山西应用科技学院

关于开展网络安全检查工作的通知

各学院、部、处、室：

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和相关单位有关工作要求，结合我校实际情况，决定即日起开展网络安全专项检查工作，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）稳定运行和数据安全。要认真贯彻网络安全工作要求，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、检查对象

学校各部门主办的各类业务系统（小程序、APP等）、网站、服务器（物理机、超融合）等。

三、工作要求

（一）落实责任制（11月6日前）

各部门党政负责人是网络安全工作的第一责任人，积极落实网络安全主体责任，负责统筹部署本部门网络安全工作，定期开展网络安全相关法律法规学习活动。各部门确定一名网络系统管

理员，负责本部门日常督促、检查工作，系统管理员按要求填写《部门网络系统管理员登记表》（附件1）并提交网络信息中心。

（二）排查信息资产（11月8日前）

各部门认真排查本部门管理的各类业务系统、网站、服务器情况，建立业务系统资产台账，按要求填写《部门业务系统资产台账》（附件2）并上报网络信息中心，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、服务器进行清理。对于未上报的业务系统、网站、服务器，网络安全责任自行负责。

各部门即时对接网络信息中心完成在用业务系统的服务器托管申请（附件3）、互联网端口开放申请（附件4）等相关工作。

（三）网络安全自查（11月10日前）

各部门要对本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。

（四）网络信息中心技术检查（11月13日前）

网络信息中心组织对全校信息系统、网站、服务器进行漏洞扫描。如果信息系统、网站等检测出高危漏洞，网络信息中心将《网络安全隐患整改通知》（附件5）发送给各部门，各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）完成业务系统等级保护备案工作（11月15日前）

各部门要严格按照《网络安全法》和《GBT 22240-2020 信息安全技术 网络安全等级保护定级指南》等法规和标准规定自

主完成业务系统网络安全等级保护备案及测评工作。网络信息中心做好相关业务培训工作。

请各部门高度重视此次检查，加强领导，明确责任，做好网络安全检查工作，督促相关人员按时认真填报相关登记表。

附件：

1.《部门网络系统管理员登记表》

2.《部门业务系统资产台账》

3.《服务器托管申请表》

4.《互联网端口开放申请表》

5.《网络安全隐患整改通知》

以上附件请从学校官网网络信息中心下载

6.《网络安全监督检查限期整改通知书》涉密，请到网络信息中心查阅原件

网络信息中心

2023年11月3日