关于做好“秋季开学”期间

网络安全保障工作的通知

各部门：
   根据教育部科学技术与信息化司关于做好“秋季开学”期间网络安全保障工作的通知安排，2024 年9月1日0时至10日24时学院将启动“秋季开学”期间网络安全重保工作，现将有关要求通知如下：

一、加强组织领导，履行工作职责

各部门要充分认识重保时期网络安全保障工作的重要性和紧迫性，不断增强“四个意识”，坚定“四个自信”，做到“两个维护”，切实提高防范化解重大风险的能力，分管领导要加强统筹部署，按照“谁运维谁负责、谁使用谁负责、谁发布谁负责”的原则，夯实网络安全主体责任，筑牢网络安全防线，高度警惕和严密防范网络攻击，不折不扣地落实好重要时期的网络安全保障工作。

二、深入排查风险，全面整改隐患

（一）梳理资产清单，明确夯实责任。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，及时做好资产更新报备。要重点加强供应链安全和数据安全风险监测，对通用产品和重要信息系统网络安全与数据安全风险隐患排查。

（二）开展系统自查，排查风险隐患。各部门应会同运维公司认真开展安全隐患自查，并对排查发现的问题隐患进行整改修复，确保问题彻底解决。应重点排查双非(非本单位IP地址、非本单位域名)信息系统(网站)和使用频率低、长期未更新、无专人运维的“僵尸”信息系统(网站)。全面排查弱口令、默认口令、通用口令、长期不变口令，高危漏洞不修复，非必要端口及服务长期开启，陈旧版本基础软件和通用软件不更新，僵尸主机、系统不整改，系统数据无备份，备份数据未验证，重要敏感数据未加密，数据传输不加密，API接口无鉴权和API接口存在越权及注入漏洞等问题，及时补齐网络安全和数据安全短板，避免“一点突破、全网皆失”。

三、加强安全监测，做好应急处置

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），经与宣传部和教务处沟通，系统于每天8：00-20：00开放，其余时间关闭所有访问；
     中心机房存放的内部一级系统使用策略（晚19：00-次日7：00）限制访问，在部门内部存放的系统根据实际情况关闭访问，不能关闭的务必安排专人现场值守；

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，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

各部门应加强网络安全教育，提升部门内教职工安全意识。使用校园网络连接互联网时应依法上网、文明上网；加强微信和企业微信工作联络群的内容管理，严禁发布和工作无关的内容，不发布、点击或转发谣言、虚假、低俗等不良信息及不明链接；做好个人办公电脑的安全管理；对不明来源邮件做到不看、不转、不发，对可疑邮件和附件提高警惕，避免钓鱼事件的发生。

   重要保障时期，一旦发生网络安全事件时，应立即启动应急响应流程，并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
                                        2024年8月30日