校政字〔2019〕91号

关于印发《郑州工程技术学院网络信息安全管理办法》的通知

学校各单位：

为加强学校网络信息安全管理，推进学校信息系统安全等级保护工作，提高网络信息安全防护能力和水平，保障学校各项事业健康有序发展，结合我校的实际情况，现将《郑州工程技术学院网络信息安全管理办法》印发给你们，请认真贯彻落实。

2019年7月5日

郑州工程技术学院网络信息安全管理办法

第一章　总 则

第一条　为加强学校网络信息安全管理，推进学校信息系统安全等级保护工作，提高网络信息安全防护能力和水平，保障学校各项事业健康有序发展，根据《中华人民共和国网络安全法》、《教育部关于加强教育行业网络与信息安全工作的指导意见》（教技〔2014〕4 号）、《教育部 公安部关于全面推进教育行业信息安全等级保护工作的通知》（教技〔2015〕2 号）等文件要求，结合我校实际，特制定本办法。

第二条 本办法所称网络信息安全工作,是指为使由学校建设、运行、维护或管理并支撑学校教学、科研和管理等各项事业的信息资产的安全性、完整性、可用性等得到保持、不被破坏所开展的相关管理和技术工作。

本办法所指学校各单位包括各机关部、处、室，学院，直属单位以及有关科研机构。

第三条 学校按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全网络信息安全责任体系，学校各单位、全体师生员工应依照本办法要求及学校相关标准规范履行网络信息安全的义务和责任。

第二章　组织机构与职责

第四条 网络安全和信息化领导小组是学校网络信息安全

的领导机构，负责统筹学校网络安全与信息化建设工作。

第五条 信息与网络管理中心是网络信息安全技术支撑单位，负责学校网络信息安全防护体系的建设、运行维护、技术指导和服务支持。

第六条 学校各单位是本单位网络安全和信息化工作的责任主体，各单位主要负责人是本单位网络安全和信息化工作第一责任人，负责按本办法落实网络信息安全工作。

第三章　校园网络安全管理

第七条 校园网络是指校园范围内连接各种信息系统及信息终端的计算机网络，包括校园有线网络、无线网络和各种虚拟专网。

第八条 校园网络与互联网及其他公共信息网络实行逻辑隔离，由信息与网络管理中心统一出口、统一管理和统一防护。未经批准，学校各单位在校园内不得擅自通过其他渠道接入互联网及其他公共信息网络。

第九条 信息与网络管理中心应采取访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等措施加强校园网络边界防护。

第十条 师生员工接入校园网络，实行“实名认证上网”制度；学校非涉密信息系统接入校园网络，实行接入审批和备案登记制度。网络接入实名管理制度由信息与网络管理中心负责实施。涉密信息系统不得接入校园网络。

第十一条 严禁任何单位和个人利用校园网络及设施开展

经营性活动。

第十二条 学校各单位主要负责人、信息化建设涉及的公司及网络与信息安全责任人等必须签订《郑州工程技术学院网络与信息安全责任书》。

（一）所属信息系统以 zzut.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、服务器托管的信息系统管理单位，必须签订《郑州工程技术学院网络与信息安全责任书（一）》；

（二）学校信息化建设涉及的公司、承担学校各类信息系统及网站开发和运维的公司或个人，必须签订《郑州工程技术学院网络与信息安全责任书（二）》。

第四章　信息系统建设及安全管理

第十三条 学校按照同步规划、同步建设、同步运行的原则，规划、设计、建设、运行、管理信息安全设施，建立健全网络信息安全防护体系，全面实施信息系统安全等级保护制度。

第十四条 网络安全和信息化领导小组负责制定学校信息系统项目规划和顶层设计。学校各单位根据《河南省高校信息化发展水平评估指标体系（试行）的通知》（教科技〔2018〕278号）结合本单位业务需求，提出信息系统建设申请，纳入学校规划的核心信息系统建设需求将获学校信息化建设经费的优先支持。

第十五条 网络安全和信息化领导小组负责统筹学校信息系统安全等级保护工作，组织学校各单位开展信息系统定级、

系统备案、等级测评、建设整改，具体负责信息系统台账管理、等级评审、系统备案、监督检查工作。按照“自主定级、自主保护”的原则，信息系统建设单位是信息系统安全等级保护的责任主体，具体负责系统定级、建设整改、安全自查、协助系统备案、等级测评并接受有关部门监督检查。信息与网络管理中心是信息系统安全等级保护工作的技术支撑保障部门，负责网络信息安全防护体系建设和等级测评组织工作，参与监督检查工作，并协助学校各单位进行系统定级、建设整改。

第十六条 为确保信息系统建设项目质量,网络安全和信息化领导小组在立项阶段组织需求、技术、预算等方面的专家论证。信息系统建设单位在立项阶段应确定安全保护等级，由网络安全和信息化领导小组对建设方案进行单独的安全论证和等级评审。对于安全等级第二级以上（含第二级）的信息系统，由网络安全和信息化领导小组统一办理系统备案。

第十七条 学校鼓励建设单位优先采购安全可靠、技术成熟和服务优质的成品软件用于信息系统建设。没有相应成品软件或成品软件不适应实际需求的，可按照学校采购与招标相关管理办法，委托资质和信誉良好的软件开发商进行开发。

第十八条 信息系统在建设阶段应按已确定安全保护等级，同步落实安全保护措施。信息系统投入试运行后，由建设单位初步验收，出具初步验收报告。对于安全等级第二级以上（含第二级）的信息系统，由网络安全和信息化领导小组会同信息与网络管理中心组织等级测评。信息系统通过初步验收和信息

安全保护等测评后，由网络安全和信息化领导小组组织竣工验收。

第十九条 新建信息系统原则上使用学校数据中心提供的云服务（虚拟机），不再单独购置服务器及网络设备。如有特殊需求，需在立项阶段提出，经专家论证通过后进行采购，并托管于学校数据中心机房。

第二十条 信息系统建设单位需自行维护信息系统，并对信息系统的网络信息安全负责。使用学校数据中心云服务（虚拟机）的信息系统，建设单位需签署《郑州工程技术学院云服务使用安全责任书》并填写《郑州工程技术学院云服务（虚拟机）备案登记表》。进行服务器托管的信息系统，建设单位需签署《郑州工程技术学院托管服务器安全责任书》并填写《郑州工程技术托管服务器备案登记表》。

第二十一条 信息系统建设单位应制定信息系统使用与维护的管理制度，规范信息系统使用者和维护者的操作行为。

第二十二条 各单位信息系统数据的管理规范必须严格执行《郑州工程技术学网络数据管理办法》。全校所有信息系统实行备案制管理，必须填写《郑州工程技术学院信息系统备案登记表》报信息与网络管理中心备案。

第二十三条 对于安全等级第二级以上（含第二级）的信息系统，网络安全和信息化领导小组将定期组织开展等级测评，查找、发现并及时整改安全问题、漏洞和隐患。根据国家和教育行业有关标准规范，四级系统应每年进行两次测评，三级系

统每年进行一次测评，二级系统每两年进行一次测评。

第五章　网站安全管理

第二十四条 信息与网络管理中心统一建设学校网站群平台，学校各单位网站须纳入网站群平台统一管理。

第二十五条 各单位网站由本单位自行管理维护,网站设安全员一名，由单位负责人担任，对网站信息安全负责。各单位网站安全员要严格审查本单位网站的信息发布，对本单位网站信息安全负责。

第二十六条 各单位应建立网站值守制度,制订应急处置流程，组织专人对网站进行监测，发现网站运行异常及时处置。

第二十七条 全校所有网站实行备案管理。网站正式上线前，网站责任单位需向网络信息中心申请备案，签署《郑州工程技术学院网站信息安全责任书》并填写《郑州工程技术学院校内网站备案登记表》,并通过网络信息中心组织的安全检查后方可正式上线。

第六章　网络信息安全应急管理

第二十八条 网络安全和信息化领导小组负责学校网络信息安全应急工作的统筹管理，信息与网络管理中心负责网络信息安全应急工作的技术支撑和保障。

第二十九条 网络安全和信息化领导小组负责制定学校网络信息安全事件报告与处置流程，信息与网络管理中心负责制订学校网络信息安全应急预案；如学校网络信息安全应急预案不能满足需求,相关单位可制订本单位网络信息安全应急预案。

网络信息安全应急预案制修订后应及时报网络安全和信息化领导小组备案。

第三十条 网络安全和信息化领导小组应组织网络信息安全应急演练，评估并适时组织网络信息安全应急预案修订。学校各单位应组织开展网络信息安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第三十一条 信息与网络管理中心负责组建学校信息安全应急技术支援队伍，完善 24 小时应急值守制度，提高信息安全事件的预防、预警和应对能力，预防和减轻信息安全事件造成的损失和危害。

第三十二条 学校各单位应按照附件 9《郑州工程技术学院网络信息安全事件报告与处置流程（试行）》，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作，做到安全事件早发现、早报告、早控制、早解决。

第三十三条 学校各单位或师生员工均有义务及时向信息与网络管理中心报告信息安全事件，不得在未授权情况下对外公布、尝试或利用所发现的安全漏洞或安全问题。

第七章　信息安全检查监督

第三十四条 学校各单位定期对本单位信息系统的安全状况、安全保护制度及措施的落实情况进行自查，并配合有关部门的信息安全检查、信息内容检查、保密检查与审批等工作。

第三十五条 信息与网络管理中心联合学校相关单位对学校各单位的网络信息安全工作落实情况进行检查，对发现的问

题下达限期整改通知书，责成相关单位制订整改方案并落实到位。

第三十六条 网络安全和信息化领导小组对年度安全检查情况进行全面总结，按照要求完成检查报告并报有关信息安全主管部门。

第八章 信息安全责任追究

第三十七条 学校建立信息安全责任追究和倒查机制。

第三十八条 有关单位在收到网络与网络信息安全限期整改通知书后，整改不力的，学校给予通报批评；玩忽职守、失职渎职造成严重后果的，依法依纪追究相关人员的责任。

第三十九条 学校各单位应按照网络信息安全事件报告与处置流程，及时、如实地报告和妥善处置网络信息安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关单位责任人进行约谈或通报。

第四十条 师生员工违反本办法规定的,由网络安全和信息化领导小组责令改正，并通报批评；拒不改正或者导致危害网络信息安全等严重后果的,根据学校有关规定给予以纪律处分。触犯刑律的，移交司法机关处理。

第九章 附 则

第四十一条 涉及国家秘密的信息系统,执行国家保密工作的相关规定和标准，由学校保密单位监督指导。

第四十二条 学校各单位可参照本办法制订本单位的实施细则。

第四十三条 本办法自发布日起实施；

第四十四条 本办法由网络安全和信息化领导小组办公室负责解释。学校原有相关规定与本办法不一致的，按本办法执行。

附件：1.郑州工程技术学院网络与信息安全责任书（一）

2.郑州工程技术学院网络与信息安全责任书（二）

3.郑州工程技术学院网站信息安全责任书

4.郑州工程技术学院校内网站备案登记表

5.郑州工程技术学院云服务使用安全责任书

6.郑州工程技术学院云服务（虚拟机）备案登记表

7.郑州工程技术学院托管服务器安全责任书

8.郑州工程技术学院托管服务器备案登记表

9.郑州工程技术学院网络信息安全事件报告与处置流程（试行）

10.郑州工程技术学院网络信息安全突发事件报告单

附件 1

郑州工程技术学院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 zzut.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，做到有害信息不上网、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网络安全和信息化领导小组办公室。

责任书签字单位或签字人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，网络安全和信息化领导小组办公室和各责任书签订单位各一份，责任书签订单位签字盖章生效。

责任单位（盖章）：

负责人（签字）：

年　　月　　日

附件 2

郑州工程技术学院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，并报告网络安全和信息化领导小组办公室。

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网络安全和信息化领导小组办公室。

责任书签字单位或签字人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，网络安全和信息化领导小组办公室和各责任书签订单位各一份，责任书签订单位签字盖章生效。

责任单位（盖章）：

负责人（签字）：

年　　月　　日

附件 3

郑州工程技术学院网站信息安全责任书

为进一步加强学校网站安全管理，落实安全责任制，严防网络信息安全事故的发生，共同营造安全和谐的网络信息环境，根据《计算机信息网络国际联网安全保护管理办法》、《互联网安全保护技术措施规定》等有关法规规定，特制定本责任书。各网站负责单位需签订安全责任书，并承担相应的安全责任。

一、不利用校园网络危害国家安全、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。

二、不利用学校网站制作、复制、查阅和传播下列信息

1.煽动抗拒、破坏宪法和法律、行政法规实施的；

2.煽动颠覆国家政权，推翻社会主义制度的；

3.煽动分裂国家、破坏国家统一的；

4.煽动民族仇恨、民族歧视，破坏民族团结的；

5.捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

6.宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

7.公然侮辱他人或者捏造事实诽谤他人的；

8.损害国家机关信誉的；

9.其他违反宪法和法律、行政法规的。

三、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。

四、严格遵守学校有关规定，做好本部门网络信息安全管理工作，对发布的信息进行实时审核，对出现重大事故并造成重大损失和恶劣影响的，承担由此引起的一切责任，并将追究部门负责人的管理责任。

五、签订本责任书的责任人工作如有调整，继任者承担本责任书的责任。

责任单位（盖章）：

负责人（签字）：

年　　月　　日

附件 4

郑州工程技术学院校内网站备案登记表

<table>
<tr><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>责任领导</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>网站域名</td><td colspan="3"></td></tr>
<tr><td>网站类型</td><td colspan="3">（注明网站编程语言、运行环境、数据库类型等）</td></tr>
<tr><td>网站
主要栏目</td><td colspan="3"></td></tr>
<tr><td>服务器
放置地点</td><td>校园网络机房□</td><td>建站方式</td><td>利用网站群建站□
带有后台数据库的网站□</td></tr>
<tr><td>管理员姓名</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>E-mail</td><td></td><td>移动电话</td><td></td></tr>
<tr><td>申请日期</td><td></td><td>开通日期</td><td></td></tr>
<tr><td>审核意见</td><td colspan="2">所在单位意见（盖章）：
年 月 日</td><td>网络信息中心意见：
年 月 日</td></tr>
<tr><td colspan="4">以下由信息与网络管理中心填写</td></tr>
<tr><td>IP 地址</td><td></td><td>IP 对外开放</td><td>是□ 否□</td></tr>
<tr><td>服务类型</td><td colspan="3">（HTTP、FTP 等）</td></tr>
<tr><td>备
注</td><td colspan="3">1、备案单位除了必须遵守国家有关互联网、信息和网络安全的规定外，还必须遵守学校关于网络和信息管理的有关规定。
2、备案网站仅允许开办与教学、科研和管理有关的网站，且不得在网页上链接任何广告和其它含有广告链接的网页，不得利用校园网从事有任何商业目的的活动。
3、备案单位提供的备案信息要真实、有效。
4、备案单位须指定一名网站管理员负责相应网站的信息安全和信息维护工作。
5、备案单位必须对本部门网站所存储的信息内容负责，保证所接入的计算机里没有存储涉及保密内容、违法的信息，如有以上情况，网络信息中心有权关闭网站并视情况进行处理。</td></tr>
</table>

附件 5

郑州工程技术学院
云服务（虚拟机）使用安全责任书

为提高我校校园网应用水平，减轻校内各单位设备维护和管理的负担，信息与网络管理中心向校内各单位提供虚拟服务器资源。申请单位需签订本安全责任书，并承担相应的安全责任。

一、申请单位负责所申请虚拟服务器的信息安全管理，对服务器的系统安全负责。

二、申请单位不得擅自更改所申请虚拟服务器用途；申请单位如果要改变服务器用途或设置，需事先报信息与网络管理中心，经中心批准后方可实施。

三、所申请虚拟服务器的系统日志和网站访问日志需开启，并至少保留 90 天备查。申请单位的系统管理员应定期做好日志备份。

四、单位所申请虚拟服务器上发布的信息，应当遵守有关法规规定，不得制作、复制、发布和传播违反国家宪法、危害国家安全、损害国家利益、破坏民族团结、宣扬邪教和封建迷信、扰乱社会秩序、破坏社会稳定、淫秽、暴力、侵犯他人合法权益等违法违纪信息。如有违反，本中心有权终止其服务器的使用。情节严重者，将移交当事人至司法机关接受处罚直至承担法律责任。

五、单位所申请虚拟服务器上不准开设 BBS 和聊天室服务，开设留言功能的网站必须建立上网用户日志留存并保持 90 天，每天定时检查留言内容，发现有害信息必须及时删除，并追查相关人员责任。

六、如发现本单位所申请虚拟服务器网站上有不良信息，在保存相关记录的同时，应立即删除该页面的链接或隔离该页面，并及时报告，

以防不良信息的扩散传播。

七、不得在本单位所申请虚拟服务器上尝试运行各种“黑客”软件，包括邮件炸弹、端口扫描等。

八、本单位所申请虚拟服务器如果感染病毒或木马，系统管理员应立即做好备份及病毒查杀；对于感染计算机病毒后不做任何防护处理，且放任病毒危害发生的申请单位，中心有权直接关闭该服务器。对于屡次出现类似情况的申请单位，中心保留进一步处理的权利。

九、申请单位的系统管理员应做好本单位所申请虚拟服务器的安全检查，落实相关安全措施。

十、申请单位如违反以上规定，信息与网络管理中心有权暂停其虚拟服务器的使用，情节严重的报相关部门处理。

申请单位（盖章）　　年　月　日

安全责任人（签名）：　　联系电话：

系统管理员（签名）：　　联系电话：

附件 6

郑州工程技术学院云服务（虚拟机）备案登记表

申请单位名称:　　年　　月　　日

申请人姓名		申请人联系方式	
所选择虚拟机类型	☐ Windows 2008 64bit　☐ Windows 2012 64bit ☐ CentOS 6.5 64bit　☐ CentOS 7 64bit ☐ 其他:		
虚拟机配置	☐ vCPU : ☐ vMem: ☐ vHD :		
预装需求	☐ DB: ☐ 应用: ☐ 其他:		
开通周期	年　月　日 至　年　月　日		
服务器用途			
备注			
申请人（签字）: 年 月 日		单位负责人签字（盖章） 年 月 日	
(以下由管理员填写)			
服务器名称			
IP 地址			
审批人签字: 年 月 日		办理人签字: 年 月 日	

说明：

1. 所申请的虚拟服务器不得从事与上述申请用途无关的一切活动。如申请人违反规定，擅自改变用途，申请人需自行承担由此带来的一切后果。申请人需自行确保数据安全，信息与网络管理中心不承担任何因数据丢失而导致的后果。

2. 虚拟机服务器使用每年需要重新备案登记，连续 3 年未进行备案登记的，信息与网络管理中心有权删除该服务器回收资源，重新分配，因此引起的数据丢失等后果由申请单位自行承担。

附件 7

郑州工程技术学院托管服务器安全责任书

为提高我校校园网应用水平，减轻校内各单位设备维护和管理的负担，信息与网络管理中心向校内各单位提供服务器托管服务。委托单位需签订本安全责任书，并承担相应的安全责任。

一、委托单位负责服务器的信息安全管理，对服务器的系统安全负责。

二、委托单位不得擅自更改服务器用途；委托单位如果要改变服务器用途或设置，需事先报信息与网络管理中心，经中心批准后方可实施。

三、托管服务器的系统日志和网站访问日志需开启，并至少保留 90 天备查。委托单位的系统管理员应定期做好日志备份。

四、托管服务器上所发布的信息，应当遵守有关法规规定，不得制作、复制、发布和传播违反国家宪法、危害国家安全、损害国家利益、破坏民族团结、宣扬邪教和封建迷信、扰乱社会秩序、破坏社会稳定、淫秽、暴力、侵犯他人合法权益等违法违纪信息。如有违反，本中心有权终止其服务器的使用。情节严重者，将移交当事人至司法机关接受处罚直至承担法律责任。

五、服务器上不准开设 BBS 和聊天室服务，开设留言功能的网站必须建立上网用户日志留存并保持 90 天，每天定时检查留言内容，发现有害信息必须及时删除，并追查相关人员责任。

六、如发现本服务器网站上有不良信息，在保存相关记录的同时，应立即删除该页面的链接或隔离该页面，并及时报告，以防不良信息的扩散传播。

七、不得在托管服务器上尝试运行各种“黑客”软件，包括邮件炸

弹、端口扫描等。

八、托管服务器如果感染病毒或木马，系统管理员应立即做好备份及病毒查杀；对于感染计算机病毒后不做任何防护处理，且放任病毒危害发生的委托单位，中心有权直接关闭该服务器。对于屡次出现类似情况的委托单位，中心保留进一步处理的权利。

九、委托单位的系统管理员应做好托管服务器的安全检查，落实相关安全措施。

十、委托单位如违反以上规定，信息与网络管理中心有权暂停其服务器的使用，情节严重的报相关部门处理。

托管单位（盖章）　　年　月　日

安全责任人（签名）：　　联系电话：

系统管理员（签名）：　　联系电话：

附件 8

郑州工程技术学院托管服务器备案登记表

托管单位名称：　　年　月　日

<table>
<tr><td>申请人姓名</td><td></td><td>申请人联系方式</td><td></td></tr>
<tr><td>服务器配置</td><td colspan="3"></td></tr>
<tr><td>网络安全设备情况</td><td colspan="3"></td></tr>
<tr><td>托管周期</td><td colspan="3">年　月　日 至　年　月　日</td></tr>
<tr><td>服务器用途</td><td colspan="3"></td></tr>
<tr><td>备注</td><td colspan="3"></td></tr>
<tr><td colspan="2">申请人（签字）：
年　月　日</td><td colspan="2">负责人签字（盖章）
年　月　日</td></tr>
<tr><td colspan="4">(以下由管理员填写)</td></tr>
<tr><td>服务器名称</td><td colspan="3"></td></tr>
<tr><td>IP 地址</td><td colspan="3"></td></tr>
<tr><td colspan="2">经办人签字：
年　月　日</td><td colspan="2">负责人签字：
年　月　日</td></tr>
</table>

附件 9

郑州工程技术学院
网络信息安全事件报告与处置流程（试行）

为加强郑州工程技术学院网络信息安全工作，及时掌握和处置网络信息安全事件，协调相关力量做好应急响应处理，降低安全事件带来的损失与影响，维护正常工作秩序和营造健康的网络环境，根据《中华人民共和国网络安全法》，结合学校实际，制定本流程。

第一条 网络信息安全事件定义。根据《信息安全事件分类分级指南》（GB/T 20986-2007，以下简称《指南》），本流程中所称的网络信息安全事件（以下简称安全事件）是指信息内容安全事件、有害程序危害事件、网络攻击事件、信息破坏事件和其他信息安全事件。

第二条 适用范围。本流程适用于郑州工程技术学院发生的网络信息安全事件的报告与处置工作。

第三条 安全事件等级划分。根据《指南》将安全事件划分为四个等级：特别重大事件（I 级）、重大事件（II 级）、较大事件（III 级）和一般事件（IV 级）。

第四条 安全事件等级由网络安全和信息化领导小组判定。各单位一旦发生安全事件，由网络安全和信息化领导小组办公室根据《指南》，视信息系统重要程度、损失情况以及对工作和社会造成的影响，提出安全事件等级，交由网络安全和信息化领导小组审定。

第五条 I 级至 III 级安全事件的报告与处置。报告与处置分为三个步骤：事发紧急报告与处置、事中情况报告与处置和事后整改报告与处

置。

（一）事发紧急报告与处置

学校各二级单位为安全事件的报告主体,一旦发现上述安全事件，相关责任单位应立即了解事件的基本情况，进行应急处置，保留现场，并在第一时间向分管（联系）校领导和网络安全和信息化领导小组办公室（信息与网络管理中心）口头报告初步情况。口头初报不得超过事发后 30 分钟，书面报告最迟不得超过事发后 1 小时。事发后 1 小时内不报的视为漏报，2 小时内不报的视为瞒报。信息与网络管理中心根据报告事件性质，协同相关部门

（二）事中情况报告与处置

1．事中情况报告应在安全事件发现后 1 小时内以书面报告的形式进行报送，报送内容和格式见《郑州工程技术学院网络信息安全突发事件报告单》（报告单见附件 10）。

2．事中情况报告由安全事件责任单位编写，负责人审核后，签字并加盖公章报送网络安全和信息化领导小组办公室。

3．安全事件的事中处置包括：及时掌握损失情况、查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为主观破坏的安全事件应积极配合公安部门开展调查。

（三）事后整改报告与处置

1．事后整改报告应在安全事件处置完毕后 1 个工作日内以书面报告的形式进行报送。

2．事后情况报告由安全事件责任单位编写，由本单位负责人审核

后，签字并加盖公章报送网络安全和信息化领导小组办公室。

3．安全事件事后处置包括：进一步总结事件教训，研判安全现状、排查安全隐患；进一步加强制度建设，提升安全防护能力。如涉及人为主观破坏的安全事件应继续配合公安部门开展调查。

第六条 一般事件（IV 级）及预警类事件的报告与处置。各单位要按时、按要求完成国家、地方有关信息安全部门以及教育部通报的预警类信息的处置工作，并按要求形成书面报告，报送网络安全和信息化领导小组办公室。

第七条 联络方式报告。各单位的联络方式发生变更的，应及时报送网络安全和信息化领导小组办公室。

第八条 相关配套机制。各单位应建立值守制度，做到安全事件早发现、早报告、早控制、早解决。

第九条 问责制度。各单位应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，将对相关单位进行相应处理。

第十条 本流程由网络安全和信息化领导小组办公室负责解释。

附件 10

郑州工程技术学院网络信息安全突发事件报告单

报告单位		报告时间	年 月 日 时 分
事发单位		事件起始时间	年 月 日 时 分
填报人		审核人	
事件分类	☐有害程序类事件 ☐网络攻击类事件 ☐信息破坏类事件 ☐信息内容安全类事件 ☐故障类事件 ☐灾害类事件 ☐其它类事件		
事件级别	☐Ⅰ级 ☐Ⅱ级 ☐Ⅲ级 ☐Ⅳ级		
危害表象	☐网络中断 ☐系统瘫痪 ☐数据毁坏 ☐数据泄密 ☐其它危害		
事件描述（包括突发事件发生原因、性质，初步原因和危害程度判断）:			
处置措施: （突发事件发生单位已采取的控制措施及其他应对措施）			
事件后果的初步估计:			
有关意见和建议			

郑州工程技术学院　　2019 年 7 月 5 日印发