

吉林医药学院文件

吉医院字〔2023〕203 号

关于开展网络安全检查工作的通知

各单位（部门）：

为深入贯彻落实《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等国家相关法律法规，结合学校实际情况，拟于 2023 年 11 月 31 日至 12 月 8 日开展网络安全工作检查，现将有关事项通知如下：

一、总体要求

本次检查旨在摸清全校信息系统的建设使用情况，重点加强对网络安全薄弱点的治理，切实保障信息系统（网站）稳定运行。严格落实网络安全自查工作要求，落实网络安全主体责任，按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”原则，突出重点、明确责任、加强监管、重在预防。

二、检查方式

检查工作分为网络安全自查、远程技术检测和现场检查等环节。

三、检查对象

1. 学校各单位（部门）主办的各类信息系统、网站、新媒体平台等。

2. 机房动力环境系统，各类服务器（物理机、超融合）。

四、检查内容

1. 落实责任制。落实网络安全责任制，网络安全责任人为单位（部门）党政主要负责人，负责统筹部署本单位（部门）网络安全工作，按要求组织填写《吉林医药学院网络安全责任书》（附件 1），并确定一名在岗人员作为网络安全管理员，负责日常督促、检查工作，明确本部门各信息系统（网站）系统管理员。

2. 梳理信息资产。各单位（部门）认真梳理本单位（部门）主办的各类信息系统、网站、新媒体平台、服务器情况，对未登记在册的信息系统、网站、服务器，特别是非学校域名及IP地址的“双非”网站进行补充，对废弃不用、无力维护、无人维护的“僵尸”信息系统、网站、新媒体平台、服务器进行清理，建立管理信息资产分台账，按要求组织填写《单位（部门）网络信息员及信息系统台账》（附件 2）。对于未上报的信息系统、网站、新媒体平台、服务器，网络与信息化建设办公室将停止其接入服务或停止互联网络域名解析服务。

3. 安全自查。各单位（部门）要对本单位（部门）的网络安全情况开展自查工作。自查工作重点包括检查信息系统、网站、服务器的安全漏洞、弱口令、身份信息泄露等风险隐患，对自查发现的问题和漏洞要及时进行安全加固、策略配置优化和改进，消除高风险安全隐患。对于各单位（部门）独立设置的机房，要

全面排查安全隐患风险，填报《机房动力环境系统及服务器自查表》（附件3）。

4. 技术检查。网络与信息化建设办公室组织对全校信息系统、网站、服务器进行漏洞扫描，将信息系统、网站等检测出的高危漏洞和报告发送给各相关单位（部门），各单位（部门）应依据整改建议限期完成整改，并提交书面整改报告。

五、工作要求

请各单位（部门）高度重视此次检查，加强领导，明确责任，做好本单位（部门）网络安全检查工作，督促相关人员按时认真填报相关材料，并于2023年12月5日（周二）下班之前将纸质版材料（附件1、2、3）报送学校网络与信息化建设办公室（图书馆综合楼1楼右侧大数据中心），附件2电子版发送到邮箱jlmuwxb@jlmue.edu.cn。

联系人：张颖，联系电话：64560367、64560368。

- 附件：1. 吉林医药学院网络安全责任书
2. 单位（部门）网络信息员及信息系统台账
3. 机房动力环境系统及服务器自查表



吉林医药学院党政办公室

2023年12月1日印发
