吉林建筑大学数据中心管理规定

（试行）

第一章 总 则

第一条 为规范数据中心的管理，保证数据中心内各类设备安全、稳定、连续地运行，消除数据中心管理中存在的风险隐患，制订本管理规定。

第二章 门禁管理

第二条 门禁系统维护与权限管理

确保门禁系统的正常工作，如有失效应立即通知管理员检查并排除故障。门禁系统的权限变更，应由相关负责人授权后方可变更，授权记录应归档保存。授权时按照正确操作方法设置机房人员门禁权限，不允许跨权限执行授权操作。

第三条 紧急门禁按钮使用规定

特殊需保持门禁常开的情况，如需要使用紧急门禁按钮，需经相关负责人批准。

第三章 环境管理

第四条 严禁下列物品带入机房

（一）食品、饮料、药品、火柴、打火机、香烟等。

（一）食品、饮料、药品、火柴、打火机、香烟等。

（二）易燃物、爆炸物、腐蚀性物品以及磁铁等。

（三）照相机、收录机、公文包、电子器件等。

（四）未经防病毒检测的各类移动存储介质或设备。

第五条 环境整理

（一）机房内各类文档、备份介质、办公用品要及时清理、收纳，需要临时保管的物品需按要求摆放整齐。

（二）设备包装箱、维修材料、工具、部件等非机房运行必要的物品禁止在机房内存放，使用后必须立即清理出机房。

（三）对于机房内的环境卫生需定期进行除尘打扫，减少安全隐患。

第四章 巡检及定期保养管理

第六条 机房值班人员日常巡检与记录

机房值班人员每日定时对机房环境及机房设备进行巡检，并认真做好机房巡检记录。

第七条 机房环境与设备巡查及应急响应

每日机房巡查检查温湿度、供电、漏水、设备报警等内容。如果发现问题应立即查找原因，并通知相关管理人员。如果发现空调、加湿器、UPS、照明等设备故障应及时联系生产厂家或者经销商维修。

第八条 空调设备定期巡检与保养

（一）每月巡检过滤网、制冷剂的使用情况，即使更换或

维修。

（二）空调室外机定期清洗。一般夏季至少每2周一次，冬季每月1次，确保空调的制冷效率。

（三）每三个月对空调风机的皮带或电机进行检查。

（四）季节交替时对空调压缩机内的氟压力进行检查。

第九条 UPS及备用发电设备巡检与维护

（一）对备用发电设备要定期检查，定期进行使用测试，并记载测试记录。由第三方负责的发电机要定期检查、测试，并保存记录。

（二）对UPS要定期检查各种工作参数，如：电池电流、电池电压、直流电压等数据。每天至少检查一次并进行登记。

（三）根据机房的市电情况，每半年应做一次深度放电。（在做放电之前先对电池组进行抽检，目测外观是否变形、漏液等，用表测浮充电压是否正常。）

第五章 技术档案管理

第十条 技术档案管理是指对运行设备的随机资料、软件介质、软件文档、数据备份介质及与运行有关的各类技术规范、制度、计划、档案、日志等的管理。

（一）技术档案的整理与归档

各类技术档案由运行相关岗位人员按规定及时整理归档。

（二）技术档案的登记与分类保管

运行相关岗位人员应对技术档案登记入册，标明内容、日

期、密级、保存期限等信息，分类保管。

（三）技术档案的物理保管要求

技术档案保管须满足防盗、防潮、防火、防水、防鼠、防虫、防磁、防震等要求。重要技术档案应有冗余保护措施。

（四）备份介质的存放与管理

备份介质要存放在专用介质库内，系统软件、应用软件及业务数据备份介质还须异地（不同建筑物内）保存。

（五）技术档案的定期检查与维护

运行相关岗位人员应定期检查技术档案的完整性和有效性，对受损档案要及时整理和修复；对介质档案还应定期采取重绕、重写、复制等维护措施。

（六）技术档案借用的规范与审批

运行机构应严格限定技术档案的借用范围，借用时要履行登记手续，并要求及时完整归还，技术档案归还时应进行必要的完整性、有效性检验。重要技术档案的借用应经运行机构负责人批准。

（七）保密技术档案的管理与保护

涉及保密内容的技术档案，任何人不得以介绍、复印（拷贝）、发表文稿等方式外泄。

（八）过期技术档案的销毁程序

对过期和报废的技术档案的销毁，运行机构应履行审批手续，并采取严格的监销措施。

第六章 网络通信管理

第十一条 网络信息中心统一规划建设的网络系统，无网络信息中心授权，不得变更网络系统的结构、设备及重要参数。

第十二条 区域性网络系统方案的设计和改造应经过充分的技术论证，形成规范的文档。

第十三条 网络的IP地址、主机名等参数应按网络信息中心规定的标准进行统一编码和分配。

第十四条 任何人不得擅自增加、删除网络节点及修改网络参数，确需增加、删除或修改时，应严格履行审批手续。

第十五条 使用单位/部门须通过零信任及堡垒机进行远程运维，制定严格的远程登录审批制度，详细记录登录原因、登录人员等内容。

第十六条 网络信息中心应及时将网络拓扑结构图、网络通信设备的配置参数、网络地址等资料归档保管，并严格保密。

第十七条 网络信息中心应做好网络通信系统的日常运行维护工作。

第十八条 密切监视网络运行状况，及时排除网络出现的故障，做好网络运行及维护记录。

第十九条 定期分析网络运行状况，形成网络性能优化方案，实施须报相关领导审批。

第二十条 严格控制网络通信连接，采取诸如防火墙等项防范措施，对内部网与外部网进行网络隔离。

第二十一条 采取切实可行的措施对内部网络各节点的通信进行控制，防止各种非法访问。

第二十二条 网络的通信线路应有备份，并应对备份线路按月进行检测。

第七章 施工改造管理

第二十三条 吉林建筑大学中心机房的改造需经相关负责人批准后方可施工改造。

第二十四条 施工人员需办理临时出入证并填写《施工人员登记表》。

第二十五条 实施改造工程时需有机房管理人员跟踪实施。

第二十六条 施工使用电源、水时需经相关负责人认可后方可使用，不得在机房内私接电源和水源。

第二十七条 施工时需到指定施工地点进行切割、搅拌等作业，严禁在机房内进行上述操作。建筑材料在施工地点制成成品后方可进入机房组装实施。

第二十八条 每天施工结束后应将施工时产生的垃圾及时清理出机房。

第八章 人员出入管理

第二十九条 核心机房实行封闭式管理，备有《网络核心机房进出登记台账》，进出核心机房必须严格履行登记审批手续。

第三十条 未经主管领导批准，严禁非工作人员进入机房，严禁无关人员直接或间接操作机房设备。

意保持机房卫生。

第三十二条 严禁携带任何易燃、易爆、腐蚀性、强电辐射性、流体物质等对设备正常运行构成威胁的物品。

第三十三条 外单位或部门需进入核心机房参观或学习时，应经过主管领导批准登记后，由工作人员陪同，讲解注意事项、履行手续后方可进入。

第三十四条 未经网络信息中心书面批准，禁止将数据中心钥匙、密码、门禁卡等物品和信息外借或透露给其他人员。对于遗失钥匙、门禁卡、泄露信息的情况要及时上报，并积极主动采取措施保证机房安全。

第三十五条 工作人员离开工作区域前，应保证工作区域内保存的资料、设备、数据处于安全保护状态。

第三十六条 最后离开核心机房的工作人员应检查和关闭机房内无用的电源和照明开关，锁好模块机房门和核心机房防盗门。

第九章 用电管理

第三十七条 机房工作人员应具备用电常识，了解机房供电布局、开关位置设备供电来源等，机房工作时间注意用电安全和自身安全。

第三十八条 机房工作人员不得私自更改设备供电线路，对自己所管设备进行断电操作时不能影响其他设备供电，新增设备需要供电应由机房电力管理员统一调配。

第三十九条 机房禁止使用高温、炽热、产生火花的大功率

第三十九条 机房禁止使用高温、炽热、产生火花的大功率或危险设备，确需使用电焊、电钻等，须经中心领导同意，并在核心机房管理员监督下用电。

第四十条 工作时发现用电安全隐患如漏电、火花、设备异常发烧等现象应立即报告机房电力管理员，并协助进行处理。

第四十一条 机房停电需要启用内部发电系统时，设备管理人须在场及时检查自管设备是否正常供电。

第四十二条 机房电力管理员应定期对机房供电设备、线路、电源、开关等相关设备进行安全检查，及时排除用电安全隐患。

第十章 应急处置预案

第四十三条 火灾应急预案

（一）发现火情，现场工作人员立即切断总电源、疏散师生并迅速报告。

（二）确定火灾发生的位置，判断出火灾发生的原因。

（三）明确火灾周围环境，判断出是否有重大危险源分布及是否会带来次生灾难发生。

（四）明确救灾的基本方法，并采取相应措施，按照应急处置程序采用适当的消防器材进行扑救。

（五）依据可能发生的危险事故类别、危害程度级别，划定危险区，对事故现场周边区域进行隔离和疏导。

（六）视火情拨打“119”报警求救，并到明显位置引导消防车。

第四十四条 电源系统应急预案

定期检查网络机房电源设备的运行状况，当发生下列突发事件时，按照以下方案进行处置:

（一）当机房发生市电供电突然停电或是电源异常时，首先应和相关单位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。

（二）发生市电供电其他异常情况或要求紧急拉闸断电时，应及时与楼内物业公司联系。

第四十五条 空调及供水系统应急预案

（一）定期对空调的运行情况进行检查，如有报警信息，应及时查找故障原因，对不能自行排除的问题，应及时向领导汇报情况并与设备提供商进行沟通联系。如果发现有漏水现象应马上关闭空调进水阀，并对漏水进行处理，定期检查，保证正常运行。

（二）当中心机房空调因故障无法进行制冷，致使机房内环境温度超过40摄氏度时，应打开机房房门，并关闭服务器及网络设备，防止设备因温度过高烧毁。

（三）对于无法自行进行处置的空调系统异常情况，及时与设备商进行联系。

第四十六条 网络事故应急预案

当人为或病毒破坏的灾害发生时，具体按以下顺序进行：判断破坏的来源及性质，断开影响安全与稳定的信息网络设备，断开与破坏来源的物理网络连接，跟踪并锁定破坏来源的IP或其他网络用户信息，修复被破坏的信息，恢复系统。

第四十七条 服务器系统故障应急预案

（一）发生服务器系统故障后，应立即电话向相关领导汇报情况，及时组织启动备份服务器系统，由备份服务器接管相关业务应用，同时安排人员将故障服务器脱离网络，保存系统状态不变，保护原始数据。

（二）在确认安全的情况下，重新启动故障服务系统：若重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系厂家，请求技术支持，做好技术处理。

（三）处置结束后，技术人员应将处理过程记录下来，以方便日后对此问题的处理。

第四十八条 雷击事故应急预案

（一）遇雷暴天气或接上级部门雷暴气象预警，应关闭所有服务器，切断电源，暂停内部计算机网络工作。

（二）雷暴天气结束后，及时开通服务器，恢复内部计算机网络工作。

（三）因雷击造成的损失，应及时进行核实、报损，并将详细情况向部门领导汇报。

第四十九条 消防事故应急预案

（一）机房在有明火或浓烟的情况会触发机房消防报警的启动，前期会在机房出入口门口上方响起刺耳的报警声，听到警报声后应立刻撤离机房，在警报声响起的30秒后会触发消防七氟丙烷喷发，七氟丙烷喷发会造成机房内绝氧，所以听到警报声后应立即撤离机房并及时上报有关领导及维护单位。

（一）机房消防系统误报警处理方式，机房棚顶有温感及烟感探测器，当温感与烟感同时检测到报警后会触发消防控制箱的动作引起七氟丙烷喷发，如果在清扫机房或维修时造成大量粉尘及烟雾也能单独触发烟感报警，烟感报警也会引起门口声光报警器的刺耳报警声，这时需要人为手动把消防控制箱的自动状态改到手动状态并及时上报有关领导及维护单位。

（二）机房消防系统手动应急启动方式，在极特殊情况下不引起温感及烟感报警导致的火灾情况，需要人为手动开启控制箱使七氟丙烷喷发，操作流程在机房门口有手动应急按钮，在紧急状态下需要手动击碎防护玻璃按下启动按钮完成应急操作并及时上报有关领导及维护单位。

（三）机房消防启动后的预后工作，即时通知维护单位进行现场关闭消防控制箱，并做好通风排气的工作。如现场紧急需要进入机房在确定消防七氟丙烷喷发后火势已经扑灭，开打开机房门时应先四周通风并两人协作，一人推住门一人缓开门放气防止压力大造成开门伤人事件及七氟丙烷突涌造成短暂的公共区域绝氧。

第五十条 本办法由网络信息中心负责解释，自发布之日起试行。

吉林建筑大学网络信息中心

2023 年 10 月 26 日