一、总则

（一）目的

为有效预防、及时控制和妥善处理我校数据中心机房可能发生的各类突发事件，如设备故障、网络中断、电力问题以及安全事故等，确保学校教学、科研、管理等核心业务系统的正常运行，最大程度减少损失和影响，特制定本应急预案。

（二）编制依据

本预案根据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规，《国家突发公共事件总体应急预案》《突发事件应急预案管理办法》《教育系统网络安全事件应急预案》《中南财经政法大学网络安全事件应急预案》等文件进行编制。

（三）适用范围

本预案适用于数据中心机房及其附属设施范围内，因人为、自然灾害、技术故障等原因引发的，导致机房运行中断或出现安全隐患，需要采取应急措施予以应对的各类情况。

（四）工作原则

1.预防为主：加强日常监测与维护，及时发现并排除潜在风险，将突发事件发生的可能性降至最低。

2.快速反应：建立健全快速响应机制，一旦发生突发事件，能够迅速启动应急程序，及时采取有效措施进行处置。

3.科学处置：充分运用专业知识和技术手段，遵循科学的处理流程，确保应急处置的准确性和有效性。

4.保障重点：优先保障学校核心业务系统的持续运行，如教务系统、学工系统、财务系统等，合理分配资源，最大限度减少对学校正常教学秩序的影响。

二、应急组织机构及职责

（一）应急指挥中心

成立以信息管理部部长为总指挥，信息管理部总工程师为副总指挥，各相关科室主任为成员的应急指挥中心。

主要职责：

1.负责统筹协调机房应急处置工作的全面开展，制定应急处置决策。

2.组织、协调各应急救援队伍和资源，确保应急处置工作高效、有序进行。

3.及时向上级领导和相关部门汇报突发事件的处理进展及结果。

（二）应急抢修组

由信息管理部的技术骨干组成。

主要职责：

1.负责机房网络、服务器、存储设备、软件系统等的日常巡检、维护与管理，及时发现并解决潜在技术问题。

2.突发事件发生时，迅速对故障进行技术诊断，确定故障原因和影响范围，制定并实施技术解决方案。

3.配合设备供应商、软件开发商等外部技术力量进行联合抢修，确保系统尽快恢复正常运行。

4.发生电力故障、火灾、浸水等突发事件时，迅速赶赴现场，与学校相关部门保持密切的信息沟通，及时传达突发事件的相关信息，协助相关部门进行救援工作。

三、应急预案体系及具体操作流程

（一）应急预案体系

包括网络故障应急处理预案、服务器故障应急处理预案、存储设备故障应急处理预案、电力故障应急处理预案、消防应急处理预案、浸水应急处理预案等。

（二）应急原则

确保人员安全：在任何情况下，将保障现场应急处置人员的生命安全放在首位，避免因应急处置不当导致人员伤亡。

业务连续性优先：以最快速度恢复学校核心业务系统的正常运行，减少业务中断时间，确保教学、科研、管理等工作的有序开展。

分级响应：根据突发事件的严重程度和影响范围，启动相应级别的应急响应程序，合理调配资源，提高应急处置效率。

（三）网络故障应急处理预案

故障监测与发现：通过全栈监控平台实时监测机房网络设备的运行状态，当出现网络中断、延迟过高、丢包严重等异常情况时，系统自动发出警报。

故障初步判断：应急抢修组接到警报后，立即对故障进行初步判断，确定故障级别。

根据核心网络设备故障对业务的影响程度，将故障分为以下三级：

一级故障

定义：核心网络设备完全瘫痪，导致学校大部分或全部业务系统中断，严重影响学校网络的正常运行。

响应时限：故障发现后 5 分钟内启动应急预案，抢修人员 10 分钟内到达现场。

二级故障

定义：核心网络设备部分功能失效，造成部分业务系统运行缓慢或局部网络中断，对业务有较大影响。

响应时限：故障发现后 10 分钟内启动应急预案，抢修人员 15 分钟内到达现场。

三级故障

定义：核心网络设备出现轻微故障，如个别端口故障、非关键模块告警等，暂时不影响业务正常运行，但如不及时处理可能升级为更严重故障。

响应时限：故障发现后 30 分钟内启动应急预案，抢修人员 60 分钟内到达现场。

应急处理措施：

如果是硬件故障，立即查看是否有备件，如有，在确保兼容性的前提下快速进行替换；若没有备用设备，及时联系设备供应商紧急调配。如果是软件故障，尝试重启相关服务、加载备份配置或进行软件升级修复。

（四）服务器故障应急处理预案

故障监测与发现：服务器管理系统实时监控服务器的 CPU、内存、硬盘、网络等关键资源的使用情况以及服务器的运行状态，当出现服务器故障时，及时发出预警。

故障初步判断：根据预警信息，远程登录服务器查看系统日志、错误提示等，初步判断故障原因。

应急处理措施：

若为普通硬件故障，如硬盘损坏、内存故障等，应急抢修组在 15 分钟内到达现场，确认故障硬件后，立即更换备用硬件，并启动服务器恢复程序。若服务器无法启动，迅速将服务器数据迁移至备用服务器，确保业务系统尽快恢复运行，并通知服务器硬件供应商进行后续维修。

（五）存储设备故障应急处理预案

故障监测与发现：存储管理系统实时监控存储设备的容量、性能、数据读写状态等指标，当出现存储阵列故障、磁盘掉线、读写错误等异常情况时，发出警报。

故障初步判断：查看存储系统日志、指示灯状态等信息，初步判断故障类型，如磁盘阵列控制器故障、硬盘故障、光纤链路故障等。

应急处理措施：

若为单块硬盘故障，应急抢修组在 15 分钟内更换备用硬盘，存储设备将自动进行数据重建，确保数据完整性，密切关注数据重建进度，及时处理重建过程中出现的异常情况。

若为磁盘阵列控制器故障，立即通知存储设备供应商提供技术支持，并启用备用存储控制器（如有）进行切换。在切换过程中，确保

业务系统对存储设备的访问不受影响，同时协调供应商技术人员尽快修复故障控制器。

若为光纤链路故障，迅速检查光纤连接、光模块等部件，修复或更换故障部件，恢复光纤链路畅通。若短时间内无法修复，启用备用光纤链路，保障存储设备与服务器之间的连接正常。

（六）电力故障应急处理预案

故障监测与发现：机房配备的智能电力监控系统实时监测市电输入、UPS 输出、发电机运行等电力参数，当出现市电停电、UPS 故障、发电机启动失败等异常情况时，发出警报。

故障初步判断：应急抢修组根据警报信息，初步判断电力故障原因，如市电供电线路故障、变电站跳闸、UPS 电池老化、发电机燃油不足等。

应急处理措施：

当市电停电时，立即检查柴油发电机、UPS 运行情况，确保其正常工作，为机房设备提供临时电力支持。同时咨询后勤保障部了解停电原因和预计停电时间。

若 UPS 出现故障，应急抢修组迅速判断故障类型，如逆变器故障、电池组故障等，尝试修复。若 15 分钟内无法修复，立即通知 UPS 设备供应商进行维修。

若发电机启动失败，应急抢修组检查燃油、启动电池、控制系统等部件，排除故障，尽快启动发电机。若短时间内无法启动，合理调整机房设备用电负载，优先保障核心业务系统的电力供应，延长 UPS 供电时间，并向应急指挥中心汇报，寻求外部支援。

（七）消防应急处理预案

火灾监测与发现：机房安装有火灾自动报警系统，通过烟雾探测器、温度探测器等设备实时监测机房内的火灾隐患。当检测到烟雾或温度异常升高时，系统自动发出告警。

火灾初步判断：应急抢修组接到警报后，迅速赶赴现场，确认火灾发生的位置和火势大小。

应急处理措施：

发生火灾时，应急抢修组在确保自身安全的前提下，立即切断机房内的非消防用电设备电源，防止火势蔓延，视情况启动机房内的气体灭火系统（如七氟丙烷灭火系统）进行灭火，同时通知学校保卫部人员赶赴现场支援。同时应配合保卫部保障消防用水、消防通道等基础设施的畅通。

在火势得到控制后，对现场进行封锁，保护火灾现场，配合消防部门进行火灾原因调查。并对受损设备进行评估，制定恢复方案，尽快恢复机房的正常运行。

（八）浸水应急处理预案

浸水监测与发现：机房安装有漏水检测系统，通过在机房地面、空调排水管道、消防喷淋管道等易积水部位设置漏水传感器，实时监测机房内的浸水情况。当检测到漏水时，系统自动发出告警。

浸水初步判断：应急抢修组接到警报后，迅速赶赴现场，查看浸水原因，如空调漏水、消防喷淋误动作、给排水管道破裂等。

应急处理措施：

发现浸水后，应急抢修组在确保自身安全的前提下，立即切断机房内可能受水浸影响的设备电源，防止短路和触电事故发生。同时，组织人员进行排水工作，利用吸水机、拖把、沙袋等工具尽快清除积水。

若浸水是由空调漏水引起的，立即关闭空调机组，通知空调维修人员进行抢修，更换损坏的部件，确保空调恢复正常排水功能。

若浸水是由消防喷淋误动作引起的，通知保卫部立即关闭消防喷淋阀门，检查喷淋系统故障原因，进行修复。同时，对受水浸影响的设备进行检查，将受损设备移至安全干燥处，进行烘干、维修等处理，确保设备恢复正常运行。

四、培训与演练

（一）培训计划

定期组织应急救援人员进行专业技术培训，包括网络技术、服务器维护、存储管理、电力知识、消防知识、应急救援技能等方面的培训，提高应急救援人员的业务水平。

（二）演练安排

制定详细的演练计划，每年至少组织一次综合性应急演练，包括网络故障、电力故障、消防事故等多种突发事件的模拟演练。演练过程中，检验应急预案的可行性、各应急组人员的协同作战能力以及应急物资的保障能力。

每次演练结束后，组织召开演练总结会议，对演练过程中发现的问题进行分析总结，提出改进措施，对应急预案进行修订完善，不断提高应急预案的科学性和实用性。

五、后期处置

（一）事件调查与评估

突发事件处理结束后，由应急指挥中心组织相关科室成立事件调查组，对事件发生的原因、经过、处理结果进行全面调查评估。撰写事件调查报告，分析事件的影响范围、损失程度，总结经验教训，提出改进建议，为今后的应急管理工作提供参考。

（二）设备修复与恢复

根据事件调查结果，制定设备修复和系统恢复方案。组织人员对受损设备进行维修或更换，对受影响的软件系统进行重新配置、数据恢复等工作，确保机房设备和系统恢复到正常运行状态。

（三）表彰与问责

对在突发事件应急处置工作中表现突出的部门和个人进行表彰奖励；对在应急处置过程中存在失职、渎职行为的部门和个人，按照学校有关规定进行问责处理。

六、附则

（一）预案管理与更新

本应急预案由信息管理部负责管理和修订。根据国家法律法规、学校发展战略、机房设备和技术的更新变化以及应急演练和实际应急处置过程中发现的问题，适时对预案进行修订完善，确保预案的科学性、实用性和有效性。

（二）预案解释

本预案由信息管理部负责解释。在实施过程中，如遇到特殊情况或疑问，可向信息管理部网络技术与运维中心咨询。

（三）预案实施时间

本应急预案自发布之日起实施。