

## 凯里学院信息中心校园网络安全职责（试行）

### 第一章 校园网络安全部门职责

1. 规划并监督实施校园网各个环节的物理安全保卫工作，包括防火、防盗、防水、防雷、防人为破坏等工作。
2. 审批校园网的建设与改动规划、灾难恢复和重建计划、校园网发生意外的应急计划和日常维护计划。制定校园网各部门和用户的具体安全规范和细则，制定安全培训计划，组织对用户进行安全教育和安全培训。
3. 定期检查国家有关互联网的法律法规和校园内网络管理条例的执行情况，特别是应经常检查面向公众提供上网服务的机房、实验室和电子阅览室等场所对上机者的登记与管理情况，以及宿舍区域私自建网络、非法向公众提供网络接入和信息服务、非法向公众提供上网代理服务。
4. 审阅校园网日常工作报告、违章报告和其它关系校园网安全的报告，及时发布和更新网络安全公告与安全建议。
5. 根据校园网的实际情况定期进行风险分析和安全审计，依法扫描校园网上的安全与保密问题，检查行政办公用户的操作是否符合安全操作规程，及时提出相应的对策并监督实施。
6. 对校园网上的信息及时进行审查，对发现的问题提出处理意见并监督实施。审查的主要内容为网站提供的软件和娱乐资源、发布的新闻和资料、提供 BBS、留言簿等服务等网站上的内容，特别是网站管理者对 BBS、留言簿的管理情况。
7. 保存关键系统的软件及配置信息备份，例如网络内所有交换机、路由器的运行软件、管理软件、文档和配置文件，网络内关键服务器的系统软件、应用软件、文档资料等，并且保证这些备份的安全性与有效性。
8. 保存关键系统的超级用户或管理员等特权用户口令，将这些口令及其备份存放在指定的保密地点。
9. 对校园网工作人员和办公用户进行政治及业务审查，应特别重视政治审查：
  - (1) 定期对校园网的所有工作人员从政治思想、业务能力、工作表现等方面进行考核，对不再适合于接触信息系统的人员适时调离；
  - (2) 对关键岗位的工作人员，例如校园网管理人员和值班人员，不仅要有严格的政审，还要考虑其现实表现，一旦发现其在日常生活和工作中有不良行为，校园网络安全部门应及时采取果断措施；
  - (3) 当校园网工作人员辞职或被调离、解职时，应履行严格的人事手续，向其申明以后的保密义务，收回一切资料和物品并立即更换相应的口令和钥匙，对校园网中与其有关的部分进行严格的安全检查。

### 第二章 网络核心设备和数据备份的管理

1. 服务器、路由器、交换机等是整个校园网服务的中枢，数据备份关系到整个校园网的灾难恢复和重建，应有严密的措施加以管理，应由专人专管，其口令只能由系统管理人员掌握。
2. 服务器、核心路由器与交换机有专门的机房，数据备份有专门的地点存放，机房和数据备份存放地点的钥匙由专人管理；数据备份的存放地点原则上不应与服务器机房在同一建筑物内；重要的数据应有多个备份并有多个存放地点。
3. 机房和数据备份存放地点应有良好的环境，应对电源、温度、湿度、振动、空气清洁度、电磁辐射、静电等提出严格要求，具体可参考国家有关主机房的建设标准。

4. 机房和数据备份存放地点应有良好的防盗、防火、防水、防雷等措施。
5. 严格限制进入机房和数据备份存放地点的人员，非工作人员进入，必须履行必要的手续并有人始终陪同。
6. 对进出服务器机房和数据备份存放地点的人员，必须有专人严格检查其带进带出物品，不得携带未经许可的物品进出服务器机房和数据备份存放地点。
7. 重要数据服务器应采用磁盘双工、磁盘镜像或其他容错措施。
8. 避免将服务器同时作为客户机使用，不得轻易在服务器上安装非服务用软件。
9. 机房内至少应有一个工作站，用于备份数据、安装软件和日常维护。
10. 服务器和网络核心路由交换设备的开关应按严格的操作规程进行，配备有良好的电源，由专人值班监视。
11. 服务器和网络核心路由交换设备的运行和日常维护等工作每天必须有记录，发现异常情况须立即报告并请有经验的维修人员处理。
12. 备份数据操作要及时进行，数据备份要定期检查其有效性。

### 第三章 校园网管理员职责

1. 校园网管理员负责具体实施对校园网的管理，包括校园网规划与实施、咨询与培训、系统维护等工作；在保证安全性的前提下，进行规划时要尽可能考虑用户的利益，为其访问校园网提供最大的方便。
2. 校园网管理员不应该有服务器机房、数据备份存放地点和其它敏感地点的钥匙。
3. 校园网管理员不应该随便使用特权用户，必须在技术上保证该用户只能在上班时间内、服务器机房里使用。
4. 校园网管理员创建用户帐号、配置系统参数、分配网络资源时，必须作好记录。
5. 校园网管理员必须对校园网的安全进行审计，采取各种可能的措施保证校园网的安全和信息的安全，及时备份(软拷贝或硬拷贝)校园网数据，制定并定期检验校园网的灾难恢复和重建计划。
6. 校园网管理员必须制定自己发生意外的应急计划，意外包括校园网管理员对校园网的恶意破坏、辞职、被撤职或因自身原因无法继续实施对校园网的管理。
7. 校园网管理员只能而且必须对许可范围内的信息进行规定数量的备份，不得制作许可范围外的任何信息的任何备份；备份只能存放在指定地点，未经校园网安全部门批准，不得以任何理由带到非指定地点保存或临时存放。
8. 校园网管理员负责校园网系统软件和应用软件的安装，上网软件必须经过严格的可靠性、安全性测试并经校园网安全部门审批，确保其不会对校园网带来任何形式的损害；上网软件应通过正常渠道引进，并采取措施尊重和保护其版权不受用户侵犯。
9. 校园网管理员负责校园网硬件的一般维修；未经校园网安全部门批准，校园网管理员不得私自变更网络拓扑、网络配置及网络参数。
10. 校园网管理员必须随时对校园网进行监视和检查，对违反条例的用户进行合适的处理；依法对通信或其他信息进行检查时，不得对任何人泄露被检查信息的任何内容，并尊重用户的隐私权和其他权利。
11. 校园网管理员应及时更新校园网资源信息并以适当的形式通知用户；对性能不好的软硬件应提出升级或修理意见，对校园网的改进提出报告。
12. 校园网管理员必须尽可能地按服务承诺为用户服务，包括提供咨询、组织培训、对用户现场指导以及帮助用户排除工作站软硬件故障，同时作好书面记

录。

13. 校园网管理员应将校园网的规划、灾难恢复和重建计划、校园网管理员发生意外的应急计划和日常维护等工作形成书面材料，报校园网络安全部门批准。

凯里学院信息网络中心

二〇一七年六月