附件1

郑东新区教育系统

集中整治虚拟货币“挖矿”活动工作方案

为贯彻国家关于整治虚拟货币“挖矿”（以下简称“挖矿”）活动要求精神，落实省委省政府、市委市政府相关安排部署，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，充分发挥各级教育管理部门和各级各类学校合力，加强全区教育系统“挖矿”活动监管，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，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”活动，形成整治高压态势；提高防护木马病毒和防御网络攻击能力，加强网络安全宣传教育，减少被动型“挖矿”活动。

坚持依法依规。要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；要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，确保社会大局稳定。

二、工作目标

全区各级各类学校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，高质量完成党工委、管委会和市教育局部署任务。

三、重点任务

（一）制定工作方案

各单位按照郑东新区教文体局整治“挖矿”活动工作方案要求，制定本单位工作方案、细化整治措施。

（二）全面摸排统计

各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。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，报上级教育主管部门。

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，利用威胁情报进行分析，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”活动整治成效做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，提升全体工作人员和师生的防范意识和能力。全体工作人员、信息资产运维人员以及发生过“挖矿”行为的其他人员要与学校签订《坚决抵制虚拟货币“挖矿”活动承诺书》，强化安全责任意识。以学校为单位签订一份《坚决抵制虚拟货币“挖矿”活动承诺书》，并将盖章扫描件于4月27日下午下班前发送至zdxqjwtjbgs@126.com。

四、实施步骤

（一）部署动员

各单位召开专题会议，对本单位“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

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

（三）常态化防控

各学校对本单位“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。各单位要摸清资产底数，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。专项整治期间，要每周至少研判一次“挖矿”活动发展态势，对照工作措施进展及成效，总结经验、分析问题，及时调整政策措施，确保“挖矿”活动整治工作巩固提升。

（二）做好保障。各单位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。

（三）加强协同。郑东新区教文体局将定期发布“挖矿”活动预警信息，通报涉及“挖矿”活动的域名和IP 地址；各学校要及时上报发现的“矿池”域名和IP地址等信息。