**组织级应急保障制度**



青岛慧海联创信息技术有限公司

2025-01-04

文档信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 文档名称编号 | 应急保障管理制度（HHLC-ITSS-YJBZGL） | | | |
| 编制单位 | 青岛慧海联创信息技术有限公司 | | | |
| 文档版本 | 版本日期 | 版本说明 | 作者 | 审核 |
| V1.0 | 2025-1-4 | 发布版本 | 宫海亭 | 张仲全 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[应急保障管理制度 1](#_Toc29938)

[文档信息 2](#_Toc7401)

[1.术语定义 4](#_Toc4942)

[2.目标 4](#_Toc22127)

[3.制定依据 4](#_Toc1676)

[4.应急响应原则 4](#_Toc1128)

[4.1.统一领导、有效组织 4](#_Toc12331)

[4.2.技术支撑，健全机制 5](#_Toc3344)

[4.3.重点突出、快速恢复 5](#_Toc9544)

[5 风险评估管理 6](#_Toc8597)

[5.1 系统重要性评估 6](#_Toc10429)

[5.2 影响度评估 7](#_Toc32331)

[5.3 发生率评估 7](#_Toc24319)

[5.4 风险等级评估 7](#_Toc29047)

[5.5 进行风险评估 8](#_Toc21057)

[6 应急事件分级 9](#_Toc1406)

# 1.术语定义

a) 重点时段保障 important period assurance

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。

b) 应急事件 emergency event

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。

c) 应急响应 emergency response

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。

# 2.目标

为预防和控制潜在的事故或紧急情况，在事故或紧急情况发生时及时作出响应，快速、有效地对事故或紧急情况进行抢险、救援，保障事故应急工作的顺利开展，最大限度地减少可能产生的后果。

# 3.制定依据

a)T/CESA 1299—2023 《信息技术服务运行维护服务能力成熟度模型》

b) GB/T 28827.1-2022《信息技术服务运行维护第1部分：通用要求》

# 4.应急响应原则

## 4.1.统一领导、有效组织

由公司分管副经理担任总负责人，遇到重大信息系统异常情况，应及时向有关领导报告，以便于统一调度、减少损失。同时成立应急管理小组，由质量中心副经理，技术骨干等组成。公司成立应急工作小组，组织开展事件预防、应急处置、恢复运行、事件通报等各项应急工作。公司相关部门要主动协调有关各方面，参与实施听从指挥。

## 4.2.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。

## 4.3.重点突出、快速恢复

应急处理的重点放在运行着重要业务系统或可能导致严重事故后果的关键信息系统上。信息系统管理人员在坚持快速恢复系统的原则下，根据职责分工，加强团结协作，必要情况下与设备供应商以及系统集成商共同谋求问题的快速解决。出现信息系统故障时，信息系统维护人员应及时发现、及时报告、及时抢修、及时控制，积极对信息系统突发事件进行防范、监测、预警、报告、响应。防范为主，

经常性地做好应对信息系统突发事件的思想准备、预案准备、机制准备和工作准备，提高基础设备和重要信息系统的综合保障水平。加强对信息系统应用的日常监视，及时发现信息系统突发性事件并采取有效措施，迅速控制事件影响范围，力争将损失降到最低程度。

# 5 风险评估管理

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：

## 5.1 系统重要性评估

|  |  |  |
| --- | --- | --- |
| **等级** | **描述** | **赋值** |
| 1 级 | 将对客户造成极严重的或灾难性的损失 | 4 |
| 2 级 | 将对客户造成较重要的损失 | 3 |
| 3 级 | 将对客户造成一定损失 | 2 |
| 4 级 | 将对客户造成有限损失 | 1 |

## 5.2 影响度评估

|  |  |  |
| --- | --- | --- |
| **等级** | **赋值** | **影响度描述** |
| 高 | 3 | 核心业务全面中断；影响大面积用户正常使用；核心业务并发高峰期；核心业务关键程序执行期； |
| 中 | 2 | 部分核心业务中断；影响一定范围内用户的正常使用；部分核心业务并发高峰期；部分核心程序执行期； |
| 低 | 1 | 单一业务中断；影响个别用户正常使用；非核心业务并发期；非核心程序执行期； |

根据上表对信息系统以及相关外部环境进行影响度评估。

**5.3** **发生率评估**

|  |  |  |
| --- | --- | --- |
| **等级** | **可能性取值** | **可能性描述（威胁发生的频率）** |
| 经常 | 3 | 可能每个季度发生一次或者以上 |
| 偶尔 | 2 | 可能每半年会发生一次 |
| 极少 | 1 | 可能每年发生一次或更少 |

根据上表对风险发生几率进行评估。

## 5.4 风险等级评估

按照重要性、影响度、发生几率赋值相乘，得出信息系统以及相关环境的风险等级。等级描述如下：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **可能性** | 1 | | | | 2 | | | 3 | | |
|  | **影响度** | 1 | | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 |
| **重要性** | 1 | 1 | | 2 | 3 | 2 | 4 | 6 | 3 | 6 | 9 |
| 2 | 2 | | 4 | 6 | 4 | 8 | 12 | 6 | 12 | 18 |
| 3 | 3 | | 6 | 9 | 6 | 12 | 18 | 9 | 18 | 27 |
| 4 | 4 | | 8 | 12 | 8 | 16 | 24 | 12 | 24 | 36 |
| **风险值** **＝** **重要性×** **风险发生可能性** **×** **风险发生的严重性（影响度）** | | | | | | | | | | | |
| **风险等级** | | | **风险值** **n** | | | | | | | | |
| 高（H） | | | n>=12 | | | | | | | | |
| 中（M） | | | 12>n>4 | | | | | | | | |
| 低（L） | | | n<=4 | | | | | | | | |

**5.5** **进行风险评估**

按照风险等级评估，列出信息系统以及相关外部环境，描述可能发生的风险，针对每一个风险制定控制措施，并明确相应责任人，形成《风险评估表》，撰写风险评估报告。

# 6 应急事件分级

根据信息系统事件的分级考虑要素，将信息系统事件划分为三个级别：I 级事件、II级事件、III 级事件。

l 一般（III 级）：综合分值在 1-4 分；

l 较大（II 级）：综合分值在 5-12 分；

l 重大（I 级）：综合分值在大于 12 分；