江西服装学院

网络与信息化管理中心文件

江服网管字〔2016〕3号

江西服装学院校园网信息安全应急处置预案

随着学校网络信息化建设的不断深入，加强中心机房核心设备、应用系统以及网络信息安全等方面的事故保障能力，应对突发事件的处理能力是我们工作中的一项重要任务。为了确保中心机房及应用系统的安全与稳定，以保证正常运行为宗旨，遵循“预防为主，积极处置”的原则，建立统一指挥、职责明确、有序运转、反应迅速的突发事件处置安全体系，将正在发生或已发生事故的损害程度降到最低，确保校园网络的安全，特制定本应急处置预案。

本预案分为应用系统故障应急措施和机房突发事件应急措施。

系统故障应急措施

一、系统故障应急流程说明

1、故障发生

系统运维人员可从以下途径得知故障的发生:

1.1、运维人员通过网络设备软件平台告警发现故障

1.2、运维人员通过维护巡检发现故障

1.3、各分院、部门发现故障，通过电话或网络报给网络中心

2、报障受理

监控系统运维服务人员得知系统故障发生后，立即响应，并向报障人或部门详细了解系统故障情况和影响范围。

3、系统故障研判

运维服务人员根据了解到的系统故障情况进行分析判断，以确定采用一般故障处理流程还是立即启动系统突发故障应急处理预案。

4、预案启动

如需启动应急预案，则立刻通知系统突发故障应急领导小组，由领导小组启动应急预案，对系统突发故障应急事件进行全面管控处理。

5、资源确认

系统突发故障应急预案启动后，首先是根据现场突发故障的实际状况、紧急程度、技术难度、备品备件等情况对相关资

源（主要是参与人员）依据经验进行调度和确认，主要有以下资源:

本单位技术支持人员；相关厂家技术支持人员；网络与安全的设备备件;

6、预案执行

按照既定的预案进行突发故障抢修，如遇到问题及时向系统突发故障应急领导小组汇报。

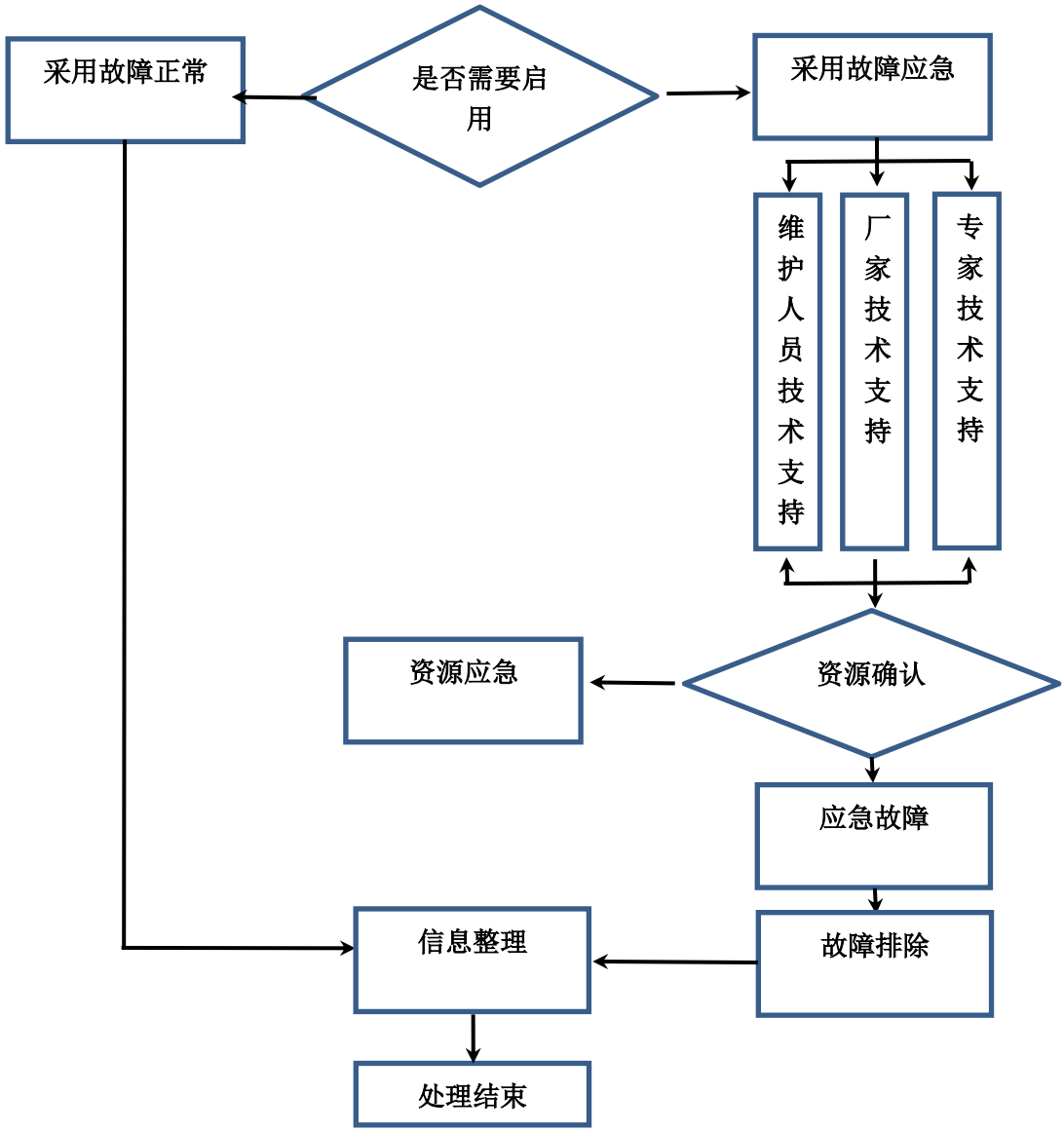
7、预案终止

预案的终止时间由故障现场技术人员根据现场的实际进展情况,在与有关部门协调后报系统突发故障应急领导小组决定。

8、结果上报

预案中止后,相关预案参与人员编写整个事件的处理文档,整理故障处理经验和教训，修改、完善事件应急预案；然后集中上报至系统突发故障应急领导小组。

二、 系统故障应急处理流程图



机房突发事件应急措施

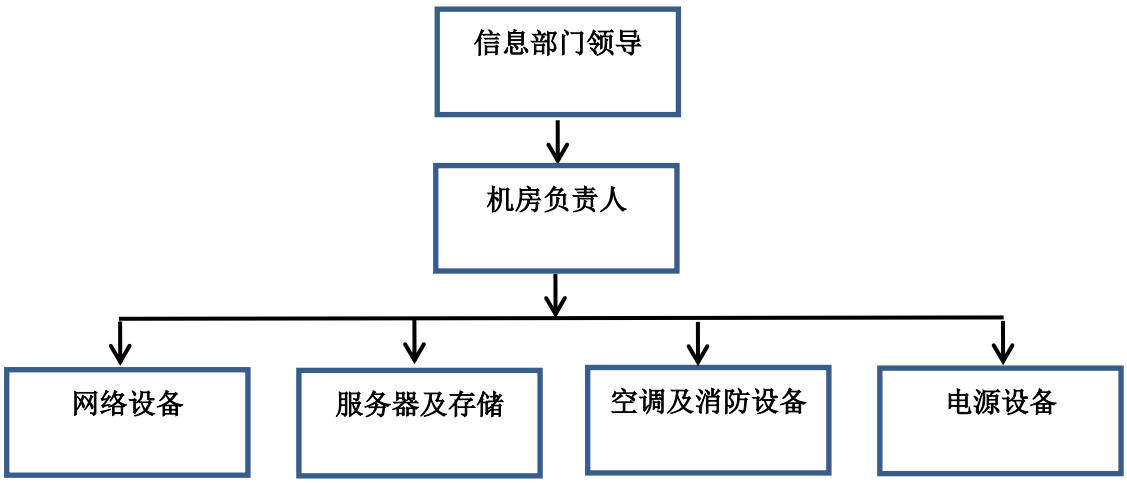
一、机房突发事件分类

1、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。

2、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。

3、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

1、应急总指挥职责

1.1、保证在任何时间，及时协调应急行动所有涉及的岗位人员；

1.2、提供必须的紧急响应设备；

1.3、在紧急情况下全面负责紧急行动；

1.4、在必要时向外界求救，例如：119、110、120 等。

2、应急副总指挥职责

2.1、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;

2.2、根据获得的应急信息下达命令。

3、各相关设备负责人职责

3.1、负责尽快收集信息向应急总指挥汇报事故情况;

3.2、负责现场临时设备抢救和对事态的控制;

3.3、听从上级指挥人员的指挥。

四、突发事件处理原则

1.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。

2.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。

3.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。

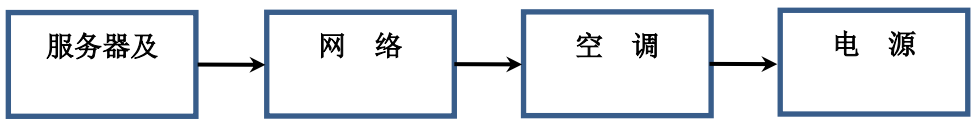
4.以人为本。把保障人员以及公共利益的安全作为首要任

务。

5.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

1、健全和完善机房管理制度

1.1 在正常工作日内，网络技术科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。

1.2 节假日期间技术人员轮流值班，负责处理有关异常情况。

1.3 机房采取来人来访登记制度，未经允许，无关人员不得进入公司机房区域。

2、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。

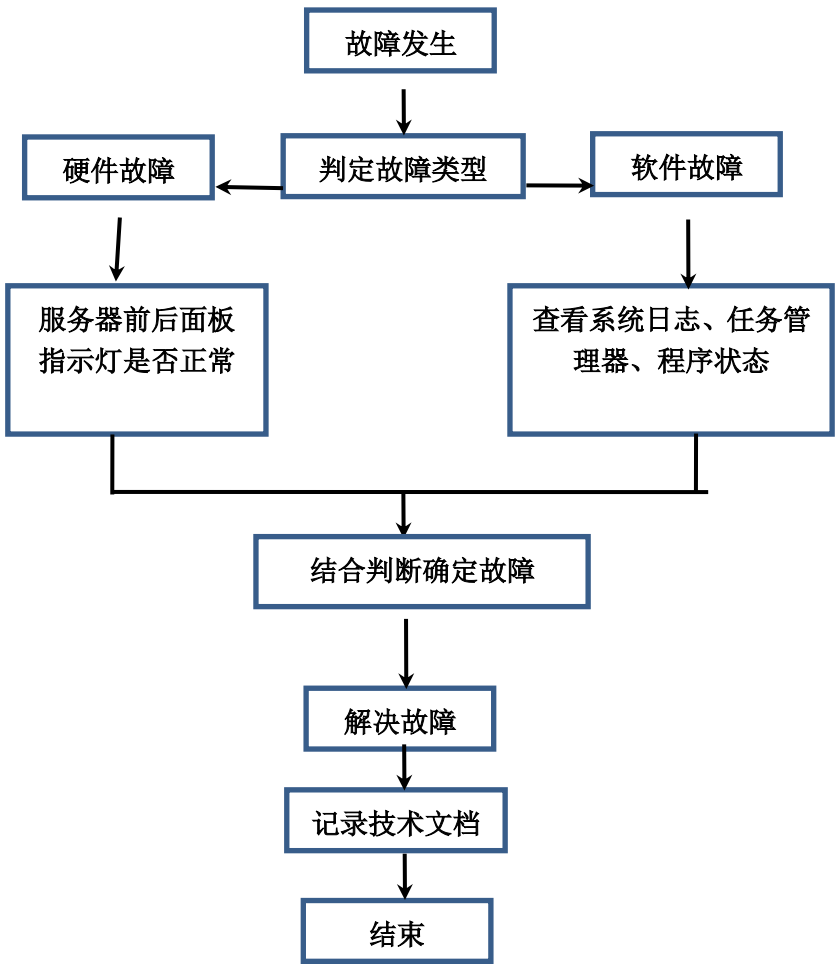
3、认真做好数据备份工作，定期做一次数据库完全备份，

每月检查服务器运行和备份情况。

4、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

1、排错流程



2、应急处置具体措施

2.1 机房漏水应急预案

（1）发生机房漏水时，第一目击者应立即通知机房负责人，并及时报告中心事故应急领导小组。

（2）若空调系统出现渗漏水，机房负责人应立即安排停用故障空调，清除机房积水，并及时联系设备供应方处理，同时启动备用空调，必要情况下可临时用备用空调对服务器进行降温。

（3）若为墙体或机房门渗漏水，机房负责人应立即采取有效措施确保机房安全，及时清除积水，维修墙体或门窗，消除渗漏水隐患。

2.2 设备发生被盗或人为损害事件应急预案

（1）发生网络设备被盗或人为损害网络设备情况时，使用者或管理者应立即报告网络与信息化管理中心，同时保护好现场。

（2）网络与信息化管理中心接报后，通知保卫部门、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相关部门进行调查，并将有关情况向网络与信息化管理中心汇报。

（4）网络与信息化管理中心安排网络技术科为事发部门及时恢复系统正常运行，并对事件进行调查。网络技术科与事发部门应在调查结束后一日内书面报告网络与信息化管理中心领导；事态或后果严重的，应向相关校领导汇报。

2.3 机房长时间停电应急预案

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:

（1）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是否正常停电、预计停电时间以及柴油发电机是否提供供电。检查不间断电源（UPS）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网络设备损坏等现象。

（2）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；然后通知机房设备的维护人员和负责人做好各设备的电源停电准备工作。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。

（3）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到达现场检修。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网络设备损坏。

（6）所有设备正常通电运行后，应对机房辅助设施、网络核心设备、网络应用服务器、各网站及系统服务器、存储服务器等设备逐一检查，是否正常运行。

2.4 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部门信息系统管理员，经初步判断后及时上报网络技术科。

（2）网络技术科接到故障报告后，应及时组织相关技术人员检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转；故障排除后编写故障处理小结。如查清通信网络故障由硬件设备损坏造成，应及时更换相应备件，做好硬件更换记录。

（3）因缺少备件、运营商网络故障等原因，不能短时间内恢复网络正常，应及时隔离故障区域，并将事态及时报告网信中心领导，通知相关网络运营商查清原因。事态或后果严重的，应向相关校领导汇报。

（4）因运营商网络故障导致的网络通信异常，启动网络故障应急预案，第一时间检查网络出口是否自动切换到备用链路，如没有切换，及时手动调整配置切换到备用链路，检查自动切换失败原因。联系运营商确认通信故障解决时间，通信恢复后切换回正常链路，及时报告网信中心领导小组。

（4）日常性故障处理小结每周提交给网信中心领导小组。设备更换记录和应急处置结束后，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网信中心领导小组。

2.5 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，信息系统管理员应立即断开网络，终止不良信息或网络病毒传播，并报告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。

2.6 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应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，作好技术处理。

（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。

2.7 黑客攻击事件应急预案

（1）当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立

即报告系统突发故障应急领导小组。

（2）接报告后，系统突发故障应急领导小组应立即指令运维服务小组核实情况，关闭服务器或系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。

（3）运维服务小组应及时清理系统，恢复数据、程序，恢复系统和网络正常；情况严重的，应向监控中心应急指挥办公室和相关领导汇报，并请求支援。

（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。

2.8 核心设备硬件故障应急预案

（1）发生核心设备硬件故障后，运维服务小组应及时报告系统突发故障应急领导小组，并组织查找、确定故障设备及故障原因，进行先期处置。

（2）若故障设备在短时间内无法修复运维服务小组应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（3）运维服务小组故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关厂商，认真填写设备故障报告单备查。

（4）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。

2.9 业务数据损坏应急预案

（1） 发生业务数据损坏时，运维服务小组应及时报告系统突发故障应急领导小组，检查、备份业务系统当前数据。

（2）运维服务小组负责调用备份服务器备份数据，若备份数据损坏，则调用磁带机中历史备份数据，若磁带机数据仍不可用，则调用异地备份数据。

（3）业务数据损坏事件超过 2 小时后，运维服务小组应及时报告系统突发故障应急领导小组，及时通知业务部门以手工方式开展业务。

（4）运维服务小组应待业务数据系统恢复后，检查历史数据和当前数据的差别，由相关系统业务员补录数据；重新备份数据，并在工作结束后一日内报告系统突发故障应急领导小组。

2.10 雷击事故应急预案

（1） 遇雷暴天气或接上级部门雷暴气象预警，运维服务小组应及时报告系统突发故障应急领导小组，经请示同意后关闭部分服务器，切断电源，暂停内部计算机部分网络工作。

（2） 雷暴天气结束后，运维服务小组报经系统突发故障应急领导小组同意，及时开通服务器，恢复内部计算机网络工

作，对设备和数据进行检查。

（3） 因雷击造成损失的，运维服务小组应会同相关部门进行核实、报损，并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。必要时，应向监控中心应急指挥办公室和相关领导汇报。

2.11 空调设备故障应急预案

若机房专用空调损坏，应第一时间启用机房备用空调，并通知厂家上门进行维修，并及时报告信息部相关领导请示，获得授权后按机房设备关闭顺序关闭各类设备。

2.12 火灾事故应急预案

（1）一旦机房发生火灾，应遵照下列原则：首先确保人员安全；其次保护关键设备、数据安全；三是保护一般设备安全；

（2)人员疏散的程序是:机房工作人员立即按响火警警报，并通过119电话向公安消防请求支援,所有人员戴上防毒面具，所有不参与灭火的人员按照预先确定的线路，迅速从机房中撤出；

（3）人员灭火的程序是：首先切断所有电源，启动自动喷淋系统或使用灭火器，灭火值班人员戴好防毒面具，从指定位置取出泡沫灭火器进行灭火。

2.13 电源设备故障应急预案

机房目前使用 UPS 系统，在紧急情况发生时，应按如下步骤进行关机:

（1）确认所有负载均已安全关机。

（2）关闭 UPS 负载电源。

（3）将 UPS 的系统启用开关切换到 off 的状态。

（4）将电池连接断路器切换到 off 的位置。

网络与信息化管理中心

2016 年 4 月 30 日

江西服装学院网络与信息化管理中心　2016 年 4 月 30 日印发