# 无锡市大数据管理局关于印发《无锡城市大数据中心信息安全突发事件应急预案》的通知

为做好应对无锡城市大数据中心信息安全突发事件的各项准备工作，提高应急处理能力，现将《无锡城市大数据中心信息安全突发事件应急预案》印发给你们，请结合实际认真组织实施。

附件：无锡城市大数据中心信息安全突发事件应急预案

（此页无正文）

# 无锡城市大数据中心信息安全

# 突发事件应急预案

2020 年 6 月

# 目 录

# 1. 总 则

## 1.1. 编制目的

为做好应对无锡城市大数据中心信息安全突发事件的各项准备工作，提高应急处理能力，结合实际，制定本预案。

## 1.2. 编制依据

《中华人民共和国网络安全法》《突发事件应急预案管理办法》《江苏省突发事件总体应急预案》《无锡市公共数据管理办法》等相关规定。

## 1.3. 适用范围

本预案适用于无锡城市大数据中心因硬件、软件、网络、人员、场所、组织等支撑性资产引起数据和系统突发信息安全事件的处理。

## 1.4. 工作原则

城市大数据中心信息安全突发事件的应急处理以确保城市大数据中心数据安全和系统稳定为目的，坚持统一领导、协同管理、职责明确、分工负责、综合防范、妥善处理的原则，快速、稳妥地处理各类信息安全突发事件。

## 1.5. 事件分级

根据业务影响范围，城市大数据中心突发事件分为三级:重大(Ⅰ级)、较大(Ⅱ级)、一般(Ⅲ级)。

### 1.5.1 重大突发事件（Ⅰ级）

符合下列情形之一的，为重大突发事件(Ⅰ级):

(1) 数据库实例异常关闭或瘫痪且无法启动;

(2) 遭到外部攻击导致所有数据库文件被恶意篡改或删除;

(3) 由于误操作导致数据库文件或相关的系统文件丢失导致数据库实例崩溃;

(4) 服务器软硬件问题导致系统无法启动;

(5) 存储故障导致与数据库有关的逻辑磁盘丢失进而造成数据丢失;

(6) 存储故障导致数据库集群瘫痪。

### 1.5.2 较大突发事件（Ⅱ级）

符合下列情形之一的，为较大突发事件（Ⅱ级）:

(1) 数据库文件坏块导致数据文件下线;

(2) 表空间的数据文件被误删导致表无法访问;

(3) 用户和表空间遭到误删或破坏导致无法使用。

(4) 数据库因 IO 问题导致读写异常缓慢;

(5) 大量死锁产生导致业务无法正常开展、需要大量消耗资源解析的SQL语句被大批量执行导致CPU使用量高居不下;

(6) 告警日志中存在如ORA-600或者ORA-7445等一些比较重要的告警。

(7) 大量外部连接不停访问导致连接数快速用完;

(8) 监听问题导致数据库实例无法连接。

### 1.5.3 一般突发事件（Ⅲ级）

符合下列情形之一的，为一般突发事件（Ⅲ级）:

(1) 历史表数据被误删、误改或误清除导致无法查询;

(2) 部分实时性较高的表存在死锁导致业务不能正常进行;

(3) 部分实时性要求较高的表访问速度异常慢;

(4) 外部连接未正常退出导致长连接大量积累影响正常访问;

(5) 日志长期未清理占用磁盘容量将数据库目录撑满从而导致无法登录;

(6) 非重要性数据库实例出现问题无法访问。

## 2. 组织机构和职责

### 2.1. 领导机构

成立无锡城市大数据中心突发事件应急指挥组（以下简称应急指挥组），组长由市大数据管理局局长担任，副组长由市大数据管理局数据资源分管局长担任，成员由局办公室、数据资源和电子政务处、政策法规处（人才发展处）、网信中心、运维单位相关负责人组成。

主要职责：负责建立完善城市大数据中心突发事件应急预案，统一领导、组织协调城市大数据中心突发事件的应急处理工作。

### 2.2. 办事机构

无锡城市大数据中心信息安全突发事件应急指挥工作办公室（以下简称应急工作办公室）设在市大数据管理局数据资源和电子政务处，作为日常办事机构，办公室主任由数据资源和电子政务处负责人担任。

主要职责：贯彻落实应急指挥组的决定，迅速了解、收集和汇总城市大数据中心突发事件信息、损害情况，及时向应急指挥组报告；组织城市大数据中心突发事件调查和评估，了解、汇总事件处理情况；组织应急预案演练，组织开展应急预案业务指导和效能评估；协调开展信息安全知识技能、

应急管理法规政策和应急预案等宣传培训；负责处理日常事务，办理应急指挥组交办的其他事项。

## 2.3. 工作机构

在应急指挥组综合协调下，各成员按照各自职责分工协作，建立应急联动机制，共同做好城市大数据中心突发事件应对工作。

**局办公室：**负责应急管理经费保障，支持信息安全应急专业队伍、基础设施和情报力量建设，支持技术研发、预案演练等工作；负责对信息安全事件应急管理对外宣传报道，组织开展宣传活动；负责信息安全专家管理。

**局政策法规处（人才发展处）：**负责城市大数据中心突发事件预防和处置的有关法律、法规和政策的宣传和普及；负责开展信息安全基本知识和技能的宣讲活动。

**市网信中心：**负责政务网络日常运行和信息安全保障工作，负责政务网络及政务机房应急预案制定，做好信息安全事件中政务网络、政务机房等基础设施应急处理。

应急指挥组各成员应当与应急工作办公室建立应急联动机制，保证联络畅通，并加强与其他应急机构的衔接配合。

需要其他部门配合时，由应急工作办公室负责协调对接。

## 2.4. 运维单位

城市大数据中心运维单位是信息安全的责任主体，履行以下职责:

1、配合市大数据管理局建立健全城市大数据中心的各项安全运维管理制度，严格执行城市大数据中心的各项安全运维管理制度与业务流程，监控城市大数据中心各系统运行状态，避免数据泄露和不当使用，保障数据安全;

2、做好各类台账登记，按要求做好各类密码的设置、保管与定期更新，并及时向无锡市大数据管理局报备所有管理员账号与密码;

3、负责本公司数据从业人员的安全教育，接触数据库的人员要严格按照权限进行操作，并做好工作记录，发现异常时应及时阻断，并上报市大数据管理局;

4、按要求做好城市大数据中心数据备份，制定应急预案，配合市大数据管理局开展应急演练;

5、完成应急指挥组交办的其他事项。

## 2.5. 应急技术支撑队伍

应急技术支撑队伍由信息安全、系统开发、系统集成、安全测评等领域专家和运维团队相关人员组成，承担城市大数据中心信息安全突发事件应急技术支援工作。

主要职责：按照应急指挥组及其办公室的指令，开展应急救援；在城市大数据中心信息安全突发事件预防与应急处置时提供咨询与建议；协助应急指挥组做好城市大数据中心信息安全突发事件应急演练工作；承办应急指挥组交办的其他事项。

## 3. 预防预警

### 3.1. 预防

运维团队应做好城市大数据中心信息安全突发事件的风险评估和隐患排查工作，制定完善应急预案，及时采取有效措施，避免和减少城市大数据中心信息安全突发事件的发生及危害。

当以下事件发生时，应当做好启动本预案的准备:

（1）支撑城市大数据中心正常运转的各类硬件设备发生故障;

（2）支撑城市大数据中心正常运转的各类信息系统、操作系统、数据库、中间件、通用插件等软件发生故障;

（3）支撑城市大数据中心正常运转的互联网、政务网等基础网络及通讯接口发生故障;

（4）涉及城市大数据中心正常运转的决策者、管理者、项目负责人、系统管理员、数据管理员、安全负责人、核心开发人员和核心运维人员岗位或人员发生变动;

（5）城市大数据中心运行场所、通讯基础设施、公用设施、容灾备份中心等基础设施发生变化;

（6）城市大数据中心运维单位发生变化;

（7）城市大数据中心运维单位组织架构及按合同提供服务或资源的分包商、供应商发生变化。

## 3.2. 监测

以运维单位为责任主体，对城市大数据中心信息安全实施技术监测，定期检查运维状态，落实各项安全管理制度、隐患整改情况，定期上报应急预案准备情况；发现异常和事故状态，要立即采取有效措施并及时上报。

应急指挥组建立并完善大数据中心突发事件信息的报送机制，做好预警信息、事件信息的汇集、预判和通报。

## 3.3. 预警

城市大数据中心突发事件预警等级分为三级：红色预警（重大，Ⅰ级）、橙色预警（较大，Ⅱ级）和蓝色预警（一般，Ⅲ级），分别对应发生或可能发生重大、较大和一般城市大数据中心突发事件。

### 3.3.1 预警发布

应急工作办公室接到运维单位上报的城市大数据中心突发事件监测信息后，及时会同有关成员进行初判，提出预警等级建议并报应急指挥组。

红色预警（重大，Ⅰ级）由应急指挥组发布，并报市政府分管领导。

橙色预警（较大，Ⅱ级）由应急指挥组发布。

蓝色预警（一般，Ⅲ级）由应急工作办公室发布。

### 3.3.2 预警响应

预警信息发布后，应依据发布的预警级别，加强对城市大数据中心数据与信息系统的安全监测，做好应急处理的各项准备工作。应急工作办公室及时跟踪了解情况。

### 3.3.3 预警解除

如果城市大数据中心信息安全突发事件未达到启动应急处置Ⅲ级响应级别，则关闭应急响应;

经跟踪监测并对监测信息进行分析评估后，认定应当结束预警状态的，由应急工作办公室向应急指挥组提出建议，由应急指挥组解除预警并公布。

# 4. 应急处置

## 4.1. 信息报告

运维单位应向应急工作办公室报告城市大数据中心信息安全突发事件。

事件信息一般包括以下要素：事件发生时间、发生事故的原因、信息来源、事件类型及性质、危害和损失程度、影响单位及业务、事件发展趋势、采取的处置措施等。

城市大数据中心信息安全突发事件发生后，运维单位在做好先期处置的同时，应立即组织研判，注意保存证据，及时收集、分析、汇总大数据中心突发事件信息，2 小时内按应急渠道上报应急工作办公室；应急工作办公室对上报信息组织研判，确属 I 级（重大）事件的经应急指挥组同意后 2 小时内报市政府；对于 II 级（较大）、III 级（一般）事件信息，按有关规定及时上报应急指挥组。

## 4.2. 分级响应

### 4.2.1 I 级响应

I 级响应由应急指挥组启动，由应急指挥组落实应急响应措施。

(1) 启动指挥体系。

应急指挥组进入应急状态，履行应急处置工作的统一领导、指挥、协调、组织的职责。应急指挥组各成员保持24小时联络畅通，在应急工作办公室24小时值班，组织相关专家指导现场处置。

(2)掌握事件动态。

应急指挥部及时了解城市大数据中心信息安全事件所涉及的信息系统，对城市大数据中心数据的影响。

(3)处置实施。

①控制事态防止蔓延。应急指挥组应指导运维单位及时采取技术措施阻止事件蔓延。

②做好处置消除隐患。尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏的信息系统和数据。

4.2.2 II级响应

II级响应由应急指挥组启动，应急工作办公室做好应急响应相关工作。

(1)启动指挥体系。

应急工作办公室进入应急状态，履行应急处置工作的统一领导、指挥、协调、组织的职责。指挥组成员保持24小时联络畅通，应急工作办公室24小时值班。必要时组织相关专家指导现场处置。

(2)掌握事件动态。

应急工作办公室及时了解城市大数据中心信息安全事件所涉及的信息系统，对城市大数据中心数据的影响。

(3) 处置实施。

①控制事态防止蔓延。应急工作办公室应会同运维单位及时采取技术措施阻止事件蔓延。

②做好处置消除隐患。尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏的信息系统和数据。

4.2.3 III级响应

III级事件响应由数据应急工作办公室启动，运维单位按照相关预案进行应急处置，必要时请求信息安全专家支援处置，尽快查明事件原因，快速处置，恢复受破坏的信息系统和数据。

## 4.3. 应急结束

经分析评估，认定可以结束应急响应状态的，由应急工作办公室向应急指挥组提出建议，由应急指挥组决定。

## 4.4. 信息发布和新闻报道

城市大数据中心突发事件的新闻报道工作，须遵守相关法律法规规定。

大数据中心突发事件发生后，需要开展新闻报道时，应指派专人负责新闻报道工作，起草新闻稿和情况公告，及时、准确、客观报道事件信息，正确引导舆论导向。

## 5. 后期处置

### 5.1. 恢复与重建

恢复重建工作由运维单位制定相关整改或重建方案，报市大数据管理局审核实施。

### 5.2. 总结评估

I 级（重大）事件由应急指挥组组织开展调查处理和总结评估。

II 级（较大）、III级（一般）事件由应急工作办公室组织进行调查处理与总结评估。

总结评估主要对事件的起因、性质、影响、责任等进行调查，提出处理意见和改进措施，并追究责任。事件调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。其中，I 级（重大）、II 级（较大）事件总结调查报告须报应急指挥组。

# 6. 保障措施

## 6.1. 专业支撑队伍

加强无锡市城市大数据中心应急队伍建设，做好大数据中心突发事件的应急救援和支援工作。

## 6.2. 应急基础设施

加强市容灾备份中心、市政务云、市大数据中心安全体系等公共安全应急基础设施建设，提高应急处置能力。

## 6.3. 技术研发

加强数据与信息安全技术、工作规范和相关标准等的研究，为应急响应工作提供技术支撑。

## 6.4. 情报力量

应急工作办公室主动对接市公安局、网信办、国家安全局、保密局等部门，获取、搜集信息安全有关情报，为城市大数据中心信息安全应急工作提供情报支持。

### 6.5. 经费保障

利用现有政策和资金渠道，支持城市大数据中心信息安全应急专业队伍、基础设施和情报力量建设，支持技术研发、预案演练等工作。

## 7. 宣传、培训和演练

### 7.1. 宣传

局办公室做好对城市大数据中心信息安全突发事件的宣传活动。

### 7.2. 培训

应急工作办公室应会同各有关处室（单位），开展城市大数据中心数据安全规范和信息安全预案编制，做好信息系统风险评估和等级保护、事件分析处置、容灾备份等方面的专业技术培训。

### 7.3. 演练

应急工作办公室每年至少组织 2 次预案演练，模拟处置重大或较大突发事件，提高实战能力，检验和完善预案。

# 8. 附 则

## 8.1. 制定与解释

本预案由市大数据管理局数据资源和电子政务处负责制定和解释。

## 8.2. 发布实施

本预案自印发之日起实施。