附件：

信息安全管理实施细则

本办法适用对象包括四川农业大学校园网主页及各校内二级网站、电子公告、留言版、聊天室、网络文件传输、网络多媒体播放等各种信息传递与交流形式中的信息系统，接入校园网的所有网络用户，包括各中层单位计算机房、公共计算机房、电子阅览室等公共场所。

一、信息安全管理要求

（一）信息内容安全管理

1.学校任何单位和个人不得在各校园信息系统上发布涉密信息和《互联网信息服务管理办法》所禁止的有害信息，各中层单位须按照学校信息系统建设与管理的总体原则，加强对本单位所建系统信息发布和信息安全的管理，并及时更新系统内容。

2.本办法所称有害信息，是指通过网络传播的包含下列内容的信息：

（1）反对宪法所确定的基本原则的；

（2）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（3）损害国家荣誉和利益的；：

（4）煽动民族仇恨、民族歧视，破坏民族团结的；

（5）破坏国家宗教政策，宣扬邪教和封建迷信的；

（6）散布谣言，扰乱社会或学校教学科研秩序，破坏社会或学校稳定的；

（7）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（8）侮辱或者诽谤他人，侵害他人合法权益的；

（9）含有法律、行政法规及校规校纪所禁止的其他内容的。

3.网络安全办公室定期对校园网进行巡查。发现有害或不规范信息后，应及时采取校园网隔离、关闭服务器等必要技术手段防止其扩散，并通知相应网站管理人员予以处理。信息安全办公室可根据需要监督其删除。

4.各中层单位主要领导应高度重视本单位网页管理，为相关工作提供方便；分管领导应切实担负内容审核的责任，以确保内容的正确；信息系统管理人员应当做到：

（1）对自行上载的信息进行审查，确保其中不包含有害信息，不提供有害网页的链接；

（2）保存必要的用户使用情况日志；

（3）经常对用户上载的内容进行检查，发现有害信息及时删除并报告分管领导，有害信息备份文件应上交，不得私自留存；

（4）根据信息安全办公室的要求，提供有关技术记录，协助对有害信息的追查；

（5）采取其他必要措施，防止有害信息的传播和扩散。

5.信息系统管理人员没有按照规定保存必要的用户日志，经警告仍不改正，或者怠于履行检查义务，致使有害信息反复出现的，信息安全办公室将责令该中层单位限期整改；情节严重的，对该信息系统予以关闭。对于信息安全第一负责人和直接责任人员，学校将进行批评教育；情节严重的，给予相应处分。

（二）信息技术安全管理

1.各类信息系统运行期间须依据学校安排做好信息系统安全等级保护工作，包括安全等级变更备案与安全测评，不符合要求的须在指定期间内完成整改，使之持续具备与其安全等级相适应的信息安全防范能力。

2.信息系统日常运行维护须从物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复等方面加强安全管理，具体要求如下：

（1）物理安全

a、信息系统主要运行设施应集中存放于指定的信息机房，运维单位加强机房管理，保障信息系统运行环境物理安全。

b、编制并保存与信息系统相关的设施清单，根据设施特点制定相应的日常巡查管理办法，通过巡查及时发现相关设施安全隐患并及时排除，保障信息系统相关设施安全运行。

c、对信息系统相关存储介质进行控制和保护，对介质存放环境、使用、维护和销毁等制定具体安全管理要求，并对介质的归档和查询等进行登记记录。

（2）网络安全

a、保障系统运行的网络结构安全合理。保证关键网络设备的业务处理能力满足系统运行需要，保证接入网络和核心网络的带宽满足系统运行需要。

b、确保系统具有合理的访问控制措施。在网络边界部署访问控制设备，启用访问控制功能。通过访问控制列表对系统资源实现允许或拒绝用户访问。

c、保证系统所用网络设备得到有效防护。对登录网络设备的用户进行身份鉴别,登录密码符合安全要求的长度和复杂程度。当需要对网络设备进行远程管理时,应采取必要措施防止信息在网络传输过程中被截取。

（3）主机安全

a、应对登录主机操作系统和数据库系统的用户进行身份标识和鉴别。

b、主机访问控制。应启用访问控制功能，依据安全策略控制用户对资源的访问。应限制默认帐户的访问权限，重命名系统默认帐户，修改默认口令。应及时删除多余的、过期的帐户，避免共享帐户的存在。

c、入侵和计算机病毒防范。操作系统应遵循最小安装的原则，按需安装组件和应用程序，并保持系统补丁及时得到更新。主机应安装防计算机病毒软件,并及时更新软件版本和病毒特征库。

d、根据安全要求设置登录终端的操作超时锁定策略，限制单个用户对系统资源的最大或最小使用限度。

（4）应用安全

a、系统身份鉴别机制。信息系统应提供专用的登录控制模块对登录用户进行身份标识和鉴别；提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；启用身份鉴别和登录失败处理功能，并根据安全策略配置相关参数。

b、访问控制机制。信息系统应提供访问控制功能,控制用户组、用户对系统功能和用户数据的访问；应由授权主体配置访问

控制策略，并严格限制默认用户的访问权限。

c、软件容错机制。信息系统应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式符合系统设定要求。在系统发生故障时，应确保部份基本功能可用。

（5）数据安全及备份恢复

a、采用密码技术确保信息系统重要数据在传输过程中的完整性、在系统中的可用性以及符合特定要求的保密性。

b、应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据传输方法。

c、信息系统应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

d、应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。

e、根据信息系统的备份技术要求，制定相应的应急预案与灾难恢复计划，并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新。

（6）安全管理措施

a、信息系统运行期间应配备相应的安全运行维护人员并加强其人员管理。

b、信息系统投入运行、网络系统接入和重要资源的访问等关键活动应进行审批、记录。

c、应对网络设备、主机系统和信息系统进行定期安全漏洞检测评估，及时修补漏洞，整改加固安全防护措施。

d、应定期对信息系统运行日志和审计数据进行分析，及时发现异常情况并调整纠正。

e、信息系统应使用符合国家密码管理规定的密码技术和产品。

f、信息系统作重大变更，应制定相应变更方案，报信息安全办公室审批后方可实施变更，并在实施后向相关业务人员通告。

g、信息系统运行期间如发生信息安全事件，应按信息安全事件处理流程进行报告处置。

3.各单位信息系统（网站）使用四川农业大学二级域名的，严禁私自将域名指向校园网之外的服务器，有极特殊需要的，须由单位信息系统安全负责人提交安全承诺书，报学校信息安全办公室批准后方可实施。

4.建立第三方漏洞扫描平台通报制度，通过学校采购的网站漏洞扫描平台定期对全校所有网站进行安全漏洞扫描，并将扫描结果通报各单位。信息与教育技术中心根据扫描结果，对存在安全问题的网站报信息安全办公室，由信息安全办公室下发公文对有轻度或中度安全问题的网站责令限期整改，对超过整改期限或有严重安全问题的网站予以隔离或关闭。

5.任何现有信息系统或子系统、信息系统设备停止使用时，为避免信息系统处于在线无管理状态，导致重要数据遭受窃取、泄露，或被黑客利用做违法事情等，各使用单位或管理者应及时提出终止运行申请。提出申请时，说明终止原因及信息系统数据

拟处理结果，按照信息系统等级保护要求已定为三级及以上的信息系统的终止，由学校信息化领导小组负责审批，二级信息系统终止由信息安全办公室审批，其它系统由使用部门自行审批。审批结果报信息与教育技术中心作备案及后续终止操作。

（三）校园网络实名认证管理要求

根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息网络国际联网安全保护管理制度》、《互联网安全保护技术措施规定》、《互联网信息服务管理规定》等规定，为维护国家安全、社会秩序和公共利益，合理分配网络资源、提高网络使用效率，保障校园网络信息安全，对所有接入校园网利用网络资源的人员和用户进行注册备案、实名制管理。

1.实名上网认证管理是指通过对校园网用户上网身份的唯一鉴别和日志记录，规范用户上网行为的网络管理方法。

2.本办法适用于所有接入校园网用户。

3.按照“谁使用，谁管理，谁负责”的原则，对校园网实名认证账号进行规范管理。

4.信息与教育技术中心负责对校园网用户上网账号进行统一管理，包括：上网账号的登记、审批、分配、备案、注销、密码更改，对账号使用者上网情况的监管和检查，制定并组织实施账号管理的有关制度及技术规范。

5.教职工因故调离、辞职、退休离校的，需及时到信息与教育技术中心销户。正常调离或者退休的，人事处每年不定期及时通知信息与教育技术中心，以核销其账户。学生网络用户在毕业1年后作销户处理。

6. 使用上网账号的用户，对自己的账号享有专用权。未经信息与教育技术中心批准，用户不得擅自转借、转让账号。

7. 用户使用账号上网时，应自觉遵守国家颁布的有关法律和规定，必须对因使用账号上网产生的一切行为负责，并承担由此产生的不良后果的法律责任。

8. 用户应自觉接受并积极配合国家有关部门及学校依法依规进行的有关计算机网络安全检查。用户发现利用校园网从事违纪违规行为的，有义务及时向学校或信息安全办公室报告。

9. 用户账号发生下述异常情况时，信息安全办公室有权对其账号实施强制封闭：利用账号访问网络发生异常国际流量的；账号被盗用的。

10. 用户账号的下述情况为违规行为：私自转借、转让上网账号；盗用他人账号上网；未经信息安全办公室批准，利用校园网内各级接入设备进行各类网络技术实验；从事与国家法律法规和学校有关规定相抵触的上网活动；阻挠学校有关部门就可疑事件或网络运行状况进行调查、检查。

11. 各学院计算机房、公共计算机房、电子阅览室等公共场所的计算机上网，须签订公共机房信息安全管理承诺书，做好本地实名登记记录，并按照规定保存日志备份；保存时间不少于 60 日上网日志记录，便于后期落地查人。对此规定未落实或落实不到位，具体管理人员和单位负责人自行承担相应后果。

二、信息安全事件报告与处置

（一）信息安全事件定义及分类

1. 信息安全事件是指由于自然或者人为以及软硬件本身缺

陷或故障的原因，对信息系统造成危害或对社会造成负面影响的事件。

2.信息安全事件分为信息内容安全事件和信息技术安全事件两类。信息内容安全事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件。除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件为信息技术安全事件。

（二）信息安全事件分级

1.根据信息安全事件所危害信息系统的重要程度、损失程度、社会影响程度及紧急程度的不同，对信息安全事件进行分级管理。

2.按信息系统的重要程度划分：安全等级保护定级为三级的信息系统为特别重要信息系统，定级为二级的信息系统为重要信息系统，其它为一般信息系统。

3.按信息系统的损失程度划分：造成信息系统大面积瘫痪业务全面中断、系统关键数据遭到严重破坏、恢复系统运行和消除负面影响的代价很大的为特别重大系统损失；造成系统长时间中断或局部瘫痪、业务处理能力受到极大影响、系统关键数据遭到破坏、恢复系统运行和消除负面影响的代价较大的为重大系统损失；造成系统暂时中断，业务处理能力受到影响、系统重要数据遭到破坏，恢复系统运行和消除负面影响的代价不大的为一般系统损失。

4.按信息系统的社会影响程度划分：极大威胁国家安全、引起社会动荡、对经济建设有极其恶劣的负面影响、或者严重损害公众利益的为特别重大社会影响；威胁到国家安全、引起社会恐

慌或对经济建设有重大负面影响、或损害到公众利益的为重大社会影响；可能影响到国家安全、社会秩序、经济建设或公众利益，或对学校及师生利益造成损害或影响学校工作秩序的为一般社会影响。

5. 按信息安全事件的紧急程度分为紧急事件和普通事件。

（1）紧急事件：

a. 可由校外访问的页面发生篡改或被替换成非法信息的事件，尤其是发生在校（院）主页、新闻网、招生就业信息网等访问量高的系统或网站的事件；

b. 影响学校系统正常运转的攻击事件，如对财务系统、公文系统、数据中心虚拟云平台的攻击；

c. 可能造成用户隐私信息窃取、丢失、损坏的漏洞；

d. 其它可能对社会公共安全或学校造成危害或不良影响的事件或漏洞。

e. 漏扫平台威胁值高于 80 的页面漏洞事件。

（2）普通事件：

a. 可校外访问的页面漏洞事件，且漏扫平台结果威胁值高于 60、低于 80 的漏洞事件；

b. 仅校内访问的页面发生无害篡改、系统或网站隐藏漏洞等事件；

c. 影响部门系统正常运转的攻击事件，或可能造成紧急安全事件的漏洞；

d. 其他不构成公共危害或社会不良影响的安全事件或漏洞。

（三）信息安全事件报告与处置

1.实行信息系统安全领导负责制，各单位党政一把手作为本单位各信息系统安全的责任主体，向学校信息化领导小组负责，各信息系统负责人作为本系统安全责任人向单位负责人负责。相关负责人的变动应及时报信息安全办公室备案。

2.学校任何单位和个人发现校园信息系统出现涉密信息、有害信息，应及时报告信息安全办公室备案处理，并根据实际情况及时取证。信息安全办公室人员接到举报或发现潜在信息安全问题时，对初判为紧急安全事件的信息系统（网站），经网络信息安全主管审批，按照管理办法规定流程立即进行隔离或关闭，并抄送责任单位或个人相关检测报告、一对一风险提示和整改通知。初判为普通事件的，经网络信息安全主管审批，由网络信息安全专员定期抄送责任单位或个人相关检测报告、一对一风险提示和整改通知。

3.信息系统关停与启用

（1）校园信息系统因过期、改版等原因停止更新与服务的，主管、主办单位应主动向信息安全办公室申请关停并履行相关手续。

（2）存在严重安全漏洞等隐患的信息系统，主管、主办单位应在收到信息安全办公室相关检测报告、一对一风险提示和整改通知后，在指定期限内落实整改措施，及时反馈进展情况。如未能按时完成或无法完成整改，为保障校园网整体安全，在通知发出 10 天后信息安全办公室实施强制隔离或关停管制。对部分重要信息系统（如财务系统、教务系统、招生就业系统等），可采用保留校内网络只断外网或全部断网等多级处理方式进行风

险调控，降低系统性风险。

（3）在信息安全整改期间，如因特殊业务需要临时启用、带病运行，须提交特情处置申请，相应申请应由申请人提交学校主要领导签字同意后转信息安全办公室，方可开通。信息系统主办方应签署信息安全责任承诺书，指定临时启用的起止时间，自行做好防护措施。按时完成整改的系统，经安全检测验证核实后，可重新启用。

（4）对于玩忽职守或有意危害造成校园信息安全事件的，学校将根据损失情况和不良影响的程度，由学校监察处等部门对信息系统主管（办）单位负责人和当事者进行追责，涉嫌违法犯罪的移送司法机关处理。

4、信息安全事件处理流程