**南阳师范学院重要信息系统及网站安全检查**

**实施方案**

一、检查目的

依据国家信息安全有关政策规定，对校属各单位的网络信息系统进行检查，发现存在的主要问题和薄弱环节，即查即改**，**进一步健全网络信息安全管理制度，完善网络信息安全技术措施，提高网络信息安全防护能力，保障我校网络信息化的健康发展。

二、检查原则

坚持“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，统筹安排、突出重点、明确责任、注重实效。

检查工作以各部门自查为主，南阳师范学院校园计算机网络信息系统安全工作领导小组（以下简称领导小组）会同有关部门统一组织检查。

三、检查范围

网络信息系统安全检查的范围是为各部门履行职能提供支撑的网络信息系统，包括自行运行维护管理以及委托其他部门运行维护管理的办公系统、各业务系统、网站系统等。

四、检查内容

**（一）网络信息安全组织管理**

1. 网络信息安全管理机构及其工作开展情况。（1）组织制定并落实网络信息安全管理规章制度情况；（2）组织制定网络信息安全工作计划或工作方案情况，需要查阅该单位网络安全工作议事或例会制度等文档材料。（3）组织开展网络信息安全教育培训和督促检查工作情况。

2. 网络信息安全人员及其工作开展情况。（1）各单位网络信息安全员（专干）指定情况；（2）网络信息安全员开展督促、检查和指导等日常工作情况。需要查阅该单位网络安全工作责任分工和岗位职责等文档材料。

**以上要求有文字材料或原始记录。**

**（二）日常网络信息安全管理**

**1.人员管理。查验相关文档、文件、记录等，重点检查：**（1）岗位网络信息安全和保密责任制落实，特别是重要岗位网络信息安全和保密协议签订情况；（2）人员离岗离职网络信息系统交接的安全管理情况；（3）外部人员访问网络信息系统管理模块的管理情况；（4）违反制度规定造成网络信息安全事件的责任查处情况等；**（5）**岗位责任制落实情况，需要查阅该单位网络安全规划和策略等文档材料。

**2.** **网络信息技术外包服务安全管理。**针对当前校内有部分网络信息系统开发或管理外包服务安全风险突出的现状，重点检查系统开发、系统集成、运行维护、灾难备份、数据处理、安全检测、系统托管等外包服务的安全管理：（1）服务机构性质与背景情况；（2）服务合同及安全保密协议签订情况，安全责任是否清晰；（3）人员现场服务记录情况，是否有现场服务监管措施；（4）系统维护方式情况，重点排查远程在线服务带来的安全风险。

**3.** **网络信息技术产品使用管理。**重点检查办公用计算机、公文处理软件、网络信息安全设备、服务器、网络设备等使用产品的安全可控情况，特别是近两年新采购办公用计算机、公文处理软件、网络信息安全设备是否满足安全可控要求。

**4.** **网络信息安全经费保障。**重点检查网络信息安全防护设施建设、运行、维护、检查及管理等费用是否纳入部门年度预算，以及本年度网络信息安全经费实际投入情况等。

**（三）网络信息安全防护管理**

**1.网络边界防护管理。**查看系统总体网络架构、子系统分布、终端节点、区域划分及边界防护措施等，重点检查：（1）网络分区分域合理性；（2）安全防护设备策略配置有效性；（3）互联网接入情况，是否有访问互联网的安全控制措施，是否留存互联网访问日志并定期进行分析。

**2.** **网络信息系统安全管理。**检查网络信息安全风险评估、等级保护等安全管理制度落实情况。

**（1）服务器安全防护。**重点检查服务器上应用、服务、端口以及系统补丁等情况，是否关闭了不必要的应用，服务、端口；账户口令强度和更新情况；病毒木马防护情况，是否使用技术工具定期进行漏洞扫描、病毒木马检测。

**（2）网络设备防护。**重点检查网络设备安全策略配置有效性；账号口令强度和更新情况；是否使用技术工具定期进行漏洞扫描。

**（3）网络信息系统安全设备部署及使用。**重点检查防病毒、防火墙、入侵检测、安全审计等安全设备部署及使用情况，以及安全策略配置的有效性。

**（4）网络信息系统**安全自查工作计划及落实情况；网络信息系统定级备案工作开展情况。需要查看信息系统定级报告和第二级（含）以上网络信息系统备案证明。系统安全监测预警、容灾备份方案及落实情况；

**3.部门网站安全管理。**以防攻击、防挂马、防篡改、防瘫痪、防窃密为目标，对门户网站安全防护情况进行全面检查：（1）系统管理账户和口令，清理无关账户，防止出现空口令、弱口令和默认口令；（2）服务器补丁更新情况，关闭不必要的端口，停止不必要的服务和应用，删除不必要的链接和插件；（3）是否为修改其他网站制作，是否有未知功能或有漏洞的控件和插件；（4）网络信息发布审核制度建立及落实情况；（5）是否使用技术工具定期进行漏洞扫描、木马检测。

**（四）网络信息安全应急管理**

**1.应急预案。**重点检查本部门网络信息安全应急预案制定、修订、备案及宣贯培训情况。

**2.应急演练。**重点检查网络信息安全应急演练情况；已开展演练的，查看演练文档、记录（包括演练计划、演练方案、演练记录、演练总结报告等）。

**3.应急技术支援。**重点检查是否明确了应急技术支援队伍。已明确的，检查其服务合同及安全保密协议签订情况，了解掌握应急技术支援队伍基本情况以及开展的技术支援活动。

**4.灾难备份。**重点检查重要数据和重要网络信息系统备份情况；对采用社会第三方灾难备份服务的，检查其服务合同及安全保密协议签订情况，了解掌握灾难备份服务设施运维安全管理情况。

**5.** **网络信息安全事件应急处置。**重点检查本年度发生的网络信息安全事件及处置情况；发生过重大网络信息安全事件的，检查是否进行了及时处置，是否按照要求上报和通报。

**（五）网络信息安全教育培训**

重点检查网络信息安全和保密形势教育及警示教育情况，部门领导和相关工作人员参加网络信息安全基本技能培训情况，网络信息安全管理和技术人员参加网络信息安全专业培训情况等。

**（六）网络信息安全检查工作**

**1.上一年度发现问题的整改情况。**重点检查：（1）制定的整改计划及采取的整改措施；（2）整改效果以及是否开展了进一步的网络信息安全风险评估；（3）年度检查情况报告完成情况，是否按学校网络信息化建设要求及时报送，报告是否完整准确、符合要求。

**2.本年度检查工作开展情况。**重点检查：（1）检查工作责任制建立和检查工作经费落实情况；（2）检查工作方案制定及组织实施情况；（3）采取的安全保密和风险控制措施，检查人员、有关文档和数据的安全保密管理情况。

**3.安全技术检测。**组织技术力量，使用必要的技术工具（包括漏洞扫描工具、WEB扫描工具等），对服务器、终端计算机、网络设备以及门户网站等网络信息系统进行安全扫描和渗透检测，检查主机以及连接因特网的公共服务网站系统和安全相关的信息和配置，发现危险或不合理的配置，排查病毒木马、安全漏洞等。

五、检查方式

各单位按照要求认真开展网络信息安全自查工作，将检查情况形成检查报告，将相关原始日志、记录、档案材料整理备查，并接受检查小组的现场质询。领导小组会同有关部门对相关部门统一组织检查。

六、整改完善

领导小组针对检查结果，下发整改通知，各部门对检查中发现的问题，必须认真整改，领导小组确保网络信息安全检查取得实效。

七、检查报告

按照《检查方案》要求，各单位在检查工作完成后及时将检查情况报领导小组办公室。

**（一）报告内容和格式**

检查报告包括主报告和附表。主报告内容应包括：本部门网络信息安全状况总体评价，网络信息安全主要工作情况，检查发现的主要问题及整改情况，对信息安全工作的意见和建议等。

主报告的内容和格式按照《2015年网络信息安全检查情况报告编写参考格式》（附件3）要求撰写。根据检查结果的敏感程度确定检查报告密级，并在检查报告上明确标识。

网站填写附件2，网络信息系统填写附件1.

**（三）报送方式**

电子档发送到邮箱wlzx@nynu.edu.cn，纸质文档盖章后交领导小组办公室（办公室设在网络中心）。

八、时间安排

**（一）网络信息安全自查。**2015年7月3日前完成自查并上报有关自查情况材料和检查报告。

**（二）整改提高。**2015年7月4日至2015年9月10日。各级部门根据自查情况进行整改。

**（二）网络信息安全检查。**2015年9月20日至2015年10月30日。领导小组会同有关部门对相关部门统一组织检查。并根据检查结果制定复查时间。

**（四）复查验收。**日期另行通知。

南阳师范学院校园计算机网络

信息系统安全工作领导小组办公室

（网络中心代章）

二〇一五年六月二十六日

附件1

**2015年网络信息系统安全检查情况**

|  |
| --- |
| **一、部门基本情况** |
| 部门名称 |  |
| 分管网络信息安全工作的领导 | 1姓名：2职务： |
| 网络信息安全管理机构（如办公室） | 1名称：2负责人： 职务：3联系人： 电话： |
| **二、网络信息系统基本情况** |
| 网络信息系统情况 | 1网络信息系统总数： 个2面向社会公众提供服务的网络信息系统数： 个3委托社会第三方进行日常运维管理的网络信息系统数： 个4本年度经过风险评估（含安全测评、等级测评）的系统数： 个 |
| 系统定级情况 | 第一级： 个 第二级： 个 第三级： 个第四级： 个 第五级： 个 未定级： 个 |
| 互联网接入情况 | 互联网接入口总数： 个其中：□校园网接入口数量： 个 接入带宽： 兆□联通接入口数量： 个 接入带宽： 兆□电信接入口数量： 个 接入带宽： 兆□其他：接入口数量： 个接入带宽： 兆 |
| **三、日常网络信息安全管理情况** |
| 人员管理 | 1岗位网络信息安全责任制度：□ 已建立 □ 未建立2重要岗位人员网络信息安全和保密协议：□ 全部签订 □ 部分签订 □ 没有签订3人员离岗离职网络信息安全管理规定：□ 已制定 □ 未制定4外部人员访问机房等重要区域或网络信息系统管理后台审批制度：□ 已建立 □ 未建立 |
| **四、网络信息安全防护管理情况** |
| 网络边界防护管理 | 1网络访问控制：□ 有访问控制措施 □ 无访问控制措施2网络访问日志：□ 留存日志 □ 未留存日志3安全防护设备策略：□ 使用默认配置 □ 根据应用自主配置 |
| **五、网络信息安全应急管理情况** |
| 网络信息安全应急预案 | □ 已制定本年度修订情况：□ 修订 □ 未修订□ 未制定 |
| 网络信息安全应急演练 | □ 本年度已开展 □ 本年度未开展 |
| 网络信息安全灾难备份 | 1重要数据： □ 备份 □ 未备份2重要网络信息系统： □ 备份 □ 未备份3灾难备份中心：□ 境内 □ 境外 |
| 应急技术支援队伍 | □部门所属单位 □外部专业机构 □无 |
| **六、信息技术产品应用情况** |
| 服务器 | 总台数：，其中国产台数：使用国产CPU的服务器台数： |
| 网络交换设备（路由器、交换机等） | 总台数：，其中国产台数： |
| 操作系统 | 1服务器操作系统情况：安装Windows操作系统的服务器台数：安装Linux操作系统的服务器台数：安装其他操作系统的服务器台数：2终端计算机操作系统情况：安装Windows操作系统的计算机台数：安装Linux操作系统的计算机台数：安装其他操作系统的计算机台数： |
| 数据库 | 总套数：，其中国产套数： |
| 网络信息安全产品 | 1安装国产防病毒产品的终端计算机台数：2防火墙（不含终端软件防火墙）台数：其中国产防火墙的台数： |
| **七、网络信息安全教育培训情况** |
| 培训人数 | 本年度接受网络信息安全教育培训的人数： 人占本部门总人数的比例： % |
| 培训次数 | 本年度开展网络信息安全教育培训的次数：次 |
| 专业培训 | 本部门网络信息安全管理和技术人员参与专业培训： 人次 |
| **八、网络信息安全经费预算投入情况** |
| 经费预算 | 本年度网络信息安全经费预算额： 万元 |
| 经费投入 | 本年度网络信息安全经费投入额： 万元（上一年度网络信息安全经费投入额： 万元） |
| **九、网络信息安全经费预算投入情况** |
| 本年度安全技术检测结果 | 病毒木马等恶意代码检测结果 | 1进行过病毒木马等恶意代码检测的服务器台数：其中感染恶意代码的服务器台数：2进行过病毒木马等恶意代码检测的终端计算机台数：其中感染恶意代码的终端计算机台数： |
| 漏洞检测结果 | 1、进行过漏洞扫描的服务器台数：2、其中存在漏洞的服务器台数：3、存在高风险漏洞的服务器台数： |
| 本年度网络信息安全事件统计 | 网络信息系统受攻击情况 | 入侵检测设备或系统检测到的网络信息系统受攻击次数： |
| 设备违规使用情况 | 1使用非涉密终端计算机处理涉密网络信息事件数：2终端计算机在非涉密系统和涉密系统间混用事件数：3移动存储介质在非涉密系统和涉密系统间交叉使用事件数： |
| 设备违规使用情况 | 1使用非涉密终端计算机处理涉密网络信息事件数：2终端计算机在非涉密系统和涉密系统间混用事件数：3移动存储介质在非涉密系统和涉密系统间交叉使用事件数： |
| **十、网络信息技术外包服务机构情况（包括参与技术检测的外部专业机构）**注：系统未外包的可不填写本项 | 机构名称 |  |
| 外包服务机构1 | 机构性质 | □国有 □民营 □外资企业 |
| 服务内容 |  |
| 网络信息安全和保密协议 | □已签订 □未签订 |
| 网络信息安全管理体系认证情况 | □已通过认证认证机构：□未通过认证 |
| 机构名称 |  |
| 外包服务机构2 | 机构性质 | □国有 □民营 □外资企业 |
| 服务内容 |  |
| 网络信息安全和保密协议 | □已签订 □未签订 |
| 网络信息安全管理体系认证情况 | □已通过认证认证机构：□未通过认证 |
| 机构名称 |  |
| 外包服务机构3 | 机构性质 | □国有 □民营 □外资企业 |
| 服务内容 |  |
| 网络信息安全和保密协议 | □已签订 □未签订 |
| 网络信息安全管理体系认证情况 | □已通过认证认证机构：□未通过认证 |
| 网络信息安全管理体系认证情况 | □已通过认证认证机构：□未通过认证 |

填表人： 手机： 单位： 办公电话：

附件2 网站安全情况自查表

|  |
| --- |
| 一、网站的基本情况 |
| 网站中文名 | 　 | IP地址 | 　 |
| 网址 | 　 |
| 网站责任单位 | 　 | 网站运行单位 | 　 |
| 网站责任单位负责人及职务 | 　 | 联系电话 | 　 |
| 网站运行安全责任人及职务 | 　 | 联系电话 | 　 |
| 等级保护定级备案 | □二级 □三级 □四级 □未定级 |
| 等级测评 | □已开展 □未开展 |
| 网站安全责任书 | □已签订 □未签订 |
| 网站服务栏目 | □新闻发布 □政策宣传 □事项办理 □论 坛 □即时通信□电子邮件 □留言版 □政务公开 □其他\_\_\_\_\_  |
| 二、网站安全保护情况 |
| 1 | 网站安全责任部门和安全责任人落实情况 | 是否落实了单位网站安全责任部门？ | □是 □否 |
| 是否落实了单位网站安全责任人？ | □是 □否 |
| 2 | 主要领导对网站网络安全工作的重视情况 | 是否将网站安全工作的执行情况纳入到年度考核指标？ | □是 □否  |
| 开展网站安全工作的经费是否纳入年度预算？ | □是 □否  |
| 3 | 单位网站网络安全责任制落实情况 | 是否明确了网站建设单位、运维单位和内容更新单位等部门的责任？ | □是 □否  |
| 是否对发生的网站安全事件（事故）按照安全责任制进行追责？ | □是 □否  |
| 4 | 关键岗位人员配备情况 | 是否有明确的安全管理员，并签订保密协议？ | □是 □否  |
| 是否有内容管理员，并签订保密协议？ | □是 □否  |
| 5 | 网站定级备案执行情况 | 单位网站是否确定了安全保护等级？ | □是 □否  |
| 6 | 网站等级测评情况 | 是否从《全国信息安全等级保护测评机构推荐目录》中选择测评机构开展等级测评？ | □是 □否  |
| 是否对网站系统定期进行安全测评？ | □是 □否  |
| 是否对网站系统进行了外部渗透测试？ | □是□否 |
| 是否根据测评和渗透测试结果对网站进行安全加固改造？ | □是□否 |
| 7 | 安全事件报告处置 | 是否制定网站安全事件（事故）报告制度？ | □是 □否 |
| 发生网站安全事件（事故）是否向属地公安机关报告？ | □是 □否  |
| 是否有完整网站安全事件处置记录？ | □是 □否 |
| 是否按照要求保留网站完整日志？ | □是 □否  |
| 8 | 开展网站安全监测和预警情况 | 本单位是否开展日常网站安全监测？ | □是 □否  |
| 是否有网站安全监测记录？ | □是 □否  |
| 是否有网站安全预警和处理记录？ | □是 □否  |
| 9 | 网站内容管理 | 是否制定网站内容发布管理制度？ | □是 □否  |
| 是否制定网站内容发布流程？ | □是 □否  |
| 10 | 应急预案的制定、演练和完善情况 | 是否有应急预案，并有相应的预案文档？ | □是 □否  |
| 是否有应急保障队伍并有人员联系方式？ | □是 □否  |
| 是否定期应急演练并有应急演练的文档记录？ | □是 □否  |
| 是否根据演练结果对应急预案进行完善？ | □是 □否  |
| 11 | 网络安全检查情况 | 是否有网站安全自查工作总结报告？ | □是 □否  |
| 12 | 网站交互式栏目信息巡查情况 | 单位网站是否有交互式栏目？ | □是 □否  |
| 是否有专人负责网站交互式栏目信息巡查？ | □是 □否  |
| 13 | 网页防篡改措施 | 是否定期对网站文件进行检测？ | □是 □否  |
| 是否采取网页防篡改措施？ | □是 □否  |
| 14 | 漏洞扫描措施及修复升级情况 | 是否进行过系统层漏洞扫描，并有详细记录？ | □是 □否  |
| 是否进行过应用层漏洞扫描，并有详细记录？ | □是 □否  |
| 发现的漏洞是否及时修复？ | □是 □否  |
| 15 | 网站恶意代码防护 | 是否有网页挂马检测系统？ | □是 □否  |
| 16 | 网站内容安全防护措施 | 内容编辑、审核及发布权限是否分离？ | □是 □否  |
| 关键信息发布是否多级审核？ | □是 □否  |
| 网站发布内容是否过滤？ | □是 □否  |
| 17 | 管理终端安全防护措施 | 是否有控制措施（如地址绑定，网络接入控制等）？ | □是 □否  |
| 18 | 网站后台管理系统防护措施 | 是否对网站后台管理系统的接口进行隐藏？ | □是 □否  |
| 网站后台管理系统登录是否采取验证机制？ | □是 □否  |
| 是否对网站后台管理系统的登录失败尝试次数进行限制？ | □是 □否  |
| 是否对网站后台管理系统的用户口令复杂度进行强度限制？ | □是 □否  |
| 19 | 网站前、后台系统隔离情况 | 是否采用逻辑隔离？ | □是 □否  |
| 20 | 网站应用远程管理情况 | 是否不允许远程管理网站的应用？ | □是 □否  |
| 应用远程管理时是否采用加密通道？ | □是 □否  |
| 21 | 网站内容远程维护情况 | 是否不允许远程维护网站内容？ | □是 □否  |
| 网站内容远程维护时是否采用加密通道？ | □是 □否  |
| **以下为非托管网站填写内容** |
| 22 | 网站服务器操作系统安全措施 | 网站服务器操作系统安全补丁是否及时更新？ | □是 □否  |
| 网站服务器操作系统是否存在弱口令？ | □是 □否  |
| 网站服务器操作系统是否共用同一管理口令？ | □是 □否  |
| 23 | 网站服务器数据库安全措施 | 网站服务器数据库是否存在弱口令？ | □是 □否  |
| 网站服务器数据库是否共用同一管理口令？ | □是 □否  |
| 24 | 网站服务器中间件安全措施 | 网站服务器中间件管理界面是否允许外部访问？ | □是 □否  |
| 网站服务器中间件是否存在弱口令？ | □是 □否  |
| 网站服务器中间件是否共用同一管理口令？ | □是 □否  |
| 25 | 机房安全管理制度执行情况 | 本单位机房进出人员管理是否按照制度执行，并有详细记录？ | □是 □否  |
| 本单位机房日常监控是否按照制度执行，并有监控记录？ | □是 □否  |
| 26 | 网络边界安全防护设备情况 | 是否部署防火墙？ | □是 □否  |
| 是否对外屏蔽了不必要的服务/端口？ | □是 □否  |
| 是否部署入侵检测（防护）设备？ | □是 □否  |
| 是否部署防病毒网关？ | □是 □否  |
| 是否部署抗拒绝服务攻击设备？ | □是 □否  |
| 是否部署Web应用防火墙？ | □是 □否  |
| 是否部署设备？ | □是 □否  |
| 27 | 主要设备可用性 | 网站服务器和数据库服务器是否双机热备？ | □是 □否  |
| 网站服务器和数据库服务器是否采用冷备方式？ | □是 □否  |

附件 3

**2015年网络信息安全检查情况报告**

编写参考格式

一、检查报告名称

X X X（部门名称）2015年度网络信息系统安全检查情况报告

二、检查报告组成

检查报告包括主报告和附表两部分。

三、主报告内容要求

应包括以下四个方面的内容：

**（一）网络信息安全状况总体评价**

概述本部门网络信息安全工作情况，与上一年度比网络信息安全工作取得的新进展，对本部门网络信息安全状况的总体评价。

**（二）2015年网络信息安全主要工作情况**

对照本次检查要求，逐项描述本部门2015年在网络信息安全组织管理、日常网络信息安全管理、网络信息安全防护管理、网络信息安全应急管理、网络信息安全教育培训、网络信息安全检查等方面开展的工作情况。

**（三）检查发现的主要问题及整改情况**

描述本部门安全检查特别是技术检测结果，总结分析本部门在安全管理、技术防护等方面存在的主要问题和薄弱环节，以及针对这些问题的整改措施或整改计划。

**（四）对网络信息安全工作的意见和建议**

对网络信息安全工作特别是网络信息安全检查工作提出意见和建议，进一步促进提高网络信息安全管理水平。

四、附表内容要求

《2015年网络信息安全检查情况报告》各项目应认真、如实、完整、正确填写，避免出现漏项、错项、数据前后不一致等情况。