中共郑州工程技术学院委员会文件

校党字〔2021〕55号

郑州工程技术学院网络安全保障工作方案

2021年5月至2022年2月，为做好建党100周年庆祝活动和冬奥会网络安全保障工作，结合上级文件精神，制订学校网络安全保障工作方案如下：

一、工作组织与分工

成立郑州工程技术学院建党100周年庆祝活动和冬奥会网络安全保障工作领导小组。

组　长：周春辉　卢　奎

副组长：苏　炜　谢霜云　孙龙国　甘　勇　李　欣

成　员：各学院、图书馆党总支书记、各行政党支部书记

领导小组办公室设在信息与网络管理中心，信息与网络管理中心负责人任办公室主任。各部门党总支书记、行政负责人发生变化时由接任者继续履行网络安全保障领导小组成员职责。其

中，学校宣传部和信息与网络管理中心要发挥统筹协调优势，积极推进对全校网络安全的检查和督促整改工作的开展，主要包括现场检查、技术测试和督查、通告及指导等具体工作的统筹安排。

学校要全面深化开展网络安全等级保护和关键信息基础设施安全保护工作，全面落实网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的三化六防措施，采用自查自评、技术检测、现场检查、反馈整改相结合的方式，确保建党100周年庆祝活动和冬奥会期间全校网络空间安全。

二、网络安全保障工作内容和流程

全校各部门网络安全责任制的落实、网站建设、重要信息系统网络安全防护情况、各机房与实训中心物理安全情况、系统日志与审计留存情况、数据加密、备份与恢复设置、安全设备部署落实、安全策略设置运行、安全漏洞发现与整改情况等。

1. 开展网络安全自查

全校各部门要全面开展年度网络安全自查。自查内容主要包括：各单位组织开展网络安全工作情况和网络安全责任制落实情况；各网站和信息系统贯彻落实国家网络安全等级保护制度情况；全校师生有关个人信息的采集、存储、传输、应用和保护情况。各部门要加强网络安全保护管理制度和网络安全技术措施的落实，全面排查、及时处置本部门存在的网络安全风险，确保万无一失。信息与网络管理中心和宣传部负责对全校各部门进行网

络安全的监督、检查和指导，要把网络安全要求通知到位，网络安全责任落实到位，对各部门网站纳入统一管理，避免网络安全案（事）件的发生。

2.梳理排查网络安全定级保护工作情况

我校目前针对全校五个应用系统做了网络安全定级保护备案工作，现信息与网络管理中心应全面梳理排查已备案部门和备案系统的运行情况，督促指导相关部门全面梳理各类网络（包括网络设施、信息系统、重要数据、网站、重点区域公共场所LED电子显示屏系统等），促使不满足要求的系统等，通过整改达到网络安全等级保护的要求。

3.组织开展网络技术检测

信息与网络管理中心应组织网络安全相关技术人员或者委托第三方公司通过技术检测和渗透测试，查找网络安全漏洞和隐患，并出具技术检测报告。6月中下旬，由信息与网络管理中心负责组织以安全事件处置为核心的校内网络攻防应急演练，对发现的问题及时通报整改，同时做好应急预案。

4.组织开展现场监督检查

信息与网络管理中心和宣传部应按计划对各部门开展网络安全现场检查。检查时，要通报当前网络形势、工作要求和技术检测中发现的问题隐患，听取被检查部门自查工作总结，了解被检查单位网络安全保护工作情况，排查安全风险、加强风险管控。对检查中发现的问题，要提出整改建议，并及时向被检查部门反

馈检查意见。

5.督促整改网络安全漏洞隐患

针对技术检测和网络攻防应急演练过程中发现的网络安全漏洞、隐患、问题和风险，信息与网络管理中心要逐条整理登记，及时向相关部门进行通报，责令其限期整改，并跟踪督办整改情况，要求其书面反馈整改情况，并对整改结果进行复测验证，确保问题整改清零。

三、时间安排

1.自查自评阶段（即日起至2021年6月6日）

各部门要迅速按照自查自评要求开展相关工作并按时提交总结报告，自查总结应重点阐述自查工作的组织开展情况，网络安全等级保护、关键信息基础设施安全保护等工作开展情况、当前网络安全方面存在的突出问题及下一步网络安全工作计划。

2.检查整改阶段（2021年6月7日至2022年2月20日）

信息与网络管理中心和宣传部应组成联合检查组，采用现场检查和平时检查相结合的方式开展网络安全监督检查工作，对发现的网络安全漏洞、隐患、问题和风险，及时向被检部门进行通报，并依法责令限期整改。相关部门应及时予以整改，并将整改情况报送信息与网络管理中心和宣传部。随后，信息与网络管理中心和宣传部根据整改情况，对有关部门进行复检，以便及时巩固整改效果，切实提高各部门的网络安全防范能力。

3.总结阶段（2022年2月21日至2022年2月28日）

全校召开网络安全总结会议，对重视网络安全工作，防范到位的部门进行表扬；对问题严重，整改不到位的部门通报批评；对发生重大网络安全案（事）件的部门，将追究责任领导及责任人的责任。

四、工作要求

1. 高度重视，加强领导

各部门一定要提高政治站位，增强“四个意识”、坚定“四个自信”，做到“两个维护”，深入学习贯彻习近平总书记关于网络安全工作的重要指示精神和中央最新决策部署，树立正确的网络安全观，严格落实网络安全主体责任，细化责任分工，做好网络安全所需人、财、物等各项保障，加强网络安全防护能力，坚决确保全校网络安全。

2. 密切协作，抓好落实

各部门要按照此次检查工作的统一部署和工作要求，认真组织开展网络安全自查，按时报送自查工作总结和联系人名单，并配合学校联合检查组进行现场检查和网络安全技术检测。

3. 强化责任，加强备案

各部门要按照“谁主管谁负责，谁运维谁负责，谁使用谁负责”的原则，明确网络安全保护责任，开展网络安全自查工作。要按照国家网络安全法律法规和网络安全等级保护制度要求，加强网络安全监测、测评和检查，要进一步落实网站防攻击、防篡改、防挂马，防范邮件攻击，防范勒索、挖矿病毒入侵，防范敏

感数据泄露，防范 LED 屏幕内容篡改等关键技术防范措施，提高抵御攻击破坏的能力。

校内各信息系统的主管单位，充分认识网络安全形势的严峻性，提高网络安全保护意识，采取必要的管理手段和技术手段等加强管理，及时修复本单位主管的信息系统安全漏洞，保障本单位主管信息系统的网络安全。

4. 加强督导，严肃纪律

各部门要按照工作要求，落实责任人，压实工作责任，对责任不明确，工作不落实、措施不到位的部门进行重点督导。导致本校发生重大网络安全事件，或在工作中弄虚作假的，将严格责任倒查，严肃追究责任，同时要严肃工作纪律，严格落实安全保密责任，严防发生失泄密事件。

中共郑州工程技术学院委员会

2021 年 6 月 7 日

中共郑州工程技术学院委员会　　2021 年 6 月 7 日印发