秘 密

河南省教育厅

教科技〔2019〕535号

河南省教育厅
关于做好庆祝中华人民共和国成立70周年网络安全保障工作的通知

各省辖市、省直管县（市）教育局，各高等学校，厅机关各处室，厅直各单位（学校），省教育科研计算机网网络中心：

庆祝中华人民共和国成立70周年（以下简称国庆70周年），是党和国家政治生活中的一件大事，确保大庆活动期间网络安全，对于庆祝活动顺利举行至关重要。根据省委网信办和教育部部署和要求，现将做好国庆70周年网络安全保障工作事项通知如下：

一、总体要求

各地各单位要充分认清做好国庆70周年网络安全保障的

重要性，增强“四个意识”，坚定“四个自信”，做到“两个维护”，深入贯彻习近平总书记关于网络安全的重要指示精神，严格落实《中华人民共和国网络安全法》等有关法律法规和政策性文件，从党和国家事业全局出发，站在维护我国政治安全和国家安全的高度，以对党和人民高度负责的态度，认真落实党委（党组）网络安全主体责任，建立“主要负责人亲自抓、分管负责人具体抓”的领导责任制，坚决防范网络安全重大风险，坚决遏制网络安全重大事故。要突出问题导向，强化依法治网，全面从严管理，落实安全责任，不折不扣地落实好重要时期网络安全保障工作，为国庆70周年营造安全的网络环境。

二、工作任务

（一）全面排查问题隐患，强化事件预防措施

1.深入开展网络安全自查。各地、各单位要开展一次全面的网络安全自查评估，深入查找问题隐患，及时整改加固。核清弄准信息系统（网站、移动类应用）底数，加强重要信息系统排查和安全防护。重点加强对系统和业务间以及系统之间的关联风险评估，严防发生连锁连片式网络安全事故，避免“一点突破、全网皆失”。要高度关注教育、网信、公安、工信、通信管理等部门和有关单位发布的风险预警，在规定时限内做好问题排查和漏洞修补，并按要求反馈处置情况。对检查、评估、监测、检测中发现的和有关部门通报的各类问题隐患，整

改后逐一复查，确保问题彻底解决，不留后患。

2.扎实做好基础预防措施。各地、各单位应重点排查“双非”（非本单位IP地址、非本单位域名）信息系统（网站）和使用频率低、长期未更新、无专人运维的“僵尸”信息系统（网站），对常见的低级错误“零容忍”，坚决杜绝弱口令、默认口令、通用口令、长期不变口令，坚决防止出现高危漏洞不修复、非必要端口及服务长期开启、陈旧版本基础软件和通用软件不更新、“僵尸”主机和系统不整改等问题，关闭或删除不必要的应用、端口和链接。确需对系统进行远程维护，或需远程登录后台管理系统的，要采取白名单、按需审批开放等方式严格访问控制。限制账户尝试登录次数，防范暴力破解账号。缩减互联网出入口和无线接入点。

（二）切实提高风险防范能力，加强网络威胁应对

各地各单位要及早研判国庆70周年重大网络安全威胁风险，有针对性地采取措施，防范敌对势力、网络黑客攻击滋扰。

1.防范邮件攻击。要加固邮件服务器，严格安全策略配置；严格审计邮件访问行为，认真核查异常地址、异常时段登陆和批量下载邮件情况。关闭政务邮件系统自动转发功能。加强工作人员邮件安全意识教育，定期更换密码，提高对钓鱼邮件、仿冒邮件的辨识能力，及时删除离职人员账号。

2.防范勒索病毒入侵。要加强业务系统安全防护能力，严格执行内网、专网设备和系统的补丁升级和漏洞修复措施，关

闭主机和终端上不必要的端口、共享访问以及远程桌面连接，安装并及时升级杀毒软件，避免勒索病毒、挖矿病毒等恶意代码攻击造成业务服务中断。定期对重要数据进行备份，防止勒索病毒破坏。

3.防范数据被窃取。要采取数据分类、备份、加密等措施，加强对个人信息和重要数据的保护。采用的密码技术和产品应符合国家管理政策要求。严格数据访问授权，存储重要数据和大量个人信息的数据库接入互联网应采取严格安全防范措施。加强日志记录和日常审计，及时发现处置非授权访问、大流量数据异常外传等情况。

4.防范网站攻击篡改。要监测网站访问情况，定时扫描页面、文件、链接，及时发现和处置页面被篡改、域名被劫持、被插入暗链和跳转代码等安全事件。加强与 CDN 服务提供商、基础电信运营企业的协调联动，防范抵御大规模拒绝服务攻击。

5.防范 LED 屏幕内容篡改。对公共区域的 LED 屏幕，要明确专人负责。避免使用远程和无线方式管理，确需使用的要采用高强度密码。有条件的单位应配备播放内容监控设备，及时屏蔽非法内容。

6.防范供应链安全风险。加强新安装软件来源的审核验证，避免从非官方渠道安装程序或更新程序。强化对第三方服务企业、机构和人员的管理要求，防止其将系统架构、软件源

码、内部数据上传至互联网。

（三）不断提升应急处置能力，保障网络平稳运行

1.加强应急基础性工作。及时修订完善网络安全事件应急预案，明确处置应对责任机构、指挥机制、响应流程，组织开展以事件处置为核心的应急演练或模拟推演。明确应急技术支撑队伍及职责任务、响应时限等方面的要求。

2.加强监测预警和应急准备。各地各单位要完善本地、行业和单位网络安全监测预警和通报体系，加强应急值守，保持联络畅通。发生安全事件或发现网络安全隐患时，按照应急预案及时开展响应处置和应对准备。发生重大安全事件时，按程序及时报告有关情况，并加强舆情应对。

三、工作要求

（一）周密研究部署。各地、各单位要迅速召开专门会议，研究部署国庆70周年网络安全保障工作，将网络安全责任落实到岗、落实到人，做到领导到位、人员到位、责任到位、措施到位，确保网络安全保障工作落到实处。

（二）按需调整策略。各单位在对信息系统运行情况研判基础上，建立“白名单”、“灰名单”制度。对单位主管的信息系统（网站），应在确保安全隐患清零后方可上线运行。原则上单位门户网站、电子邮件系统和重要对外服务网站在做好重点防护基础上，保障访问畅通。对国庆期间无重要业务加载、无专人运维的信息系统（网站），可采取互联网访问控制措施。

（三）做好应急值守。各单位在国庆期间应严格执行7×24小时值守和领导带班制度，保持通讯联络畅通。网络安全职能部门人员信息发生变更应及时登录教育系统网络安全管理平台（https://xxaq.moe.edu.cn）进行更新。发生网络安全事件，应按照《信息技术安全事件报告与处置流程（试行）》的要求，立即通告省教育厅24小时值守电话，并采取果断措施，将负面影响降到最低。

（四）强化督查检查。省教育厅将会同有关部门加强督促检查，确保网络安全保障工作落到实处。对管理责任落实不到位、服务保障不力的，严肃通报；对工作中存在失职、渎职行为、造成严重后果的，依法依规严肃问责。

联系人：科学技术与信息化处　麦世奎

电话：0371—69691767　手机：18037199909

省教育信息安全监测中心24小时值守电话：0371—67763189

河南省教育厅

2019年7月29日

河南省教育厅办公室　　2019年7月30日印发