云计算资源管理制度

第一章 总则

第一条 保障云计算资源数据中心的安全可靠运行，是每个管理者追求的目标。长期运行的设备客观上存在着运行风险，另外也可能由于人员的疏忽大意造成风险。为科学、有效地管理数据中心，促进网络系统安全的应用、高效运行，管理人员应认请潜在风险，并制定相应的规章制度，并严格要求执行。

第二章 机房管理

第二条 路由器、交换机和服务器以及通信设备是网络的关键设备，须放置计算机机房内，不得自行配置或更换，更不能挪作它用。

第三条 计算机房要保持清洁、卫生，并由专人 7*24 负责管理和维护（包括温度、湿度、电力系统、网络设备等），无关人员未经管理人员批准严禁进入机房。

第四条 严禁易燃易爆和强磁物品及其它与机房工作无关的物品进入机房。

第五条 建立机房登记制度，对本地局域网络、广域网的运行，建立档案。未发生故障或故障隐患时当班人员不可对中继、光纤、网线及各种设备进行任何调试，对所发生的故障、处理过程和结果等做好详细登记。

第六条 网管人员应做好网络安全工作，服务器的各种帐号严格保密。监控网络上的数据流，

从中检测出攻击的行为并给予响应和处理。

第七条 网管人员统一管理计算机及其相关设备，完整保存计算机及其相关设备的驱动程序、保修卡及重要随机文件。

第八条 计算机及其相关设备的报废需经过管理部门或专职人员鉴定，确认不符合使用要求后方可申请报废。

第九条 对数据实施严格的安全与保密管理，防止系统数据的非法生成、变更、泄露、丢失及破坏。当班人员应在数据库的系统认证、系统授权、系统完整性、补丁和修正程序方面实时修改。

第三章 计算机病毒防范制度

第十条 网络管理人员应有较强的病毒防范意识，定期进行病毒检测，发现病毒立即处理并通知管理部门或专职人员。

第十一条 采用国家许可的正版防病毒软件并及时更新软件版本。

第十二条 未经上级管理人员许可，当班人员不得在服务器上安装新软件，若确为需要安装，安装前应进行病毒例行检测。

第十三条 经远程通信传送的程序或数据，必须经过检测确认无病毒后方可使用。

第四章 数据保密及数据备份制度

第十四条 禁止泄露、外借和转移专业数据信息。

第十五条 制定业务数据的更改审批制度，未经批准不得随意更改业务数据。

第十六条 每周当班人员制作数据的备份并异地存放，确保系统一旦发生故障时能够快速恢复，备份数据不得更改。

第十七条 业务数据必须定期、完整、真实、准确地转储到不可更改的介质上，并要求集中和异地保存，保存期限至少 2 年。

第十八条 备份的数据必须指定专人负责保管，由管理人员按规定的方法同数据保管员进行数据的交接。交接后的备份数据应在指定的数据保管室或指定的场所保管。

第十九条 备份数据资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。

第五章 网络安全管理员的职责

第二十条 主要负责全校网络（包含局域网、广域网）的系统安全性。

第二十一条 负责日常操作系统、网管系统、漏洞检测及修补、病毒防治等工作。

第二十二条 应经常保持对最新技术的掌握，实时了解 INTERNET 的动向，做到预防为主。

第二十三条 良好周密的日志记录以及细致的分析经常是预测攻击，定位攻击，以及遭受攻击后追查攻击者的有力武器。察觉到网络处于被攻击状态后，网络安全管理员应确定其身份，并对其发出警告，提前制止可能的网络犯罪，若对方不听劝告，在保护系统安全的情况下可做善意阻击并向主管领导汇报。

第二十四条 在做好本职工作的同时，应协助机房管理人员进行机房管理，严格按照机房制度执行日常维护。

第二十五条 每月安全管理人员应向主管人员提交当月值班及事件记录，并对系统记录文件保存收档，以备查阅。具体文件及方法见附件。