

# 湘潭大学网络与信息安全检查方案

为全面贯彻落实习近平总书记和党中央关于网络安全的重要指示和决策部署，规范指导 2016 年湘潭大学网络与信息安全检查工作，根据《关于开展全省教育系统网络与信息安全检查的通知》（湘教通[2016]271）文件精神，结合我校实际，特制定本方案。

## 一、检查目的

通过开展网络与信息安全检查，认真查找突出问题和薄弱环节，全面排查安全隐患和安全漏洞，分析评估网络与信息安全状况和防护水平，有针对性地采取管理和技术防护措施，促进安全防范水平和安全可控能力提升，预防和减少重大信息安全事件的发生，切实保障湘潭大学网络与信息系统的安全稳定运行。

## 二、检查范围

此次检查工作范围是辖内的网络与信息系统，包括网站系统、办公系统、业务系统以及有线无线网络环境等。涉及国家秘密的信息系统安全检查，按照国家保密管理规定和标准执行。

## 三、检查内容

### （一）网络与信息安全管理情况

1、网络与信息安全管理规章制度及落实情况。

检查是否建立了涵盖人员管理、资产管理、外包管理、教育培训等方面的网络与信息安全管理体制体系并以正式文件等形式发布。

2、网络与信息安全工作组织落实情况。

网络与信息安全主管领导明确及工作落实情况、网络与信息安全管理部指定及工作落实情况、网络与信息安全工作人员配备及工作落实情况。

### 3、网络与信息安全责任制落实及事故责任追究情况。

网络与信息安全事件倒查、领导责任追究等制度建立和执行情况。

### 4、人员、资产、外包服务等日常安全管理情况。

检查重点岗位人员有无签订安全保密协议，人员离岗离职时是否收回其相关权限，签署安全保密承诺书；外来人员访问机房等重要区域时是否有相应审批制度等；检查是否有专人负责资产管理，职责责任明确，资产台账完整，设备维修维护和报废管理制度完整；检查外包方是否有委派专人常驻学校，现场调试、维护、管理等是否有详细记录；网站信息发布前是否采取了内容核查、审批等安全管理措施；是否配备了必要的电子信息消除和销毁设备，对变更用途的存储介质进行信息消除，对废弃的存储介质进行销毁。

### 5、信息安全经费保障情况。

检查网络与信息安全设备运维、日常管理、教育培训、检查评估等费用是否有专项经费或预算。

## **（二）网络与信息安全技术防护情况**

### 1、物理环境安全

检查机房是否具备防盗窃、防雷击、防火、防水、防潮、防静电、备用电力供应、温湿度控制、电磁防护等安全措施；机房是否配备门禁系统或有专人值守。

## 2、网络边界安全

网络边界是否部署访问控制设备，能阻断非授权访问；是否部署入侵检测设备，定期更新检测规则库；是否部署了安全审计设备，对网络访问等情况进行定期分析审计并记录审计情况。

## 3、设备安全

检查是否部署防病毒网关或统一安装防病毒软件，并定期更新恶意代码库；是否定期对服务器、网络设备、安全设备等进行安全漏洞扫描；是否配置了口令策略保证服务器、网络设备、安全设备等设备的口令强度和更新频率；是否启用了安全审计功能并进行定期分析；是否及时更新了服务器操作系统补丁和数据库管理系统补丁；终端计算机是否安装了杀毒软件等防护软件，是否及时安装了系统漏洞补丁；是否采取了技术措施对接入校园网的终端计算机进行控制。

## 4、应用系统安全

检查网站是否采取了相应措施防止网页篡改、网页挂马、敏感信息泄露、拒绝服务攻击等威胁；检查并统计各应用系统用户身份鉴别情况、用户权限分离情况、服务器防病毒程序部署情况等；电子邮件账号开通是否有审批程序，电子邮箱账号口令策略是否能保证电子邮箱口令强度和更新频率。

## 5、数据安全

对存储的重要数据是否采取了加密、分区存储等技术措施进行保护；对重要数据的传输是否采取了加密和校验等技术措施；对重要的数据和系统是否采取了相应技术进行定期备份。

### **(三) 网络与信息安全应急工作情况**

#### **1、应急预案**

是否制定了网络与信息安全事件应急预案，并使相关人员熟悉应急预案。

#### **2、应急演练**

是否开展应急演练，并留存演练计划、方案、记录、总结等文档。

#### **3、应急资源**

是否指定了应急技术支撑队伍，配备了必要的备机、备件等应急物资。

#### **4、事件处理**

发生网络与信息安全事件后，是否及时向主管领导报告，按照预案开展处置工作；重大事件是否及时通报网络与信息安全主管部门。

### **(四) 网络与信息安全教育培训情况**

#### **1、意识教育**

是否向全校师生开展网络与信息安全形势与警示教育、基本技能培训等活动。

#### **2、专业培训**

是否定期开展网络与信息安全管理和技术人员专业培训。

### **(五) 网络与信息系统等级保护情况**

检查湘教通[2015]550号《关于全面推进全省教育行业信息安全等级保护工作的通知》的落实情况，重点检查重要信息系统定级备案、安全测评和安全建设整改等等级保护制度落实情况。

## **(六) 安全问题整改情况**

重点检查网络与信息管理中心安全检查中发现的问题的整改情况，包括整改措施、整改效果及复查情况，以及本年度类似问题的排查情况等。

## **四、检查方式**

### **(一) 自查**

为全面评估网络与信息安全工作，校各二级单位应根据《湘潭大学二级单位网络与信息安全检查表》，学校网络与信息管理中心应根据《湘潭大学网络与信息管理中心网络与信息安全检查表》，结合《湘潭大学网络与信息安全检查方案》，从网络与信息安全管理、防护管理、应急管理、教育培训等方面进行总体评估，总结成绩、查找不足，更好地推动网络与信息安全管理工作的开展。

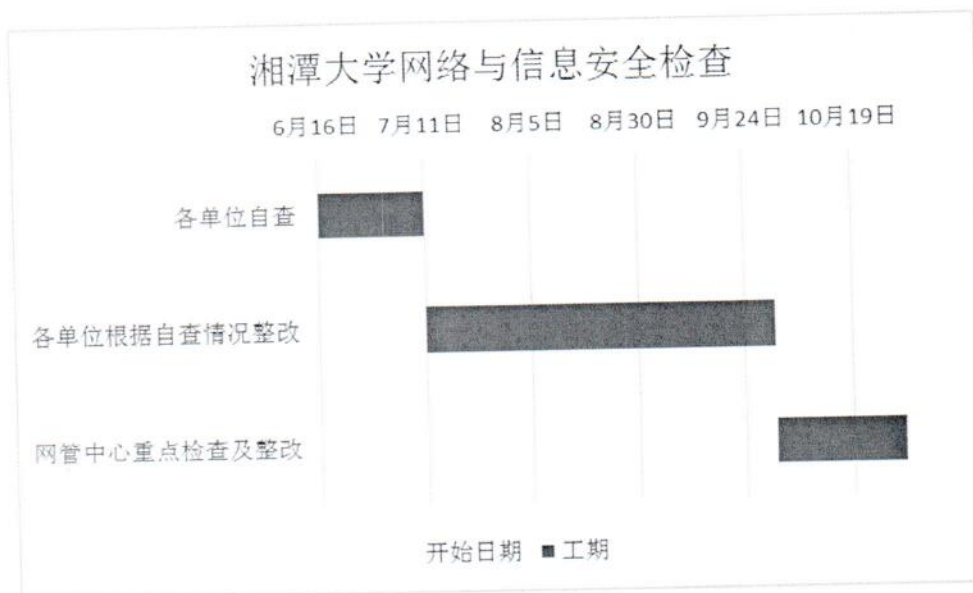
### **(二) 重点检查**

网络与信息管理中心不定期对学校进行远程巡查，并根据巡查情况，决定是否进行现场重点检查。各单位在自查的基础上，组织技术力量会同网络与信息管理中心组成联合检查组对所辖单位的重要网络、信息系统等进行重点检查，查找安全漏洞和隐患，评估安全防护能力，研究提出改进和加强网络与信息安全保障的措施及建议。

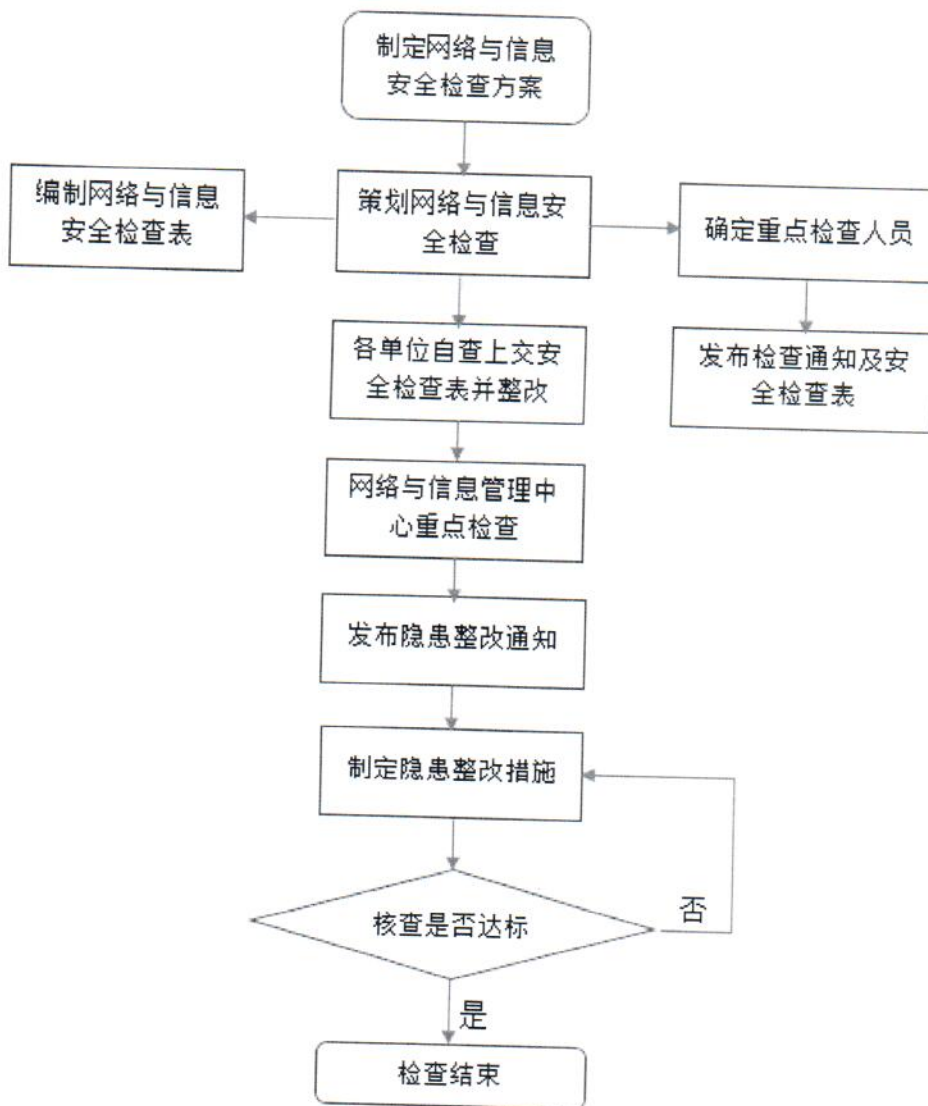
## **五、时间安排**

2016年7月10日前，各单位组织开展网络与信息安全工作，网络与信息管理中心对自查工作进行跟踪、指导、督促和检查。2016年7月11日至2016年9月30日，各单位根据自查情况，对发现的

问题进行整改。2016年10月1日至2016年10月31日，网络与信息管理中心组织重点检查，对发现的问题及时整改，因条件不具备暂时不能整改的问题应采取临时措施，保证系统安全正常运行。



# 湘潭大学网络与信息安全检查流程图



## 六、工作要求

### (一) 加强领导，落实责任。

各单位要把网络与信息安全检查工作列入重要议事日程，加强组织领导，明确检查机构、检查人员、检查经费及其他保障条件，落实工作责任，确保检查顺利实施并取得实效。

### (二) 注重源头，深入检查。

全面细致开展检查工作，注重采用技术检测等手段，深入查找安

全问题和隐患，确保检查工作不走过场、不漏环节、不留死角。

### **（三）即查即改，确保成效。**

对发现的问题要及时整改，因条件不具备暂时不能整改的问题应采取临时措施，防止引发网络与信息安全事件。网络与信息管理中心及时将复查中发现的问题通报给相关单位，督促相关单位落实整改措施，对于逾期未进行整改的问题系统做下线处理，对于逾期未进行整改的单位将予以通报。

### **（四）控制风险，强化保密。**

各单位要强化风险控制，有针对性地制定检查工作应急预案，确保被检查系统的正常运行。要加强对检查活动、检查人员及相关文档和数据的安全保密管理。委托外部机构进行安全检测，要对其机构背景、技术能力、服务水平、人员资质及安全保密管理措施等进行严格审查，并明确外部机构及人员的安全责任。

