北京市教育委员会

北京市教育委员会
关于开展2019年网络安全自查工作的通知

各市属高校、直属单位:

为全面贯彻落实《2019年公安机关网络安全执法检查工作方案》文件精神，根据市公安局《关于开展2019年网络安全自查工作通知》要求，北京教育系统于2019年5月20日至6月20日期间，全面开展网络安全自查工作。现将有关事项通知如下:

一、目标任务

认真贯彻网络安全自查工作要求，落实党委（党组）网络安全主体责任，加强组织领导，明确责任分工，抓好工作落实，通过严格自查，切实摸清底数，封堵安全漏洞，排除安全隐患，确保2019年本单位网络安全。

二、自查方式及内容

制定本单位网络安全自查工作实施方案，重点开展6个方面情况自查：积极落实网络安全主体责任情况；年度网络安全工作要点制定情况；年度等级保护制度落实情况；网站、信息系统运营使用基本情况、运营使用安全工作情况；信息系统、重要数据及公民个人信息底数和安全保护情况；年度网络安全工作成绩和存在问题，下一步工作计划。

自查期间，市教委将组织技术力量对直属单位、市属高

校的网站、互联网信息系统、移动 APP、互联网数据库等系统开展远程技术检测和渗透测试，查找网络安全漏洞和隐患，提出网络安全工作整改要求。

三、重点报送内容

（一）各单位网络安全责任制落实情况。

（二）单位信息系统基本情况、运营使用情况，网站基本情况、联网信息情况，网络安全工作情况。

（三）重要数据和公民个人信息底数情况。

（四）工作总结。主要包括自查工作开展情况，网络安全等级保护和信息通报、值班值守“零报告”制度落实情况，国庆 70 周年网络安全保卫工作组织筹备情况，当前网络安全存在的问题及下一步工作打算。

四、材料报送方式

（一）报送材料类目。本单位《2019 年公安机关网络安全执法检查自查表》、年度自查工作总结、《信息安全承诺书》（需签字加盖公章）。

（二）报送时限及方式。6 月 10 日前，各单位将报送材料电子版发市教委邮箱 xxbs@jw.beijing.gov.cn。

（三）自查工具说明。各单位需统一使用公安部指定的自查工具填报网络安全自查情况（自查工作总结上传至自查软件）。完成填报后，导出自查结果数据包（扩展名为.sez，默认加密存储）报送。自查工具可生成 word 版《2019 年公安机关网络安全执法检查自查表》。

可通过访问“中国网络安全等级保护网”（www.djbh.net）下载自查工具包、安装及使用说明。

五、相关工作要求

（一）高度重视，加强领导。请将此次自查工作向本单位主要领导汇报，并成立单位领导挂帅的自查工作领导小组，统筹部署和检查督促自查工作。要制定具体的自查工作实施方案，明确任务分工，落实各项保障，确保自查工作顺利开展。

（二）加强沟通，密切配合。各单位应加强与公安机关和网络安全部门的沟通协调，及时反馈自查工作中遇到的问题，同时加强值班值守，落实应急预案和重大突发事件应急处置措施，确保网络安全工作制度落到实处。

（三）提高认识，推进落实。各单位要严格按照《网络安全法》和国家网络安全等级保护制度要求，认真组织开展网络安全等级保护定级备案、等级测评和安全建设等重点工作，不断提高网络安全管理水平和技术防护能力。本次自查将纳入“平安北京”网络安全保障考核，请各单位务必加大工作力度，切实开展好自查工作。

联系人及联系方式：

张如双（信息化处）51994994，13366607922

徐　晶（信息中心）66074926，13811661785

附件：网络与信息安全责任承诺书

北京市教育委员会

2019 年 5 月 17 日

附件 1

网络与信息安全责任承诺书

为进一步明确网络与信息安全责任，确保我单位网络与信息系统安全、稳定运行，依据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）、《北京市信息化促进条例》《信息安全等级保护管理办法》（公通字[2007]43号）等法律及文件精神，我单位郑重承诺严格落实以下工作并承担相关责任:

一、按照“谁主管，谁负责；谁运营，谁负责”的原则，法人代表为第一责任人，逐级落实网络与信息安全责任制，并为网络安全提供必要的人员和经费保障。

二、明确本单位网络与信息安全工作职责和任务，加强组织领导，明确职责任务，将网络与信息安全职责层层分解、落实到具体部门、具体岗位和具体人员。

三、主动配合公安机关的监督、检查和指导，对本单位建设、运营、使用的网络与信息系统开展定级、备案、安全建设整改及等级测评工作。

四、依据国家有关规定和标准，落实网络安全等级保护管理制度和技术防护措施，及时查找本单位安全隐患和漏洞，对薄弱环节和潜在威胁采取措施进行整改，确保网络与信息系统运行安全、数据安全。

五、按照北京市突发公共事件应急委员会印发的《北京市网络与信息安全事件应急处置预案》要求，与公安机关建立信息网络安全事件（事故）发现、报告、处置等工作机制，开展对本单位网络与信息系统的实时监测工作，留存相关日志，及时向公安机关上报本单位出现的网络与信息安全事件。

六、制定本单位网络与信息安全应急预案，明确应急处置流程，加强应急队伍建设、物资储备、人员培训和应急值守工作，定期组织开展应急演练，发生网络与信息安全事件后立即启动应急预案进行快速妥善处置。

七、认真执行国家和北京市其他网络与信息安全工作要求的工作事项，如发生网络与信息系统安全问题，造成损失和影响的，自愿承担相关责任。

承诺单位（盖章）：

法人或负责人（签字）：

二〇　　年　　月　　日