

郑州工程技术学院文件

校政字〔2026〕52号

关于印发《郑州工程技术学院供应链 安全管理办法》的通知

学校各单位：

为全面落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规，规范我校信息化项目外包、软硬件设备采购、技术运维、第三方技术服务全链条安全管理，防范信息化供应链引入后门程序、数据泄露、恶意攻击、运维管控失范等各类安全风险，结合学校管理实际，经学校校长办公会议研究，特制定《郑州工程技术学院供应链安全管理办法》，现印发给你们，请认真贯彻执行。



郑州工程技术学院供应链安全管理办法

第一章 总 则

第一条 按照“源头管控、安全可靠、持续监管、风险可控”原则，选择合规合格的供应商，保障其为学校提供符合安全要求的产品与服务，加强风险控制，消除供应链安全隐患。

第二条 本办法适用于向我校提供网络信息化产品和业务系统服务的所有供应商，包括但不限于规划设计、开发建设、网络安全产品、IT 产品、网络运维、技术检测、等级检测、风险评估、安全测评、外包运维等单位。

第二章 职责划分

第三条 网络安全和信息化工作领导小组总体指导相关工作，小组办公室负责具体工作，其职责包括：

- 1.负责组织供应链安全日常管理工作。
- 2.负责根据供应链安全工作的要求和规范，制定内部的安全检查计划及方案，上报网络安全和信息化工作领导小组。
- 3.负责定期组织对项目开展安全技术检测及整改工作，检测整改情况上报网络安全和信息化工作领导小组。
- 4.制定完善供应链安全事件的应急响应预案，及时上报重大安全事件，第一时间处理并消除安全隐患。

第四条 全校各二级单位是学校各网络和信息安全责任部门（后简称责任部门），其职责包括：

1.负责本部门项目的建设、开发、运维过程中供应链安全管理。

2.负责调研项目相关供应商，并检查相关资质，确认供应商已建设符合国家标准的信息安全体系。

3.负责与供应商签订安全协议。

4.负责对第三方人员的安全教育，重要岗位人员进行背景调查并签订保密协议。

5.负责定期对项目进行漏洞修复。

第三章 安全建设管理规定

第五条 各责任部门应检查项目中使用的包括电子邮件系统、网络监控软件、文件共享平台、源代码仓库、VPN 产品、云桌面系统、虚拟化软件、视频会议软件、财务软件、行业专用、数据库等软件、中间件及网络设备、安全设备、服务器、手持设备等硬件及软件，查清重要供应链产品的版本、型号、生产厂商、开发类型、涉及操作系统、是否有信息回传厂商及回传信息的主要内容等基本要素，形成供应链产品清单并上报网络安全和信息化工作领导小组办公室备案。

第六条 各责任部门应对重要网络和大数提供服务和产品的供应链企业进行梳理排查，主要包括设计方、开发方、承建方、网络安全产品提供方、信息化产品提供方、运维方、安全服务提供方、信息安全测评方及其他参与方等企业，形成供应链企业清单。

第七条 各责任部门应根据供应链产品清单，检查各供应商销售许可证并采用源代码安全审计、开源组件安全检查、软件安全性深度测试等技术检测手段对产品开展安全自查和技术检测，最终形成供应链产品安全隐患清单并上报网络安全和信息化工作领导小组办公室备案。此类检查可委托有资质的第三方公司进行。

第八条 各责任部门应对供应链企业进行调研，梳理供应商组织架构、软件类别、软件来源、软件功能、软件源代码量、软件开发语言及供应商自身企业网络整体安全建设内容，形成供应链企业安全隐患清单并上报网络安全和信息化工作领导小组办公室备案。

第九条 各责任部门应根据供应链产品安全隐患清单、供应链企业安全隐患清单开展供应链产品、企业安全隐患整改，形成供应链安全隐患整改清单并上报网络安全和信息化工作领导小组办公室备案。

第十条 项目涉及的市场采购软件产品需满足信息安全规范要求，定制开发软件必须通过第三方测评机构的审查。

第四章 安全运维管理规定

第十一条 各责任部门应将供应链安全例行检查纳入日常运维工作中，相关检查结果记录留档备查。

第十二条 各责任部门应根据项目变更情况及时更新供应链产品安全清单及供应链企业安全清单，组织自查并更新供应链产

品安全隐患清单及供应链企业安全隐患清单，及时整改并形成供应链安全隐患整改清单，更新间隔时间不宜超过一年。

第五章 外包及第三方管理

第十三条 各责任部门应重视供应链安全管理。应选择具有相关专业资质的单位提供外包服务，严格界定外包服务业务范围和工作内容，明确敏感信息访问、处理等所有相关的安全要求，签订保密协议，并对外包服务单位工作人员进行必要的背景审查和保密审查，关键岗位严禁由外包人员担任。

第十四条 对接触核心系统、数据或拥有管理权限的外部人员需要进行背景审查和保密审查，提出书面申请后，经网络安全和信息化工作领导小组办公室同意批准后聘用，并进行上报备案。

第十五条 各责任部门对外部人员进场开展运维和技术服务应建立登记备案制度，通过专人全程陪同或堡垒机等技术手段监测操作行为，规范外包服务人员的终端接入，严禁非授权接入和操作，严禁复制和泄露任何敏感信息。

第十六条 外包服务人员因履行服务内容需要带出的设备、资料和介质均需事先审核批准，并记录带出人、带出时间、归还时间和用途等。

第十七条 外包服务人员对开展工作所需的各类账户，须向被服务部门提前申请并获得批准。各部门应遵循“最小权限原则”

合理分配外包服务人员操作权限，减小外包服务人员误操作或滥用权限导致发生各种意外事件带来的影响。

第十八条 各部门应加强对外包服务人员变更管理，建立完善的变更流程。外包服务团队中人员若需变更，须向被服务部门申请并获得批准及备案。

第十九条 外包服务项目结束时，归还所有属于责任部门的设施设备，视具体情况冻结或删除该服务项目所需的全部账号，关闭所有本地或远程访问通道。

第六章 风险管控和预警应急

第二十条 应每年对供应商开展一次信息安全评估工作，并保留评估记录。

第二十一条 各责任部门应对有关部门通报的安全风险隐患和预警及时组织处置，准确研判受漏洞等威胁因素影响的供应链产品并整改修复，无法修复的应采取必要补救措施控制风险。主动及时掌握供应链产品和服务相关的安全信息，对通用型产品和服务的风险漏洞，运行单位应在厂商和安全机构修复方案公开发布后立即核查整改。因技术条件限制，不能按期整改但需继续运行的，应采取必要措施，避免发生安全事件，并报告网络安全和信息化工作领导小组办公室。

第二十二条 各责任部门应加强供应链安全事件应急管理，按照《郑州工程技术学院网络安全事件应急预案》要求，强化安全事件处置措施，可定期开展应急演练，并根据演练结果完善应

急预案，相关演练计划、脚本、记录、总结等资料留档提交网络安全和信息化工作领导小组备查。

第二十三条 安全事件发生后，各责任部门应根据事件类型和级别，立即启动应急预案，做好事件处置，最大程度减少损失和危害，及时开展信息通报。

第二十四条 安全事件处置完成后，责任部门应及时完成事件调查和评估工作，对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。

第七章 附 则

第二十五条 本办法由网络安全和信息化工作领导小组负责解释。

第二十六条 本办法自公布之日起实行。

郑州工程技术学院

2026 年 7 月 16 日印发