高新兴科技集团股份有限公司

受　　控

# 应急响应管理制度

文件编号：GSB／T 316.16

文件版本：A0

批　　准：刘伟辉

实施日期：2015-1-1

受控状态：受控

# 版本记录

| 版本 | 日期 | 修订页次 | 制/修订记录 | 制/修订者 |
|---|---|---|---|---|
| A0 | 2015-08-18 | / | 新版制定 | 李旻 |
| | | | | |
| | | | | |
| | | | | |

# 目　　录

1　目的 ..... 1
2　应急管理原则 ..... 1
3　分级响应 ..... 1
4　应急管理机构 ..... 3
5　应急响应组织结构 ..... 4
6　风险识别评估 ..... 5
7　应急预案实施基本流程 ..... 6
8　日常检测与预警 ..... 6
9　运行机制 ..... 7
10　应急事件关闭 ..... 8
11　培训与演练 ..... 9
12　应急工作总结 ..... 9
13　应急工作审核 ..... 9
14　应急工作改进 ..... 10

# 应急响应管理制度

## 1 目的

运维项目组制定了详尽的应急处理预案，整个流程严谨而有序。但在服务维护过程中，意外情况将难以完全避免。规范应急事件应急管理，提高应对应急事件的管理水平和应急处理能力，有效防范信息系统风险，减少信息系统故障对生产业务造成的影响，确保信息系统运行的连续性。，特制定本制度。

## 2 应急管理原则

准备充分，监测有力，应急得当，改进提升。对可能发生的应急事件从建立组织和制度、识别风险、制定预案、开展培训和演练等方面进行充分准备。通过日常监测及时发现应急事件。在基于预案开展故障排查与诊断，快速处理应急事件所造成的运行中断、运行质量降低的同时，及时通报并提供持续性服务保障。在关闭事件后，对应急事件发生原因、处理过程和结果进行总结分析，持续改进应急工作，优化完善信息系统。

统一指挥，有效组织。确定应急总指挥、成立应急指挥小组和应急工作小组，组织开展风险识别、事件预防、应急处置、恢复运行、事件通报等各项应急工作。相关部门要主动协调有关各方面，参与实施部门要听从指挥、步调一致。

突出重点，加强演练。对已识别出的关键信息系统加大监控和应急处理力度，确保应急信息及时准确传递。每年开展应急演练工作，确保应急措施合理、有效。

技术支撑，健全机制。在充分利用客户现有的信息资源、系统和设备基础上，采用先进适用的预测、预防、预警和应急处置技术，改进和完善应急处理的装备、设施和手段，提高应对信息系统应急事件的技术支撑。建立健全应对信息系统应急事件的有效机制。

## 3 分级响应

应急工作按照事故的应急程度、波及和影响范围，实施分级应急响应。

### 3.1 信息系统重要程度

信息系统的重要性由以下要素决定：

1) 信息系统支撑的业务类别。
2) 信息系统所属类型，即信息系统资产的安全利益主体。
3) 信息系统主要处理的业务信息类别。
4) 信息系统服务范围，包括服务对象和服务网络覆盖范围。
5) 业务对信息系统的依赖程度。

其中第 1 个要素决定信息系统所支撑业务的重要性，第 2、3 个要素决定信息系统内信息资产的重要性，第 4、5 个要素决定信息系统所提供服务的重要性，而信息系统所支撑业务的重要性、信息系统内信息资产的重要性以及信息信息系统服务的重要性决定了信息系统的重要程度。

信息系统重要程度分级及赋值如下：

| 赋值 | 描述 |
|---|---|
| 1 | 4 级信息系统 |
| 2 | 3 级信息系统 |
| 3 | 2 级信息系统 |
| 4 | 1 级信息系统。 |

### 3.2 信息系统服务时段

信息系统服务时段划分为 3 级。依据应急事件发生的不同时间，对信息系统恢复正常服务所需的时间要求而确定。

| 赋值 | 描述 |
|---|---|
| 1 | 非系统服务时段（不含系统服务时段即将开始） |
| 2 | 系统服务时段或系统服务时段即将开始 |
| 3 | 系统处于重点时段保障或处于服务高峰时段 |

### 3.3 信息系统损失程度赋值

应急事件造成的信息系统损失程度划分为 3 级。依据故障发生对信息系统提供的服务能力的下降程度而确定。

| 系统性能 | 系统功能 | | |
|---|---|---|---|
| | 功能无损 | 部分损失 | 全部损失 |
| 小于阈值 | — | 1 | 3 |
| 大于或等于阈值 | 1 | 2 | 3 |
| 重点时段保障的损失程度赋值为 3 | | | |

### 3.4 事件定级及响应

将以上应急事件三个要素的赋值相乘，事件级别如下表所示：

| 范围 | 级别 |
|---|---|
| 1~6 | III 级事件 |
| 8~18 | II 级事件 |
| 26~36 | I 级事件 |

发生 I 级事件，由应急工作小组初步判定事件级别后，将信息通知应急指挥小组并注意持续监控事态、收集信息、做出应急准备；应急指挥小组响应判断为 I 级事件后，立即通知应急总指挥，并由应急总指挥启动应急预案。

发生 II、III 级事件，由应急工作小组初步判定事件级别后，将信息通知应急指挥小组并注意持续监控事态、收集信息、做出应急准备；应急指挥小组响应判断为 II、III 级事件

后，立即启动应急预案。

应急事件的级别应置于动态调整控制中。

## 4 应急管理机构

### 4.1 领导机构

公司总部是突发事故应急管理工作的最高邻导机构。在运营业务部总监领导下，由公司相关突发事故应急指挥机构负责突发事故的应急管理工作。

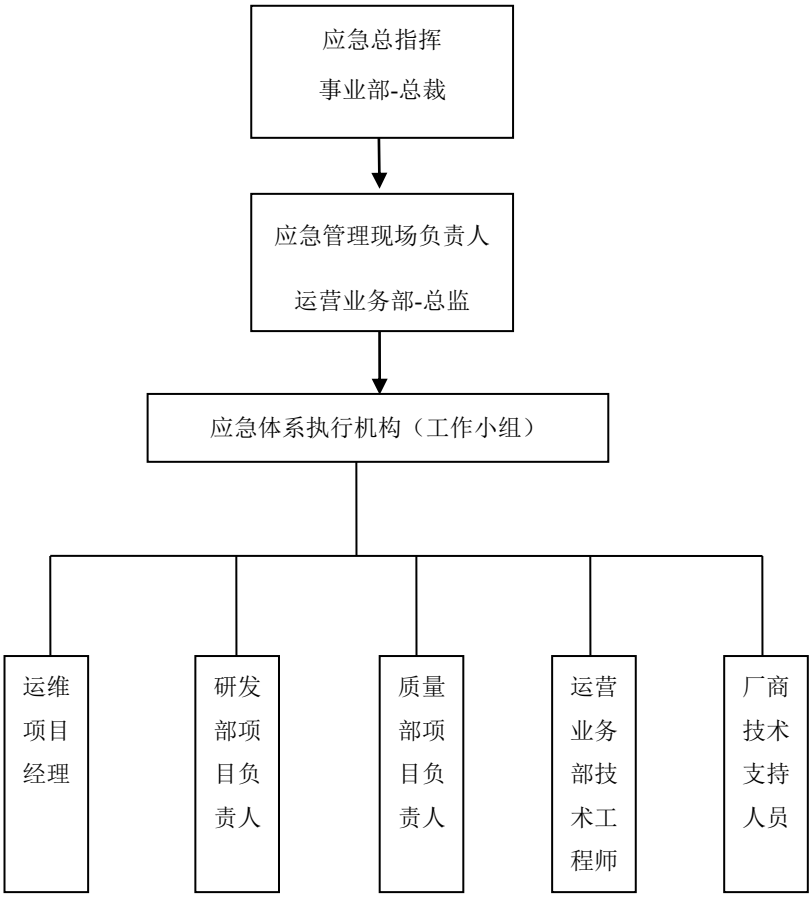
### 4.2 办事机构

运营业务部设应急管理办公室，履行值守应急、信息汇总和综合协调职责，发挥运转枢纽作用.

### 4.3 工作机构

相关部门依据相关程序文件、管理制度和各自的职责权限，负责相关类别突发事故的应急管理工作。具体负责相关类别的突发事故专项和部门应急预案的起草与实施，贯彻落实公司有关决定事项。

## 5 应急响应组织结构




### 5.1 角色及职责

#### 5.1.1 应急总指挥

统一领导信息系统的应急事件的公司内部应急处理工作，发起研究重大应急决策和部署，决定实施和终止应急预案。负责 I 级事件的指挥和协调。及时向服务需方应急响应负责人通报应急事件进度。

#### 5.1.2 现场负责人

接受应急总指挥的领导，传达和落实应急总指挥的各项指令，汇总和上报应急信息，负责应急工作小组成员的协调沟通，协调应急事件处置工作中的重大问题。接到应急响应事件报告后，判断应急响应事件登记。承担现场应急工作指挥，负责应急事件监测与预警、应急处置等现场工作；负责 II、III 级事件的指挥和协调。及时向服务需方应急响应负责人通报应急事件进度。

#### 5.1.3 应急工作小组

在现场负责人带领下进行各项应急工作。落实应急总指挥及应急指挥小组布置的各项任

务；组织制定应急预案，并监督执行情况；掌握应急事件处理情况，及时向应急总指挥和应急指挥小组报告应急过程中的重大问题。

#### 5.1.4 各分组负责人

在应急工作小组中承担应急响应中各专业性工作；负责提交应急事件关闭申请。

#### 5.1.5 厂商技术支持

配合公司要求，在指定时间、指定交货地点提供应急响应所需的设备、配件等。及时向应急指挥小组报告应急过程中的重大问题。

## 6 风险识别评估

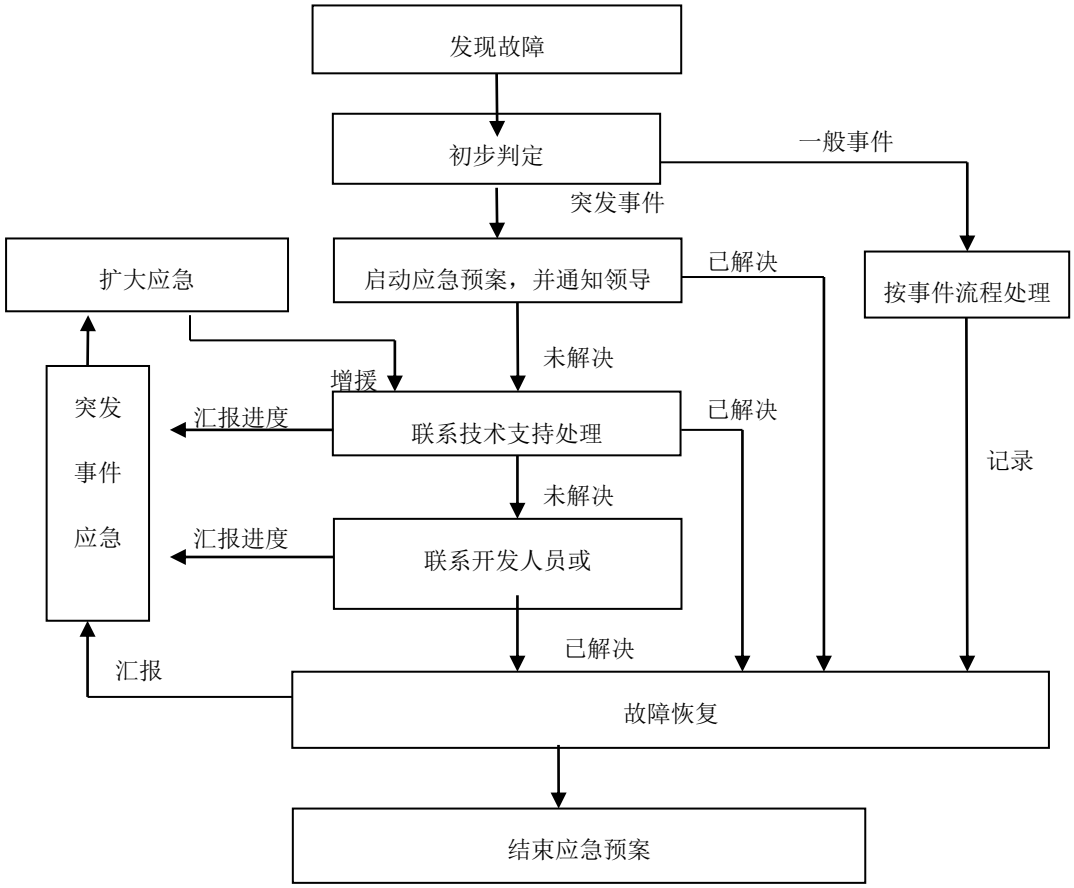
应急响应小组每年对重要信息系统进行一次风险评估，并根据风险评估结果来制定或更新应急预案。风险评估方法如下：

1) 判定哪些是重要信息系统；
2) 确定每一个重要信息系统可能面临的风险要素及其发生的几率。风险要素可包括下表中的种类：

| 种类 | 描述 |
| --- | --- |
| 软硬件故障 | 由于设备硬件故障、系统本身或软件 Bug 导致对业务高效稳定运行的影响 |
| 物理环境威胁 | 断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题和自然灾害 |
| 无作为或操作失误 | 由于应该执行而没有执行相应的操作，或无意地执行了错误的操作，对系统造成影响 |
| 管理不到位 | 安全管理无法落实，不到位，造成安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行 |
| 恶意代码和病毒 | 具有自我复制、自我传播能力，对信息系统构成破坏的程序代码 |
| 越权或滥用 | 通过采用一些措施，超越自己的权限，访问了本来无法访问的系统 |

1) 描述风险发生后会造成的影响和后果；
2) 针对每一个风险制定控制措施，并明确相应责任人；
3) 撰写风险评估报告。

## 7 应急预案实施基本流程




## 8 日常检测与预警

运维项目组应该对运行维护服务对象的运行情况进行监测与预警，以跟踪和判别以下对象的容量、可用性和连续性：

1) 应用系统；
2) 支撑应用系统运行的系统软件、工具软件；
3) 网络及网络设备；
4) 安全设备；
5) 主机、存储、外设、终端等设备；
6) 电力、空调、消防等基础环境。

如发现有异常情况时，要及时处理报告，并及时排除信息系统中存在的风险隐患。同时应对信息系统所承载的业务数据进行监测，以跟踪和判别业务数据是否超出了预警条件

## 9 运行机制

### 9.1 应急启动

应急预案的启动有以下两种方式：

1) 遇到 I 级事件，事件信息由值班人员提供并提交给现场负责人，现场负责人做出初步判断和初步事件级别的确认，初步确认为 I 级事件的，呈报应急总指挥，由应急总指挥下达启动应急预案。
2) 遇到 II、III 级事件，现场负责人与应急工作小组磋商后自行启动应急预案，并及时上报应急总指挥。

### 9.2 事件报告

当发现各类信息系统事件时，应按照事件等级逐级汇报。报告分为紧急报告和详细汇报。

1) 紧急报告：是指相应部门在事件发生后，立即向本部门应急工作小组以口头和应急报告表形式汇报事件的简要情况；
2) 详细汇报：是指由相应部门应急处理机构在事件处理暂告一段落后，以书面形式向应急总指挥提交的详细报告。

应急工作小组对各类事件的影响进行初步判断，汇报矩阵如下：

| 事件级别 | 报告时间要求 | 报告对象 |
|---|---|---|
| I | 10 分钟内 | 应急总指挥 |
| II | 30 分钟内 | 应急总指挥 |
| III | 60 分钟内 | 应急总指挥 |

报告内容应准确、详实，任何部门和个人均不得缓报、瞒报、谎报或者授意他人缓报、瞒报、谎报事件。事件报告信息一般包括以下要素：发生事件的信息系统名称及业务部门、地点、原因、信息来源、事件类型及性质、危害和损失程度、影响部门及业务、事件发展趋势、采取的处置措施等。

### 9.3 应急调度

公司应该按照预案开展统一的应急调度，包括人员、资金和设备等。应急调度由应急总指挥授权应急指挥小组执行。

### 9.4 处理与恢复

应急事件的处理与恢复应基于应急响应预案、配置管理数据库、知识库等进行故障处理和系统恢复。必要时可启用备品备件、灾备系统等。应急事件的处置与恢复流程参考《事件与服务请求过程》，处理与恢复过程需在《应急事件报告》进行记录，并及时告知利益相关方。在处理和恢复应急事件时,应在满足事件级别处置时间要求的前提下，尽快恢复服务。

事件级别处置时间要求如下：

| 事件级别 | 处置时间要求 |
|---|---|
| I | 2 小时 |

| | |
|---|---|
| II | 4 小时 |
| III | 6 小时 |

### 9.5 事件升级

当实际处置时间超过事件级别处置时间要求时，应急工作小组应考虑向应急总指挥申请事件升级，事件升级的实施授权应由应急总指挥启动。应急工作小组应对事件升级可能造成的影响进行评估，并在相关利益方间达成一致。

### 9.6 持续服务

完成处理与恢复后，还应提供持续性服务。应急响应组织应对持续性服务的效果进行评价。持续服务的评价结果，应作为应急事件关闭的输入。

I 级应急事件应急处理结束后应密切关注，监测系统 2 周，确认无异常现象。

II 级应急事件应急处理结束后应密切关注，监测系统 1 周，确认无异常现象。

III 级应急事件应急处理结束后应密切关注，监测系统 3 天，确认无异常现象。

## 10 应急事件关闭

### 10.1 申请

在同时满足下列条件下时，应急分组负责人可向应急工作小组提出关闭申请。

应急事件处理已经结束，设备、系统已经恢复运行。

1) 持续服务阶段系统无异常，持续服务阶段结束。
2) 服务需方应急响应负责人同意事件关闭。
3) 现场负责人已逐项核实报告内容。
4) 应急事件处置的过程文档已整理完成。

### 10.2 核实

应急工作小组接到关闭申请后，应逐项核实报告内容，以判别应急事件处置过程和结果信息是否属实之后通报应急总指挥，由应急总指挥做出关闭决定。

### 10.3 事件通报

应急总指挥应授权应急工作小组向相关利益方通报事件信息，内容应包括：

1) 事件发生的原因、事件级别及影响范围；
2) 事件对应的预案；
3) 事件的处置过程和方法；
4) 事件的调整升级情况；
5) 持续性服务情况；
6) 事件处置评价；
7) 事件关闭申请的处理意见；

8) 关闭通报的范围和涉及接受者。

应急事件发生的原因、分析、处置过程和方法应记入知识库。

## 11 培训与演练

公司负责制定应急响应培训计划。组织各信息系统应急预案涉及人员定期开展应急响应培训，应急响应预案作为培训的主要内容。做好信息系统相关知识的宣传和普及。增强应急预案涉及人员的责任意识。

通过培训使得应急预案涉及人员明确其在应急响应过程中的责任范围、接口关系，明确应急处置的操作规范和操作流程。

培训每年举办一次。

公司要组织对预案进行定期演练，通过演练验证预案的合理性，及时修订和完善不符合实际的应急处置情况，有针对性地改进信息系统应急事件处置能力，确保事件发生后应急处理手段及时到位和有效。

相关部门在做应急演练前要做好相关准备工作，确保演练工作的安全。要明确演练的目的和要求，记录演练过程，对演练结果进行评估和总结。

## 12 应急工作总结

组织应定期对应急响应工作进行分析和回顾，总结经验教训，并采取适当的后续措施。对应急响应工作的分析和回顾应考虑以下方面：

1) 应急响应工作的绩效；
2) 应急准备工作的充分性和有针对性；
3) 应急事件发生原因、数量及频率；
4) 应急事件处置的经验得失；
5) 应急事件的趋势信息；
6) 信息系统中潜在的类似隐患。

对应急响应工作的分析和回顾应形成《应急响应工作总结》，并将总结作为改进应急响应工作及信息系统的重要依据

## 13 应急工作审核

应急总指挥应定期发起对应急响应工作的评审，以确保应急响应过程和管理符合预定的标准和要求。审核的结果应该正式存档并通知给相关利益方。评审至少每年一次，可于公司内审时进行。

审核时应考虑的要素包括：

1) 相关利益方的要求和反馈；
2) 组织所采纳的用于支持应急响应的各种资源和流程；

3) 风险评估的结果及可接受的风险水平；
4) 应急预案的测试结果及实际执行效果；
5) 上次评审的后续活动跟踪；
6) 可能影响应急响应的各种业务变更；
7) 近期在处置应急事件过程中总结的经验和教训；
8) 培训的结果和反馈。

审核的输出结果应该包括：

1) 改进目标；
2) 改进的具体工作内容；
3) 所需的各种资源，包括人员、资金和设备等。

## 14 应急工作改进

根据应急事件总结、应急工作审核报告、客户方的要求、技术的革新和发展等因素，对应急工作进行持续完善和改进。