河南大学

校园计算机网络信息安全管理制度

河南大学信息化管理办公室

2016 年 5 月

目录

1、信息安全工作总体方针和原则 3
2、办公环境管理制度 6
3、网络安全管理工作人员岗位职责 7
4、外部人员安全管理制度 8
5、授权和审批 10
6、各部门信息主管、信息员管理制度 11
7、河南大学校园网用户守则 13
8、安全教育和培训制度 14
9、河南大学电子邮件管理制度 15
10、河南大学各级政务网站建设与管理基本规范（试行） 17
11、河南大学校园网信息发布审核登记制度 21
12、河南大学信息化管理办公室机房安全保护制度 23
13、河南大学校园网络楼宇网络设备间管理规定 25
14、信息化管理办公室资源管理暂行规定 26
15、IT 设备管理规定 27
16、介质安全管理制度 29
17、河南大学校园网安全保护管理办法 30
18、河南大学网络系统安全管理制度 33
19、河南大学校园计算机网络信息安全管理办法 36
20、信息系统建设与运维管理制度 37
21、河南大学网络信息监视、保存、清除和备份制度 39
22、河南大学数据保密及数据备份制度 40
23、河南大学校园网安全保密管理制度 41
24、河南大学校园网 VPN 使用管理办法 43
25、河南大学信息化管理办公室计算机病毒防范制度 44
26、河南大学网络安全审查暨漏洞检测制度 45
27、河南大学校园网应急保障制度暨计算机事件报告制度 47
28、河南大学网络与信息安全责任书（一） 48

29、河南大学网络与信息安全责任书（二） 50

1、信息安全工作总体方针和原则

1.1 总则

为加强和规范河南大学网络信息的安全管理，提高整体的安全防护水平，实现信息安全的可控、能控、在控，依据国家有关法律、法规，制定本文档。

本文档的目的是为安全管理提供一个总体的策略性架构，该文件将指导信息系统的安全管理体系的建立。安全管理体系的建立是为平台的安全管理工作提供指导和支持，以实现统一的安全策略管理，提高整体的网络与信息安全水平，确保安全控制措施落实到位，保障网络通信畅通和业务系统的正常运营。

本文档适用于各部门信息系统资产和信息技术人员的安全管理和指导，适用于指导平台安全策略的制定、安全方案的规划和安全建设的实施，适用于安全管理体系中安全管理措施的选择。

1.2 信息安全管理制度制定方针、目标和原则

信息系统安全坚持“安全第一、预防为主，管理和技术并重，综合防范”的总体方针，实现信息系统安全可控、能控、在控。依照“分区、分级、分域”总体安全防护策略，并执行信息系统安全等级保护制度。

信息系统安全总体目标是确保信息系统持续、稳定、可靠运行和确保信息内容的机密性、完整性、可用性，防止因信息系统本身故障导致信息系统不能正常使用和系统崩溃，抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏，防止信息内容及数据丢失和失密，防止有害信息在网上传播，防止对外服务中断和由此造成的系统运行事故。

1.3 信息安全工作的总体原则

(1) 基于安全需求原则

组织机构应根据其信息系统担负的使命，积累的信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上恰当地平衡安全投入与效果；

(2) 主要领导负责原则

主要领导应确立其组织统一的信息安全保障的宗旨和政策，负责提高人员的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理

工作与各部门工作的关系，并确保其落实、有效；

(3) 全员参与原则

信息系统所有相关人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全；

(4) 系统方法原则

按照系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标的有效性和效率；

(5) 持续改进原则

安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性；

(6) 依法管理原则

信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响；

(7) 分权和授权原则

对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，减少未授权的修改或滥用系统资源的机会。任何实体（如管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限；

(8) 选用成熟技术原则

成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先局部试点然后逐步推广，以减少或避免可能出现的失误；

(9) 管理与技术并重原则

坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标；

(10) 自我保护和国家监管结合原则

对信息系统安全实行自我保护和国家保护相结合。组织机构要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全。

在规划和建设信息系统时，信息系统安全防护措施应按照“三同步”原则，与信息系统建设同步规划、同步建设、同步投入运行。

2、办公环境管理制度

第一节　总 则

第一条 为了加强办公环境的安全管理，保护办公区人员和信息资产安全，规范办公区人员的活动，特制定本规定。

第二条 本规定适用于内部员工和进入办公区域的外部人员。

第二节　职 责

第三条 管理部门职责：

各部门主管领导负责管理本部门区域内的安全控制。

第四条 员工职责：

做好安全防范措施，认真执行本规定中的各项要求。

第三节　管理要求

第五条 加强对办公环境的安全管理，提高员工日常工作中的安全意识，严格控制办公环境的访问。

第六条 办公环境内的所有设备必须明确使用者，计算机设备的访问必须得到其使用者或管理者的授权。

第七条 工作人员离开座位时计算机要锁屏，桌面上不能有内部敏感信息文档。工作人员下班后应将重要文件、贵重物品和仪器放在抽屉或柜子内并加锁。

第八条 各部门内的复印机、传真机、打印机使用后产生的内部废弃文件不得堆积，应及时取走并销毁，不可留做二次用纸。

第九条 未经授权任何人不允许调换信息处理设备；不允许擅自将内部信息设备、移动硬盘、实体信息和软件等带离办公区。

第十条 未经批准，限制外部人员使用内部信息处理设备，如果使用信息处理设备，必须对其访问行为进行监控。

第十一条　维护人员进入办公区域进行设备维修时，应事先和相关部门取得联系，在维修的过程中应有专人进行监督。

3、网络安全管理工作人员岗位职责

第一条　负责校园网（包含局域网、广域网）系统的安全。

第二条　负责日常操作系统、网管系统、邮件系统的安全补丁、漏洞检测修补、病毒防治等工作。

第三条　网络安全管理员应经常保持对最新技术的掌握，及时了解 INTERNET 的动向，做到提前预防。

第四条　做好良好周密的网络日志以及细致的分析。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。

第五条　在做好本职工作的同时，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。

第六条　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归档，以备查阅。

4、外部人员安全管理制度

第一章　总 则

第一条 为加强对外部人员的信息安全管理，防范外部人员带来的信息安全风险，规范外部人员在信息系统中的各项与信息系统相关的活动所要遵守的行为准则，特制定本规定。

第二条 本规定适用于外部人员安全管理工作。

第二章　定 义

第三条 本规定中外部人员包括软件开发商、产品供应商、系统集成商、设备维护商、服务提供商、业务合作伙伴、临时雇工、实习生等外来人员，外部人员分为临时外部人员和非临时外部人员。

(1) 临时外部人员指因业务洽谈、技术交流、提供短期和不频繁的技术支持服务而临时来访的外部人员；

(2) 非临时外部人员指因从事合作开发、参与项目工程、提供技术支持或顾问服务，必须在相关单位办公的外部人员。

第四条 接待人是指受访部门派出的、负责接待外部人员的接口人。

第三章　外部人员风险识别

第五条 各部门在与外部人员进行接触过程中，应防范外部人员对于可能带来的各类信息安全风险，这些风险包括但不限于如下内容：

(1) 外部人员的物理访问带来的设备、资料盗窃；

(2) 外部人员的误操作导致各种软硬件故障；

(3) 外部人员对资料、信息管理不当导致敏感信息泄露；

(4) 外部人员对计算机系统的滥用和越权访问；

(5) 外部人员给计算机系统、软件留下后门；

(6) 外部人员对计算机系统的恶意攻击。

第四章　外部人员管理要求

第六条 临时外部人员进入时，接待人必须全程陪同，告知有关安全管理规定，未经允许不得使用的计算机和电子网络设备。

第七条 非临时外部人员必须签署安全保密协议后才能进场工作。

第八条 业务洽谈和技术交流应当在会议室进行，招标、谈判等正式洽谈和重大

项目的会谈应当在专门的会议室进行。

第九条 外部人员进入机房等重要区域时，应遵从《机房环境安全管理规定》等规定。

第十条 未经相关领导许可，外部人员不得在办公区域、设备间、机房等关键区域摄影、拍照。

第十一条 在未经相关部门主管领导的审核审批情况下，禁止外部人员了解和查阅敏感、重要信息、文档等。

第十二条 外部人员如因业务需要查阅敏感资料或访问网络和信息系统资源，必须经过安全管理员批准并详细登记。

第十三条 未经允许，禁止外部人员远程访问网络。如确因工作需要（例如维护、故障处理）需要远程访问，必须经安全管理员批准并详细登记。

第十四条 外部人员在机房内的所有操作，都必需说明该操作可能引起的安全风险，并由接待人认可后才能操作。接待人必须对外部人员的操作进行全程监控，记录外部人员的操作内容并存档备案。

第十五条 外部人员对机房附属设备（如空调、UPS 等）的维护和保养，事先要由接待人员上报相关部门主管领导批准后选择合适的时间进行，确保操作不影响系统的正常运行。

第十六条 未经批准，禁止外部人员携带移动存储介质进入机房。

第十七条 外部人员如因工作需要使用移动存储介质，必须在接待人的监控下使用，由此而产生的安全风险由接待人承担。

5、授权和审批

第一条 各部门需要明确各自的岗位和职责，部门内实行逐级审批制度。

第二条 审批流程要按照如下几个流程进行：提出申请、相关负责人审批、审批通过、登记记录、备案归档。

第三条 针对系统的变更或重要操作，需要向信息提出申请，要明确变更内容或操作过程，以及分析可能的影响，待审批通过后，方可进行变更或操作。

第四条 出入机房等，需要填写机房出入登记表，并经允许后方可出入，具体参考《河南大学信息化管理办公室机房安全保护制度》。

第五条 机房新增设备或系统，要在信息报备并经许可后方可实施。

第六条 应对审批过程进行记录并保存审批的文档。

6、各部门信息主管、信息员管理制度

第一节 总则

第一条 根据我校信息化建设工作实际，建设一支过硬的部门信息主管、信息员队伍并进行规范管理，是信息化建设发挥最大功用的必要条件。各应设立信息主管和信息员，并在信息化管理办公室备案。

第二节 信息主管管理制度

第二条 学校各职能部门、二级单位应明确具体负责信息化工作的分管领导与信息员，信息化工作应列入年度工作计划。分管领导具体负责业务系统的规划、升级，本部门业务系统建设、推广和信息安全工作，监督学校信息化建设相关规章制度在本部门的执行；部门信息员负责部门相关业务系统数据和网站信息的及时更新和维护，保证信息的准确性、实时性、完整性和安全性。各职能部门、二级单位应切实做好与本部门本单位业务相关的各项信息化建设工作，完成本部门本单位的信息化建设任务。

第三条 信息主管应由各单位党政领导班子成员担任，是各单位信息化建设和管理的第一责任人，对分管工作范围内的信息系统安全管理工作负领导责任。

第四条 各职能部门、二级单位信息员应参加相关部门组织的应用系统培训活动，熟练掌握各应用系统的操作方法，及时做好部门内人员的培训工作，做好应用系统的推广使用。

第三节 信息员管理制度

第五条 熟悉相关信息业务，遵守组织纪律，服务意识强；有较强的综合分析能力和熟练的电脑及网络应用能力。

第六条 负责本单位信息化业务，遇到信息化业务相关问题时，要及时处理；自己不能处理的应及时联系相关单位处理。

第七条 未经信息主管同意，不得擅自更改业务系统帐户、密码等，以免造成无法登录管理系统的现象发生。业务系统的账户及密码信息应在信息主管领导备份，变更时保证同步更新。

第八条 信息员要及时更新本单位网站栏目的内容，确保栏目内容充实、新颖。所发布的信息要经信息主管审核后发布。

第九条 对单位内部的系统故障进行分析及处理。

第十条 信息员因工作变动或其他原因不能继续担任该项工作的，信息主管应及时向信息化管理办公室反馈并补充推荐合适人选。

第十一条 本管理制度自发布之日起试行，并由信息化管理办公室负责解释。

7、河南大学校园网用户守则

第一条　用户必须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国教育和科研计算机网络管理办法》和国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。

第二条　用户不得利用计算机网络从事危害国家机密、破坏社会安定的违法犯罪活动，不得查阅、发送各种有害信息。

第三条　用户都有义务配合国家安全部门依法对网络使用情况等进行监督检查，采取必要措施。

第四条　任何用户未经许可不得在网上进行商业和其他任何盈利性活动。

第五条　用户不得进行任何干扰其他网络用户，破坏网络设施的活动。这些活动包括(但并不仅限于)商业公告、散布计算机病毒、进入未经授权的计算机系统、盗用 IP 地址入网等等。

第六条　用户必须遵守交费规定，按时交纳费用。

第七条　用户必须服从和配合信息化管理办公室的网络管理工作，并有义务向网络管理员报告任何违反用户守则的行为，并对自己在网络使用中的行为负责。

第八条　对于违反计算机网络政策的用户，网络管理员有权停止对其的服务，必要时将诉诸法律。

8、安全教育和培训制度

第一条　组织网络管理和网站管理人员认真学习《计算机信息网络国际互联网安全保护管理办法》、《网络安全管理制度》及《信息发布审核、登记制度》，提高工作人员的维护网络安全的警惕性和自觉性。

第二条　在师生中进行安全教育和培训，使他们自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，杜绝发布违犯《计算机信息网络国际互联网安全保护管理办法》的信息内容。

第三条　不定期地邀请网络相关人员进行信息安全方面的培训，加强对有害信息，特别是影射性有害信息的识别能力，提高防范能力。

第四条　每学期对学生网络管理员和各单位网络信息管理员进行安全培训，讲解最新的安全知识。

第五条　在信息化管理办公室网站上，不定期发布安全相关的内容供大家学习参考。

9、河南大学电子邮件管理制度

第一条　为加强校园网电子邮件系统的管理，使电子邮件系统更好地为师生服务，根据国家和学校相关规定，特制定本办法。

第二条　信息化管理办公室负责电子邮件系统的管理、维护工作，确保电子邮件系统的正常运行。邮件服务器因维护须暂停服务时，信息化管理办公室应提前以网站公告等方式通知用户。

第三条　电子邮件账号的申请、开通、注销

1．本校已申请上网账号的教职工及学生都有权使用学校电子邮件信箱，可在学校主页相关栏目在线注册邮箱账号，并获得相应密码，用户可自行更改密码。

2．教职员工离职后，信息化管理办公室将在12个月后注销该用户的电子邮箱。离职人员如需保留电子邮箱，须提出书面申请，说明原因并注明保留期限。学生邮箱帐号在其毕业后保留12个月，期满由系统统一注销。

第四条　邮箱账户仅限本人使用，禁止将本人账户转借他人或借用他人账户。用户账号和密码由用户负责保管，用户应当对以其用户账号进行的所以活动和事件负法律责任，并承担由自身行为导致的一切任何直接、间接、偶然、特殊及后续的后果及损失。

第五条　遵守国家相关的法律和法规，遵守所有与电子邮件服务有关的网络协议、规定和程序。如因用户违反有关法律、法规或本协议项下的任何条款而给学校网络或任何其他第三人造成的损失，用户应承担由此造成的损害赔偿责任。

第六条 如发现任何非法使用用户账号或账号出现安全漏洞的情况，用户有义务立即通告学校信息化管理办公室。

第七条 如发生下列任何一种情形，信息化管理办公室有权随时中断或终止向用户提供邮件服务而无需通知用户，并将立即清除该用户账号并按学校有关规定对用户进行处理。

1．利用邮件故意传播不健康信息；

2．违反信息安全保密条例造成失密；

3．利用电子邮件对他人进行骚扰；

4．盗用、破坏他人账号；

5．其它违反有关网络信息安全管理条例的行为；

第八条　本办法由信息化管理办公室负责解释。

10、河南大学各级政务网站建设与管理基本规范（试行）

为了进一步规范学校各部门、院系政务网站建设与管理，提高各级网站的设计水平、服务水平、管理水平，特制定本规范，凡我校部门、院系建立的政务网站必须遵照本规范，非政务网站可参照本规范。

第一节 网站建设规范

第一条 校属各部门、院系政务网站是校园网主站点的二级政务站点，只能建于校园网。

第二条 各单位二级站点统一使用我校网站群管理系统来搭建，域名统一由学校信息化管理办公室分配。

第三条 技术上接受信息化管理办公室指导，以保证与校园网主站点的正常链接。

第四条 院系必须建立独立的政务网站，国家和省部级重点实验室、国家工程研究（技术）中心也应建立独立的网站或网页，其他职能部门按学校统一规划单建或合建网站或网页。

第五条 开办二级网站或与二级网站平行的站点，必须首先依据《河南大学校园网络管理办法》向党委宣传部提出申请，经批准后方可向信息化管理办公室申请域名、备案登记。院属系（教研室）、教师、学生社团开办非政务网站或网页，必须向所属单位、党委宣传部提出申请，信息化管理办公室登记备案后方可开办。

第二节 网页设计规范

第一条 网页的版式设计原则上采用纵向延伸和单幅版式，不用横向延伸版式，视觉设计应力求简洁明快，功能设计应考虑用户习惯，要方便使用。

第二条 网页基本要素应包括：校名、网站名、网站主办单位、网站建设时间、网站管理员信箱和电话、学校网站首页的链接。

第三条 至少应在首页上呈现学校全称，校名原则上应在网站名左侧、上侧或左上侧。学校全称可使用校名题词手迹，也可使用标宋、黑体、楷体、仿宋体，但不应使用其他字体，以保证学校名称的庄严、规范。以部门、院系名称作为网站名的，原则上也应这样。

第四条 首页必须提供学校网站首页的链接，进入首页后，也应通过设置链接让用户随时随处能方便地访问学校网站首页。

第五条 使用学校校名、校徽及其它标称、标志、图案、图片等作为版权信息或

链接时必须规范。

第六条　网站的导航栏应清晰反映本网站的结构，应避免在同一个网站出现不同形式的导航栏。

第七条　同一网站的网页风格要协调统一，主页同下层页面设计上要有所差异，但每层页面的色彩、版面风格要尽量保持和谐。

第八条　按照《中华人民共和国语言文字法》的规定，网页名称、标题、正文均必须使用简体中文，需要开办外文网页或繁体中文网页的，必须同时设简体中文网页，且外文、繁体中文、简体中文版本内容应一致。网页中的文章标题字体和大小应统一，可选用标宋、黑体、楷体、仿宋体，字号为 14 磅；正文字号一律用 10 磅宋体。数字和标点符号用法必须执行国家标准。

第九条　部门、院系政务网页应端庄、严谨、规范，原则上不在首页使用弹出窗口、漫画，尽可能不用或少用动画，重要通知不能用弹出窗口发布，以免被具有过滤功能的 Web 浏览器或软件过滤。

第十条　由于中国教育科研网的网页不能发布商业广告,所以各部门网站严禁发布商业广告。

第三节 网页内容规范

第一条　网站内容要遵守有关法律法规，不得侵犯他人版权、署名权、肖像权、隐私权等合法权益。

第二条　内容建设应注重实用性和服务性。

第三条　上网信息，文字要简洁流畅，文字和图片内容要清晰、健康。

第四条　上网信息必须是非涉密信息。

第五条　部门政务网站应包括部门职能介绍或工作职责、部门管理制度、办事指南、机构设置、部门负责人简介、本部门应用系统的链接，本部门工作动态和信息、公开信箱、办公联系方式等内容。

第六条　院系政务网站应包括院系介绍、现任领导、内设机构、本科专业、硕（博）士专业点、师资力量、办学条件、学科建设、教学科研成果、党的建设、团学工作、成人教育、招生就业、本院系动态和信息、办公联系方式等内容。院系政务网站原则上不允许开通交互式栏目，若确需开通，必须设置为先审后发，做好信息发布的审核工作。院系的研究生教育、成人教育、班级主页、同学录、自设研

究机构和其他实体，一律整合在院系政务网站上，校园网导航栏原则上不单独提供链接。

第七条　部门、院系政务网站在网页中引用学校基本情况方面的数据、提法、表述风格和宣传口径，必须与学校政务网站保持一致。

第八条　政务网站发布师生等个人相关信息时，需经单位主管领导审核。网站上一律不准发布师生等个人敏感信息。

第九条　各部门政务网站上应由本单位评建创优的支撑材料等相关文档可供校内浏览和下载。

第四节 网站管理规范

第一条　网站主办单位必须对所开办的网站进行管理，并对该网站的形式、内容、运行负全责。各部门、院系政务网站实行管、监、制三结合的管理运行机制。

第二条　网站管理实行领导分管负责。开办网站的单位必须指定 1 名处级领导分管网站建设，负责规划、统筹、督导、检查此项工作，并对网站规划、建设、管理、运行负总责。网站建设管理工作要列入单位年度工作计划和办公会议程，专题工作研究每学期不少于 1 次。

第三条　网站信息监控实行专人负责。开办单位必须指定不少于 1 名的政治素质好、责任心强、熟悉网络的教师或学生政治辅导员监控本单位网站的内容，发现问题要及时与制作人员联系，提出处理意见，并督促改进；发现重大问题要及时向分管领导报告。

第四条　网站制作维护实行专人负责。开办单位要指定不少于 1 名的政治素质好、责任心强、懂网络技术的教师或学生担任网络管理员，负责网站设计制作、日常管理维护和信息更新。

第五条　网络工作分管领导、网站信息监管人员、网络制作维护人员如果由于各种原因暂时不能行使职责的，单位要指派替代人员，并做好交接工作，办理交接手续。

第六条　各部门、院系政务网站的信息更新期限不超过 30 天。超过期限未更新的，将给予通报批评；超过 60 天未更新的责令停办，关闭该单位的网站，并上报校领导。

第七条　因疏于管理而导致网络安全事故和信息管理事故的，将依据各部门和信

息化管理办公室签订的安全协议追究该单位网络工作分管领导、信息监管人员、制作维护人员的责任，视事故严重程度给予相关责任人以行政处罚。

11、河南大学校园网信息发布审核登记制度

校园网信息发布审核登记制度综述

我校网站自建立以来，为全校师生工作学习提供了极大的便利条件，成为我校师生获取信息的主要渠道。为加强我校网络信息安全，切实杜绝网络不良信息的上传，从源头把关，特制定本制度。

第一条　审稿要求

1、严格审稿程序。各院系、部处的来稿要经过单位领导把关审批，以保证稿件的真实性；电子信箱传来的稿件要同时送交加盖单位公章和领导签字的文字稿；若遇敏感信息，要求送稿单位报请主管校领导审阅。

2、严格履行编辑程序。网页编辑可得到可靠的稿件后，对稿件进行文字处理，传主管部长审阅，按照部长意见对稿件进行再次修改，并认真校对无文字及标点错误后上网。

第二条　上传稿件要求

1、上网的稿件必须经过认真加工，稿件内容真实，语句通顺，无文字及标点错误。

2、反映学校重大活动的稿件，校领导若无讲话，网页上只显示姓名不在显示职务；处级干部参加活动无具体实质性发言的，姓名不在网页上出现。

3、首页稿件上传，一般为学校的重要会议和重大活动（包括教学、科研、学术活动及相关成果和有影响力的学生活动），有特色的院系活动和有新闻价值的其他新闻稿件；同一类院系新闻稿件如岁末茶花会等，上传第一条院系投稿和有特色的新闻稿件；有中央或省部级领导考察或学校的重大新闻，在首页首条显示三至五天后卸掉。

第三条　校园文化网审稿要求

1、以引导健康时尚的网络文化为己任，活跃师生生活，营造良好的校园文化氛围。为师生的工作、学习和生活提供帮助。

2、稿件要求思想内容健康向上，切实反映大学生活，融思想性、知识性、趣味性于一体，提供师生喜闻乐见的网络文化。

3、稿件文理通顺，结构完整，语言规范，杜绝文字和标点错误。

第四条　首页信息滚动窗口发布信息

1、需要所发布部门签字盖章，并同时传送数字稿。

2、部里主管部长签字后方可上传。

12、河南大学信息化管理办公室机房安全保护制度

第一条　信息化管理办公室机房属机要重地，除工作人员以外，其他人员未经允许严禁入内；

第二条　信息化管理办公室工作人员应妥善保管好有关办公室、机房的钥匙，禁止随意委托他人管理。计算机、服务器的密码等，严禁外传；

第三条　中心机房除原有计算机、服务器等工作需要设备外，严禁私自携带使用其它电器；

第四条　信息化管理办公室办公室、机房等应配备必要的灭火器材；

第五条　经常宣传防火、灭火知识。工作人员都要掌握使用灭火器材，防止火灾事故的发生；

第六条　严禁将易燃、易爆物品带入中心，严禁在中心使用明火；

第七条　定期检查消防设施，发现问题及时报告有关部门予以解决，消除不安全隐患；

第八条　信息化管理办公室工作人员应及时检查暖气、水管等设施，发现问题及时向有关部门反映解决；

第九条　信息化管理办公室工作人员应定时检查机房，及机房附近有无渗水情况，雷雨季节要经常进行防水、防雷电的安全防范工作；

第十条　中心机房必须有良好的电源避雷和接地措施。中心机房必须保证相关设备每天二十四小时连续通电工作；

第十一条 中心机房避免阳光直射、强磁场及强辐射源；避免通风及尘烟的侵袭；

第十二条 中心机房应设置空调机，使市内温度保持在摄氏 22 度，相对湿度 50%左右；

第十三条　信息化管理办公室工作人员应及时检查电源设备有无故障，有无漏电、错相等问题，发现问题及时向有关部门反映解决；

第十四条　严禁在中心机房附近，或进入机房所经过的通道堆放杂物，保持通道的畅通；

第十五条　信息化管理办公室除值班人员外，不得留宿他人；

第十六条　未经允许，禁止将私人电脑及配件以及移动存储设备带入中心机房，禁止非专职维修人员携带工具进入机房；

第十七条　离开中心时，最后离开者必须锁门，下班时要检查电、水情况，关好门窗；

第十八条　凡在中心进行偷盗设备财物的，一经查实，将向学校保卫部门报告，视情节给予相应的行政纪律处分；造成重大影响和损失的将向公安部门报告，由个人依法承担相关责任；

第十九条　凡违反第二、三、六、十四、十六条规定的行为一经查实，将视其情节严重给予行政处分；对网络中心造成经济损失的，由本人照价赔偿损失，造成重大损失的，将向公安部门报案；

第二十条　凡故意破坏中心设备者，一经查实，将向学校保卫部门报告，造成重大影响和损失的将向公安部门报告，由个人依法承担相关责任；

13、河南大学校园网络楼宇网络设备间管理规定

各楼栋设备间内放置提供公共服务的网络交换机，为学校公共财产，统一放置于专用的网络设备机柜内；提供该设备间覆盖范围内的网络接入。网络设备间由网络中心统一管理。

第一条　网络设备间环境卫生要保持整洁、无尘；

第二条　室温保持在 18-30℃之间；

第三条　增强安全防范意识，防范于未然，杜绝安全事故的发生；

第四条　严禁在网络机柜周围（0.5 米内）堆放杂物；

第五条　严禁对网络机柜进行移动；

第六条　严禁私自开启机柜，严禁私自乱动机柜内的网络设备；

第七条　严禁私自拔插网络设备上的跳线，乱拉、乱接网线；

第八条　严禁私自中断网络设备的电源供应；

第九条　对于违反上述规定而导致公共网络设备损坏，造成重大教学及安全事故，影响日常的教学、科研、办公工作的开展，学校将依据有关规定追究相关人员责任；

第十条　如有任何问题请与信息化管理办公室联系。

14、信息化管理办公室资源管理暂行规定

第一条　学校主干网的出口是学校计算机信息网唯一出口，任何单位或个人不得自行建立其它信道为校园网出口。

第二条　学校校园网络设备、信道和线路是学校校园网的基础，任何人不得破坏，未经允许不得作为其他用途。其主干网设备和线路的使用、分配、维护由信息化管理办公室统一实施。任何单位要使用这些设备和线路，必须提出书面申请，批准后方可实施。

第三条　学校校园计算机网的 IP 地址属于学校的公共资源，由信息化管理办公室统一分配。严禁私自定义 IP 地址。任何单位和个人在未经许可的情况下，不得擅自租借，盗用，占用校园网的 IP 地址。

第四条　学校校园网的域名为国家认可的域名，任何单位和个人不得擅自租借、盗用和占用，学校的域名解析由信息化管理办公室的域名服务器统一配置，任何单位和个人未经许可，不得私自设立域名服务器。

第五条　学校校园网设置的 WEB 服务器、OA.MAIL 服务器、DNS 服务器、FTP 服务器、数据库等服务器，由信息化管理办公室统一操作、配置、管理和维护。其它单位和个人在未经许可的情况下，不得租借、盗用、挪用、占用学校校园网的各种服务器及其资源。

第六条　任何单位和个人在未经许可的情况下，不得私自开设各种服务器。

15、IT 设备管理规定

第一节　通则

第一条 凡是已经开通投入运行的主备用设备和即将投入业务运行的设备，均属于维护和管理的范围。网络设备主要包括：核心路由器、接入路由器、接入交换机、接入服务器、应用服务器、网络测试设备和相应的连线等。

第二条 各类设备，在工程施工合格，技术指标良好，设计施工文件、图纸、技术资料完整准确，经学校相关部门验收合格后，经上级同意，即应开始执行本办法有关管理和维护规定。

第三条 网络设备管理应严格遵循下列原则：

1. 所有网络设备严格执行专人负责制。
2. 未经相关领导同意，严禁设备维护人员拆卸、调试设备。
3. 有关人员应全面、及时地向主管领导反映设备运行情况。
4. 各有关人员应该相互配合协作，严格执行本办法之规定。

第四条 应按规定的考核标准加强管理，以确保设备的完好。设备完好的主要标准为：

1. 各类设备的性能应符合相应的技术指标要求。
2. 结构完整，部件、备品（备盘）及备份软件齐全，设备清洁。
3. 运行正常，使用良好。
4. 技术资料齐全、完整、图纸与设备相符。

第二节　设备的日常管理

第五条 严格执行学校设备管理部门有关设备管理的各项规章制度，对本中心管理的设备进行编号、登记、建立完善、准确的台账。

第六条 实行设备领用人责任制，谁领用，谁使用，谁保管。

第七条 对信息化管理办公室所属重要设备，要建立档案系统，保证技术资料完整。

第八条 设备的调拨、停用、报废、拆除、转让等应经学校批准方可进行。

第九条 购进设备时，信息化管理办公室有关负责人必须与供货人或调入人共同启封，核对设备规格、型号、数目及软件和文字资料，并进行质量检验。核对无误，验收合格后，方可签字并办理有关手续。

第十条 备用设备及备用盘、附属器件、技术档案、资料和原始记录均应完整无缺。

第十一条 配线架的改线和配线，应做详细记录。

第十二条 非信息化管理办公室工作人员，不得擅自启动、关闭、动用、迁移各种网络设备。

第十三条 凡故意破坏、偷盗学校设备者，一经查实，将向学校保卫部门报告，造成重大影响和损失的将向公安部门报告，由个人依法承担相关责任。

第三节 设备的更新

第十四条 设备更新的条件：

1. 设备长期使用（已超过设计使用年限），性能严重下降，经常接触不良或多次故障难以修复的可以更新。

2. 设备的某些重要性能下降，多次调整修复仍达不到指标的，可以更新。

3. 设备陈旧，可由其他技术先进的设备代替的，可以停用。

第十五条 设备更新前，应对设备现状进行详细调查，提出更新的理由，根据规定编制计划报上级审批。

第十六条 设备更新后，应组织有关人员进行验收，并有详细的测试调整记录，各种资料归档保管。

16、介质安全管理制度

第一节　总 则

第一条 为保证存储介质能够被正常管理及使用，防止存储有重要数据的介质遭受未授权的使用、移动、丢失或损毁，造成重要数据的泄漏，特制定本规定。

第二条 本规定适用于存储介质的安全管理。

第二节　存储介质管理要求

第三条 存储介质是指记录存储数据的设备，主要包括磁带、磁盘、光盘等。

第四条 存储介质在接入系统前，安全管理员负责对介质进行病毒检查，如发现病毒，立即进行处理后再接入系统。

第五条 应对磁盘阵列、磁带库等存储核心数据的介质进行标识，统一存放在固定的位置，并由机房管理员负责管理。

第六条 移动硬盘、U 盘等由介质使用人负责管理。

第七条 应建立《存储介质管理登记表》，对介质归档和查询等进行登记记录，并由资产管理员负责定期盘点。

第八条 数据管理员应每半年对介质中的数据进行测试，如发现介质硬件老化或发现介质运行缓慢，立即将其中数据转移到新的介质中，以防止由于介质老化、失效而导致的重要数据丢失。

第九条 当介质损坏需要送出维修或销毁时，应首先清除其中的敏感数据，以防止内部信息的非法泄漏。

第十条 对介质在物理传输过程中的人员选择、打包、交付等情况进行控制。

第十一条　对于需要报废的介质，应填写《信息介质报废登记表》，并做集中报废处置。

17、河南大学校园网安全保护管理办法

第一节 总 则

第一条　为了加强对校园网的安全保护，维护社会稳定和学校正常教学秩序，根据《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》、《中国教育和科研计算机网暂行管理办法》及其他有关法律、行政法规的规定，制定本办法。

第二条　本办法适用于接入河南大学校园网的计算机信息网络（简称校园网，下同）。

第三条　河南大学信息化管理办公室是在学校计算机信息网络安全保护领导小组指导下，负责校园网的信息安全保护管理工作。信息化管理办公室保护校园网络信息的公共安全，维护接入校园网的单位和个人的合法权益和利益。

第四条　河南大学所有主干网的公共设备(包括光纤,交换机,设备箱,网线,模块等)的安装,维护等操作由信息化管理办公室工作人员进行.其他任何人不得破坏或擅自维修,如有异常,应及时与信息化管理办公室联系.任何单位和个人不得从事下列危害计算机网络信息安全的活动：

（一） 未经允许，进入计算机信息网络或者使用计算机网络信息资源；

（二） 未经允许，对计算机网络中存储、处理或者传输的数据和应用 程序进行删除、修改或者增加；

（三） 故意制作、传播计算机病毒等破坏性程序；

（四） 其他危害计算机信息网络安全。

第五条　用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用校园网侵犯用户的通信自由和通信秘密。

第六条　任何单位和个人不得利用校园网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、学校的、集体的利益和公民的合法权益，不得从事违法犯罪活动，不得利用校园网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权、推翻社会主义制度的；

（三）煽动分裂国家、破坏国家统一的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

（七）公然侮辱他人或者捏造事实诽谤他人的；

（八）损害学校形象和学校利益的；

（九）其他违反宪法和法律、行政法规和学校有关规定的。

第二节 安全保护责任

第七条 信息化管理办公室会同宣传部、保卫处及有关管理机构对接入校园网的用户进行安全监督、检查，用户应如实向上述部门提供有关安全保护的信息、资料及数据文件，协助查处通过校园网进行违法犯罪的人员。

第八条 使用校园网的单位应当履行下列安全保护职责：

（一）负责本单位网络的保护管理工作，建立健全安全保护管理制度；

（二）落实安全保护技术措施，保障本单位网络的运行安全和信息安全；

（三）负责对本单位网络用户的安全教育和培训；

（四）对本单位发布的信息进行登记、审核；

（五）对建立计算机信息网络电子公告系统的用户进行登记并建立相应的信息管理制度；

（六）发现有本办法第四条、第五条所列情形之一的，应当保留有关原始记录，并及时向信息化管理办公室、宣传部、保卫处报告；经信息化管理办公室授意删除本办法第五条内容的地址、目录或者关闭服务器。

第九条 用户在办理入网手续时，应当如实填写用户入网登记表。

第十条 使用公用账号的注册者应当加强对公用账号的管理，建立账号使用登记制度。用户账号不得转借、转让。公用账号被他人盗用，造成损失和责任由拥有该公用账号的用户负责。

第三节 安全监督

第十一条 学校计算机信息网络安全保护领导小组负责网上信息的安全检查、监督。

第十二条 信息化管理办公室在学校计算机信息网络安全保护领导小组指导下，负责追踪和查处通过计算机信息网络实施的违法行为。

第十三条 信息化管理办公室掌握用户的入网情况，建立备案档案，进行备案统

计。

第十四条　各单位应建立健全安全保护管理制度。网络管理员应经常检查网络安全保护管理以及技术措施的落实情况。信息化管理办公室在组织安全检查时，各单位网络管理员必须参加。

第十五条　信息化管理办公室对安全检查发现的问题，提出改进意见，并作详细记录，存档备查。如发现违法犯罪行为，上报有关司法部门处理。

第四节 法律责任

第十六条　有下列行为之一的单位，由网络中心通知其限期改正，给予警告。情节严重的，给予三个月以内的停止联网的处罚，必要时取消联网资格。

（一）未建立安全保护管理制度的；

（二）未采取安全技术保护措施的；

（三）未对网络用户进行安全教育和培训的；

（四）未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的；

（五）转借、转让用户账号的。

第十七条　有本办法第四条、第五条所列行为之一的，由网络中心给予警告，并上报学校；情节严重，违反治安管理条例、法律、法规的，转交保卫处或司法部门处理。

第十八条　违反本办法第六条规定的，转交保卫处或司法部门处理。

第五节 附则

第十九条　根据校园网运行的实际情况并结合上级部门有关规定，将对本办法适时予以修订。

第二十条　本办法由河南大学校计算机信息网络安全保护领导小组负责解释，自发布之日起执行。

18、河南大学网络系统安全管理制度

第一节 总则

第一条　为了保护河南大学校园网络系统的安全、促进学校计算机网络的应用和发展、保证校园网络的正常运行和网络用户的使用权益，制定本安全管理制度。

第二条　本管理制度所称的校园网络系统，是指由学校投资购买、由网络中心负责维护和管理的校园网络主、辅节点设备、配套的网络线缆设施及网络服务器、工作站所构成的、为校园网络应用及服务的硬件、软件的集成系统。

第三条　校园网系统的安全运行和系统设备管理维护工作由网络中心负责，网络中心可以委托相关单位指定人员代为管理子节点设备。任何单位和个人，未经校园网负责单位同意、不得擅自安装、拆卸或改变网络设备。

第四条　任何单位和个人、不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动，不得危害或侵入未授权的(包括 CERNET 或其它互联网在内的)服务器、工作站。

第二节 安全保护运行

第五条　除校园网负责单位，其他单位或个人不得以任何方式试图登陆进入校园网主、辅节点、服务器等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施，这些行为被视为对校园网安全运行的破坏行为。

第六条　校园网对外发布的信息的内容必须经各单位领导审核，单位负责人签署意见，审核备案后，由信息化管理办公室从技术上开通其对外的信息服务。

第七条　校园网各类服务器中开设的账户和口令为个人用户所拥有，信息化管理办公室对用户口令保密，不得向任何单位和个人提供这些信息。

第八条　用户不得利用各种网络设备或软件技术从事用户账户及口令的侦听、盗用活动，该活动被认为是对网络用户权益的侵犯。

第九条　校园内从事施工、建设，不得危害计算机网络系统的安全。

第十条　校园网主、辅节点设备及服务器等发生案件、以及遭到黑客攻击后，校园网负责单位必须在二十四小时内向校保卫部门及公安机关报告。

第十一条　严禁在校园网上使用来历不明、引发病毒传染的软件；对于来历不明的可能引起计算机病毒的软件应使用公安部门推荐的杀毒软件检查、杀毒。

第十二条　任何单位和个人不得在校园网及其联网计算机上传送危害国家安全信息(包括多媒体信息)、录阅传送淫秽、色情资料。

第十三条　校园网及子网的系统软件、应用软件及信息数据要实施保密措施。信息资源保密等级可分为：

(1)可向 Internet 公开的；

(2)可向校内公开的；

(3)可向本系(单位)公开的；

(4)可向有关单位或个人公开的；

(5)仅限于本单位内使用的；

(6)仅限于个人使用的。

第十四条　对所有联网计算机及上网人员要及时、准确登记备案。多人共用计算机上网的各级行政单位、教学业务单位上网计算机的使用要严格管理，部门负责人为网络安全负责人。学校公共机房一律不准对社会开放，上网人员必须出示学生证、教师证，机房工作人员记录上网人员身份和上下网时间、机号、机器 IP 地址。公共机房使用网络的记录要保持一年。

第十五条　校园网负责单位必须制定和完善各项管理制度和技术规范，监控、封堵、删除网上有害信息。为了有效地防范网上非法活动，校园网要统一出口管理、统一用户管理，进出校园网访问信息的所有用户必须使用校园负责单位设立的代理服务器、Email 服务器。未经校园网负责单位批准，各单位一律不得开设代理服务器、Email 服务器。

第十六条　经批准开设的服务器必须保持日志记录功能，历史记录保持时间不得低于 3 个月。服务器上开设的用户必须通过 Email 按月报信息化管理办公室。校园网负责单位要不定期地检查各开通服务器的计算机日志。

第三节 法律责任

第十七条　违反第五条及第十二条规定的行为一经查实，将向学校保卫部门报告，视情节给予相应的行政纪律处分；造成重大影响和损失的将向公安部门报告，由个人依法承担相关责任。

第十八条　违反第八条规定的侦听、盗用行为一经查实，将提请学校给予行政处分，并在校园网上公布；对他人造成经济损失的，由本人照价赔偿受害人损失，

关闭其拥有的各类服务账号；行为恶劣、影响面大、造成他人重大损失的，将向公安部门报案。

第十九条　故意传播或制造计算机病毒，造成危害校园网系统安全的按《中华人民共和国计算机信息系统安全保护条例》中第二十三条的规定予以处罚。

第四节 其他

第二十条　本管理制度中所指出的校园网负责单位为信息化管理办公室。

第二十一条　本管理制度自公布之日起实行。

19、河南大学校园计算机网络信息安全管理办法

第一条　学校成立河南大学网络安全和信息化工作领导小组，负责学校的网络安全和信息化工作。领导小组办公室设在信息化管理办公室，负责学校网络资源的统一管理。各学院、部处要指定一名领导分管网络安全与信息化工作，设立单位信息主管和信息员，负责本单位的网络安全和信息化工作。

第二条　用户在使用校园网时，必须遵守《河南大学计算机网络信息安全管理办法》及国家的有关法律、行政法规，严格执行安全保密制度。不得利用校园网和国际互联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得从事危害国家利益、集体利益和公民合法权益的活动，不得危害计算机网络和信息系统的安全，发现网络有害信息时保留原始记录，及时向信息化管理办公室、宣传部和保卫处报告。

第三条　校园网用户使用账号、ip 地址进行身份认证，任何用户不得将网络账号、密码用于商业活动或转借他人使用，如有违约、违纪等行为，将由入网登记人负责。

第四条　校园网络的工作人员和校园网用户须接受并配合国家有关部门及学校的监督检查，须接受信息化管理办公室进行的网络系统及信息系统的安全检查。

20、信息系统建设与运维管理制度

第一条 为规范信息系统的建设与运行维护管理工作，确保信息系统的安全可靠运行，切实提高访问效率和服务质量，使信息系统更好地服务于全校师生，特制订本管理办法。

第二条 各信息系统（网站）的主管单位负责人是系统安全第一责任人，各单位应安排专人负责所管系统（网站）的安全管理工作。

第三条 学校各类信息系统应统一部署于学校数据中心内，信息化管理办公室依托校园网数据中心安全体系为信息系统提供运行安全和数据安全所需的基础环境，系统建设和使用单位负责系统的应用安全，并接受信息化管理办公室的测评、扫描，落实信息化管理办公室和上级有关部门提出的网络信息安全整改意见。信息化管理办公室可根据网络安全事件的性质和威胁程度直接采取封堵、隔离、强制下线等措施。

第四条 各学院、各职能部处的网站要求统一使用网站群系统来搭建，各单位要严格落实值班读网制度，安排值班人员每天登录网站读网，认真查看页面显示状况，查看各项功能的有效性，查看所发布的信息特别是重要信息是否存在错漏，查看是否存在暗链，发现问题立即纠正。

第五条 严格落实信息系统（网站）维护管理制度。只在校园网内进行运维管理，若需要远程运维或第三方单位（如网站开发单位）远程接入运维，需要采用 VPN 加密、堡垒机登录等安全方式接入，不允许直接远程桌面或直接开放管理相关端口到互联网。

第六条 妥善保管信息系统（网站）管理账户信息，使用复杂度较高的密码，并定期更新；对信息系统（网站）管理人员和用户加强网络安全意识教育和业务培训。

第七条 在信息系统的建设、使用、维护、升级过程中，建设主管单位和使用单位须组织参与信息系统建设维护的相关单位和人员签订并履行《河南大学网络与信息安全责任书》，促使对方落实学校数据保密和网络信息系统安全有关要求。

第八条 定期进行数据备份和系统备份，确保紧急情况下信息系统能够及时恢复。

第九条 原则上，应对各项操作进行日志记录，内容应包括操作人、操作时间和操作内容等详细信息。维护人员应定时对操作日志、安全日志进行审查，对异常

事件及时跟进解决。

第十条 各单位应严格落实《信息安全技术网络安全等级保护基本要求》的要求，准确划分系统安全保护等级，定期开展等级保护测评，按等级对网络信息系统开展网络安全保护工作。

21、河南大学网络信息监视、保存、清除和备份制度

第一条　严格执行国家及地方制定的信息安全条例；

第二条　上网用户必须严格遵守网络安全保密制度；

第三条　提供的上网信息，必须统一经过校宣传部审核后方可上网，并及时予以登记；

第四条　用户必须配合有关部门依法进行信息安全检查；

第五条　建立健全网络安全管理制度，采取安全技术措施、落实安全管理责任、加强交互式栏目信息发布的审核、网络运行日志的管理、并将系统运行日志完整保存 3 个月以上，以备公安机关的监督检查；

第六条　“网络安全员”要加强网络信息的检测，定期检查安全情况。检测计算机是否感染病毒并及时清除，同时应配合网络管理员对各开通服务器的系统日志进行不定期检查，及时发现隐患、及时汇报与处理；

第七条　对网络上的有害信息及时控制并删除。严防非法用户侵入我校网络从事非法活动，一经发现应及时进行相应的技术处理，如及时清除有害信息的传播途径、关闭相应的服务器等，同时要保护好相关的日志等数据，并及时向有关部门报告；

第八条　加强对用户数据的管理，发现异常用户，及时处理并备案；

第九条　定期组织网络管理人员进行安全管理学习和培训；

22、河南大学数据保密及数据备份制度

第一条　根据数据的保密规定和用途，确定使用人员的存取权限、存取方式和审批手续。

第二条　禁止泄露、外借和转移专业数据信息。

第三条　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。

第四条　定期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。

第五条　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。

第六条　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和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。

第七条　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。

23、河南大学校园网安全保密管理制度

第一条　用户必须遵守＜中华人民共和国计算机信息网络国际联网管理暂行规定＞、＜中国教育和科研计算机网络管理办法＞和国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。

第二条　用户不得利用计算机网络从事危害国家机密、破坏社会安定的违法犯罪活动，不得查阅、发送各种有害信息。

第三条　用户都有义务配合国家安全部门依法对网络使用情况等进行监督检查，采取必要措施。

第四条　校园网及子网的系统软件、应用软件及信息数据要实施保密措施。信息资源保密等级可分为：

(1)可向 Internet 公开的；

(2)可向校内公开的；

(3)可向本系(单位)公开的；

(4)可向有关单位或个人公开的；

(5)仅限于本单位内使用的；

(6)仅限于个人使用的。

第五条　根据数据的保密规定和用途，确定使用人员的存取权限、存取方式和审批手续。

第六条　禁止泄露、外借和转移专业数据信息。

第七条　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。

第八条　建立信息安全保密制度和用户信息安全管理制度，不在网上传送密件，不泄漏用户个人资料。

第九条　对所有联网计算机及上网人员要及时、准确登记备案。多人共用计算机上网的各级行政单位、教学业务单位上网计算机的使用要严格管理，部门负责人为网络安全负责人。学校公共机房一律不准对社会开放，上网人员必须出示学生证、教师证，机房工作人员记录上网人员身份和上下网时间、机号、机器 IP 地址。公共机房使用网络的记录要保持一年。

第十条　信息化管理办公室工作人员必须严格遵守国家法律法令，严禁越权调取各类服务器中存储的用户信息、留存转发的电子邮件等信息；严禁使用无保密措

施的设备传递涉密信息；涉密文件、资料和软件一律放入文件柜。

第十一条　校园网各类服务器中开设的账户和口令为个人用户所拥有，信息化管理办公室对用户口令保密，不得向任何单位和个人提供这些信息。

第十二条　用户网络访问日志和网站信息内容日志记录备份保存不少于 60 日，在国家有关机关依法查询时予以提供，信息化管理办公室将不定期进行抽查，抽查不合格的，断网 3-12 月。

第十三条　各单位应建立健全安全保护管理制度。网络管理员应经常检查网络安全保护管理以及技术措施的落实情况。信息化管理办公室在组织安全检查时，各单位网络管理员必须参加。

第十四条　信息化管理办公室对安全检查发现的问题，提出改进意见，并作详细记录，存档备查。如发现违法犯罪行为，上报有关司法部门处理。

24、河南大学校园网 VPN 使用管理办法

第一条 为更好地为教职工生创造教学、科研、办公和学习条件，方便大家在校园网以外充分使用校内网络资源，我校搭建了 VPN(虚拟专用拨号网络)服务平台。根据《中华人民共和国计算机信息系统安全保护条例》，为保证校园网内部系统和信息资源的安全，规范教职工生使用 VPN 服务安全访问校内网络资源，制定本使用管理办法。

第二条 VPN 系统主要用于校内用户在校外网上能够访问仅限于在校内网才能访问的网络资源。例如在校外网上就可以用 VPN 访问校内图书馆的数字资源和校内的各应用信息系统。

第三条 用户使用 VPN 服务接入校园网时，必须遵守国家相关法律法规及学校校园网的有关规定，不得通过 VPN 服务从事网络违纪、违法活动。

第四条 VPN 仅服务于学校正式教职工生，在校教职工和学生统一使用数字校园帐号和密码，VPN 用户必须保管好自己的帐号和密码，帐号仅限本人使用。

第五条 任何 VPN 用户不得利用 VPN 服务把校内资源提供给他人使用，否则构成侵权，由此引发的法律纠纷由 VPN 帐号持有者承担；若 VPN 用户的帐号和密码被盗、不慎丢失、工作调离，用户有责任及时与信息化管理办公室联系，以便注销或者更改用户信息。

第六条 故意泄露 VPN 帐号密码或将 VPN 帐号借给他人使用者，或其 VPN 帐号被其他人控制出现异常登录者，信息化管理办公室将停止其帐号的使用并追究该用户责任；第一次发现故意泄露 VPN 帐号密码或将 VPN 帐号借给他人使用者，该帐号将立即被封闭三个月，封闭期满本人提出申请经用户所在部门领导签字同意后方可开通，第二次发现此类情况将永久禁止该用户接入 VPN。

第七条 在完成登录、使用 VPN 期间，不要关闭 VPN 应用程序，以保证电脑和校内网络连接；VPN 使用完毕后，请及时退出该程序，以免影响他人正常使用。

第八条 VPN 专用于访问校内资源，请勿使用迅雷等 P2P 软件进行下载，并且请勿登录 VPN 后去下载校外资源，以免占用 VPN 带宽，影响他人使用。

第九条 本办法由信息化管理办公室负责解释。

第十条 本办法自发布之日起实施。

25、河南大学信息化管理办公室计算机病毒防范制度

第一条　信息化管理办公室管理人员应有较强的病毒防范意识，跟踪计算机病毒发展的最新动态，及时了解计算机病毒，特别是有严重破坏力的计算机病毒的爆发日期或爆发条件，在一些破坏性较大的计算机病毒发作日期前，要及时在校园网上发布通知；

第二条　信息化管理办公室必须采用国家许可的正版防病毒软件并及时更新软件版本；

第三条　当班人员未经上级管理人员许可，不得在服务器上安装新软件，若确实需要安装，安装前应进行病毒例行检测；

第四条　经远程通信传送的程序或数据，必须经过严格检测确认无病毒后方可使用；

第五条　服务器要定期进行计算机病毒检查，系统中的程序要定期进行比较测试和分析；发现病毒立即处理并通知上级管理人员；

第六条　服务器要尽量做到专机专用，特别是具有读写权限、身份确认功能的认证服务器一定要专用；对共享的网络文件服务器，应特别加以维护，控制读写权限，不在服务器上运行无关软件程序。

26、河南大学网络安全审查暨漏洞检测制度

背景介绍

随着我校校园网建设的进一步深入，各个院系的上网工程也在如火如荼地展开，如何防黑防毒，保障校园网的安全运行也已经成为一个实际而重要的问题放到我们的日程上来。为了保证我校网络的安全运转，特为接入的和正在校园网运转的制订安全审查制度，其目的在于增强各机关、院系的网络安全防范意识，提高河南大学网络整体安全水平。

适用范围

适用于全校所有已接入校园网或正准备接入校园网的所有联网设备。

检查周期

每月对学校的服务器进行轮流检查。

审查标准

通用扫描工具和安全分析工具（Network Scanner Or Security Analyse Tools）。信息化管理办公室将依据安全工具的对联网设备的分析结果将所接入设备的安全等级划分安全等级。

A 级：联网设备处于较为安全的运行状态。被确认为本级别内的联网设备可以接入校园网。

B 级：联网设备处于一般安全的运行状态。列入本级别内的个人计算机可以接入校园网，列入本级别内的服务器设备应立即断开与校园网的物理连接，并进行整改，为了防止意外发生，信息化管理办公室有权对列于本级别内的计算机进行网络屏蔽，直至该服务器安全标准被再次确认为 A 级为止。

C 级：联网设备处于不安全的运行状态。被确认为本级别内的所有联网设备应断开校园网的物理连接，立即进行整改，信息化管理办公室有权对列入本级别内的计算机进行网络屏蔽，直至该级别内的联网设备安全标准被再次确认为更高安全级别为止。

安全等级划分标准

A 级：系统已安装最新的系统补丁（Service Pack）。已经安装杀毒软件和防火墙工具，仅打开必须的服务和端口。系统扫描无明显的弱口令漏洞，对所有的外界访问已经建立日志记录并保证保留 3 个月以上的外界来访记录。

B 级：系统已经安装最新的系统补丁，已安装杀毒软件。

C 级：所有低于 B 级的设备。

系统补丁发布与升级办法

根据相关安全公告版的公告，及时下载补丁到本地并在河大首页上公布补丁的链接地址以方便用户下载安装；利用软件自身的智能升级方式对软件进行升级和打补丁。

关键词定义：

系统补丁（Service Pack）：是指软件制造商在软件发行后对其发行软件的修补程序的集合。一般可以从发行软件的厂商网站免费获得。

服务器：服务器是计算机的一种，它是网络上一种为客户端计算机提供各种服务的高性能的计算机，它在网络操作系统的控制下，将与其相连的硬盘、磁带、打印机、Modem 及各种专用通讯设备提供给网络上的客户站点共享，也能为网络用户提供集中计算、信息发表及数据管理等服务。

联网设备：可以与计算机网络相联接并可以对外或被外界访问的设备，如计算机、网络打印机、路由器等。

扫描工具（安全分析工具）：扫描器是检测远程或本地系统安全脆弱性的软件；通过与目标主机 TCP/IP 端口建立连接和请求某些服务（如 TELNET、FTP 等），记录目标主机的应答，搜集目标主机相关信息（如匿名用户是否可以登录等），从而发现目标主机某些内在的安全弱点。扫描器的重要性在于把极为烦琐的安全检测，通过程序来自动完成，这不仅减轻管理者的工作，而且缩短了检测时间，使问题发现更快。当然，也可以认为扫描器是一种网络安全性评估软件。一般而言，扫描器可以快速、深入地对网络或目标主机进行评估。

27、河南大学校园网应急保障制度暨计算机事件报告制度

适用范围

适用于对正常情况下校园网运行中出现的各类案件事件，如黑客攻击，或校园网不能正常运转等情况下的人员操作步骤。

事件定义

1) 人为破坏事件

指人为的，利用工具软件（包括黑客软件）主动或非主动对校园网节点侦听，扫描或攻击事件。

2) 非正常校园网运作事件

在未接到主管部门或相关单位通知情况下，导致校园网运作出现的不能正常运转的事件。

应急步骤

无论是对问题（1）或（2）中的任何一类事件，应急步骤框架如下：

1) 确定攻击源及攻击形式，如果是校内用户应分析其单位，如果为校外用户应得到其 IP 地址并尽可能得到其详细信息。

2) 分析事件性质并针对攻击类型对受影响单位采取补救或防御性措施。措施包括通知其主管领导并同时保护性中断局域网对外连接等，以确保网络安全。

3) 分析受影响范围，确定受损幅面并对攻击的性质进行进一步的分析。

4) 事件备案，以便于后期相关部分的介入的查证工作顺利进行。

5) 将事件描述向相关部门汇报

6) 刑事案件应在 24 小时内报告公安机关

7) 凡校园网上的电子公告栏、论坛、聊天室、留言板等交互式栏目均须明确专门的信息安全管理员，敏感时期按有关部门的通知要求 24 小时值班巡查。若发现栏目内出现有害信息、不良信息及其他违反国家法律法规的信息，须在保存好有关记录（发贴人的 IP、发贴时间和内容等）后立即删除有害信息，并及时上报信息化管理办公室，必要时上报公安网安部门，同时协助有关部门查证。

28、河南大学网络与信息安全责任书（一）

为进一步落实网络信息安全管理责任，确保我校网络信息安全，根据《全国人大常委会关于维护互联网安全的决定》、《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》，结合我校情况，特制订本责任书。

一、本责任书适用范围：所属信息系统以 henu.edu.cn 为域名结尾的二级单位，以归属我校的 IP 地址提供信息服务的信息系统所属单位，服务器托管在我校的信息系统管理单位。

二、自觉遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《互联网信息服务管理办法》等国家相关法律法规。

三、本单位主管领导为网络与信息安全第一责任人，负责建立和完善本单位网络与信息安全组织，建立健全相关管理制度，制定网络安全事故处置措施和应急预案，配备专职信息安全管理员，具体负责本单位网络与信息安全工作。

四、用户上传的公共信息在本部门网站上发布前，必须经过本部门领导审核后，方能上网发布。要明确责任，坚持“谁发布，谁审核，谁负责”原则，作到有害信息不上网，涉密信息不上网。

五、严禁窃取或者以其他非法方式获取我校师生各类电子信息，不得出售或者非法向他人提供我校师生各类电子信息。未经允许不得擅自使用或破坏我校师生各类电子信息。

六、网站信息内容记录备份保存不少于 60 日，在国家有关机关依法查询时予以提供。

七、各单位对本单位网站应加强监控管理，不得将管理权限和管理员密码转交其他非管理人员。网站所使用的脚本、程序来源必须安全可靠，必须及时修补漏洞；后台管理入口不得公开，管理账户必须使用强密码，凡重要管理账户密码必须按保密规定进行备份。

八、建立网络与信息安全责任人联系制度，保证信息化管理办公室可以随时与网站安全责任人沟通联系。网站安全责任人具有删除违法信息的责任和义务。责任人变更后，应在两天内以书面形式通知信息化管理办公室。

九、严格实行网络与信息安全责任追究制度。如因管理不善致使本单位内发生重、特大信息安全事故或严重违纪违法事件的，按有关规定对单位和有关责任人进行处理，情节特别严重的依法追究相关责任人的法律责任。

十、在责任期内，责任书各条款不因负责人变化而变更或解除，接任负责人应相应履行职责 。

十一、本责任书最终解释权归信息化管理办公室。

双方确认在签署本责任书前已经详细审阅过责任书的全部内容，并悉知责任书各条款的规定。

本责任书一式两份，信息化管理办公室和各责任书签订单位各一份，双方签字盖章生效。

信息化管理办公室（盖章）　　单位负责人（签字）：

年　月　日　　年　月　日

29、河南大学网络与信息安全责任书（二）

为进一步落实网络信息安全管理责任，确保我校网络信息安全，根据《全国人大常委会关于维护互联网安全的决定》、《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》，结合我校情况，特制订本责任书。

一、本责任书适用范围：我校信息化建设涉及的公司，承担我校各类信息系统及网站开发和运维的公司或个人。

二、不利用互联网危害国家安全、泄漏国家秘密，不侵犯国家、社会、集体的利益和公民的合法权益，不从事犯罪活动。

三、不在网上制作、复制、发布、传播《互联网信息服务管理办法》第十五条禁止的九类有害信息。发现有害信息，按照有关规定及时处理，并报告信息化管理办公室。

四、不从事下列危害网络信息安全的行为：

1.制作或者故意传播计算机病毒以及其他破坏性程序；

2.非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序；

3.法律、行政法规禁止的其他行为。

五、严禁窃取或者以其他非法方式获取我校师生各类电子信息，不得出售或者非法向他人提供我校师生各类电子信息。未经允许不得擅自使用或破坏我校师生各类电子信息。

六、建立信息安全保密制度和用户信息安全管理制度，不在网上传送密件，不泄露用户个人资料。

七、建立和完善网络安全技术措施，定期进行安全风险分析与系统漏洞测试，防止病毒传播和被非法控制为网络攻击的跳板，适时对软硬件进行升级，确保系统安全可靠运行。

八、在运维过程中发现安全事故及时控制和处理，保留有关原始记录，并在 24 小时内向相关主管部门报告。

九、严格实行网络与信息安全责任追究制度。如因未遵守规定出现网络信息安全事故，愿意承担相应的经济责任及法律责任。

十、在责任期内，责任书各条款不因负责人变化而变更或解除，接任负责人应相

应履行职责 。

十一、本责任书最终解释权归信息化管理办公室。

双方确认在签署本责任书前已经详细审阅过责任书的全部内容，并悉知责任书各条款的规定。

本责任书一式两份，信息化管理办公室和各责任书签订单位各一份，双方签字盖章生效。

信息化管理办公室（盖章）　　单位负责人（签字）：

年　月　日　　年　月　日