湖北大学文件

校信建管字〔2017〕2号

关于印发《湖北大学网络安全综合治理行动方案》的通知

校内各单位：

根据省教育厅统一部署，结合我校工作实际，现将《湖北大学网络安全综合治理行动方案》予以印发，请遵照执行。

湖北大学

2017年6月12日

湖北大学网络安全综合治理行动方案

近年来，按照省教育厅网络安全的总体部署，在全校各单位、部门共同努力下，我校网络信息安全意识显著提高，形势明显好转，工作机制基本建立，防护能力不断加强。但也要看到，我校应用系统多、关键数据多和影响面广，网络信息安全形势依然严峻，网络信息安全工作仍存在一些须进一步加强的地方，主要体现在：安全责任须进一步夯实、管理规范须进一步加强、安全防护能力须进一步提高等方面。按照省教育厅发布的《湖北省教育行业网络安全综合治理行动方案》要求，为全面贯彻落实《中华人民共和国网络安全法》，迎接党的十九大胜利召开，根据省教育厅的统一部署，自 2017 年 6 月至 10 月，我校将在全校范围内开展以“清理、堵漏、补短、规范”为目标的网络安全综合治理行动，综合治理行动方案如下：

一、 工作目标

面向校内各单位，坚持以问题导向，突出重点、完善机制、狠抓落实，重点加强对网站和信息系统的清理、堵塞安全漏洞、补齐等保短板、规范安全管理。同时，兼顾近期与长远、综合治理与源头治理相结合，全面提升我校网络信息安全水平，增强网站和信息系统安全防护能力，有效防范和抵御安全风险，切实保障网站和信息系统的稳定运行和数据安全。

二、 工作内容

（一）高度重视网络信息安全工作

1.提高网络信息安全责任意识。各单位要充分认识做好网络信息安全工作的重要性和紧迫性，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立“主要负责人负总责，分管负责人牵头抓”的“一把手”领导责任制和安全应急响应机制，做到人员落实、制度落实、责任落实，认真做好网络信息安全自查整改工作，强化措施，发现异常情况及时报告、处理，确保本单位网站和信息系统的安全稳定运行。

2.确保应用系统（网站）良好稳定运行。各单位要在前阶段学校组织的网络信息安全清理整顿工作的基础上，进一步清理各类应用系统（网站）安全运行情况。按学校要求，各单位门户网站（网页）一律纳入网站群系统，课程网站一律纳入教学平台系统，各单位原则上不得自行建设单体网站（网页）；因教学和工作需要，凡在校外服务器和虚拟机上托管应用服务、网站（网页）并冠有“湖北大学”名称的，各有关单位应与托管方签订网络信息安全责任书，要求对方按照有关要求切实履行安全责任。

（二）做好网络信息安全防护工作

各单位应全面检查网站信息发布情况，如有发布的信息中存在法律和行政法规禁止发布或传输的信息、涉及个人隐私和国家或单位秘密的信息，应采取删除或更正等措施立即整改。

各单位要认真做好本单位网站、信息系统或相关设备（如本单位所属服务器、虚拟机）的管理和信息安全保障工作，做好网站、信息系统的安全管理，对网站、信息系统的账号、口令、软

件补丁进行清理检查，及时修改账号密码，确保无弱口令、空口令，及时整改安全隐患，确保无漏洞、无篡改、无后门、无暗链、无“挂马”等问题。学校宣传和信息安全管理部门重点做好信息内容的审核，网站、信息系统监测和整改落实工作，全面提高网络安全防护能力，降低突发网络信息安全事件的风险。如发现问题，应做到及时修复、跟踪核查和整改落实，尽快消除安全隐患。

（三）规范安全管理工作，提升治理水平。

1.加强和规范数据管理。教育部将制定出台《教育部教育数据管理办法》，学校将参照制定相应的数据管理办法，各单位应规范本单位的数据采集、存储、使用和开放共享，推进对重要数据的加密存储和传输，及其容灾备份。

2.加强重要信息基础设施规范管理。按照《省教育厅省公安厅关于进一步加强全省教育系统信息安全等级保护工作的通知》要求，学校将开展重要信息基础设施安全评估和等级保护，研究制定重要信息基础设施管理和防护规范，明确网络信息安全技术人员管理工作要求，指导、监督重要信息基础设施的运行安全，新建系统在上线前必须完成信息系统安全等级保护定级备案和测评整改。根据《湖北大学信息化工作管理办法（试行）》规定，各单位申报信息化建设项目，应向信息化建设与管理处进行备案，否则，学校有关部门将不予采购、费用核销和上线运行。

（四）建立健全应急响应机制，做好应急预案。

各单位网站或信息系统一旦发生被攻击等情况，应用单位应

立即启动应急处置预案，及时采取切断服务器或关闭服务等处置措施，并第一时间向信息化建设与管理处报送有关情况，如涉及政治言论等敏感内容，须同时向党委宣传部报送有关情况。如果情节较严重，学校会及时向上级有关部门汇报有关情况。如发现有隐瞒、缓报、谎报网络与信息安全事件的情况，将在全校范围内予以通报。

三、 工作要求

（一）提高思想认识，加强组织领导。各单位应充分认识开展综合治理行动的重要性和紧迫性，将此项工作纳入重要议事日程予以部署，明确主管领导、分管领导和具体责任人，提供必要的工作保障，确保各项工作落到实处。

（二）加强协调配合，形成工作合力。各单位应加强与信息化建设与管理部门的沟通配合，在提高网络安全防护能力、应急处置网络安全事件等方面形成合力。

（三）开展宣传教育，提升安全意识。学校将于6月下旬组织各单位信息员开展网络信息安全知识培训。各单位应组织开展网络信息安全宣传教育，积极参加面向网络管理人员和技术人员的专题培训，切实提高网络安全意识、管理水平和防护能力。各单位利用新生入学教育、网络安全宣传周等契机，通过形势政策课、讲座、报告会等形式向广大师生开展网络信息安全宣传教育，提高网络信息安全意识和素养。

（四）加强信息安全保密管理，增强保密意识。各单位要高

度重视信息安全保密管理，规范保密制度，夯实保密工作基础，增强工作人员保密安全意识，增强保密敏感性，做到常提醒、多学习、早预防，确保计算机保密工作规范严谨，提升信息安全保密管理水平。

（五）全面清理本单位网站或系统，认真完成自查工作。请各单位填写附件中《湖北大学网络安全综合治理网站/系统自查表》，每个网站或系统一份表格，填写完成盖章签字后于 2017 年 6 月 22 日前交给我处 307 办公室周老师（电话：027-88665038）。

附件：湖北大学网络安全综合治理网站/系统自查表

附件：

湖北大学网络安全综合治理网站/系统自查表

单位名称（公章）：　　填报人：　　填报时间：

网站/系统名称		单位名称	
网站域名		IP 地址	
管理员姓名		联系方式	
分管领导姓名		联系方式	
是否迁入网站群	☐是　　☐否		
独立服务器/虚拟主机（包含版本和型号）			
网站/系统建设时间及维护服务截止时间			
独立服务器/虚拟主机所在位置	☐校内中心机房　　☐本单位 ☐校外，签订安全责任书　　☐校外，未签订安全责任书		
是否与信管处签订服务器/虚拟主机托管协议	☐是　　☐否		
是否存在弱口令/空口令	☐是　　☐否		
是否及时打补丁	☐是　　☐否		
是否按时备份数据	☐是　　☐否		
是否定时安全监测	☐是　　☐否		
是否曾被下发整改通知书	（如是请填写下发时间及是否已整改完成）		
是否存在安全隐患及具体情况描述			
网站/系统安全情况总结（包括是否完成等保备案，如未完成，是否有意愿）： 单位负责人签字：　　时间：			

注：如已迁移到学校网站群管理系统，只需填写前 5 行（IP 地址除外）以及“是否存在弱口令”、“网站 /系统信息安全情况介绍”栏

湖北大学学校办公室　　2017 年 6 月 12 日印发

校对:周文荣