

湖南省教育厅

湘教通〔2017〕146号

关于印发《湖南省教育网络安全综合治理行动方案》的通知

各市州教育（体）局，各高等学校，厅委直属各单位：

为全面贯彻中央、省委和教育部关于网络安全的工作部署，落实《网络安全法》，净化我省教育网络环境，迎接党的十九大胜利召开，根据《教育部办公厅关于印发〈教育行业网络安全综合治理行动方案〉的通知》（教技厅〔2017〕3号）要求，我厅决定开展教育网络安全综合治理行动。现将《湖南省教育网络安全综合治理行动方案》印发给你们，请结合本单位实际，认真落实。

联系人：许鞍铭 吴日云，联系电话：0731-89728306。

湖南省教育厅

2017年4月27日

湖南省教育网络安全综合治理行动方案

近年来，我省教育系统各单位认真贯彻中央、教育部和省委有关网络安全的工作部署，强化工作管理，加强基础设施建设，全省教育系统网络安全意识明显提高，防护能力不断增强。但由于教育系统战线长、系统多、影响广、投入相对不足，我省教育网络安全仍然存在安全责任体系不健全，责任落实不到位，技术防护措施滞后，安全隐患修复不及时，技术人员严重不足，安全监测预警和响应处置能力明显不够等问题，导致网络安全事件时有发生。这些问题危害了师生切身利益，给我省深化教育改革造成了不良影响，一定程度阻碍了教育事业的发展。为落实《网络安全法》，净化我省教育网络环境，迎接党的十九大胜利召开，根据《教育部办公厅关于印发〈教育行业网络安全综合治理行动方案〉的通知》（教技厅〔2017〕3号），按照网络安全和信息化“统一谋划、统一部署、统一推进、统一实施”的总体要求，省教育厅决定自2017年4月至10月，开展全省教育网络安全综合治理行动，特制订本工作方案。

一、组织管理

全省教育网络安全综合治理行动在省教育厅网络与信息安全领导小组的领导下，由厅信息化办负责统筹全省的综合治理行动，省教育厅信息中心组织技术力量做好综合治理

的技术保障，确保整治行动落到实处，取得实效。

二、工作目标

全省教育网络安全综合治理行动按照“问题导向、突出重点、完善机制、安全优先”的总体思路，狠抓落实。采取近期与长远、综合治理与源头治理相结合的方式，重点对网站管理、安全漏洞、安全等级保护、安全规范管理、安全责任体系等存在的问题进行整治，全面提升我省教育网络安全管理水平和技术防护能力，有效抵御网络安全风险，杜绝信息系统（网站）“带病”运行。

三、主要内容

（一）建立健全网络安全组织体系，规范安全管理

1. 成立网络安全和信息化领导小组。各单位建立“主要负责人负总责，分管负责人牵头抓”的网络安全领导机构，明确主要负责人是本单位网络安全第一责任人，全面统筹网络安全工作，负责落实网络安全主体责任；分管负责人协助主要负责人履行本单位网络安全职责，承担组织实施、综合管理和监督等责任。结合本单位实际，设立并进一步明确网络安全的职能部门和技术保障部门，归口管理和支撑本单位网络安全工作。（持续推进）

2. 落实网络安全的主体责任。各单位要建立健全网络安全管理制度，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立网络安全责任体系，针对每个信息

系统（网站）落实相应主管单位、运维单位和使用单位的网络安全主体责任。（持续推进）

（二）治理网站乱象，强化主体责任

1. 进一步明确和落实安全管理责任。各单位加强对网站安全的领导，建立健全网站信息发布审核和保密审查制度，明确审核审查程序，指定机构和人员负责审核审查工作，建立审核审查记录档案，确保信息内容的准确性、真实性和严肃性，确保信息内容不涉及国家秘密和内部敏感信息。（持续推进）

2. 进一步落实网站统一标识工作。各级教育行政部门及其直属单位要按照《党政机关网站开办审核、资格复核和网站标识管理办法》要求，到机构编制部门完成网站开办审核、资格复核和挂标工作。（2017年5月20日前）

3. 加强网站信息发布和邮件系统管理。各单位要全面检查网站信息发布情况，对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、涉及个人隐私和单位秘密的信息，必须采取措施立即整改。加强对单位电子邮件系统的管理，对非在职人员电子邮箱账号予以注销，对使用简单密码的必须采取措施更换，并建立定期更新密码的制度。（持续推进）

（三）堵塞安全漏洞，有效预防安全事件

1. 全面监测网络安全威胁。各单位要建立信息系统（网

站)常态化监测机制,及时发现存在漏洞、后门、暗链、弱口令等安全威胁的信息系统(网站),对安全管理不到位、安全责任体系不健全、技术防范措施缺乏的信息系统必须按安全等级保护的要求限期整改,消除安全隐患。信息系统(网站)整改期间上线运行的,必须24小时进行安全监控。(持续推进)

2. 加强和规范数据管理。各单位要制订数据管理办法,规范数据采集、存储、使用和开放共享工作,加快推进对重要数据的加密存储、传输和容灾备份,防止数据失、泄密事件发生。(持续推进)

3. 加强关键信息基础设施规范管理。各单位必须开展关键信息基础设施专项检查和评估,制订关键信息基础设施管理和防护方案,明确产品和服务采购、人员管理工作要求,保障关键信息基础设施运行安全。(持续推进)

4. 加快推进教育实名制上网工作。各单位要按照《湖南教育系统网络与信息安全工作实施方案》的要求,加快推进教育网络安全综合管控平台建设并与省级平台对接,全面普及师生校园内通过教育电子身份证号(EEID)实名制上网;加快推进教育舆情管控系统建设,第一时间对教育网络舆情进行预报和跟踪分析,由事后追查转为事前防范。(2017年10月底前)

(四) 补齐信息系统(网站)等保短板,履行安全保护

法定义务

1. 加快完成信息系统（网站）的梳理与定级。各单位按照《关于做好全省教育网站和信息系统网络安全排查工作的紧急通知》，组织开展信息系统（网站）的清理，并建立信息系统（网站）基本信息库（见附件1）。按照《教育厅 公安厅关于全面推进教育行业信息安全等级保护工作的通知》要求，制订信息系统（网站）安全等级保护制度和程序，组织开展信息系统（网站）等级保护定级工作。每年3月底前完成新建设信息系统（网站）梳理与定级工作。（2017年4月底前完成）

2. 尽快完成信息系统（网站）备案。各单位按照《教育部 教育行业信息系统安全等级保护定级工作指南》，尽快完成已运行但未定级及定级不准的信息系统（网站）重新定级工作，并及时到当地公安机关进行备案。同时，将备案结果及时报我厅。新建、扩建、改建信息系统应在系统设计阶段确定安全保护等级，与系统建设同步实施，信息系统上线前完成定级备案和测评整改。（2017年5月底前完成）

3. 加快推进信息系统（网站）测评与整改。各单位按照国家 and 教育行业有关标准规范要求，开展信息系统（网站）安全等级保护测评和整改工作。重点加强对关键信息基础设施的保护，明确安全管理负责人，制订专门应急预案，完成测评和整改工作。已建设系统必须按照系统所定级别和测评

结果进行安全整改，新建系统必须在系统设计实施阶段同步建设安全防护措施。（2017年6月底前完成）

四、工作要求

（一）加强领导，全面部署并落实网络安全综合治理行动。省教育厅将网络安全综合治理行动作为2017年网络安全和信息化重点工作，各单位要充分认识开展网络安全综合治理行动的重要性和紧迫性，党委要将工作摆上重要议事日程予以部署，提供必需的人、财、物等保障条件，确保各项工作落到实处。同时，省教育厅将网络安全工作纳入校园及周边治安综合治理工作考核评价体系、高校党委书记履行党建工作责任述职评议考核、教育督导考核、教育网络安全和信息化目标管理考核体系。

（二）加强监督检查，建立常态化通报机制。各单位要制订年度网络安全检查工作方案，定期开展网络安全自查工作，通过常规检查和专项整治相结合的方式，建立网络安全长效监督检查机制。各单位要在每月底报送当月工作进展情况，填写《教育网络安全专项整治行动进展统计表》（见附件2），我厅将网络安全整治行动纳入教育信息化工作月报内容定期通报，同时作为“教育网络与信息专项建设项目”的重要考核依据。

（三）加强培训教育，不断提高网络安全意识。各单位要制订信息系统（网站）管理人员、技术人员和运维人员培

训方案，开展专题培训，全面提高网络安全意识、管理水平和防护能力。要制订《中华人民共和国网络安全法》学习宣传方案，利用学生入学教育、网络安全宣传周等活动，通过形势政策课、讲座、报告会等方式广泛开展网络安全宣传教育，提高师生网络安全意识和素养。

（四）加强创新，建立多渠道的网络安全保障机制。网络安全是一个系统工程，涉及到信息化基础设施建设、信息系统建设、信息系统应用与运维等方面，各单位要创新网络安全保障机制，鼓励有条件的安全专业机构、安全企业参与教育网络安全建设，在安全信息共享、技术支持、教育培训等方面开展多方位合作，提高网络安全整体防护能力。

（五）严控治理风险，确保信息系统（网站）运行安全。各单位网络安全综合整治过程中要强化风险控制，避免检查工作影响网络和信息系统的正常运行。特别是关键信息基础设施的正常运行。要加强保密管理，综合整治结果严格按照规定报送，不得擅自对外发布或提供给无关机构。涉及国家秘密的网络和信息系统的检查，按照国家保密管理规定执行。

- 附件：1. 信息系统（网站）基本信息表
2. 湖南省教育网络安全综合治理行动进展统计表

附件 1

信息系统（网站）基本信息表

序号	信息系统（网站）基本情况									安全运维情况					
	名称	建设单位	使用单位	运维单位	安全等级	使用的数据库	建设形式	使用频率	经费投入	部署方式	是否有应急预案	是否完成备案、测评、整改	是否建立责任体系	累计发现的漏洞数	是否灾备

备注：安全等级指按信息系统安全保护制度确定的等级；建设形式指自建、购买、上级部门建设等；使用频率指次/天、次/月、次/年；部署方式指网络中心机房集中部署、租用 IDC、自备环境部署；存在漏洞指专项整治发现的漏洞个数及级别。

附件 2

湖南省教育网络安全综合治理 行动进展统计表

单位名称:

一、单位基本情况						
主管领导		职 务		联系方式		
职能部门		责任人		职 务		
移动电话		电子邮箱		QQ 号		
二、月度工作部署情况						
部署综合治理行动的会议、发文情况；完善综合治理行动的工作机制情况；推进本月完成综合治理行动相关工作措施；综合治理行动的创新或可借鉴的经验案例。						
三、月度工作进展情况						
(一) 网站规范管理工作						
本单位信息系统数量				完成信息发布整改数量		
完成网站开办审核工作				完成网络挂标工作		
事业单位门户网站数量				完成网站挂标工作数量		
(二) 安全威胁处置工作						
是否开展监测工作				开展监测工作的方式		
发现的安全威胁数量	漏洞		完成整改的数量	漏洞		
	后门			后门		
	暗链			暗链		
(三) 网络安全等级保护工作						
	系统总数	一级	二级	三级	四级	未定级
定级备案						
测评整改						
	关键信息基础设施数量			已完成测评数量		

- 备注： 1、各级教育行政部门、厅委直属单位需填写网站开办、挂标工作完成情况。
 2、如本单位未开展监测工作，则无需填写安全威胁处置工作栏目的相关内容；发现和完成整改的安全威胁数量，仅需要填写本单位监测工作涉及的相关数据。
 3、开展监测的方式包括自行组织、专业机构合作、购买第三方服务等。