巩固网络安全，助力教育发展

朝阳教育系统网络安全办公室

各位领导、各位同志们，上午好：

朝阳教育系统网络安全工作，在网络安全形势依然严峻，境外攻击持续不断，教育行业网络安全事件频发的情况下，2018-2019学年度年朝阳教育系统实现了网络安全零事故，在北京市教育行业网络安全综合整治检查、区委网信办2019年护网行动检查中，由于各项管理制度齐备，领导重视程度和责任落实到实处，应急保障完善，材料文档齐备，受到领导、专家们的一致肯定。成绩的取得主要来源于：

一、教工委、教委领导将网络安全放在信息化工作的首位，统筹规划、监督管理网络安全工作，落实上级各项关于网络安全的工作要求。

二、各单位严格遵守与教委签订的《网络安全承诺书》内容，加强自身建设，加强问题整改，重点时期按要求值守，按时零报告。

三、网络安全办公室牢记使命，落实守土有责、守土负责、守土尽责的要求，确保制度落地。加强网络安全监控、防控，指导学校排查整改问题（其中下校协助学校整改30余次），开展网络安全宣贯（每年429首都网络安全宣传日、国家网络安全宣传周期间，都举办各种宣传活动），加快人才队伍建设培养（目前朝阳教育系统内已有58名老师取得专业网络安全认证）。

朝阳教育系统网络安全工作取得了一定成效，我们清醒的看到真正的考验还在路上，2019年重大活动多，是大事喜事之年，网络安全工作尤其重要，当前，国内外网络攻击现象频繁，大有向教育行业蔓延的趋势，（ 7月底，江苏南通某中学官网，被黑客攻击并加入了涉黄的违法有害信息，直到警方上门，学校还浑然不觉，完全没发现自己学校的网站被黑了，由于没有履行法律规定的安全保护义务，涉事中学被罚款三万元，直接责任人也被罚款一万元），反共黑客活动猖獗，每三天攻破一次国内网站，其中涉及教育行业的17次，北京地区10次。

朝阳教育系统也面临着风险考验，据统计，2019年共监测境外严重攻击860次；信息中心2019年向教育单位下发安全漏洞安全整改函27件；通过日常巡检发现，下发了79件安全问题整改函；对551个存在风险的IP外部地址进行了访问限制。

朝阳教育系统还存在一些网络安全隐患，需要我们重视：

一、双非僵尸网站清理不彻底

去年一年网络安全办公室共清理14个双非僵尸网站。例如：某幼儿园网站，购买公网域名到期后，未采取措施及时注销，被篡改为赌博网站，受到区委网信办通告。

1. 安全设置简单，存在弱密码弱口令。

部分单位口令设置为初始密码或简单密码，比如：123456、ADMIN、或连续字符、连续数字，从未进行修改，易被猜测攻击。

1. 应用系统漏洞补丁升级不及时，中间件版本过低。

在中心日常巡检发现的安全问题中，大部分为此类现象，易被不法分子利用，造成保密性、完整性、可用性下降。

四、IP管理存在风险

个别学校对IP管理不严格，存在一个IP对应多台电脑情况，出现问题无法溯源、追责。

为切实做好朝阳区教育系统网络安全工作，防范网络安全风险、遏制网络安全事故，各单位应做到：

1. 高度重视，落实主体责任、监督责任

中央印发的《党委（党组）网络安全工作责任制实施办法》，明确了党委（党组）的主体责任、领导班子主要负责人的第一责任，主管网络安全的领导班子成员的直接责任，同时也明确了责任追究的具体形式，各单位应严格落实网络安全工作责任制，健全完善本单位各项网络安全工作制度，做到领导到位、人员到位、责任到位、措施到位。（2019年朝阳区教育系统网络安全承诺书，我们将随同会议材料放到中心网站上，请各单位按要求签订）

二、提升意识，提高能力，准确把握网络意识形态

加强网络安全宣贯，进一步提升网络意识形态管理、网络舆情处置和网络安全工作的业务能力和专业化水平。

网络安全的攻防较量时刻都在发生，潜在的风险隐患不容忽视。网络舆情存在内容发布快、传播快；影响持续时间长；涉及话题议题点更多、面更广。突发敏感舆情易被别有用心之人加工利用。意识形态渗透通常潜伏于网络舆情中；自媒体平台越来越成为新闻媒体采编的重要信息源等特点，这些风险挑战给我们的网络意识形态管理、网络舆情监测处置和网络安全工作敲响了警钟。这就要求我们要以更严格的标准和更实在的举措，守住底线，奋力完成好各项工作任务。

三、完善制度，梳理底数，消除隐患

1、对本单位的网络安全管理体系、管理制度进行完善，加强对本单位教职员工开展网络安全宣传、网络安全教育活动，规范教职工上网行为（包括不翻墙、不浏览不良网站、不下载与教育教学无关内容、根据网络安全法要求，朝阳教育系统将严格实名上网，对出现问题的行为将给予追责），提高认识，增强紧迫感，全面提高网络安全防范意识；

2、各单位应定期开展网络安全自查工作，梳理网络安全资产(包含各种硬件设备及应用系统，应用系统填报，各单位应如实、准确的填报好办单位的各类在线、下线应用系统)，建立本单位网站、信息系统台账，清理双非、僵尸网站。对上级单位下发的整改函及时有效的整改，强化口令控制（按要求三个月进行更换，密码要求数字字母字符结合）、及时更新漏洞补丁等基础安全。

3、对本单位使用的APP、微信群、QQ群等互联网群组和微信公众号、微博账号等互联网公众账号进行排查统计工作，加强日常监管，严格按要求规范使用，规范信息内容，遵守法律法规，不在网络上传播低俗文化、散布虚假信息、制造有害影音，发布内容符合党的教育方针和政策；

4、各单位要统筹做好教育宣传工作和对外信息发布工作，严格落实教委宣传工作相关制度。各单位要加强对本单位门户网站、官方微博、官方微信公众号等各类宣传平台的信息安全管理，信息发布实行“谁审核谁负责，谁发布谁负责”的分层分级管理制度。做到正面宣传、正面引导、信息准确。

5、各单位应加强对安全视频监控系统的自查和日常巡检，每日早、中、晚不少于3次巡检，确保各路摄像头、图像存储工作正常，发现问题及时处理,发生故障及时报修。各单位应规范机房管理制度，做好人员进出机房登记，加强机房巡检工作，做好机房防火防盗工作。

6、加强对网络传真机、打印机的安全管控

传真机应指定专人管理和操作，传真文件需进行登记，不得传真涉密文件、资料，应关闭传真机自动接收模式，采用手动接收模式操作。网络打印机应加强管理，采取相应安全策略限定使用范围，不得接入互联网；

7、加强公共区域电子屏的安全管控

各公共区域电子屏责任部门要对可以采取物理隔离的电子屏及控制端，必须采取物理隔离的方式进行断网；对无法进行物理隔离的电子屏及控制端，要加强对控制端和系统后台的网络安全防护，严格落实7×24小时专人值守制度，保证控制室和控制设备实时有人看守，保证值守人员离开后设备断电，控制室上锁，确保整个大屏显示系统的安全。

四、制订切实可行的应急响应机制，加强处置能力，

各单位明确应细化网络突发事件应急处置流程和责任分工，定期开展应急演练。在各重要时期节点，对本单位应用系统做好重点防护， 制定有效管控措施，确保专人专岗24小时值守，按时上报本单位每日网络安全零报告。一旦发生网络安全事件应及时有效处置，做好记录，按照相关的制度逐级报告。

今天参加会议的还有民办学校的领导、老师，由于民办学校使用公共网络及域名，不在朝阳教育城域网内，各民办学校应按上述要求，落实好本单位网络安全工作，对于上级网安部门下发的问题，按时整改，对因整改不及时出现的后果，将联合区委网信依法给予处治。

同志们，网络安全工作责任重大，来不得半点疏忽，国庆70周年即将来临，让我们共同努力，做好朝阳教育系统网络安全工作，为朝阳教育系统撑起一片安全的网络空间，