普洱学院网络信息安全管理制度

为加强校园网网络系统的安全管理，防止因偶发性事件、网络病毒等造成系统故障，妨碍正常的工作秩序，特制定本管理办法。

一、网络系统的安全运行，是学校安全保障的一个重要内容，学校安排专人负责全院网络系统的安全运行工作。

二、网络系统的安全运行包括三个方面的内容：一是网络系统数据资源的安全保护，二是网络硬件设备及机房环境的安全运行，三是网络病毒的防治管理，四是上网信息安全及电子邮件。

（一）数据资源的安全保护。网络系统中存贮的各种数据信息，是供用电生产和管理所必须的重要数据，数据资源的破坏将严重影响生产与管理工作的正常运行。数据资源安全保护的主要手段是数据备份，规定如下：

1、重要部门的数据必须做到每日一备份。

2、网络系统的重要数据及时备份。

3、一般部门做到每周一备份。

4、系统软件和各种应用软件采用磁盘或光盘及时备份。

5、数据备份时必须登记以备检查，数据备份必须正确、可靠。

6、严格网络用户权限及入网用户名及口令管理。

（二）硬件设备及机房环境的安全运行

1、硬件设备的供电电源必须保证电压及频率质量，一般应同时配有不间断供电电源，避免因市电不稳定造成硬件设备损坏。

2、安装有保护接地线的，必须保证接地电阻符合技术要求（接地电阻≤2Ω，零地电压≤2V），避免因接地安装不良损坏设备。

3、设备的检修或维护、操作必须严格按要求办理，杜绝因人为因素破坏硬件设备。

4、各类网络机房必须有防盗及防火措施。

5、保证网络运行环境的清洁，避免因集灰影响设备正常运行。

（三）网络病毒的防治

1、各单位服务器必须安装防病毒软件，上网电脑保证每台电脑有防病毒软件。

2、定期对网络系统进行病毒检查及清理。

3、所有 U 盘须检查确认无病毒后，方能上机使用。

4、严格控制磁盘交换和外来 U 磁的使用，各单位各部门使用外来磁盘须经检验认可，私自使用造成病毒侵害要追究当事人责任。

（四）上网信息安全及电子邮件

1、各单位网络管理员必须定期对网上论坛及上网信息检查，发现有关泄漏企业机密及反动言论与不健康信息要及时删除，并记录，随时上报网络中心。

2、所有上网人员如收到反动邮件有责任及时上报学校保卫科，如不上报，一经发现，学校将视情节轻重，做相应处罚，情节严重者，学校可提请刑事处罚。

三、要严格执行国家相关法律法规，防止发生窃密、泄密事件。外来人员未经单位主管领导批准同意，任何人不得私自让外来人员使用我院的网络系统作任何用途。

四、各部门要加强对各网络安全的管理、检查、监督，一旦发现问题及时上报学院负责人。单位计算机安全负责人分析并指导有关部门作好善后处理，对造成事故的责任人要依据情节给予必要的经济及行政处理。

五、未经单位负责人批准,联结在学校网络上的所有用户,严禁再通过其它入口接入互联网或学院外单位网络。