筑牢网络安全防线 全力护航党的二十大
——我校开展网络安全应急演练工作

为扎实做好党的二十大召开期间校园网络安全保障工作，进一步提高校园网络和应用系统安全防护水平，提升各类网络应急事件的响应化解能力，9 月 16 日，信息部会同图书馆、保卫处、一分校和多家第三方技术运维团队联合开展了校（院）网络安全应急演练工作，切实提高教职工安全防范意识，明确各业务部门职责及应急事件处理流程，持续推进我校网络安全防范治理工作高质量开展。

本年度网络安全应急演练针对党的二十大重保任务进行实战模拟，前期做好详细的演练计划和准备工作的基础上，重点以云端应用系统、基础设施环境、市级政务网络、终端安全等方面的应急事件为演练目标。云端系统应用方面，与图书馆进行市政务云上 ILAS 知识

平台检索系统突发情况进行模拟，检验云端重点系统安全保障响应速度，加强云上各系统的安全防范、预警和风险化解能力。接到模拟警情后，信息部按照相应预案发起应急响应，图书馆相关老师参与沟通调度，系统运维人员参照技术手册迅速通过 VPN 和堡垒机登录云端服务器，确保能有效应对意外发生的页面篡改、服务中断、环境告警等可能事故，并将初步处置结果汇报党校方面和政务云运维团队，整个过程仅用时 8 分钟。

机房基础设施环境方面，通过模拟烟感报警，与保卫处进行主楼核心机房的消防安全演练。从值守人员收到“主楼核心机房烟感异常”短信报警开始计时，通过应急预案紧急联络渠道，信息部和保卫处相关人员的快速通报协调，仅用时 2 分 40 秒，我校消防团队人员便携带消防应急设备赶到主楼核心机房发现模拟烟感触发点、精确判断、排除隐患，以确保能最大限度防范可能出现的类似情况。

市级政务网络方面，演练对市政务外网的终端异常流量进行检测追查，模拟僵尸网络等妨害校园网络安全正常运行的应急事件处置，着力解决防范化解校园专网的难点和堵点，通过值守人员巡检发现异常流量、开展风险研判识别、明确安全事特征和级别等，依据应急预案确保处理突发事件时各个环节有章可循、迅速反应，最终定位风险终端，断网杀毒、重装系统后排除安全隐患。

终端安全方面，联合一分校对其办公、教学电脑作进行应急事件模拟，通过防火墙上定位异常终端 IP 地址，远程连接交换机确定终端端口，并由一分校电教信息部组织相关人员进行现场核对和终端处置，重点检验已有网络安全防护体系的有效性和突发事件处理的完成度，确保校园的网络全方位安全保障，持续为广大学员和教职工的网络信息安全保驾护航。

网络安全应急演练工作是我校事关网络安全风险防范治理的年度常规动作，主要为加强研究诱发网络安全风险的源头性要素，建全科

学完善的管理体系和应急保障机制，提升突发事件风险防范化解能力，紧贴防范化解各部门网络安全风险的全过程各环节，做实做好我校的网络安全防范治理工作。在本次网络安全应急演练工作中，信息部提前研究制定出科学合理的应急预案，充分调动队伍的积极性，做到层层压实责任，与各部门就网络、应用、核心机房及政务内网这四个方面进行突发故障模拟，确保不落下任何风险点位。

秉承着“加强完善，优化提升”的态度，信息部以点带面，举一反三，全面梳理网络安全应急保障工作的关键节点和要素。在党的二十大召开前夕，对网络安全应急演练涉及的全网络设施、全业务系统再次进行细致排查，对应急演练中发现的部分不足进行了全面的分析和完善，及时提醒各方运维单位高度警惕、整改优化，着力提高我校的网络安全应急保障能力，为今后校（院）信息化建设工作的稳步开展营造出更为良好的网络安全环境。

（申长虹）