关于进一步加强全国“两会”期间

网络安全保障工作部署的通知

各部门：
   根据教育部、市委网信办、市公安局、市教育系统网络安全和信息化工作领导小组关于进一步加强全国“两会”期间网络安全保障工作部署的通知安排， 2025年3月3日0时至14日24时学院将启动“两会”重保工作，现将有关要求通知如下：

一、加强组织领导，履行工作职责

各部门要充分认识“两会”网络安全保障工作的敏感性、重要性和紧迫性，按照“谁运维谁负责、谁使用谁负责、谁发布谁负责”的原则，夯实网络安全责任，筑牢网络安全防线，高度警惕和严密防范网络攻击，坚决防范重大网络安全风险，坚决遏制重大网络安全事故，全力做好网络安全保障工作。

二、深入排查风险，全面整改隐患

（一）强化资产排查，明确安全责任。各部门要认真梳理本部门重要系统和资产清单，摸清底数，明确各项网络资产责任人。重点加强与全国“两会”直接相关、包含大量敏感信息和个人隐私信息、直接影响党政机关运转和公共生活工作的的关键业务系统梳理。重点加强电子屏梳理及风险评估，强化安全防护措施，突出重点、不留空白，做到点面结合、立体防御。

（二）开展系统自查，排查风险隐患。各部门会同运维公司3月2日前认真开展信息系统及资产的网络安全隐患排查工作，及时完成漏洞整改。重点加强对学校网站、电子显示屏、校园论坛等信息发布系统的安全排查，杜绝发生内容篡改、插播反标、虚假煽动性言论等安全事件。

三、加强安全监测，做好应急处突

重保期间，各部门扎实做好应急处置工作，完善应急预案，加强监测值守，强化应急保障，全力做好全国“两会”特别是直播时段重要网络系统安全防护。根据实际使用情况，对学院基础网络、信息系统和信息化设备执行分级管控，具体如下：

（一）基础网络要求

信息化办公室开展网络安全值守，严格7\*24小时实时监控，加强技术支撑和巡检检测，强化安全防护措施，坚决防止发生网络安全事件。

（二）信息系统要求

重要三级系统（北京教师学习网、电子邮件），因系统重要性和使用需求无需关闭，应做好7\*24小时专人值守，加强实时监测预警；

政务云二级系统（学院主页、继续教育管理系统、教育科研创新服务平台），经与宣传部、教务处、科研处沟通，系统于每天8:00 - 20:00开放，其余时间关闭所有访问；

院内存放的一级系统原则上在工作时间开放，其余时间关闭访问，如工作时间外有业务使用需求的系统，严格落实“白名单”管理（详见附件），于3月2日16时前向学院信息化办公室报备，列入“白名单”管理的信息系统务必安排专人值守。

学院各信息系统、公众号严格信息发布，强化正面宣传和舆论引导，确保信息发布的准确性和权威性，杜绝出现因信息内容事件引发负面舆情等情况。

（三）信息化设备要求

重保期间，所有公共区域联网电子屏和各校区联网打印机，原则上要求做到断网关闭，如需使用务必安排专人值守。

四、加强宣传，提高意识

各部门应加强教职工和服务人员的网络安全教育，依法依规使用网络，加强微信和企业微信工作联络群的内容管理，做好个人办公电脑的安全管理，定期杀毒，高度警惕钓鱼事件的发生。

在“两会”重保期间，每日14 时由信息化办公室向市教委进行“零报告”反馈。各部门一旦发生网络安全事件时，应立即启动应急响应流程，第一时间报告并按照应急预案开展响应处置，及时联系信息化办公室。

联系人：宋慧波
联系电话：13651266120

                                        信息化办公室
                                        2025年2月28日

附件

**北京教育学院**

**信息系统“白名单”管理审批表**

部门： 申请日期：

|  |  |
| --- | --- |
| 系统名称 |  |
| 开放时间 |  年 月 日 ——— 年 月 日 |
| 申请理由：*示例：本系统由于......原因在重保期无法关闭，本部门承诺在此期间做好网络安全值守工作，若发生安全事件可做到第一时间发现、报告及处置。* |
| 系统管理员签字： |
| 部门负责人意见： |
| 主管院领导意见： |