# 云南腾电科技有限公司

# 应急管理制度

# （YNTD-ITSS-1001）

编制人:谢广胜　　编制时间:2025.01.07

审核人:赵建中　　编制时间:2025.01.07

批准人:陆涛　　审批时间:2025.01.07

文件编制和变更履历

| 版本 | 编制/更改 | | 发布 | | 实施 | | 更改记录 |
|---|---|---|---|---|---|---|---|
| | 作者 | 日期 | 审核 | 日期 | 批准 | 日期 | |
| V1.0 | 谢广胜 | 2025.1.7 | 赵建中 | 2025.1.7 | 陆涛 | 2025.1.7 | 首次发布 |
| | | | | | | | |
| | | | | | | | |

目录

# 1. 目的

为了规范运维业务应急响应管理过程，有效管理应急事件，以快速消除或降低事件影响，特制定本规范。

# 2. 适用范围

本规范适用于青岛通产智能运维业务应急响应管理，包括应急准备、监测与预警、应急处置和总结改进四个阶段的应急管理活动。

# 3. 原则

预防为主原则：提高安全意识，实施风险评估，完善安全措施，加强监测与预警。

统一管理原则：建立应急响应管理组织，突发事件统一管理，统一指挥。

分级处理原则：划分突发事件级别，按事件级别响应处理，建立事件升级机制。

协商一致原则：识别利益相关方，统筹协调应急响应工作。

有效快速原则：有效制定预案，及时发现，尽快恢复服务。

及时通报原则：建立通报流程，及时汇报突发事件情况。

先主后次原则：应急处理应首先保障主要信息系统的持续稳定运行。

# 4. 术语

应急事件：导致或即将导致运行维护服务对象运行中断、运行质量降低，以及需要实施重点时段保障的事件。

重点时段保障：提升服务级别以确保某一时间段内重要活动或重点业务的开展所采取的措施和活动。

应急响应：组织为预防、监控、处置和管理应急事件所采取的措施和活动。

利益相关方：在组织的决策或活动中有重要利益的个人或团体，包括服务需方、服务供方、分包方、供应商等。

# 5. 角色与职责

| 角色 | 主要职责 | 职能岗位 |
| --- | --- | --- |
| 应急响应管理组织 | 应急响应的最高管理组织，负责统筹、协调和决策应急响应工作。 | 总经理 |
| 应急响应责任人 | 统筹协调应急响应工作，可由服务需方的信息化部门最高管理者担任。 | 需方部门经理 |
| 现场负责人 | 由应急响应责任人授权，负责应急事件监测与预警、应急处置等现场工作。 | 项目经理 |
| 分组负责人 | 可在组织内成立多个分项小组并设定负责人，承担应急响应中各专业性工作。 | 项目经理 |
| 值班人员 | 组织内承担现场值守工作的人员。 | 运维工程师 |
| 应急响应处理人员 | 负责应急事件的分析、处理与恢复。 | 运维部 |

# 6. 应急响应过程

## 6.1. 应急准备

### 6.1.1. 建立应急管理部

首先应识别利益相关方，包括服务需方、服务供方、分包方、供应商等。应在运行维护服务组织基础上建立应急管理部，要求如下：

应急管理部的人员应属于运行维护服务组织的人员，也可包括其他机构的专家和人员；

应规定运行维护服务及应急响应所有相关利益方的角色及职责，并为关键角色提供备份人选；应明确应急响应责任人、现场负责人、分组负责人、值班人员；

应就应急响应服务的范围、要求等与相关利益方达成一致，确定沟通流程和方式，并形成记录；

运行维护过程中涉及组织和人员的变更应与相关利益方达成一致，并形成记录；

应建立对应急管理部内人员的考核机制，明确考核指标及方法。考核至少每年进行一次，以确保组织能持续满足应急响应要求。

### 6.1.2. 风险评估与改进

1. 风险评估

应急管理部应按照确定的方法和流程对重要信息系统实施风险评估，确保组织了解其在运行维护过程中的关键活动、所需资源、限制条件及信息系统面临的各种风险要素。应了解当风险演变为应急事件时所产生的影响和后果，以及信息系统服务中断所带来的损失。

应急管理部应授权公司内或公司外的服务供方进行风险识别，并将授权通知到所有相关利益方。被授权的服务供方应结合具体的信息系统现状和要求，从技术和管理等方面确定风险要素。

应对风险要素进行评估，形成风险评估报告，报告内容应包括：

1. 结论摘要；
2. 背景及现状；
3. 风险要素；
4. 识别出的风险及风险分析；
5. 建议的应对措施。

应在需方授权范围内对风险评估报告进行评审和沟通，并达成一致。

6. 改进

对于识别出的各种风险，应急管理部应该制定明确的控制策略，必要时应对信息系统进行升级改造。可供选择的风险控制策略包括：风险规避、风险转移、风险降低、风险接受。根据风险评估报告，组织应该形成改进方案并实施。

### 6.1.3. 划分应急事件级别

应急事件分级的主要参考要素为：信息系统的重要程度、信息系统服务时段、

信息系统受损程度。对可能发生的应急事件进行级别划分（级别划分方法参见《附件A：应急事件级别划分指南》）。应结合自身的业务要求，对应急事件级别对应的响应时间、处置完成时间等达成一致，并根据应急事件级别配置响应的保障措施，如人员、资金和设备等。

#### 6.1.4. 应急响应预案制定

1. 预案制定

应急管理部应根据应急事件级别制定应急响应预案。应急响应预案可以分为总体预案和针对某个核心系统的专项预案。应急响应预案的格式应该能够为应急管理部进行系统恢复操作提供快速明确的指导。应急响应预案应该明确、简洁，易于在紧急情况下执行，并使用检查列表。应急响应预案的内容应包括：

应急响应预案的编制目的、依据和适用范围；

1. 具体的组织体系结构及人员职责；
2. 应急响应的监测和预警机制；
3. 应急响应预案的启动；
4. 应急事件级别及对应的处置流程、方法；
5. 应急响应的保障措施；
6. 应急预案的附则。

由应急响应责任人负责组织服务需方对应急响应预案进行评审、与相关利益方达成一致，并负责预案的发布。

7. 培训与演练

应制定应急响应培训计划，并组织相关人员参与。应急响应预案应作为培训的主要内容。培训应使得应急管理部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。培训应至少每年举办一次。

为检验应急响应预案的有效性，同时使相关人员了解运行维护预案的目标和内容，熟悉应急响应的操作规程，应进行应急演练，必要时，组织可根据演练的效果，对应急响应预案进行完善。演练应至少每年组织一次。

## 6.2. 监测与预警

### 6.2.1. 日常监测与预警

交付团队应持续开展日常监测活动，实施有效预警，范围如下：

1. 应该结合服务范围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。
2. 组织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。
3. 交付团队应建立监测、预警的记录和报告制度，并按照约定的形式和时间间隔上报现场负责人。发现应急事件时，值班人员应提交报告，报告内容应包括：
   (1) 应急事件发生及发现的时间、位置；
   (2) 现象描述；
   (3) 影响的范围；
   (4) 初步原因分析；
   (5) 报告人。

### 6.2.2. 核实与评估

现场负责人应对报告内容进行逐项核实。核实确认后的应急事件报告，应提交给应急响应责任者。应急事件报告应作为事件级别评估的输入。重点时段保障需求也应作为事件级别评估的输入。

现场负责人应根据事件级别定义，初步确定应急事件所对应的事件级别。应将事件级别置于动态调整控制中。

#### 6.2.3. 应急响应预案启动

组织应建立、审议应急响应预案启动的策略和程序，以控制预案启动的授权和实施。

组织应就应急响应预案启动可能造成的影响进行评估。相关利益方之间应就启动何种类型预案达成一致，包括当应急事件升级时，与之相对应的预案调整的方式。可根据先期处置要求进行应急响应预案的自动启动，或由应急响应责任者或现场负责人启动预案。应记录应急响应预案启动的过程和结果。

现场负责人应向相关利益方通报应急响应预案启动信息，内容应包括：

1. 预案启动的原因；
2. 事件级别；
3. 事件对应的预案；
4. 要求采取的技术应对措施或处置的目标；
5. 实现目标所应采取的保障措施，如人员、资金和设备等；
6. 对应急处置过程及结果的报告要求，如报告程序、报告内容、报告频率等；
7. 信息通报的范围和接收者。

信息通报应选取适当的方式，如电话、邮件、传真、书面文件等。所有相关利益方应对收到的通报信息进行确认和反馈。

通报信息应作为监测与预警状态调整的输入，调整内容包括监测范围、监测频率等。

监测与预警状态的调整应通知各相关利益方。

### 6.3. 应急处置

#### 6.3.1. 应急调度

按照预案，开展统一的应急调度，包括人员、资金和设备等。

应急调度中应：

1. 获取现场信息；
2. 组织必要人员进行勘察、分析；
3. 下达调度命令并保持跟踪；

4. 保护可追查的相关线索。

### 6.3.2. 排查与诊断

故障排查与诊断的流程应包含以下内容：

1. 现场负责人调度处置人员进行现场故障排查；
2. 现场处置人员进行故障排查和诊断，必要时可寻求组织其他人员以现场或远程方式进行支持，在此过程中可借助各类排查诊断分析工具，如应用软件、电子分析工具、故障排查服务知识等；
3. 现场处置人员应随时向现场负责人汇报故障排查情况、诊断信息、故障定位结果等；
4. 将排查与诊断的过程与结果信息进行整理与归档。

处置过程中，现场负责人应及时与相关利益方进行沟通，沟通的内容主要包括系统故障点、造成故障的原因、排查诊断状况等。现场负责人应组织相关利益方对问题进行确认。问题确认过程不应延误处理与恢复工作的开展。

### 6.3.3. 处理与恢复

应基于应急响应预案、配置管理数据库、服务知识等进行故障处理和系统恢复，处理与恢复的原则包括：

1. 应在满足事件级别处置时间要求的前提下，尽快恢复服务；
2. 采用的方法、手段不应造成次生、衍生事件的发生。
3. 必要时可启用备品备件、灾备系统等。应该对过程及结果信息进行记录，并及时告知相关利益方。现场负责人应组织对处理与恢复的结果进行初步确认。

### 6.3.4. 事件升级

1. 升级

公司应建立、审议应急事件升级的策略和程序，以控制应急事件升级的授权和实施。当实际处置时间超过事件级别处置时间要求时，应作为事件升级的参考要素。公司应该对事件升级可能造成的影响进行评估，并在相关利益方之间达成一致。升级内容应包含预案调整、人员调整、资金调整以及设备调整。

事件升级的实施授权应由现场负责人启动。应该对事件升级的过程和结果信息进行整理与归档。

2. 信息通报

现场负责人应向相关利益方通报事件升级信息，内容应包括：

(1) 事件升级的原因；

(2) 事件升级后的级别；

(3) 事件升级后与之对应的预案；

(4) 对升级事件处置过程及结果的报告要求，如：报告程序、报告对象、报告内容、报告频率等；

(5) 信息通报的范围和涉及的接受者。

信息通报应选择适当的方式，如电话、邮件、传真、书面文件等。

事件升级信息应作为处理与恢复的参考要素。

### 6.3.5. 持续服务

完成处理与恢复后，应组织运行维护人员提供持续性服务。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。

### 6.3.6. 事件关闭

1. 申请

组织应建立、审议事件关闭的策略和程序，以控制事件关闭的授权和实施。

应该对应急事件处置的过程文档进行整理。

事件关闭申请应由相关的分组负责人提出，并提交相关文档资料。

事件关闭申请和文档资料，应作为事件关闭核实的参考要素。

2. 核实

现场负责人接到事件关闭申请后，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。

3. 调查和取证

当应急事件涉及到责任认定、赔偿或诉讼时，应收集、保留和呈递证据。证据可能用于：

(1) 内部问题分析；

(2) 用作合同违约或其他纠纷的法律取证；

(3) 与相关方谈判赔偿事宜。

4. 关闭通报

组织应建立、审议应急事件关闭通报制度。

现场负责人应向相关利益方通报事件关闭信息，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。

(9) 应急事件发生的原因、处置过程和方法应记入服务知识。

## 6.4. 总结改进

### 6.4.1. 应急工作总结

公司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总结报告，并将总结报告作为改进应急响应工作及信息系统的重要依据。

### 6.4.2. 应急工作审核

为保证应急响应的有效性和时效性，应急响应责任者应定期组织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。评审应至少每年举行一次。

1. 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。

2. 审核的输出结果应该包括：

改进目标；

(1) 改进的具体工作内容；

(2) 所需的各种资源，包括人员、资金和设备等。

### 6.4.3. 应急工作改进

应急事件总结、应急工作审核的结果应该作为应急准备阶段各项工作的改进要素。组织应根据总结报告中给出的建议项和评审结果，完善信息系统，深化应急准备工作。

## 7. KPI指标

| 指标名称 | 计算公式 | 考核要求 | 考核周期 |
|---|---|---|---|
| 应急演练次数 | 次数，项目进行应急演练的次数 | ≥1次 | 年度 |

## 8. 输出文件与记录

风险评估报告

应急响应预案

应急响应培训记录

应急响应演练记录

应急工作总结报告