郑州轻工业大学网络安全和信息化领导小组办公室文件

郑轻大网信〔2022〕1号

郑州轻工业大学虚拟货币“挖矿”活动专项整治工作方案

为贯彻国家关于整治虚拟货币“挖矿”（以下简称“挖矿”）活动精神，落实省委省政府、省教育厅相关安排部署，有效防范处置“挖矿”活动带来的风险隐患，形成常态化的整治处置机制，特制定本方案。

一、总体要求

（一）指导思想

以习近平新时代特色社会主义思想为指导，全面贯彻党的十九大和历次全会精神，深入贯彻习近平生态文明思想和关于教育工作重要论述精神，坚定不移贯彻新发展理念。按照“严密监测、严防风险、严禁增量、压减总量”的总体思路，通力合作，加强我校“挖矿”活动集中整治，杜绝使用公共资源“挖矿”行为，助力碳达峰、碳中和目标如期实现。

（二）基本原则

坚持分级负责。学校网络安全与信息化领导小组办公室统筹指导全校“挖矿”活动整治推进工作，各单位具体负责本单位专项整治工作。

坚持统筹兼顾。将专项整治活动与提升常态化网络安全管理能力相结合，在开展“挖矿”活动全面排查整治的同时，深入落实单位网络安全责任制，突出公共信息资产管理和防护，打好整治“挖矿”活动攻坚战、持久战，巩固整治成效。

坚持分类处置。从严从重查处主动参与“挖矿”行为，形成整治高压态势；提高防御木马病毒和网络攻击能力，加强网络安全宣传教育，减少被动型“挖矿”行为。

坚持依法依规。充分运用法治思维和法制方式，严格执行有关法律法规和规章制度；严格按照国家有关部门文件要求，加强教育引导，防范化解矛盾纠纷，及时回应社会关切，确保学校稳定发展。

二、工作目标

各单位利用公共资源主动参与“挖矿”现象全面杜绝，因木马病毒或网络攻击导致的被动型“挖矿”IP 动态清零，形成“挖矿”活动常态化监测和治理机制，高质量完成省委省政府部署任务，助力我省“挖矿”整治工作逐步进入全国前列。

三、重点任务

（一）加强组织领导

各单位按照省教育厅和学校“挖矿”专项治理活动要求，认真贯彻落实。

（二）全面摸排统计

各相关单位结合前期摸排情况，对有较高计算能力的服务器、GPU 工作站等高性能计算设备在内的信息资产进行再梳理，统计信息资产部署位置、管理部门、责任人、网络标识等信息，完善单位信息资产台账。信息化管理中心负责统计互联网线路出口信息，明确本单位负责管理的 IP 地址段，加强互联网线路使用（租用）管理。

（三）提升防护能力

1.开展自查整改。对本单位的机房、高性能计算设备及个人办公设备组织开展全面自查，消除安全隐患。接到涉及“挖矿”相关通报后，要 48 小时内完成排查、锁定设备及责任人，72 小时内形成书面报告，报学校网络安全与信息化工作领导小组办公室。

2.加固网络出口。在网络出口边界部署安全设备，制定安全规则，及时更新特征库，检测、识别、阻止恶意请求行为，及时封禁恶意域名和地址。

3.监测网络流量。收集分析网络流量日志，加大“挖矿”行为监测力度，分析威胁情报，确定恶意 IP 及域名，拒绝恶意域名的解析。

4.强化终端管理。严格落实终端入网实名认证，安装防病毒软件，定期查杀病毒，阻止恶意程序横向传播。对连续

出现“挖矿”行为的终端，停止互联网接入。

5.提高溯源能力。综合分析安全日志、上网认证日志、交换机日志等网络痕迹信息，预警、查找风险主机并及时处置。

6.积极推进软件正版化工作，从源头上杜绝“挖矿”病毒传播。

（四）加强安全教育

各单位要把“挖矿”活动整治成效作为检验能力作风提升的重要内容，通过多种形式，深入开展“挖矿”活动危害性的宣传教育，提升本单位师生的防范意识。各单位负责人及相关工作人员、信息资产运维人员以及发生过“挖矿”行为的其他人员要签订《坚决抵制虚拟货币“挖矿”活动承诺书》，强化安全责任意识。

四、实施步骤

（一）部署动员阶段（2022 年 3 月 20 日前）

各二级单位对本“挖矿”整治工作开展动员部署，明确整治工作的目标、内容和标准，细化措施、压实责任。组织所属单位和人员签订《坚决抵制虚拟货币“挖矿”活动承诺书》。

（二）集中攻坚整治阶段（2022 年 3 月 25 日前）

各单位开展集中整治，对标时间节点，抓好任务落实，确保本单位主动挖矿全面杜绝，被动“挖矿”IP 坚决消减。

（三）常态化防控阶段（2022 年 3 月 26 日后）

各单位对“挖矿”活动整治工作坚决做到再巩固、再加强、再深入，针对集中整治工作中发现的问题短板，进一步完善各项规章制度，建立健全长效工作机制，巩固扩大整治成果，严防“挖矿”活动反弹。

五、保障措施

（一）压实责任。各单位校要深入贯彻落实《网络安全责任制》，摸清资产底数，细化工作台账，形成责任清单，明确责任边界，确保落实到岗、落实到人，形成“纵向到底、横向到边”的监管体系。

（二）做好保障。信息化管理中心要加紧处置专项整治期间发现的设备配置不足、技术能力不强等问题，补充配置必要的软硬件设备，组织应急处置队伍，为技术能力不足的单位及时提供指导和支持。

（三）加强协同。信息化管理中心要加强“挖矿”活动监测，定期发布“挖矿”活动预警信息，通报涉及“挖矿”活动的域名和 IP 地址，及时转发教育、公安、网信、通讯管理等部门发布的“挖矿”活动预警信息，及时通过网络安全联系机制及时上报发现的“矿池”域名和IP地址等信息。

郑州轻工业大学网络安全和信息化领导小组办公室

2022 年 3 月 17 日

郑州轻工业大学网信办　　2022 年 3 月 18 日印发