梯、报警等特种设备设施的安装、改造、维护应由具有相关许可资质的专业机构派出相应资质的专业人员，按照安全技术规范进行。
5.2.2.4　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。
5.2.2.5　宜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。
5.2.2.6　应定期检查水电气暖线路、管道，对井盖、阀门和仪表等水电气暖设施的改装、拆除、迁移、检修改造应取得相关产权单位的同意，开展维护、维修、清洁时应设置安全警示牌。

5.2.3　交易场所安保维护

5.2.3.1　应委派业机构或明确部门承担安全保卫机构职责，具体负责管理公共资源交易中心的办公区域、外围公共区域的安全保卫。
5.2.3.2　安全保卫机构应落实从事安保工作的人员；安保人员应着专用工作服，配备防刺服、防暴盾、钢叉、防暴棍、强光手电等必要的防暴器材。
5.2.3.3　安全保卫机构应建立健全登记、巡检、交接、值班等安全保卫制度。
5.2.3.4　安全保卫机构应安排专人对进入公共资源交易（服务）中心的人员、物品开展安全检查和引导，防止易燃易爆等危险物品进入交易场所，防止场内人员拥堵。
5.2.3.5　应定期检查、维护摄像仪、监控大屏等安全监控设施。

5.2.4　交易场所重大疫情防控

应做好疫情防控日常准备：
—— 按疫情防控政策制定应急预案；
—— 配备具有基本疫情防控知识的工作人员；
—— 配备相应的防护物资，并做好物资储备和管理；
—— 保持场所环境清洁，做好通风换气。

6　应急处置

6.1　应急预案

应针对交易场所安全、公共安全、信息安全的突发事件制定应急处置预案。

6.2　突发事件应急处置

6.2.1　信息化系统突发事件

公共资源交易信息系统发生突发事件时，应急处理宜参照附录A执行。

6.2.2 火情应急处置

交易场所发生火情时，参照附录B执行。

6.2.3 突然停电事故

交易场所突然停电时，参照附录B执行。

6.2.4 斗殴、骚乱、抢劫、畜意破坏等突发治安事件处置

交易场所发生斗殴、骚乱、抢劫、畜意破坏等突发治安事件时，参照附录B执行。

6.2.5 可疑爆炸物及其他危险物品

交易场所发现可疑爆炸物及其他危险物品时，参照附录B执行。

6.2.6 群众上访、聚集等突发事件

交易场所发生上访、人员聚集等事件时，参照附录B执行。

6.2.7 重大疫情

交易场所发生重大疫情时，参照附录B执行。

附 录 A
（资料性）
网络与信息化系统安全事件应急处置预案

A.1 事件分类分级

A.1.1 事件分类

网络与信息化系统安全事件包括但不限于有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件,具体划分如下:

——有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件；

——网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；

——信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件；

——信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件；

——设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障；

——灾害性事件是指由自然灾害等其他突发事件导致的网络信息安全事件。

A.1.2 事件分级

根据对业务可能造成的影响或已经造成影响的严重程度并结合资产的重要程度，把网络信息安全事件分为四级：Ⅰ级（特别重大网络信息安全事件）、Ⅱ级（重大网络信息安全事件）、Ⅲ级（较大网络信息安全事件）、Ⅳ级（一般网络信息安全事件）。

—— **Ⅰ级（特别重大网络信息安全事件）。**信息系统发生大规模瘫痪，事态发展超出管理单位的控制能力，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的突发公共事件，超过工作时间16小时不能恢复；

—— **II级（重大网络信息安全事件）。**信息系统发生大规模瘫痪，对国家安全、社会秩序、经济建设和公共利益造成严重损害，超过工作时间8小时未能恢复，需要其他单位协同处置的突发公共事件；

——**III级（较大网络信息安全事件）。**信息系统发生瘫痪，对业务使用单位造成一定损害，但在工作时间8小时内可以恢复的恶意攻击行为；

——**Ⅳ级（一般网络信息安全事件）。**信息系统受到一定程度的损坏，对所在用户的权益有一定影响，但在工作时间4小时内可以恢复。

A.2 事件预防处置

A.2.1 预防预警

A.2.1.1 加强信息系统日常管理，做好信息系统监控和运行管理、数据备份和安全管理等工作，做到早发现、早报告、早处置，防患于未然。

A.2.1.2 加强重要业务系统、数据库系统等关键设备设施和软件系统运行情况的监测和分析，在更换

关键硬件、重大更新等工作前，提前做好应急准备。

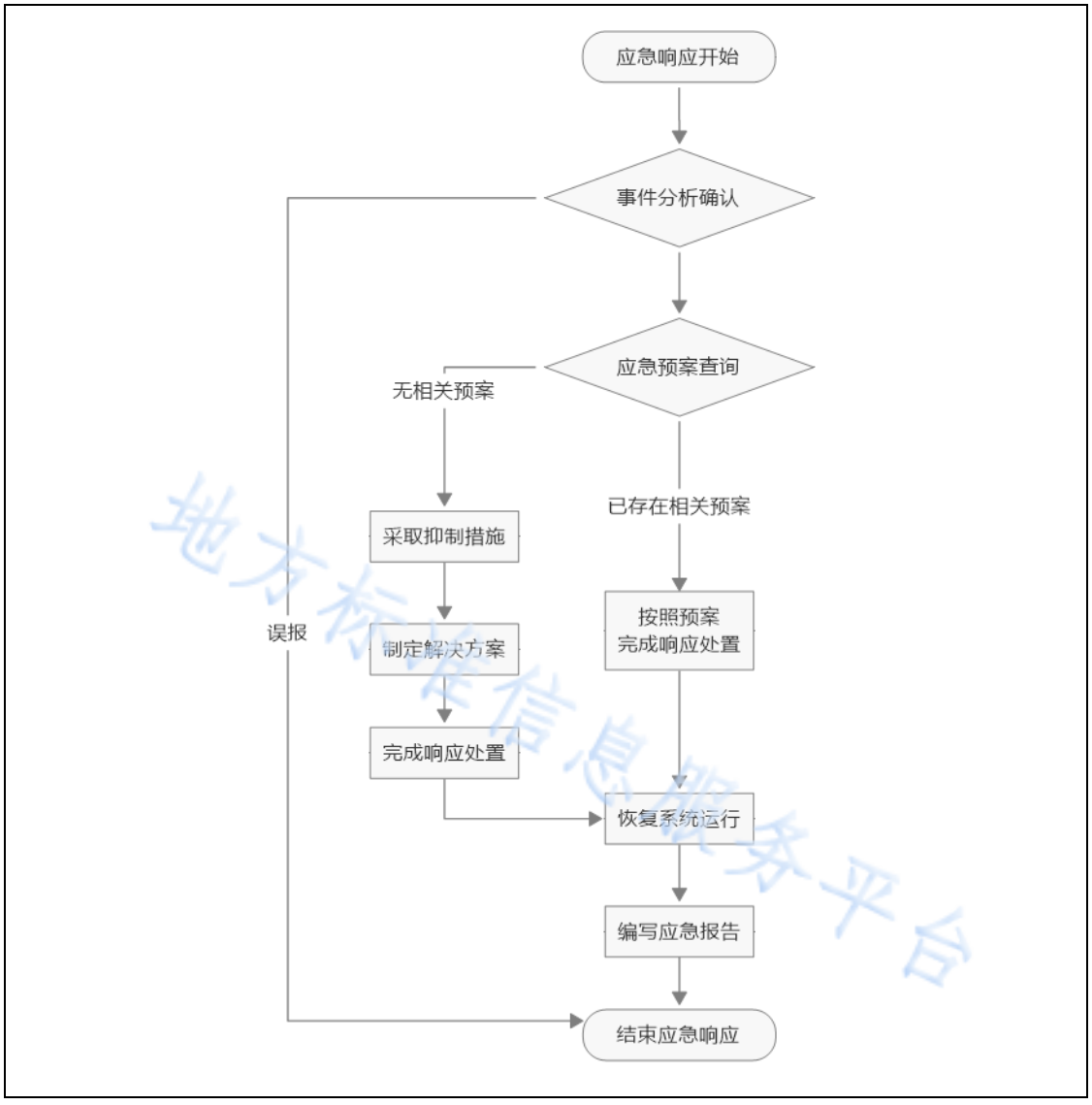
A.2.1.3　应要求网络运营商、云服务商确保基础设施的正常、稳定运行。若相关运营服务商有临时维护或变更，一定程度影响业务系统正常运行，应要求相关运营服务商提前 2 小时通知网络信息安全工作组。

A.2.2　处置报告

网络信息安全事件报告采取“谁发现，谁报告”的原则，由发现网络信息安全事件的人员或部门及时将事件上报，对网络安全事件进行调查和评估，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大。如遇重大网络信息安全事件，需立即上报分管网络信息安全领导批示，评估是否是否报公安机关。

A.2.3　响应流程

响应流程见图A.1。



图A.1　响应流程图

A.3 事件应急响应

A.3.1 有害信息处置预案

A.3.1.1 当发现业务系统网站出现有害信息后，应及时上报，并通知相关业务部门和系统运维人员。
A.3.1.2 组织人员对有害信息进行清除，应尽快采取屏蔽、删除等有效措施对有害信息进行清理，并做好相关记录；短时间内难以清除的，应先保存证据、关停系统或网站，再进行处理。
A.3.1.3 采取技术手段追查有害信息来源，避免有害信息二次出现。
A.3.1.4 发现涉及国家安全、稳定的重大有害信息，立即向公安部门、网信办报告。

A.3.2 攻击处置预案

通过入侵监测系统发现有黑客进行攻击时，应立即通知信息技术人员采取以下措施处理：
—— 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或设备；
—— 通过查看被攻击服务器硬件、软件配置参数、审计记录等进行调查取证，收集攻击者证据；
—— 恢复或重建被破坏的系统，视其严重程度研究决定是否需要报公安部门、网信办。

A.3.3 病毒侵入处置预案

A.3.3.1 发现计算机系统感染病毒后，应立即将该计算机从网络中隔离，并评估是否需要恢复备份数据。
A.3.3.2 启用防病毒软件进行杀毒处理，并使用病毒检测软件对其他计算机等设备进行病毒扫描和清除；一时无法查杀的新病毒，应迅速与相关病毒软件供应商或安全专家联系解决。
A.3.3.3 感染病毒的是服务器或主机系统的，应立即告知使用部门并做好相应清查工作。

A.3.4 重要软件系统故障处置预案

A.3.4.1 重要软件系统及其相关数据应每月进行备份。
A.3.4.2 重要软件系统及其相关数据发生故障后，应立即报告。
A.3.4.3 系统管理维护人员应立即检查软件系统日志等，排查故障原因，并根据实际情况评估确定应采取的具体措施；可通过打补丁、优化系统设置、恢复软件和数据等方式恢复系统正常运行，并加强系统运行情况监控。

A.3.5 数据库崩溃处置预案

A.3.5.1 数据库发生崩溃，应立即立即启用备用数据库、通知使用单位暂缓使用，再组织人员对主机系统进行维修。
A.3.5.2 遇无法解决的问题，立即请求数据库维保单位或相关专家协助解决。
A.3.5.3 数据库修复后，应尽快进行数据恢复，评估数据丢失或损毁情况，必要性时恢复备份数据。

A.3.6 网络线路中断处置预案

网络线路中断后，应迅速判断故障节点，查明原因、尽快修复：

——属网络运营商负责维护运营的线路，立即与电信运营商维护部门联系，切换备用链路，及时进行修复；
——属局域网内部线路故障，应立即判断故障节点，查明故障原因，迅速组织修复；
——属路由器、交换机等网络设备故障，立即与网络设备供应商联系修复；
——属路由器、交换机配置文件破坏，迅速导出最新配置备份按照要求重新配置，恢复网络正常运行。

A.3.7 重要设备损坏处置预案

发现服务器等关键设备损坏，应立即组织人员查明设备故障原因：
——能自行恢复的，立即用备件替换受损部件；难以自行恢复的，立即与设备维保单位联系，请求派维修人员前来维修；
——不能修复的，应及时采取措施，并告知用户单位暂缓使用，尽快确定可行的修复方案，抓紧完成修复或重新购置，恢复网络和信息系统正常使用。

A.3.8 供电中断处置预案

A.3.8.1 外电中断后，UPS 系统自动切换到备用电源，检查是否切换成功。
A.3.8.2 应尽快查明断电原因，因内部线路故障，马上组织恢复；因供电部门原因，立即与供电单位联系，尽快恢复供电。
A.3.8.3 被告知将长时间停电的，立即启动发电机；遇发电机无法工作的，应做好以下工作：
——预计停电 1 小时以内的，保持由 UPS 供电并做好监控工作；
——预计停电 1-4 小时的，应关掉非关键设备，确保服务器、网络设备供电；
——预计停电超过 4 小时以上的，做好数据备份工作，及时关闭有关设备。

A.3.9 数据信息泄密突发事件

A.3.9.1 应在发现数据泄密的第一时间保护现场，并向领导报告泄密事件发生的地点、时间和简要过程，研究处置方案。
A.3.9.2 应查明被泄密的主要内容、密级、数量及载体形式、危害程度、重要情节和有关责任人。
A.3.9.3 应调查泄密原因，尽快找到或锁定范围，必要时报公安部门。
A.3.9.4 启动网络舆情预案，会同相关部门协作预防媒体或网络对泄密信息的报道或炒作。
A.3.9.5 对出现在公共网络、出版物、广播、电视等媒体上的泄密信息，应协调相关职能部门要求有关单位立即删除、收缴、停播、销售,收缴有关涉密载体。
A.3.9.6 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.3.10 其他处置预案

本文件中没有列出的、属不确定因素造成的网络信息安全突发事件，应根据安全原则，结合具体情况做出相应处理；无法独立处理的，协调外部应急专家进行处置。

A.4 事件后期处置

A.4.1 **善后处理**。在应急处置工作结束后，业务系统运维人员应迅速采取措施，组织抢修系统，尽快恢复正常工作。统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，

认真制定恢复重建计划，并迅速组织实施。

A.4.2 **评估总结**。在应急处置工作结束后，应立即组织有关人员，对事件发生及其处置过程进行全面调查，查清事件发生的原因及影响情况，总结经验教训，对应急响应过程中的相关人员的行为进行奖惩。

应急保障措施

A.4.3 **应急队伍保障**。应急响应的牵头部门应协调运维单位、业务机构等单位，组建信息系统安全应急响应工作队伍，制定应急培训和演练计划，提高应对网络与网络信息安全事件的能力。

A.4.4 **设备保障**。结合实际工作需要，应提前配备应急处置工作所必须的设备或工具软件，加强应急处置工具及设备的维护调试，保证其随时可用。

A.4.5 **数据保障**。重要设备、重要信息系统及业务数据应建立相应的备份机制，保证重要设备、重要信息系统及业务数据受到破坏后能够紧急恢复。

A.4.6 **技术资料保障**。应建立专门技术档案库，对网络拓扑结构、信息资产情况、重要系统或设备的型号及配置、协作厂商信息等技术资料进行管理和维护，并及时更新。

A.5 应急培训与演练

应开展网络和数据安全的培训和应急演练，并在演练结束后，对演练效果、存在问题、改进措施等进行评估和总结。

附 录 B
（资料性）
突发事件应急处置

B.1 斗殴、骚乱、抢劫、畜意破坏等突发治安事件处置

B.1.1 交易场所发生斗殴、骚乱、抢劫、畜意破坏等突发治安事件，工作人员应立即向安保人员和领导报告，并向公安机关报警；安保人员或警察到场后，作好配合协调。

B.1.2 处理斗殴、骚乱、抢劫、畜意破坏等突发治安事件时，应遵循以下要求：

——保持冷静，尽量避免人体冲撞，以保护群众和自身安全为重；

——有工作人员和办事群众受伤，应立即向 120 急救中心求救；

——注意保护现场，积极配合公安机关处理。

B.1.3 现场处置完成后，及时关注相关舆情，作好应对。

B.2 停电事故处置

B.2.1 提前接到断电通知的，由办公室（综合机构）通知各业务机构做好应对。

B.2.2 项目交易过程中突发断电的，应按以下要求处理：

——立即通知物业服务机构检查供电系统，排查故障，立即抢修；属交易场所外部供电线路及故障的，立即与供电机构联系；

——有发电机等备用电源的，立即采取发电等措施临时供电，保障交易顺利推进；

——有电梯的，应安排逐一检查电梯内有无被困人员；

——向现场的各方主体做好解释，必要时引导场内人员就近从消防安全通道撤离；

B.2.3 恢复正常供电后，相关部门应立即组织维修人员检查场内用电设备，确保正常运行。

B.3 可疑爆炸物及其他危险物品处置

B.3.1 交易场所发现可疑爆炸物及其他危险物品时，工作人员应立即向现场安保人员和管理机构报告，并向公安机关报警；安保人员和中心管理人员不宜擅自对可疑物采取处置行动，应等候公安人员到场处置了。

B.3.2 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；

—— 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；

—— 立即向公安机关报警，组织安保人员保护现场；

—— 有人员伤亡时，立即向 120 急救中心求救；

—— 准备协同处理可能发生的火灾等并发灾情。

B.4 群众上访、聚集等突发事件处置

办公区域发生群众上访、聚集等事件时，应按以下要求处理：

—— 现场安保人员应维护现场秩序，防止过激行为或其它意外事件发生；

—— 现场工作人员应立即向领导报告，并安抚情绪、做好疏导，防止事态激化；

—— 应在上访者情绪相对稳定后，了解事由；根据上访事由，通知相关部门到场处理、疏散人员；

—— 应密切关注事态的发展和处置情况，视情及时向政府领导、应急管理机构或公安机关报告。

B.5 重大疫情防控应急处置

B.5.1 交易场所所在地区出现重大疫情时，应按以下要求开展疫情防控：

——启动疫情防控应急预案，做好宣传提示、人员防护、卫生消毒、应急处置等工作。

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

——要求工作人员及现场参与交易人员严格执行疫情管理要求，主动做好个人健康监测与防护。

——开通电话预约、不见面开标等网上办事渠道，引导市场主体网上办理交易业务。

B.5.2 交易场所发生重大传染病疫情时，应立即停止营业，并在当地疾病预防控制机构指导下，配合开展疫情防控工作。

B.5.3 交易场所发生新新冠肺炎疫情时，参照DB51/T2775-2021处置。

B.6 火情处置

交易场所发现火情时，采取如下措施：

——立即按下场所火灾报警按钮（如有）并拨打 119 火警电话；

——使用消防设施、器材扑救初起火灾；

——按应急疏散预案畅通消防通道，引导消防人员进入现场，组织引导人员疏散；

——协助 120 抢救、护送受伤人员；

——维持现场秩序，阻止无关人员进入火场。

参 考 文 献

[1]《中华人民共和国消防法》
[2]《中华人民共和国保守国家秘密法》
[3]《中华人民共和国突发事件应对法》
[4]《中华人民共和国保守国家秘密法实施条例》
[5]《突发公共卫生事件应急条例》
[6]《机关、团体、企业、事业单位消防安全管理规定》（中华人民共和国公安部令第61号）