北京市教育委员会

京教函〔2017〕424号

北京市教育委员会关于
做好近期网络安全工作的通知

各区教委、各市属高校、市教委有关直属单位:

为深入学习贯彻《网络安全法》，落实国家及北京市关于网络安全的各项要求，进一步提高网络安全意识，健全安全保障体系，促进教育行业网络安全稳定，根据教育部及市委市政府统一部署安排，现就做好近期北京市教育行业网络安全工作的有关事项通知如下:

一、加强组织领导，落实领导责任

各区教委、各单位要进一步增强政治意识、大局意识、责任意识，深刻认识网络安全工作的重要性和紧迫性，把网络安全当成近期工作的首要任务来抓，摆在突出位置，采取有效措施，纳入重要议事日程予以部署，严标准、硬质量、高效率完成各项工作任务。各区教委负责本区内各类中小学等教育单位网络安全工作任务的全面落实。

各区教委、各单位要高度重视并加强对网络安全工作的组织领导，单位主要负责人是网络安全工作的第一责任人，要亲自部署，切实明确牵头部门和责任人，务必确保各项工作落到实处，从根本上为做好网络安全提供组织保障。按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则，强化技术防范措施，坚决防止各类网络安全事件的发生。要切实做到领导到位、人员到位、责任到位、措施到位。对不能按时保质完成工作的，将按照《网络安全法》的相关规定予以处理。

二、全面清理普查，整合信息系统

（一）开展信息系统（网站）普查

1.进一步梳理本单位所属信息系统（网站）情况，明确 10 月底前必须开放的系统，并将其名称及概况（参见附件）于 9 月 25 日前上报市教委。建议除门户网站和重要的对外服务信息系统（网站）外，其他系统可采取限制互联网访问的措施。

2.各单位及其所属单位的信息系统（网站）基本信息（域名和 IP 地址，后同）须在指定的管理平台中完成报送工作。其中：

各区教委登录教育行业信息资产管理平台，录入本单位及其所属事业单位、高中阶段教育（包括高中、中职）、义务教育阶段（中小学）、学前教育阶段（幼儿园）的信息系统（网站）基本信息。9 月 22 日前完成区级教育行政部门及其直属单位的信息系统（网站）基本信息录入工作；9 月 29 日前完成区级教育行政部门所属学校的信息系统（网站）基本信息录入工作。

各市教委直属单位登录教育行业信息资产管理平台，9月20日前录入本单位信息系统（网站）基本信息。

各市属高校登录教育行业ip地址数据库系统（ipdb），9月20日前录入本单位的信息系统（网站）基本信息。

（二）清理“僵尸”信息系统

1.各单位在信息系统自查的基础上，系统分析本单位信息系统（网站）的运行情况，并组织所属单位对“僵尸”信息系统进行排查。

2.重点清理涉及以下条件的系统：对存在安全威胁长期不修复的信息系统；所占用资源长期处于空闲状态；运行维护停止更新服务；系统使用与实际业务流程长期脱节的；网站年访问量在1000人次以下；网站长期180天以上未更新；系统每年录入的信息在100条以下；专题网站已完成工作使命；网站系统无人运维或运维缺乏基本保障。

3.以清理“僵尸”信息系统为契机，着力解决信息系统小散乱问题。专题工作网站应纳入网站群管理，在完成专题工作或非专题工作期间，应下线处理；对内部信息系统（办公、财务、人事等）进行整合，避免互联网访问，确有需求可通过VPN的方式进行访问。

（三）加强信息系统（网站）域名和IP地址管理

1. 建立IP地址和域名审核机制，加强信息系统（网站）的集中管理。各单位应组织技术力量对本单位的“双非”信息系统

进行调查。

2.“双非”信息系统的认定标准以信息系统（网站）普查上报数据为准，以 IP 地址和域名为依据，形成本单位信息系统的清单。对非本单位的“双非”信息系统（网站）进行清理，采取停止服务、限制访问或纳入统一管理等措施，及时消除安全隐患。对于确有需要独立运行的，应明确安全责任，签订安全承诺书。

3.各单位可根据网络搜索结果，对“双非”信息系统的性质进行确认。对于钓鱼网站和仿冒网站，通过中国互联网违法和不良信息举报中心（www.12377.cn）提交举报。

各区教委负责指导、监督本地区中小学等教育单位网络安全工作，做好信息系统（网站）基本信息报送及“僵尸”信息系统清理，组织技术力量对本地区教育机构的 “双非”信息系统进行调查，根据网络搜索结果，对“双非”信息系统的性质进行确认。以上工作务必在 9 月 28 日前逐项落实完成。

三、集中排查梳理，加强防护措施

（一）加强基础网络的防护措施

1.梳理本单位互联网出口。控制互联网接入点的数量；对无线热点进行集中排查，办公区原则上必须使用具有身份认证功能的 WIFI 热点；禁用无授权、无安全措施的无线热点，无线密码不得使用弱口令，且不得共享到互联网和 APP。

2.梳理网络架构及网络层安全策略。对核心系统和核心数据采取分区分域措施；优化网络安全访问策略，限制潜在攻击来源

访问；通过网络设备与安全设备相结合的方式进行区域边界安全隔离，防火墙须采用白名单机制，按需开放策略，实现端口级访问控制，应用安全防护设备需根据重要信息系统（网站）业务需求，按照最小化原则进行安全策略设置。

（二）加强重点网站的防护措施

1.保障重要时期重点网站的正常访问，提高抗分布式拒绝服务供给能力。可采用与运营商、安全服务商购买流量清洗服务或部署抗分布式拒绝服务攻击设备的方式进行防御。

2.建议各单位采取“前台静态呈现，前后台分离部署”的防护策略。对重点网站的系统架构进行梳理与优化，加强后台管理系统的防护。重点时期，单位首页可关闭动态服务。

3.从严控制新增栏目和功能。针对新上线的栏目及功能，需委托具备信息安全评估资质的专业机构进行安全评估，确认整改完成后方可上线运行。重点时期，建议暂时停止系统变更。

（三）加强重要信息系统（网站）的防护措施

1.加强账户管理。对重要信息系统（网站）进行资产与账户进行排查，清理非在岗人员账户，加强口令强度，有条件的单位可以采用双因素认证等其它安全模式进行高强度用户认证。

2.加强数据防护。重要信息系统（网站）应建立独立的数据库实例，根据业务需求制定数据离线保存策略，做好数据离线保存及数据转移工作。针对各信息系统数据库实例设置最小权限的管理账户，加强对重要信息系统非授权访问行为的安全审计。

四、专项重点监测，提高评估水平

各单位应对所属信息系统（网站）进行检测，专项检测后门木马、排除非法暗链，要对涉及 Struts2 的系统网站进行重点排查，及时消除安全威胁。

开展关键信息基础设施安全评估工作，包括业务系统自身安全评估和承载重要业务系统的基础环境的安全评估工作，排查薄弱环节，重点检查系统间、业务间关联风险，确保重要信息系统（网站）不被其它系统影响。

五、健全值守制度，完善应急机制

（一）健全网络安全事件应急响应机制

各单位可参考《北京市网络与信息安全事件应急预案》和《教育行业网络安全事件应急预案》有关规定和要求，研究制定网络安全应急预案，加强应急处置队伍建设，建立安全事件分级响应、跨部门协同处置的工作机制。组织开展应急演练，完善本单位应急报告及处置流程。

（二）网络安全值守工作

各单位要确保重点时期网络安全应急值守工作，务必做到 7*24 小时在岗值班，保证网络安全工作渠道畅通，相关工作人员要进一步增强网络安全保卫工作的责任感，认真做好信息核实上报传达落实，切实增强信息报送的时效性、规范性，强化突发事件和突出情况的收集、分析研判和报送，对影响较大的突发事件，要立即向主管部门上报，不得迟报、谎报、漏报和瞒报。

（三）零报告制度

10月8日至10月27日期间，各单位每日下午4点前将当日的网络安全情况，以邮件方式报北京市教委xxbs@bjedu.gov.cn。对于影响较大的突发事件，要做到电话口头报告不晚于接报后10分钟，书面报告不晚于接报后1小时，详细信息报告不晚于事件发生后2小时。暂时无法判明性质或等级的突发事件，应在接报后30分钟内报告。

联 系 人：徐晶

联系电话：66074926

地　　址：北京市西城区前门西大街109号516室

附件：北京市教育行业近期对外服务信息系统（网站）清单

北京市教育委员会

2017年9月14日

附件

北京市教育行业近期对外服务信息系统（网站）清单

单位名称（盖章）：

网络安全责任部门：			责任部门负责人及联系方式：			网络安全联系人及联系方式：		
序号	信息系统（含网站）	信息系统（含网站）基本情况	ICP 备案情况	定级备案	建设整改	等级测评	信息系统服务信息	信息系统运维情况
1		备注：1.确定有开放对外服务信息系统（网站）的单位，请登录邮箱(用户名:bjjwxxzx@sina.com，密码:xxzx@2016）下载清单详细版本； 2.没有开放对外服务信息系统（网站）的单位，仅填写责任部门、负责人及网络安全联系人； 3.各单位需将清单加盖单位公章，于 9 月 25 日前送北京市教委。					
2								
3								
4								
5								