

校党字〔2020〕21号

## 郑州工程技术学院 落实党委网络安全工作责任制实施办法

为贯彻落实《中央办公厅关于印发〈党委（党组）网络安全工作责任制实施办法〉的通知》、河南省教育厅关于印发贯彻落实《教育系统落实党委网络安全工作责任制实施办法》和《网络安全责任制考评办法通知》要求，结合学校的实际情况，现制定郑州工程技术学院落实党委网络安全工作责任制实施办法。

### 一、责任分工

（一）按照网络安全工作中“谁主管谁负责”的基本原则，校党委对学校网络安全工作负主体责任。网络安全和信息化领导小组（以下简称“网信领导小组”）负责具体落实党委的工作部

署，学校党委书记为第一责任人，党委主管网络安全工作的副校长（CIO）为直接责任人。

（二）按照“谁运营谁负责”的原则，网络安全和信息化领导小组办公室（以下简称“网信办”）负责学校网信领导小组的日常事务工作，以及统筹协调、指导网络安全具体工作。

（三）各学院党总支、各处室（党支部：下同）对本单位网络安全工作负主体责任，党总支书记和各处室（党支部书记：下同）负责人是第一责任人，分管网络安全的党政班子成员是直接责任人。各党总支、各处室按有关规定做好本单位的网络安全工作，完成目标考核任务。

## **二、基本要求**

（一）认真贯彻落实党中央和上级部门的决策部署，落实习近平总书记关于网络安全工作的重要指示精神 and 决策部署，贯彻落实网络安全法律法规，明确网络安全工作的主要目标、基本要求、工作任务与保护措施等。

（二）制定和落实网络安全责任制度，把网络安全工作纳入党委重要议事日程，明确工作机构，加大人力、财力与物力的支持和保障力度。

（三）校党委对学校网络安全工作负指导监管责任，统一组织领导对学校网络安全保护和重大安全事件处置工作，研究解决主要问题。

（四）在全校范围内依法组织开展网络安全检查，处置网络安全事件，并及时将相关情况通报上级主管部门。

（五）在全校范围内组织开展网络安全宣传教育活动，采取多种方式培养网络安全人才，支持网络安全工作的有效开展。

（六）学校各党总支、各处室应严格按照“谁主管谁负责，谁运维谁负责，谁使用谁负责”的原则，组织部署网络安全工作。学校网信领导小组办公室对网络安全负指导监督责任，在开展网络安全检查、处置网络安全事件时，应积极配合网信和公安部门开展工作。

（七）学校各党总支、各处室相关单位应定期依法在本单位内部开展网络安全检查，及时处置网络安全事件，并将处置结果上报网信领导小组。

（八）学校各党总支、各处室相关单位应当加强和规范本单位网络安全信息汇集、分析和研判工作；及时向网信领导小组报告网络安全信息和网络安全重大事项，统筹协调开展网络安全检查。

### **三、保障措施**

（一）网信办与各责任部门要把贯彻本方案作为一项严肃的政治任务，严格执行责任分工，明确责任部门与责任人，采取切实可行的方式方法，组织和配合学校全面完成相关任务。

（二）学校各党总支、各处室相关单位要认真依据本方案开展检查，确保各项任务落实到位。对出现应当问责的失职失责情

形，依据《中国共产党问责条例》及相关法律、法规和规章制度予以问责。

（三）网信办把对学校各党总支、各处室相关单位的年度评价意见提交网信领导小组，作为党委对学校各党总支、各处室相关单位综合考核和平安建设考核的重要内容。

## **四、工作方案**

### **（一）建立领导责任制**

#### **1. 调整修订网络安全和信息化领导小组**

调整修订《郑州工程技术学院网络安全和信息化领导小组》，领导小组下设办公室，办公室设在信息与网络管理中心。主管网络安全工作的副校长兼任网络安全和信息化领导小组办公室主任。

#### **2. 党组织主要负责人签订《网络安全承诺书》**

学校党委主要负责人签订《网络安全承诺书》（见附件一），并按规定要求上报教育厅网信办；党组织主要负责人发生变更时应于变更后 10 个工作日内重新签订承诺书并的报教育厅网信办。

#### **3. 党委召开网络安全工作专题会议**

（1）学校党委每年召开一次专题会议研究部署网络安全与信息化建设工作。（2）学校 CIO 每季度召集一次会议听取网络安全相关工作汇报，研究网络安全工作。（3）相关会议纪要应按规定上报教育厅网信办。

#### **4. 制定网信领导小组年度工作要点或网络安全年度工作要点**

学校需制定本单位年度工作要点或网络安全年度工作要点，在每年第一季度以文件形式正式下发，并及时报教育厅网信办。

## **5. 总结网络安全工作进展情况**

学校应于每年12月15日前根据教育厅要求总结网络安全工作进展情况，并形成总结报告（总结报告内容参见当年教育厅网信办相关文件要求）按规定上报教育厅网信办。

### **（二）网络安全通报机制建设**

#### **1. 明确本部门网络安全相关责任人及签订网络安全承诺书**

学校各党总支、各处室相关单位明确指定网络安全第一责任人、直接责任人、网络安全管理员（见附件1：网络安全责任人登记表）。学校各党总支、各处室相关单位签订网络安全承诺书（见附件2：郑州工程技术学院网络安全承诺书）。各单位网络安全责任人发生变化后应在5个工作日内报校网信办。校级网络安全责任人等信息由校网信办及时在教育系统网络安全管理平台（<https://xxaq.moe.edu.cn>）上更新。

#### **2. 排查建立信息系统名录制度**

各党总支、各处室相关单位应排查本单位的所有信息系统、网站、公众号、企业微信、钉钉等以学校或本单位名称建立的各种信息系统并报校网信办。各单位严格按照相关网络安全法律法规对本单位负责的信息平台进行管理。学校网信办将各单位信息系统平台名录及时准确地上报教育系统网络安全管理平台，并根据系统更新情况及时更新。

### **(三) 网络安全威胁监测预警**

#### **1. 及时处置通报的安全威胁**

学校网信办安排专人负责接收来自教育部、教育厅的安全威胁通报平台（平台地址：<http://aqtb.xxaq.moe.edu.cn>），并在接到通报起的 10 个工作日内完成处置工作并在平台反馈处置结果并上传处置报告。

#### **2. 开展本单位安全监测预警通报**

(1) 学校制定本单位的监测预警通报工作相关制度文件，并将相关制度文件加盖单位公章报送教育厅网信办。

(2) 有序开展网络安全监测预警工作，对学校的信息系统（网站）进行监测，将监测工作机制复印件加盖单位公章报送教育厅网信办。

#### **3. 共享威胁信息**

学校通过接口等方式与教育部、厅通报平台对接，共享威胁（漏洞、预警、威胁信息等）信息。

### **(四) 落实网络安全等级保护工作**

学校按照等级保护定级工作要求和时间完成本单位各类信息系统（网站）的定级备案工作；二级以上系统应完成公安机关备案，一级系统组织相关专家进行等级保护评测并在校网信办备案，备案证明文件复印件于当年 12 月 15 日前报送教育厅网信办。

### **(五) 保障关键信息基础设施**

配合开展关键信息基础设施认定工作。学校根据教育部组织的关键信息基础设施识别认定工作要求，及时梳理并上报本单位纳入关键信息基础设施的系统名单；每年组织关键信息基础设施开展网络安全评估，评估报告加盖单位公章后于当年12月15日前报厅网信办。

#### **（六）配合开展网络安全检查工作**

（1）学校根据教育厅网信办要求及时开展网络安全自查工作，并按时提交自查报告；（2）配合开展教育厅网信办组织的网络安全检查工作（包括远程技术检测、现场安全检查等），并根据检查情况进行整改，及时提交整改报告；（3）学校各党总支、各处室相关单位每年12月前完成本部门网络安全自查报告并提交校网信办。

#### **（七）重要时期网络安全保障**

重要时期履行报平安制度。学校应按照教育部、教育厅网信办的重要时期保障通知要求，履行报平安制度，有事件的及时上报事件，没有事件报平安。

#### **（八）网络安全应急管理**

##### **1. 制定应急预案并开展应急演练**

（1）制定学校网络安全应急预案，并将应急预案报教育厅网信办。

（2）学校每年组织一次实战型攻防演练活动，各党总支、各处室相关单位要积极配合攻防演练活动，学校网信办将相关材

料（不限于通知文件、工作方案、演练记录和总结报告等）及时报教育厅网信办。

## **2. 网络安全事件应急处置**

学校各党总支、各处室相关单位应当在发生网络安全事件后参考《郑州工程技术学院网络安全事件应急预案》要求，及时上报学校网信办（如30分钟内电话上报，24小时内将处置报告加盖单位公章报送到校网信办）。由学校网信办根据相关文件要求报教育厅网信办。

### **（九）网络安全经费保障**

学校要切实保障网络安全经费。学校年度网络安全经费情况随年度总结按规定一并报教育厅网信办。新增信息化预算，网络安全占总经费的比例不低于5%。

### **（十）网络安全宣传教育培训**

#### **1. 在职人员安全培训**

学校各党总支、各处室相关单位每年应组织本单位教工参加网络安全讲座、网上平台学习、外部培训等，培训后将学时证明提交校网信办。在职人员年度人均接受网络安全培训时间不少于4个学时；对信息化管理人员和技术人员开展网络安全培训，年度人均培训时间不少于8个学时。

#### **2. 技术人员安全资质培训**

（1）学校从事信息化和从事网络安全工作的人员拥有网络安全专业资质占比应达到60%，并将技术人员名单和资质信息在

教育系统网络安全工作管理平台上备案，人员发生变动时，及时更新相关信息。

(2) 网络安全专业资质包含国家级或者教育系统网络安全相关技术培训认证（如：中国信息安全测评中心-CISP 注册信息安全专业人员、中国网络安全审查技术与认证中心 CISAW 信息安全保障人员认证、工信部教育与考试中心-全国计算机技术与软件专业技术资格（信息安全工程师）、公安部信息安全等级保护评估中心-CIIP 国家重要信息系统保护人员、教育部教育管理信息中心-ECSP 教育系统网络安全保障专业人员等）。各党总支、各处室相关单位教职工拥有网络安全专业资质证书人员应报校网信办备案。

- 附件：1. 郑州工程技术学院网络安全责任人登记表  
2. 郑州工程技术学院网络安全承诺书  
3. 郑州工程技术学院各单位网络信息安全承诺书  
4. 郑州工程技术学院 2020 年度网络安全和信息化工作要点  
5. 郑州工程技术学院 2020 年网络安全和信息化建设项目预算立项表

2020 年 5 月 6 日

附件 1:

## 郑州工程技术学院网络安全责任人登记表

责任单位名称		郑州工程技术学院		
第一 责任 人	姓名	周春辉	职务	党委书记
	办公电话	68229699	移动电话	13903712336
	电子邮箱	20121003@zzut.edu.cn		
直接 责任 人	姓名	孙龙国	职务	副校长
	办公电话	68229889	移动电话	13838196688
	电子邮箱	20141001@zzut.edu.cn		
网络 安全 管理 员	姓名	张志强	职务	副主任
	办公电话	68229977	移动电话	13014693700
	电子邮箱	19961001@zzut.edu.cn		

党委书记（签字）：

党委公章（盖章）

年 月 日

## 郑州工程技术学院网络安全责任人登记表

责任单位		信息与网络管理中心		
第一 责任 人	姓名	张志强	职务	支部书记
	办公电话	68229977	移动电话	13014693700
	电子邮箱	19961001@zzut.edu.cn		
直接 责任 人	姓名	赵冰	职务	负责人
	办公电话	68229858	移动电话	13213073232
	电子邮箱	20081036@zzut.edu.cn		
网络 安全 管理 员	姓名	张东	职务	网络安全员
	办公电话	68229858	移动电话	15093265325
	电子邮箱	20011007@zzut.edu.cn		

第一责任人（签字）：

党组织或单位公章（盖章）

年 月 日

附件 2:

## 郑州工程技术学院网络安全承诺书

本单位郑重承诺遵守本承诺书的所列事项，对所列事项负责，如有违反，由本单位承担由此带来的相应责任。

一、本单位承诺遵守《中华人民共和国网络安全法》《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互联安全保护管理办法》和《信息安全等级保护管理办法》及其他国家信息技术安全的有关法律、法规和行政规章制度。

二、本单位已知悉并承诺执行《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》《教育部关于进一步加强直属高校直属单位信息技术安全工作的通知》《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》《教育行业信息系统安全等级保护定级工作指南》《信息技术安全事件报告与处置流程》和《教育系统落实党委（党组）网络安全责任制实施细则》等教育部信息技术安全有关工作的文件规定。

三、本单位保证不利用网络危害国家安全、泄露国家秘密，不侵犯国家的、社会的、集体的利益和第三方的合法权益，不从事违法犯罪活动。

四、本单位承诺完善本单位的信息技术安全管理，建立健全信息技术安全责任制和相关规章制度、操作规程。

五、本单位承诺加强信息系统安全，落实信息系统安全等

级保护制度，提高信息系统安全防护能力。

六、本单位承诺加强终端计算机安全，落实软件正版化，推进具有自主知识产权的软硬件应用，规范工作人员的使用行为。

七、本单位承诺规范本单位数据采集和使用，不采集超越职能范围的数据，保障数据安全。

八、本单位承诺提升应急响应能力，制定本单位应急预案，组织开展应急演练。

九、本单位承诺对本单位的信息系统进行安全监测，并对监测发现和通报的安全问题进行限时整改。

十、本单位承诺保障信息技术安全工作经费，将经费纳入年度预算并确保落实到位，保障信息技术安全工作开展。

十一、本单位承诺加强本单位信息技术安全教育，组织工作人员参加培训，提高管理人员的安全意识和技术人员的防护能力。

十二、本单位承诺当信息系统发生信息技术安全事件，迅速进行报告与处置，将损害和影响降到最小范围，并按照规定及时进行整改。

十三、若违反本承诺书有关条款和国家相关法律法规的，本单位愿承担责任。

十四、本承诺书自签署之日起生效。

党委书记（签字）：

党委公章（盖章）

年 月 日

附件 3:

## 郑州工程技术学院各单位网络信息安全承诺书

本单位郑重承诺遵守本承诺书的所列事项，对所列事项负责，如有违反，由本单位承担由此带来的相应责任。

一、本单位承诺遵守《中华人民共和国网络安全法》及教育部、省教育厅、学校制订的网络安全和信息化工作的各种管理制度和管理办法。

二、本单位保证不利用网络危害国家安全、泄露国家秘密，不侵犯国家的、社会的、集体的利益和第三方的合法权益，不从事违法犯罪活动。

三、本单位承诺完善本单位的信息技术安全管理，建立健全信息技术安全责任制和相关规章制度、操作规程。

四、本单位承诺加强终端计算机安全，落实软件正版化，推进具有自主知识产权的软硬件应用，规范工作人员的使用行为。

五、本单位承诺规范本单位数据采集和使用，不采集超越职能范围的数据，不泄露任何校内电子信息，加强数据信息安全意识，保障数据信息安全。

六、本单位承诺提升应急响应能力，制定本单位应急预案，组织开展应急演练。

七、本单位承诺对本单位的信息系统进行安全备份和安全监测，并对监测发现和通报的安全问题进行限时整改。

八、本单位承诺按校网信办要求及时准确报告网络安全责任人、安全管理员（信息管理员）、信息系统等相关信息，保障信息安全各项工作正常运转。

九、本单位承诺信息发布遵守“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。

十、本单位承诺对本单位网站加强监控管理，包括但不限于管理员账号密码、网站脚本、有害程序的安全防护和安全检查。

十一、本单位承诺加强本单位信息技术安全教育，组织工作人员参加培训，提高管理人员的安全意识和技术人员的防护能力。

十二、本单位承诺当信息系统发生信息技术安全事件，迅速进行报告与处置，将损害和影响降到最小范围，并按照要求及时进行整改。

十三、若违反本承诺书有关条款和国家相关法律法规的，本单位愿承担责任。

十四、责任书各条款不因负责人变化而变更或解除，接任负责人应履行相应职责。

十五、本责任书最终解释权归学校网信办。

十六、本承诺书自签署之日起生效。

第一责任人（签字）：

党组织或单位公章（盖章）

年 月 日

附件 4:

## 郑州工程技术学院 2020 年度网络安全和信息化 工作要点

### 一、目标任务

2020 年工作的指导思想和目标任务：以习近平新时代中国特色社会主义思想为指导，深入贯彻落实全国、全省教育大会精神，按照教育部《教育信息化 2.0 行动计划》和省教育厅等八部门《关于加快发展“互联网+教育”的实施意见》要求，以河南省“三区一群”和郑州市国家中心城市建设为契机，以服务地方经济社会发展为宗旨，以“一二三四”工程为统揽，继续坚持以立德树人为根本，以人才培养为中心，以本科教学合格评估为引领，以网络安全作为重要保障，为全校各单位的在线开放课程“金课”建设和“双万计划”提供现代化信息技术支持（5G、区块链），激发和释放学校发展活力，培养高素质应用型人才，推动教育信息化转段升级，以教育信息化支撑引领教育现代化。

### 二、重点工作

#### （一）强化党对网络安全和教育信息化工作的全面领导

我们要深入学习贯彻习近平总书记关于网络安全和信息化的重要论述，强化互联网思维，抓好省教育厅等八部门《关于加快发展“互联网+教育”的实施意见》（豫教科技〔2019〕113号）的要求，严格落实党委网络安全责任制，学校领导班子主要负责人是第一责任人，分管网络安全的领导是直接责任人，调整

修订网络安全和信息化领导小组由党委机关部部门负责领导小组办公室。学校党委（党组）今年内至少召开一次专题会议研究部署网络安全及 2020 年度网络安全和信息化建设项目预算立项工作，分管负责同志每季度至少召集一次会议听取网络安全汇报，研究网络安全及信息化建设相关问题。

## （二）持之以恒抓好网络安全工作

我们会根据国家《网络安全法》严格落实网络安全等级保护 2.0 的要求，完成信息系统定级备案和等保测评，做到物理安全、系统安全、应用安全、网络安全及存储安全。

平时工作中加强网络安全监测预警，提高数据分析和态势感知能力，年内组织开展至少一次实战化网络安全攻防演练，针对攻防结果做出分析和整改措施，加强校园网的安全运行。同时，我校要与知名网络安全公司加强平时业务联系，组织校园网运维技术人员积极培训学习最新网络安全技术。构建网络安全应急处理小组和技术支撑体系，全面提高偶发网络安全事件的快速应对处置能力。

## （三）做好疫情防控期间的联防联控及复工开学工作

进一步开发企业微信平台的应用功能，发挥网络信息平台在联防联控和复工开学中的重要作用。确保网上教学工作的实效性，加强与学生、家长的及时沟通。

在疫情防控期间，积极参与教学管理与教学单位的各种教学平台（学堂在线、慕课堂、智慧树）和在线教学软件（企业微信会议、直播、钉钉、腾讯课堂、雨课堂）技术支持沟通，熟悉平

台和软件使用流程，做好校内技术支持和指导，提升学生远程在线课程的学习效果。

#### （四）优化改善学校信息化基础条件

加强数字化教学环境的构建。配合教学管理部门做好在线课程建设、网络教学空间建设、校级及校际间的线上课程资源平台建设、人工智能和区块链技术等教学管理、服务等应用过程的技术支持和软硬件的服务保障工作。

同时，进一步加大我校智慧校园建设，推动“最多跑一次”改革，建设网上一站式服务大厅，早日实现教师和学生校内业务一网通办的便捷化目标，提高在校师生的获得感，同时推进物联网、大数据、云计算等先进技术在校园网络服务上的应用。

积极准备校园网 IPV6 的研究和部署，随时应对省级教育网 IPV6 的规模化部署应用。

#### （五）开展网络安全及信息素养提升行动

网络安全行业的发展很快，为了提升校园网络运维者的岗位能力建设，我们年内会积极选派有关人员参与教育系统网络安全保障专业人员（ECSP）培训；配合相关部门提前选拔校内相关专业学生通过培训，参与第五届高校网络安全攻防大赛，达到以赛促学、学以致用目标。

#### （六）普及宣传网络安全法律法规

为了把国家的《网络安全法》、《密码法》等相关法律法规宣传到校内每位师生，在年内组织一到两次网络安全公开讲座宣传、解读相关政策，做好网络安全周的宣传及活动组织工作。

## 附件 5:

## 2020 年网络安全和信息化建设项目预算立项表

项目活动内容	活动内容细化	预算(万元)	资金来源	情况说明
信息化基础设施建设(经费到账后实施)	双活存储系统	100.00	省教育厅项目经费	双活存储项目共计 160 万元 省教育厅批 100 万元, 年度经费 60 万元
邮电费	宽带线路及电话费	110.00	年度预算	教育科研网、电信等宽带、 线路及固定电话费
维护费	软硬件服务及 维修维护费	130.00	年度预算	校园网运行服务费、软件正版 化、网络安全系统、应用系统 及网络设备维修维护费
网络信息安全建设	网络基础安全建设	80.00	年度预算	网络安全态势感知平台、数据 库安全审计等
网络信息安全建设	数据安全建设	40.00	年度预算	二级等保测评、网络安全监控 中心等
信息化基础设施建设	双活存储系统 (补充)	60.00	年度预算	补充省教育厅项目经费不足
信息化基础设施建设	网络设施建设	35.00	年度预算	服务器负载均衡、网络会议 室、网络设备等
信息化基础支撑平台建设	基础服务平台	50.00	年度预算	一站式服务大厅及流程引擎 服务等
智慧教育平台建设	智慧服务	35.00	年度预算	智慧校园平台、微应用服务模 块等
总计			640.00	

---

中共郑州工程技术学院委员会

2020年5月6日印发

---