西南林业大学普通本科招生信息管理办法（试行）

第一章　总　则

第一条　为了进一步加强和规范高等学校招生信息管理工作，确保招生信息的真实、安全、完整和准确，根据教育部办公厅、公安部制定的《高等学校招生信息管理规定（试行）》的有关规定，结合我校实际，制定本办法。

第二条　本办法适用于我校普通本科（含本科层次少数民族预科）招生信息管理工作。

第三条　招生信息管理工作实行招生办公室总体负责的工作体制。

第二章　信息与信息标准

第四条　普通本科及少数民族预科招生信息（以下简称“招生信息”）根据其保密性质可分为涉密信息和普通信息，涉密信息必需严格按照学校相关保密条例管理。普通信息及超过保密期的涉密信息必需按照学校“深化招生阳光工程”的要求及“招生信息公开条例”进行适当公开。

第五条　　招生信息主要包括招生宣传信息、投档信息、录取信息、学生信息、电子档案信息、工作信息等，形式主要分为电子信息和纸质信息两类。

招生宣传信息主要包括学校对外宣传所用到的招生章程、学校简介、本科来源招生计划、近年全国各地录取情况、本科招生专业介绍、答考生问、校园平面图等。

投档信息主要包括投档分数情况、投档考生预录状态、投档考生信息等。在正常录取期间，为确保尽量减少外界对招生录取工作的影响，投档信息在投档开始到各批次正式录取结束前属保密信息，录取过程中必须按保密信息进行管理。

录取信息主要包括录取结束后的录取新生名册、录取分数等。

学生信息主要包括各专业新生的姓名、身份证号码、生源地等。为防止社会欺诈现象的发生，学生信息在确定录取到新生报到期间属于涉密信息，在此期间须按保密信息进行管理。

电子档案信息主要包括从录取系统所下载的已经被我校录取的考生电子档案，包括考生照片图像信息、高中学业水平、综合素质评价信息、考生诚信信息、考生体检信息、考生成绩信息、考生志愿信息、以及享受政策加分的项目及分值信息等。电子档案信息涉及内容较多，应参照涉密信息进行管理，任何单位及个人不得私自拷贝和打印，新生报到后按学校相关管理办法对学生工作处进行档案移交。

工作信息主要包括招生工作过程中各类汇总、分析、统计信息及其它相关信息，此类信息招生办公室应及时向社会发布。

第六条　　招生信息标准按各省教育厅颁布的技术规范和信息标准执行，未制定部分由学校招生办公室根据实际情况请示校招生委员会研究确定。

第三章　　人员与设备

第七条　　招生信息管理人员应具备以下条件：

（一）严格执行国家的法律、法规及招生政策、规定，原则性强。

（二）工作认真、细致、踏实、责任心强。

（三）遵守国家招生人员的有关规定、廉洁自律。

（四）具有必需的计算机应用水平，并能在实践中不断提高。

（五）身体健康、吃苦耐劳。

第八条　　为适应招生改革和技术进步，结合学校招生规模不断扩大的实际，学校应重视招生信息管理队伍的建设，并适当配备专（兼）职信息管理人员，对从事招生信息管理的工作人员加强技术培训，促进其积极参加相关技术培训，加强学习，更新知识，不断提高招生业务和技术水平。

第九条　学校在招生录取期间要建立临时机房，包括组长机室、阅档室、打印室。

（一）机房建设：按照工作实际，建立适当的机房，必须为单独专用房间。

（二）电源配置：电源必须采用可靠的接地措施；配备专用在线式不断电源设备，能够为所保护的设备提供不小于三十分钟的断电保护；供电线路要符合要求，不得超负荷，电源闸刀处须有保险装置；要配备维修专用工具，以便及时进行维修及保养。

（三）安全设施：要保持机房清洁、卫生，注意防火、防水、防盗、防雷击；严禁在机房内私自配接电器；严禁在电线、电缆上悬挂、堆放物品；严禁在UPS电源上私拉乱接用电器；严禁在机房内存放或使用放易燃、易爆、腐蚀性、挥发性物品；严禁在机房内吸烟和随意放置茶水。

（四）出入管理：机房实行出入控制，工作人员进入机房要佩戴工作卡，外来检修人员、外来公务人员等进入机房必须有机房工作人员始终陪同，并做好详细的登记。

（五）网络要求：具备合理网络拓扑结构和稳定可靠网络连接线路的局域网应用环境；配备能够正常接入互联网的高速接入线路；安装上级部门指定的防病毒软件和防火墙软件，如有条件可购买安装硬件防火墙及入侵检测设备。

第十条　　学校招生办公室应建立与招生信息管理发展相适应的软、硬件环境。

（一）配置满足招生信息管理工作需要的硬件设备，包括计算机、不间断电源、打印机、条码扫描仪和网络设备；

（二）设备采购、保管、维护、更新应符合学校相关制度要求。设备选型、购置必须适应招生工作需要，做到全面规划、合理配置、择优选购、适时更新、不断改善和提高技术装备，使设备随时处于良好技术状态。

（三）配置常用的系统软件、数据库软件、工具软件、应用软件、定制软件、建立招生专用软件存档备份制度，保证工作正常使用。

第四章　　管理职责

第十一条　　招生工作的主管领导是招生信息管理工作的第一责任人，信息管理人员是直接责任人，主要职责是：

（一）执行教育部及省教育考试院有关招生信息管理工作的规定和工作要求。

（二）负责招生信息的采集、统计、分析、质量控制、修改、发布、分发。

第十二条　　对信息管理工作中成绩突出的单位与个人应予以表彰奖励。对违反信息管理规定并造成不良影响的单位和个人，对直接责任人须按有关规定严肃处理，触犯法律的，依法追究法律责任。

第十三条　　招生信息的采集由信息管理员完成，信息的采集过程必须遵循客观、严谨的原则。宣传信息从往年录取情况、校内各部门、本校高校高基报表采集；投档信息从录取期间的投档情况采集；录取信息、学生信息及电子档案从录取系统采集；工作信息主要在日常的管理工作中进行记载和整理。

第十四条　　招生信息一旦采集完成，严禁随意修改。如确有需要更改的地方，必须由信息管理员向招生办公室提出修改申请并附相关修改依据材料、信息更改负面影响预测材料。对确需修改的信息应做好修改记录。

第十五条　　招生信息应由招生办公室严格控制使用范围。向学校内部部门及个人提供电子数据时必须做好相关登记（包括数据范围、数据量、使用范围、接收人、提供人、提供日期等）、对外发布信息应做好检查审核及跟踪工作、不对外发布信息应做好保管工作。

宣传信息主要通过教育主管部门官方网媒体、学校网站、学校印制宣传材料的方式进行发布。

投档信息仅限在招生办公室内使用，招生期间不对外发布。

录取新生信息通过招生办公室对外提供有效身份验证查询；相关录取信息在完成招生录取工作后，由招生办公室统一整理后对外公布；招生办公室指定工作人员向中国邮政速递物流公司指定工作人员交寄通知书特快信件，严禁任何人对新生录取通知书特快详情单进行非法复制、摘抄、扫描等。

学生信息在新生名册产生后由招生办公室向学校内各部门提供。录取结束5个工作日内，向教务处信息中心提供学生个人信息电子数据（包括考生号、学号、姓名、专业、性别、民族、政治面貌、身份证号码、来源地区、地区名称）；在录取通知书寄出前5至3个工作日内，向财务处提供学生个人信息电子数据（包括学号、姓名、专业、身份证号码）；在开学前7至3个工作日内，向学校校园卡管理部、后勤管理处、图书馆、学生处、保卫处提供学生个人信息电子数据（学号、姓名、专业、性别、民族、政治面貌、身份证号码）。

电子档案信息由招生办公室负责保管，学生处可根据需要向招生办公室提出档案打印要求，一般应在新生入学阶段提出对当年录取新生进行材料打印，各年度新生电子档案打印工作当年12月31日前完成。

第十六条　　严格管理招生信息，维护招生信息的严肃性和权威性。

（一）需要阶段性保密的招生信息，必须加强管理，在正式公布之前，任何单位和个人不得擅自泄漏。

（二）对属于考生个人信息及有关录取过程中需保密的工作内容，任何单位及任何个人都不得擅自公开。涉及考生权益的信息查询，只向考生本人提供。

（三）信息的发布以方便考生，服务考生为目的，保护考生的合法权益。不得利用招生信息搞以盈利为目的的经营活动。

（四）招生办公室应按规定及时发布本校招生信息。

（五）招生办公室及时应对、处理、上报违反信息管理规定的相关事宜。

第五章　　信息安全

第十七条　　信息管理要坚持安全第一的原则，树立数据安全意识。招生办公室要安排专人负责网络和信息的安全保密工作，用制度管理信息，维护招生信息的严肃性和权威性，保证信息系统安全。

第十八条　　严禁任何人私自泄露未正式公布的招生信息。对于招生信息管理过程中使用过的准备废弃的数据载体（如使用的软盘、光盘、打印纸以及报废的计算机），在丢弃前要进行相应的技术处理，防止数据的泄密和丢弃。

第十九条　　加强对招生信息的安全管理。

（一）对涉及招生信息处理的计算机实行严格控制，未经学校招生办公室负责人授权，任何人不得操作、使用组长机室内任何计算机。非组长机室未经许可不得擅自上机操作及更改设备设置。

（二）认真落实用户识别、授权操作、上机登记及账号管理制度。网络账号采用分组管理。并详细登记，包括用户姓名、部门名称、账号名及口令、开通时间、网络资源分配情况等。用户账号下的数据属各个用户的私人数据，网络管理员具有管理及备份权限，其他人员均无权访问（账号当事人授权访问情况除外）。网络管理员必须严守职业道德和职业纪律，不得将任何用户的密码、账号等保密信息、个人隐私等资料泄露出去，防止非法入侵、改动及人为破坏和失泄情况的发生。如发现可疑情况应立即向有关负责人报告。

（三）考生数据库由数据管理员和系统管理员共同负责，数据管理员负责定时对数据进行备份。系统管理员密码和数据库管理员密码各自独立保管，数据服务器必须有两人共同管理，相互监督。

（四）按照“谁主管，谁负责；谁操作，谁负责”的信息管理责任制和责任追究制，严格程序、规范操作。招生信息管理工作实行逐级负责制，层层落实责任。对重要岗位、重要环节的信息管理人员签订安全保密责任书。因工作人员不负责任，玩忽职守造成数据有误、丢失，致使招生工作受到严重影响，或违反信息管理规定及招生工作纪律造成严重后果的，将视其情节轻重给予通报批评、调离信息管理工作岗位及

必要的行政处分，直至追究法律责任，同时追究主管领导及相关负责人责任。

第二十条　以病毒防范为重点，加强对招生各环节相关计算机软硬件的安全检查。

（一）为保证计算机病毒防治的有效性，要使用国家许可的正版防病毒软件，严禁使用未经安全检测的防病毒软件和盗版防病毒软件，并由专人负责我校防病毒软件的定时更新。

（二）各项招生工作开始前要对每台计算机进行计算机病毒查毒、杀毒处理，工作中使用的可移动存储介质须经杀毒处理后方可使用。

（三）安装各种软件时，应先对软件安装源进行杀毒处理，光盘软件在安装后要立即进行查、杀毒处理，确保计算机干净无毒。

（四）对接入网络的各类终端主机和服务器，在接入前必须进行强制性系统升级和病毒查、杀工作，确保不向服务器或对方主机传送带毒信息。

（五）已安装防病毒软件的计算机，需要及时升级病毒库，并对计算机进行定期杀毒处理。

第二十一条　加强网络安全防范，确保网络和服务器安全。

（一）牢固树立安全保密“慎之又慎”的思想，强化安全保密观念，增强忧患意识，克服松懈麻痹思想。严格落实安全保密制度，做到安全设备到位，管理措施到位，监督检查到位，确保万无一失。

（二）加强对服务器管理和重要数据的监控。考生数据库由数据管理员和系统管理员共同负责，数据管理员负责定时对数据进行备份。系统管理员密码和数据库管理员密码各自独立保管，数据服务器必须有两人以上共同管理，相互监督制约。在安装服务器（或修改服务器配置）时，系统管理员应向领导提出申请，并对新安装或修改的服务器硬件、软件情况进行登记，其内容包括：服务器名称及域名、处理器类型及数量、内存类型及容量、硬盘类型及容量、网卡类型及速率、操作系统类型及版本、服务器逻辑名及 IP 地址、支撑软件的配置、应用软件的配置、硬件及软件配置的变更情况等。

每周要检查各个服务器的日志文件，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，系统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。保留所有用户访问站点的日志文件，每两个月要对的日志文件进行异地备份， 备份日志不得更改，刻录光盘保留。

（三）系统安全未经领导批准，任何人不得改变网络拓扑结构、网络设备布置、服务器配置和网络参数。任何人不得擅自进入未经许可的网络系统，不得篡改系统信息和用户数据。

值班人员应及时监控网络运行状况，对不成功进入、不成功访问、越权存取尝试等进行记录、整理、分析，并提出针对性措施。任何人不得利用计算机技术侵犯用户合法权益；不得制作、复制和传播妨害单位稳定、淫秽色情等有害信息。

（四）网络安全关键岗位宜实行轮岗制，时间期限视情况而定；操作系统管理、数据库系统管理、网络程序设计、网络数据备份等与系统安全和数据安全相关的工作宜由多人承担；涉及网络安全的重要网络操作或实体检修工作应有两人（或多人）参与，并通过注册、记录、签字等方式予以证明。

（五）网络设备、网络线路要定期进行检查和测试，关键设备和线路要提供备份。对网络环境定期进行安全风险评估，并根据评估报告对网络上运行的所有客户端、软硬件及网络设备实施加固，堵塞安全漏洞，防患于未然。

（六）以防止黑客攻击为重点，建立网络安全实时监控系统和应急预案。通过设立防火墙、入侵检测、流量实时监控、安全堡垒等技术措施，构建网络安全立体防范体系。

第六章　　附　　则

第二十二条　　本办法自发布之日起施行。

第二十三条　　本办法由教务处负责解释。