

# 内 部 明 电

发往 见报头

签批 王巨涛  
盖章

等级：急

郑教明电〔2021〕146号

## 郑州市教育局 关于进一步加强教育系统网络与信息安全管理工作的通知

各开发区教育局，各区县（市）教育局，局直属各学校（单位），市属事业办及各民办学校：

为全面提高郑州市教育系统网络与信息安全意识，建立网络安全体系架构、安全监管体系、安全协作体系，落实国家信息安全等级保护制度，有效防范、控制和抵御信息安全风险，增强安全预警、应急处置和灾难恢复能力，形成与教育信息化发展相适应的、完备的网络与信息安全保障体系。

现就进一步加强郑州市教育系统网络与信息安全管理工作的有关问题通知如下：

（共6页）

## 一、要进一步明确工作责任

按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则开展网络与信息安全管理。市教育局统筹指导全市教育系统的网络与信息安全工作，由郑州市现代教育信息技术中心具体实施；各开发区教育局、各区县（市）教育局负责规划监督所属学校的网络与信息安全工作，各学校要将网络与信息安全责任落实到相关责任人。各单位承担所属信息系统与网络的安全管理责任。

## 二、要进一步完善工作机制

各单位要成立“网络与信息安全工作领导小组”（以下简称领导小组），由单位法人担任组长，并选拔和充实政治可靠、业务能力强、有责任心的人员具体负责本单位网络与信息安全工作。与本地政府网络与信息安全管理、公安机关、网络运维单位建立协调和事件处理机制，充分发挥纵向衔接、横向协调的组织保障作用。对于外包网络及信息服务的企业及个人必须签订相应的安全责任协议。

## 三、要进一步加强网络安全管理

（一）各单位网络管理中心机房要做好控温、防湿、稳压、接地、防雷、防火、防盗等措施，定期检查设备是否正常，保证网络及核心设备的安全稳定运行，要建立完整、规范的网络设备运行档案及账目，认真做好各项资料（配置）的记录、分类和备份妥善保存工作。确认单位自主运维服务器的相关配置信息，并有

相应的网络安全防范系统和设备，定期做好服务器漏洞扫描及安全加固，减少不必要的端口开放。

（二）连入本单位网络的所有设备必须严格使用网络管理员分配的 IP 地址，并由网络管理员对设备、使用者、场地进行准确登记备案。任何人不得擅自修改 IP 地址及网络设置，不得盗用 IP 地址及用户账号。接入网络的所有用户必须实名登记认证，使用上网行为管理设备进行管控，并按照规定留存相关的网络日志不少于六个月。

（三）各单位应保护好网络设备和线路，未经允许不准个人擅自改动网络接线，不准个人私自添加无线网络设备，如需添加必须由单位网络管理员做好相应的地址及人员使用备案，且设置强密码认证功能，不准擅自将无线密码外借。

（四）各单位要采取积极有效的措施，坚决封堵色情、暴力、封建迷信等不良信息，确保网络机房等公共上网场所文明健康的上网环境。

#### **四、要进一步加强信息系统安全管理**

（一）各单位新建信息系统需向上级教育主管部门上报，并保证安全技术措施同步规划、同步建设、同步使用。已建信息系统要按国家等级保护标准定级或整改，并到相关安全管理部门备案。对关键信息基础设施要进行重点保护，每年至少进行一次检测评估。各单位未完成安全定级及备案的信息系统不得上线运行。

（二）各单位的门户网站必须按照信息安全等级保护工作规

定，完成定级、备案等工作，定期修改网站管理密码，留存安全审查日志。建立先审核后发布工作制度，指派专人对文字和图片信息进行审核，不得发布不利于社会稳定、未成年人健康成长及易造成社会负面影响的不良信息。各单位门户网站不得链接企业网站，不得发布商业广告，不得在网页中设置或植入任何商品、商业服务的二维码。

（三）各单位对开办的网站（论坛）、微信、微博、公众号等信息发布平台，要按规定进行备案，并制订专门的管理办法。各单位要加强因工作和教学需要通过网络建立的各类交流群、社区、圈子的使用管理，要明确责任人，制定值守制度，做好舆情的引导与监督。

（四）各单位自建或通过其它方式使用的云服务、大数据应用等信息系统，应优先考虑各类数据信息的安全，对掌握的教育信息及相关数据，未经教育部门审批，不得用于商业用途。信息系统中提供有交流功能的论坛、社区、圈子等必须设置严格管理制度并有专人管理。

## **五、要进一步加强数据信息安全管理**

（一）各单位和从事网络系统运行维护的单位在教育管理活动中收集、使用个人电子信息，应当遵循合法、正当、必要的原则，明示收集或使用信息的目的、方式和范围，并建立信息收集、处理及其相关活动的工作流程和管理制度。各单位和从事网络服务的单位应对掌握的个人电子信息严格保密，不得以电子表格、

文档等形式随意上报、发布学生的姓名、出生日期、身份证件号码、个人生物识别信息、家庭住址、电话号码等个人信息，不得泄露、篡改、毁损、出售或者非法向他人提供个人电子信息。其它有关单位和个人提取学生个人电子信息应严格履行审批手续。

（二）各单位各类信息系统中开设的账户和密码为个人用户所拥有，不得向任何单位和个人提供。校园局域网内的平台系统、应用工具及信息数据要实施保密措施。

（三）各单位使用“国家教育资源公共服务平台”、“郑州基础教育资源公共服务平台”等各类教育行政部门统一建设或使用平台的管理员账户、密码需要进行妥善保管，且初始密码必须进行修改。管理人员使用平台必须注意必要的设备安全防护以及重要信息数据的保护，谨防数据、密码、地址类信息的外泄。

## 六、要进一步加强个人用户安全规范

（一）各单位必须确保每台计算机上安装防病毒软件，切实做好防病毒措施及补丁安装，随时注意杀毒软件是否开启，及时在线升级杀毒软件更新系统补丁，及时向网络管理员报告计算机病毒感染、非法访问、可疑应用等异常情况。

（二）各单位的计算机网络用户禁止删除或卸载单位指定、统一安装的杀毒软件和系统管理类软件以及计算机的相关设置，不使用盗版软件，不允许安装与教育教学无关的游戏、股票、娱乐等应用程序，不允许使用计算机进行与工作无关的操作。

（三）严禁使用来历不明、容易引发病毒传染的软件或文件；

对于外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行查杀毒。

（四）手机、平板电脑、笔记本电脑等移动设备应做好相应的网络接入认证工作，建立相应准入制度，做好个人手机应用的安全应用及防护培训，针对单位公共使用的平板电脑或终端设备做好定期安全扫描及病毒防护检查。

（五）各单位要加强师生使用学校空间、班级空间、教师空间、个人空间的数据信息安全管理。

## **七、要做好网络与信息安全的应急处置**

（一）各单位应制订网络与信息安全应急预案，建立网络与信息安全事件处置和报告制度，并报上级教育信息安全管理部門备案，明确应急处置流程和权限，落实应急处置技术支撑队伍，并定期组织演练，提高网络与信息安全应急处置能力。

（二）郑州市教育局统一建立“郑州教育网络应用安全监测预警通报平台”，对郑州教育城域网开展安全监测及监督检查等监管工作。郑州市教育局将根据网络安全事件分类分级标准，对涉事单位、相关责任人采取通报批评、切断网络、关停系统等处置。

（三）各单位对网信、公安等相关部门依法实施的监督检查应当予以配合，对反馈的问题要及时处理并上报，对出现问题造成严重影响或拒不整改的单位和个人将依规依法处置。

2021年3月25日