吉 林 省 教 育 厅

关于进一步做好重要时期网络安全保障工作的通知

各市（州）教育局，长白山管委会教育科技局，梅河口市教育局，各省属高校、各民办高校（含独立学院）:

根据教育部、省委网信办关于做好党的二十大网络安全保障工作的有关通知要求，为进一步强化重要时期的工作部署，防范化解全省教育系统网络安全风险隐患，现将有关事宜通知如下。

一、加强重要时期的组织领导。主要负责同志要组织对党的二十大网络安全保障进行再研究、再审视、再部署，以最高标准、最严要求、最周密措施全力以赴做好各项工作。网络安全分管负责同志要抓好具体落实，进一步明确工作职责，突出工作重点，坚持问题导向，查部署工作情况、主体责任是否落实到位，查落实任务情况、执行要求是否从严从紧，查监督检查情况、安全隐患是否整改清零，做到领导到位、责任到位、人员到位、经费到位和措施到位。

二、加强计算机恶意程序防范处置。计算机及信息系统必须安装杀毒软件，定期扫描系统、查杀病毒。移动存储设备要专人

管理，使用前进行病毒查杀。重点防范僵尸木马程序。禁止点击不明来源的电子邮件及其附件，禁止点击不明网页链接，禁止下载不明来历软件等。

三、排查信息系统（网站）安全隐患。进一步梳理本单位、本地区的信息系统（网站）情况，将网络开发建设、运营维护、服务保障等第三方供应链纳入管理范畴，登录教育系统网络安全工作管理平台（网址：https://xxaq.moe.edu.cn）更新信息资产名录。对安全监测、攻防演习、安全检查等环节发现的安全问题进行逐一整改、复测、销账；清理非本单位域名和IP地址的双非网站，内容长期不更新、长期无人运维的僵尸网站和测试网站。对本单位的信息系统（网站）进行安全风险研判，综合考虑系统安全情况和业务必要性，采取不同访问策略，保障信息系统（网站）合法合规运行，杜绝“带病”运行。

四、提升重要对象网络安全保障水平。各单位应完善网络安全防护手段，构筑网络安全综合防控体系，保障重要对象的高标准安全运行。智慧教育平台、资源平台和重要对外服务网站应运用云防护、CDN等技术确保系统访问流畅，提高抗DDoS攻击的能力；门户网站、内容管理系统、公共展示屏应严格落实内容审核制度，提高防页面篡改的能力；教务系统、办公系统、视频会议系统等涉及面广的管理系统应强化业务连续性，提高防业务瘫

痪能力。电子邮箱系统、即时通讯工具应强化账号管理，提高防垃圾信息和防钓鱼攻击能力。

五、强化数据安全保护能力。各单位应开展数据分类分级工作，摸清重要数据底数。严格落实数据安全主体责任，规范技术服务外包活动的数据安全责任，对接触重要数据的技术服务商和项目人员进行备案，签署数据保密协议。面向本单位、本地区开展数据安全风险排查，聚焦国家和教育系统关键信息基础设施，对数据全生命周期中存在的安全隐患进行排查整改，特别是超职能范围采集业务数据、违规使用个人信息、数据技术服务外包、供应链风险等方面的问题，建立问题台账，防范化解数据安全风险隐患。

六、健全网络安全应急值守工作机制。各单位应严格实行领导带班和 7x24 小时值班制度，保持通讯联络畅通，重点对象应逐个信息系统（网站）制定应急预案。强化与电信运营商、运维厂商、安全服务厂商和供应链厂商的协调配合，做好应急响应准备，确保第一时间发现、处置和报告网络安全突发情况。10 月 1 日至 10 月 24 日是党的二十大重要保障时期，各单位实行“零报告“制度，每日 13 时前向省教育厅网信办报送前 24 小时网络安全工作情况。发生网络安全事件，应按照《吉林省教育系统网络安全事件报告和处置流程》要求，第一时间进行应急报告，并采

取有效措施将负面影响降到最低，严防形成负面炒作，2日内完成处置并反馈处置结果。因客观因素确实无法第一时间完成整改的，需说明情况并报送后续处置工作计划。

各单位应严格落实各项工作任务，网络安全隐患要在9月30日前彻底清零。

省教育厅网信办24小时值守电话：王成 13341411556

吉林省教育厅

2022年9月26日