

教育部办公厅文件

教技厅〔2017〕3号

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

各省、自治区、直辖市教育厅(教委),新疆生产建设兵团教育局,部属各高等学校,部内各司局、各直属单位,中国教育和科研计算机网网络信息中心:

为全面贯彻党中央、国务院关于网络安全的统筹部署,落实《网络安全法》,迎接党的十九大胜利召开,按照教育部网络安全和信息化领导小组的统一部署,教育部将于3月至8月开展以“治乱、堵漏、补短、规范”为目标的网络安全综合治理行动。现将《教育行业网络安全综合治理行动方案》印发给你们,请遵照执行。

联系人:科技司,潘润恺,010-66096823



教育行业网络安全综合治理行动方案

教育行业网络安全是国家网络安全的重要组成部分。近年来,按照国家网络安全的总体部署,在全行业共同努力下,教育行业网络安全意识显著提高,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,教育行业机构多、系统多、数据多、影响面广,网络安全工作仍存在许多问题,主要表现在:安全责任不落实、管理不规范、安全隐患修复不及时、监测预警和应急响应能力不足、网络安全事件时有发生等问题。这些问题给教育行业不仅造成了不良影响,同时危害到师生的切身利益。为全面贯彻党中央、国务院关于网络安全的统筹部署,落实《网络安全法》,迎接党的十九大胜利召开,按照教育部网络安全和信息化领导小组的统一部署,自2017年3月至8月,教育部将在全行业开展以“治乱、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

面向各级教育行政部门及其直属单位、高等学校(以下简称各单位),坚持以问题导向、突出重点、完善机制、狠抓落实,重点加强对网站乱象的治理、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,全面提升教育行业网络安全水平,增强信息系统防护能力,有效防范和

抵御安全风险隐患,切实保障信息系统(网站)稳定运行和数据安全。

二、工作内容

(一)治理网站乱象,强化主体责任。

1.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应按照《党政机关网站开办审核、资格复核和网站标识管理办法》和各地要求,尽快到各地机构编制部门完成网站开办审核、资格复核和挂标工作。如未按期完成,将根据有关职能部门要求对网站主管单位予以督办。(2017年5月底前完成)

2.加强教育行业网站信息发布管理。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、涉及个人隐私和单位秘密的信息,应采取删除或更正等措施立即整改。加强对电子邮箱的管理,对非在职人员电子邮箱账号予以注销,对使用简单密码的应采取有效措施要求更换,并建立定期更新密码的制度。(2017年5月底前完成)

3.开展教育机构网站域名清理工作。中国教育和科研计算机网网络信息中心根据教育机构名录核对注册.edu.cn域名的机构情况,根据实际情况对非教育机构的网站使用该域名的进行清理。教育部研究加强对教育机构网上名称的管理,规范教育机构域名,提升教育机构网站的公信力和权威性。(2017年8月底完成)

(二)堵塞安全漏洞,增强防护能力。

1.全面监测网络安全威胁。各级教育行政部门及其有条件的

直属单位、高校应对本地区、本单位主管的信息系统(网站)开展常态化监测,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),应及时通报、限时修复、跟踪核查整改结果,尽快消除安全隐患。持续推进。

2.检测应用软件安全风险。教育部深入分析支撑教育行业重要业务管理、教育教学活动中使用范围较广的应用软件产品的安全性,通过测试发掘软件存在的安全缺陷、漏洞等风险隐患,告知开发单位及时采取补救措施,并尽快协助教育行业用户完成对软件的升级和修复。持续推进。

(三)补齐等保短板,履行安全保护义务。

1.加快完成定级备案。各单位应清楚掌握主管的信息系统(网站)情况,按照《教育部 公安部关于全面推进教育行业信息安全等级保护工作的通知》(以下简称《通知》)的要求,建立信息安全等级保护制度和程序,尽快完成信息系统(网站)等级保护定级工作,并到当地公安机关进行备案。新建系统应在正式上线前完成信息系统定级备案和测评整改。(2017年5月底完成)

2.有序推进测评整改。各单位应按照《通知》要求,对主管的信息系统(网站)开展网络安全等级测评整改工作。重点加强对主管的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,完成年度测评工作,深入查找薄弱环节并迅速整改。(2017年6月底完成)

(四)规范安全管理,提升治理水平。

1.加强和规范数据管理。教育部加快制定出台《教育部教育数据管理办法》，各省级教育行政部门参照制定相应的数据管理办法，各单位应规范数据采集、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。（2017年8月底前完成）

2.加强关键信息基础设施规范管理。各单位应开展关键信息基础设施专项检查和评估，研究制定关键信息基础设施管理和防护规范，明确产品和服务采购、人员管理工作要求，指导、监督关键信息基础设施的运行安全。（2017年底前完成）

3.健全网络安全事件应急响应机制。各单位应研究制定信息技术安全应急预案，建立安全事件分级响应、跨部门协同处置的工作机制。加强应急处置队伍建设，落实24小时值守，并定期开展安全演练，提高教育信息系统（网站）应急处置水平。（2017年底前完成）

三、工作要求

（一）提高思想认识，加强组织领导。教育部负责统筹部署本次综合治理行动，省级教育行政部门负责统筹本地区的综合治理行动。各单位应充分认识开展综合治理行动的重要性和紧迫性，将工作纳入重要议事日程予以部署，明确主管领导、牵头部门和责任人，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。各单位应加强与网信部门、公安机关、工信部门等网络安全职能部门的沟通配合，在打击网络违法行为、处置网络安全事件等方面形成合力。探索与网络

安全专业机构、安全企业建立合作机制或购买第三方服务,在信息共享、技术支持、教育培训等方面开展多方位的合作。

(三)加强监督检查,完善通报机制。各单位应在每月底报送当月工作进展情况,填写《教育行业网络安全综合治理行动进展统计表》(见附件)。教育部将综合治理行动纳入教育信息化工作月报内容定期通报。同时,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和网络安全生产大检查,建立网络安全长效监督机制。

(四)开展宣传教育,提升安全意识。各单位应组织开展网络安全宣传教育,面向网络安全管理人员和技术人员开展专题培训,切实提高网络安全意识、管理水平和防护能力。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、报告会等方式面向广大师生开展网络安全宣传教育,提高网络安全意识和素养。

附件:教育行业网络安全综合治理行动进展统计表

附件

教育行业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			
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；推进本月工作完成综合治理行动相关工作的措施；综合治理行动的创新或可资借鉴的经验案例。					

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	<input type="checkbox"/> 是 <input type="checkbox"/> 否		完成网站挂标工作	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
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	<input type="checkbox"/> 是 <input type="checkbox"/> 否		开展监测的工作方式			
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.省级教育行政部门、部直属单位需填写网站开办审核、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。

(此件不予公开)

部内发送:有关部领导

教育部办公厅

2017年3月22日印发

