信息化运维服务应急预案

目　录

第一节 应急服务响应措施 2
一、突发事件应急流程 2
二、预防措施及处理办法 3
第二节 机房突发事件应急流程 4
一、机房突发事件分类 4
二、应急处理人员组织机构 4
三、应急机构人员岗位职责 5
四、突发事件处理原则 6
五、机房应急开关机具体措施 7
六、机房日常维护 7
七、服务器及存储设备故障处理 7
第三节 信息化系统应急预案 15
一、目的 15
二、组织保障要求 15
三、预警和预防要求 16
四、信息化系统突发事件分类定级 17
五、应急预案启动 18
六、现场应急处理 19
七、保障措施 20
八、恶意攻击时的紧急处置措施 21
九、病毒安全紧急处置措施 22
十、软件系统遭破坏性攻击的紧急处置措施 22

十一、广域网外部线路中断紧急处置措施 23
十二、局域网中断紧急处置措施 24
十三、设备安全紧急处置措施 24
十四、人员疏散与机房灭火预案 25
十五、供电中断后的设备运行预案 25
十六、关键人员不在岗的紧急处置措施 26

第一节 应急服务响应措施

一、突发事件应急流程

在日常运维中可能会出现突发事件，一旦出现如下问题我公司将遵循应急流程处理突发事件。

我公司承诺：

派遣至少三名驻场工程师采取坐班制常驻现场，与招标方正常作息时间（5×8 小时），7×24 小时待命，在接到故障报修或技术服务要求后在 1 小时内响应，4 小时内赶到故障现场进行现场技术服务；节假日期间安排一名驻场工程师值班，或根据招标方要求进行现场巡查。

当巡检维护过程中发现故障，或者设备运行发生告警、业务部门反馈时，一旦发生驻点工程师第一时间告知客户，并将具体的情况一同告知，以最快速度联系公司相关技术专家和公司相关高层领导,与专家进行充分沟通初步定为故障，并将故障定级，同时告知客户，如遇到驻点工程师无法解决的故障时，公司内相关领域技术专家会以最快速度赶到事故现场进行故障处理，直至问题解决，在问题解决之后。由技术专家和驻点工程师共同完成事件问题报告，将事故的发生原因，处理的方式，以及如何避免再次发生的方法进行详细记录，录入客户的运维管理文件中，同时由公司技术专家完成将此案例录入公司内部知识案例库，作为以后借鉴依据，当事故处理完毕后，由驻点工程师或技术专家将结果告知客户和公司相关领导。

二、预防措施及处理办法

系统运维应急方案是对中断或严重影响业务的故障，如宕机、数据丢失、业务中断等，进行快速响应和处理，在最短时间内恢复业务系统，将损失降到最低。在系统维护过程中，突发事件的出现将是很难完全避免的，针对这种情况，我公司设计了完善的突发事件应急策略。

系统巡检人员要定期规范检查各硬件设备的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期安全备份。对发现的问题在报各级负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免

造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

对发现的问题在报负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

当获悉出现突发事件时，驻点工程师可以立即从知识库中获取相应的应急策略，并综合用户方的具体情况，与公司技术专家沟通，给出相关解决方案，然后在第一时间以电话、邮件支持或现场服务的方式帮助用户解决问题，尽最大努力减小突发事件对用户日常应用的影响。

第二节 机房突发事件应急流程

一、机房突发事件分类

（一）自然灾害

指地震、火灾等因自然因素引起的网络与信息系统的损坏。

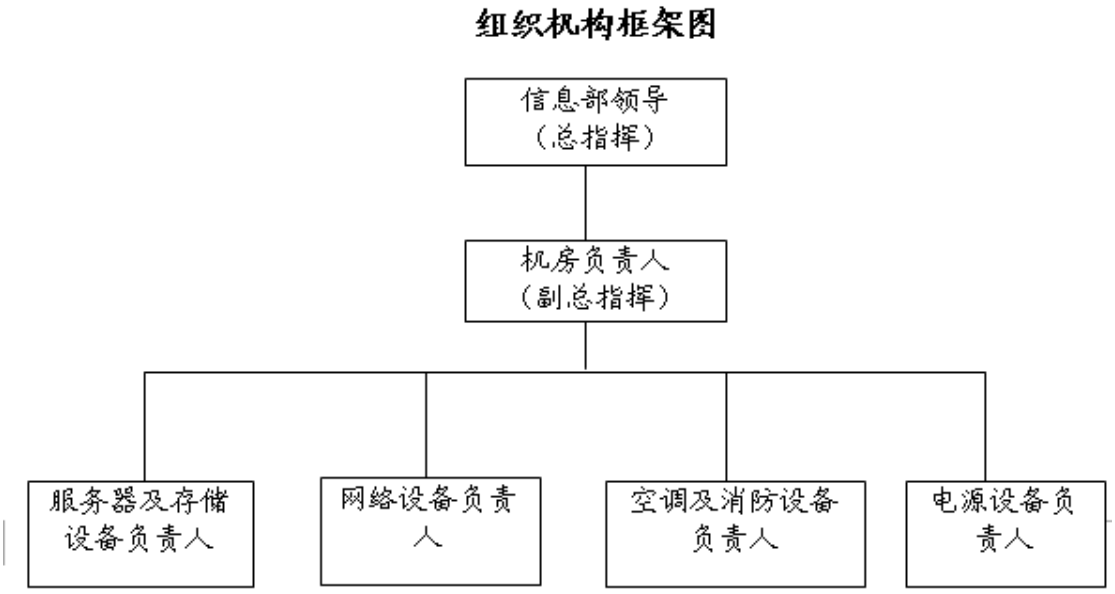
（二）事故灾难

指电力中断、网络损坏、软件、硬件设备故障等引起的网络与信息系统的损坏。

（三）人为破坏

指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏。

二、应急处理人员组织机构



三、应急机构人员岗位职责

（一）应急总指挥职责

1.保证在任何时间，及时协调应急行动所有涉及的岗位人员；

2.提供必需的紧急响应设备；

3.在紧急情况下全面负责紧急行动；

4.在必要时向外界求救，例如：119、110、120 等。

（二）应急副总指挥职责

1.在总指挥领导下具体开展工作，当总指挥不在时履行总指挥职责；

2.根据获得的应急信息下达命令。

（三）各相关设备负责人职责

1.负责尽快收集信息向应急总指挥汇报事故情况；

2.负责现场临时设备抢救和对事态的控制；

3.听从上级指挥人员的指挥。

四、突发事件处理原则

（一）预防为主

立足安全防护，加强预警，重点保护基础信息网络和关系信息安全、稳定的重要信息系统，从预防、监控、应急处理、应急保障等环节，在管理、技术、人员等方面采取多种措施充分发挥各方面的作用，共同构筑安全保障体系。

（二）快速反应

突发事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

（三）分级负责

按照“谁主管，谁负责”的原则，建立和完善安全责任制及联动工作机制。根据各负责人的职能，各司其职，加强各负责人的协调与配合,共同履行应急处置工作的管理职责。

（四）以人为本

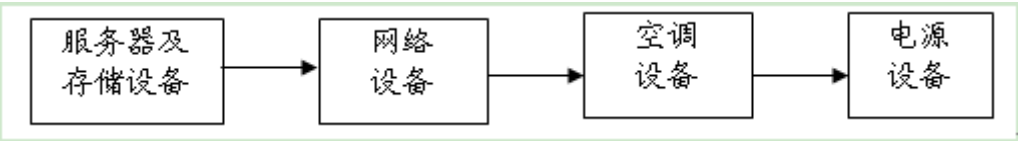
把保障人员以及公共利益的安全作为首要任务。

（五）常备不懈

加强技术储备，规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发公共事件应急处置的科学化、程序化与规范化。

五、机房应急开关机具体措施

机房各设备关闭顺序如下：



六、机房日常维护

（一）建立健全机房管理制度

1.在正常工作日内，信息技术部人员负责对机房进行监控，主要职责是：巡视网络设备及系统的运行情况，发生异常情况及时处理，消除网络故障隐患。

2.节假日期间技术人员轮流值班，负责处理有关异常情况。

3.机房采取来人来访登记制度，未经允许，无关人员不得进入机房区域。

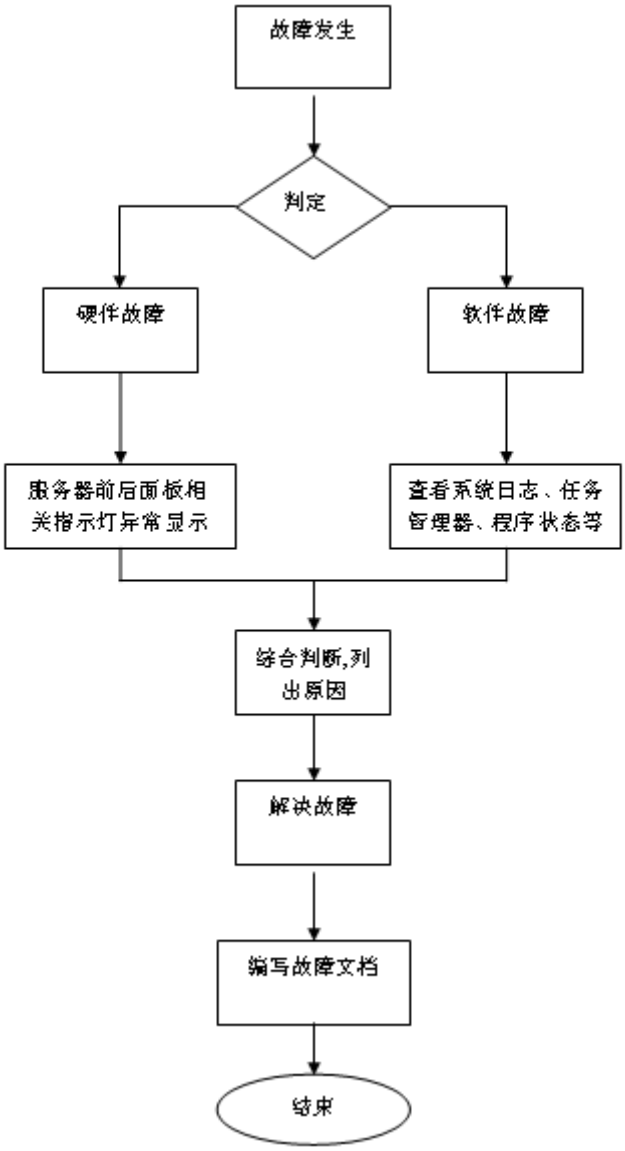
（二）机房内严格采取防雷、防火、防尘、防静电等措施以及机房 24 小时监控等措施。

（三）认真做好数据备份工作，定期做一次数据库完全备份，每月检查服务器运行和备份情况。

（四）对机房的主要网络设备（路由器、主干交换机等）进行工作时间内全程监控，发现异常情况应及时进行处理，确保整个网络的正常运行。

七、服务器及存储设备故障处理

（一）排错流程



（二）应急处置具体措施

1.设备发生被盗或人为损害事件应急预案

（1）发生设备被盗或人为损害设备情况时，使用者或管理者立即报告系统突发故障应急领导小组，同时保护好现场。

（2）

系统突发故障应急领导小组接报后，通知用户保卫部门、相关领导，一同核实审定现场情况，清点被盗物资或盘查人为损害情况，做好必要的影像记录和文字记录。

（3）事发单位和当事人应当积极配合公安部门进行调查，并将有关情况向系统突发故障应急领导小组汇报。

（4）系统突发故障应急领导小组安排运维服务小组、事发单位及时恢复系统正常运行，并对事件进行调查。运维服务小组和事发单位应在调查结束后一日内书面报告系统突发故障应急领导小组。事态或后果严重的，应向相关领导汇报。

2.机房长时间停电应急预案

（1）定期检查机房供电设备的运行状况和电路线缆器材情况，当发生下列突发事件时，按照以下方案进行处置：

（2）当机房发生市电供电突然停电或是电源异常时。首先应和后勤部门联系确认正常停电以及预计停电时间。检查不间断电源的电池可供电时间，确保设备正常运行，如遇到突然断电，应及时将空调等不在 UPS 电源供电范围内的设备及时断电，预防突然来电时瞬间电流过大导致设备损坏等现象。

（3）当确定停电时间超出机房 UPS 承载范围后，首先确定停电的范围以及受影响的设备范围。并及时通知各部门做好停电应急准备。然后通知机房电源维护人和设备的负责人到达现场，做好各设备的电源停电准备。在 UPS 供电电量仅剩 10%之后，严格按操作手册停掉各服务器的电源，最后

停核心交换机和路由器，等待电力恢复。

（4）

当确定停电原因是在本身供电系统范围内，立即汇报给负责领导，并及时联系相关维护人员达到现场检修。对于恢复时间无法预计的，要通知后勤部门做好柴油机发电及移动电源车供电准备

（5）恢复供电后，严格按照操作程序逐步恢复机房设备和 UPS 的供电，以防瞬间电流过大造成设备损坏。

3.通信网络故障应急预案

（1）发生通信线路中断、路由故障、流量异常、域名系统故障后，操作员应及时通知本单位信息系统管理员，经初步判断后及时上报运维服务小组和系统突发故障应急领导小组。

（2）运维服务小组接报告后，应及时查清通信网络故障位置，隔离故障区域，并将事态及时报告系统突发故障应急领导小组，通知相关通信网络运营商查清原因；同时及时组织相关技术人员检测故障区域，逐步恢复故障区域服务器的网络连接，恢复通信网络，保证正常运转。

（3）事态或后果严重的，应向应急指挥办公室和相关领导汇报。

（4）应急处置结束后，运维服务小组应将故障分析报告，在调查结束后一日内书面报告系统突发故障应急领导小组。

4.不良信息和网络病毒事件应急预案

（1）发现不良信息或网络病毒时，信息系统管理员立即断开网线，终止不良信息或网络病毒传播，并报告指挥调

度中心运维服务小组和系统突发故障应急领导小组。

（2）运维服务小组应根据系统突发故障应急领导小组指令，采取隔离网络等措施，及时杀毒或清除不良信息，并追查不良信息来源。

（3）事态或后果严重的，应向监控中心办公室和相关领导汇报。

（4）处置结束后，运维服务小组应将事发经过、造成影响、处置结果在调查工作结束后一日内书面报告系统突发故障应急领导小组。

5.服务器软件系统故障应急预案

（1）发生服务器软件系统故障后，运维服务小组负责人立即组织启动备份服务器系统，由备份服务器接管业务应用，并及时报告系统突发故障应急领导小组；同时安排相关责任人将故障服务器脱离网络，保存系统状态不变，取出系统镜像备份磁盘，保持原始数据。

（2）运维服务小组应根据系统突发故障应急领导小组的指令，在确认安全的情况下，重新启动故障服务器系统；重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系相关厂商和上级单位，请求技术支援，做好技术处理。

（3）事态或后果严重的，应向监控中心应急指挥办公室和相关领导汇报。

（4）处置结束后，运维服务小组应将事发经过、处置结果等在调查工作结束后一日内报告系统突发故障应急领导小组。