四川农业大学信息与教育技术中心文件

信教发〔2024〕 9 号

四川农业大学网络应急预案

为迅速、高效处置网络中断事件，保障校园网络、信息系统正常运行，最大限度减少对教学、科研、管理的影响，明确应急职责与处置流程，确保响应科学、协同有效，特制定本预案。

一、适用范围

本预案适用于信息与教育技术中心（以下简称“中心”）负责的三校区校园网、校区间互联链路、出口带宽链路、数据中心、超算中心等网络基础设施的应急响应工作。

二、组织机构与职责

（一）应急领导小组

组长：中心主任

副组长：中心副主任

成员：各业务部主管

职责：决策重大事件处置方案、协调校内外资源、监督预案

执行、向校领导汇报故障进度、上报上级主管部门。

（二）技术组

组长：中心副主任

副组长：网络部业务主管

成员：网络部全体人员、通服驻场人员、运营商维护团队

职责：实时监测网络状态、分析事件根源、故障申报、安排现场故障抢修等技术操作。

（三）联络协调组

组长：中心副主任

成员：综合行政部全体人员、网络部全体人员

职责：对外联络、发布故障通知、制定舆情应对方案等。

三、网络中断事件分类与分级标准

根据《教育行业网络安全等级保护基本要求》（教育系统信息系统安全等级保护定级指南）、《GBT 37088-2018 信息安全技术网络安全事件分类分级指南》对网络中断事件进行如下分类分级。

（一）事件分类

分类编码	类别名称	定义说明
A 类	骨干网络中断	影响三校区互联的骨干网络传输（如核心路由故障、光纤环

		网断裂），导致校区数据传输延迟≥200ms 或丢包率≥10%
B 类	**接入层网络中断**	局部区域网络接入服务中断（楼层/楼宇级），包括接入交换机宕机、无线 AP 集中掉线
C 类	**出口带宽中断**	校园网互联网出口链路中断（单线或双线全断），影响外网访问能力
D 类	**数据中心内部中断**	数据中心内核心资源（服务器、存储、虚拟化平台）可用性异常，导致关键业务系统无法访问
E 类	**设备级硬件故障**	单一网络设备（核心/汇聚交换机、防火墙、负载均衡）因硬件损坏引起的局部服务中断

（二）事件分级

等级	判定标准	响应要求
I 级	- **全校性中断**：三校区同时断网≥10 分钟； - **关键业务瘫痪**：核心系统中断≥10 分钟； - **数据灾难**：存储阵列 RAID 组失效，数据恢复耗时≥24 小时； - **重大舆情**：社会媒体传播断网事件并引发热议。	- 领导小组全员应急，协调跨校区资源； -上报分管校领导； - 启动异地容灾系统接管业务。

Ⅱ级	- **区域级中断**：单校区 50%以上区域断网≥半小时； - **重要业务受阻**：两个以上业务系统中断服务≥2 小时； - **设备级全断**：骨干网核心设备冗余失效造成单点故障。	- 报应急领导小组 - 技术执行组驻场抢修，每 30 分钟通报进展； - 启用冷备设备替换； - 限时完成根因分析报告。
Ⅲ级	- **局部中断**：单栋建筑或楼层网络中断≥30 分钟； - **一般业务降级**：非核心系统故障且冗余链路可维持基础服务； - **接入层设备批量下线**（AP/交换机≥10 台）。	- 业务负责老师主导处理，4 小时内恢复； - 记录故障现象及处理日志； - 汇总上报分析结果。
Ⅳ级	- **单点中断**：个别终端或小型设备故障（如单台 AP 掉线）； - **不影响整体服务**：用户可自主切换至备用接入点； - 恢复时间≤30 分钟。	- 用户自助报修或远程指导解决； - 运维系统自动生成事件工单； - 无需启动专项应急流程。

四、应急响应流程

（一）事件接报与初步判断

当网络中断事件发生时，首先由技术组 5 分钟内响应并登记

工单，并对事件进行初步判断，确定事件等级和可能的影响范围。

（二）启动应急预案

根据事件等级，启动相应的应急预案。对于**Ⅲ级**及以下事件，可由技术组直接处理；对于更高级别的事件，则需报告应急领导小组，并启动更高级别的应急响应流程。

（三）事件处理与恢复

技术组根据应急预案，迅速组织力量进行事件处理。处理过程中，需保持与应急领导小组和联络协调组的沟通，及时反馈处理进展和可能遇到的问题。在事件得到有效控制后，立即着手进行网络恢复工作，确保服务尽快恢复正常。

（四）总结与评估

事件处理完毕后，技术组在 48 小时内需对事件进行总结与评估，分析事件原因、处理过程及效果，提出改进措施和建议。同时，将事件处理过程和结果记录备案，为后续应急响应提供参考。

（五）上报与通报

对于达到一定级别的事件，需按照相关规定向上级主管部门和相关部门进行上报和通报，确保信息透明、共享。

五、预防与保障措施

（一）加强日常监测与维护

定期对网络基础设施进行巡检和维护，其中业务主管负责每

天一次巡检核心设备，三校区网络管理员每周一次巡检接入层设备，及时发现并处理潜在故障，确保网络设备处于良好运行状态。

（二）建立备份与恢复机制

对关键网络设备和数据进行备份，确保在发生网络中断时能够迅速恢复。定期进行备份数据的恢复演练，验证备份数据的可用性。技术组每半年至少进行 1 次全链路容灾演练，并记录演练结果。

（三）提升应急响应能力

加强应急响应团队的技术培训和演练，提高团队在网络中断事件中的快速反应和处置能力。同时，完善应急预案，明确各应急小组的职责和应急处置流程。

（四）加强网络安全防护

加强网络安全防护措施，定期对网络进行安全漏洞扫描和风险评估，及时发现并修复安全漏洞，防范网络攻击和病毒入侵。

（五）建立跨部门协作机制

加强与其他相关部门的沟通与协作，建立跨部门协作机制，共同应对网络中断事件。在事件发生时，能够迅速调动各方资源，协同进行应急处置。

六、附则

本预案自发布之日起实施，由信息与教育技术中心负责解释。若其他有关文件规定与本预案不一致的，以本预案为准；与上级

文件不一致的，则以上级文件规定为准。

信息与教育技术中心

2024 年 12 月 18 日