中共衡阳师范学院委员会文件

校党字〔2017〕28 号

关于印发《衡阳师范学院网络安全应急处理预案》等方案的通知

校属各部门:

经党委会研究同意，现将《衡阳师范学院网络安全应急处理预案》、《衡阳师范学院网络安全综合治理行动方案》印发给你们，请结合实际，认真贯彻执行。

附件：1. 衡阳师范学院网络安全应急处理预案

2. 衡阳师范学院网络安全综合治理行动方案

衡阳师范学院

2017 年 6 月 27 日

附件 1:

衡阳师范学院网络安全应急处理预案

为确保发生网络安全问题时各项应急工作能高效、有序地进行，最大限度地减少损失，根据互联网网络安全相关条例及上级相关部门文件精神，结合我校工作实际，特制定本预案。

一、学校成立网络安全应急处理领导小组

学校成立网络安全应急处理领导小组（以下简称“领导小组”），在学校网络安全和信息化领导小组的指导下开展工作。领导小组主要职责:

1. 负责学校网络安全应急处理预案的制定和各项措施的落实。

2. 负责网络安全知识的宣传教育，广泛开展网络安全和有关技能训练，不断提高广大师生的网络安全防范意识和基本技能。

3. 领导小组成员得悉紧急情况后应立即赶赴指定地点，指挥、协调、组织人员迅速进行抢险防护，进行有效的网络安全事件处理，防控安全事件的蔓延或扩大，尽最大努力降低损失，及时向学校网络安全和信息化领导小组报告事件的有关情况。

4. 严格按照预案要求配备网络安全设施设备，落实网络线路、交换设备、网络安全设备等物资的备勤工作，强化管理措施，使之保持良好工作状态。

5. 建立网络安全防护重要时期值班与值守情况日报制度，全面保证和促进学校网络安全稳定运行。

二、网络安全各类事件处理预案

各部门所管辖范围内发生网络信息安全突发事件后，应立即报告学校领导小组。领导小组应立即启动应急处理预案，分析、研判事件的来源和危害程度，并予以快速处置。影响全校网络运行和信息安全的重大事件由领导小组统一指挥，协调处置。

1. 网站不良信息事件处理预案

（1）发现学校网站上出现不良信息（如：被黑客攻击修改了网页），立即关停网站。

（2）备份不良信息所在的文件及目录，备份前后一个星期内的 HTTP 连接日志，备份防火墙中不良信息及前后一个星期内的网络连接日志。

（3）打印不良信息页面留存。

（4）清查问题网站所有内容，确保其不再存在不良信息。对受损网站实施安全级别升级和相关程序修改，测试通过后重新开通网站服务。

（5）全面查对 HTTP 日志，防火墙网络连接日志，确定该不良信息的源 IP 地址，及时向领导小组组长汇报，领导小组视情节严重程度决定是否向公安机关报案。

（6）事件处理后必须及时向领导小组汇报此次事故的发生情况、发生原因和处理情况。

2. 网络恶意攻击事件处理预案

（1）发现学校的某个网站遭受网络恶意攻击，信息与网络中心应迅速组织相关技术人员确定该攻击源与影响范围、危害程

度，研判是否需要紧急切断校园网的服务器及公网的网络连接，采取有效措施保护重要数据及信息。

（2）如果攻击来自校外，立刻从防火墙中查出对方 IP 地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。

（3）如果攻击来自校内，立刻确定该攻击源或使用者。关闭该计算机网络连接，并立刻对该计算机进行分析处理。

（4）对攻击源进行分析，清除所有病毒、恶意程序、木马程序以及垃圾文件，并进行实时监控。

（5）重新启动相关的网络设备，直至完全恢复网络通信。

（6）事故处理后，必须及时向领导小组汇报此次事故的发生情况、发生原因、处理情况。

3. 学校重大事件网络保障处理预案

（1）对学校重大事件（如校庆、评估等对网络安全有特别要求的事件）进行网络风险评估、确定防控网络风险所需的网络设备及环境。

（2）学校重大事件活动期间若出现网络安全隐情，信息与网络中心应及时关闭与该网络相连的有可能对该网络造成不利影响的一切网络设备及计算机设备，保障该网络的畅通。

（3）重要网络设备应及时进行信息备份，出现网络安全问题时要尽快更换设备。

（4）事先应向领导小组汇报本次事件中所需用到的设备、工具软件以及可能出现的事故及影响，在事件活动过程中出现任何问题均应立刻向领导小组组长汇报。

（5）对外网连接进行监控，清除非法连接，出现重大网络安全或技术问题立刻向上级部门求助。

4. 网络环境安全事件应急处理预案

（1）网络环境安全突发事件原则上由发生事件的部门自行处置，涉及全校性事件由信息与网络中心负责处置。对火灾、盗窃、破坏等紧急事件按照国家有关法律法规及学校有关规定处理。

（2）遇与供电相关的紧急事件，由学校后勤处作现场紧急处置，根据停电时间、用电功耗、电池电能储备、网络和信息运行情况等条件作调度，采取包括次要系统停电、减轻负载等措施，密切跟踪参数变化并反馈调整控制，联系相关单位和人员作现场维护。

5. 网络运行事件应急处理预案

网络运行相关事件包括：线路中断、路由故障、流量异常、域名系统故障等。由信息与网络中心向领导小组报告，由领导小组统一指挥，协调处置。

三、日常管理

1. 领导小组依法发布有关消息和警报，全面组织各项网络安全防御、处理工作。各小组成员随时准备执行应急任务。

2. 网络管理员对校园内外所属网络硬件软件设备及接入网络的计算机设备定期进行全面检查，封堵网络漏洞，升级、更换有安全隐患的设备。各部门要建立网络安全检查台账，及时记录检查情况。

3. 加强对校园网内计算机设备的管理，加强对学校网络的使用者的网络安全教育。加强对重要网络设备的软件防护以及硬件防护，确保正常的运行软件硬件环境。

4. 加强网络值班值勤，值班人员在值班期间必须保持通讯畅通，及时掌握学校情况，全力维护正常教学、工作和生活秩序。

5. 按预案落实各项物资准备。

四、后期处置

对网络和信息安全应急事件，除在事发时按要求上报省教育厅、地方公安、网监和有关部门以外，应急处置后还应对重大事件进行总结评估，并进行归档工作。通过备案工作，积累经验，发现问题，总结规律，提取典型案例作为相关人员的培训内容。

五、其他

1. 在应急行动中，学校各部门要服从指挥，密切配合，确保应急行动快速有效。

2. 各部门应根据本预案，结合本部门实际情况，认真制定本部门的应急处理预案，并切实落实各项组织措施。

3. 本预案从发布之日起施行，最终解释权归学校网络安全和信息化工作办公室。

附件 2:

衡阳师范学院网络安全综合治理行动方案

为全面贯彻党中央、国务院关于网络安全的统筹部署，落实《中华人民共和国网络安全法》(以下简称《网络安全法》)，迎接党的十九大胜利召开，按照《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)和湖南省教育厅《关于印发<湖南省教育网络安全综合治理行动方案>的通知》(湘教通〔2017〕146 号)文件要求，结合学校实际，制订本工作方案。

一、组织管理

学校网络安全和信息化领导小组负责统筹部署本次综合治理行动。信息与网络中心负责方案的实施及进展情况上报工作，并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

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，全面提升我校网络安全管理水平，增强信息系统防护能力，及时消除网络安全隐患，有效抵御网络安全风险，切实保障校内网络信息系统（网站）稳定运行和数据安全。

三、主要内容

（一）开展校内网站系统排查，加强信息发布审核管理

1. 做好校内网站系统排查工作。根据学校下发的《关于做好我校网络与信息安全专项排查工作的通知》（校办通〔2017〕4号），各部门须按要求完成信息系统、网站清理排查工作，并及时上报排查结果。信息与网络中心根据校内网站、信息系统摸底排查情况，建立校内网络信息系统（网站）基本数据库。

2. 加强网站信息发布管理。根据《衡阳师范学院校园网信息发布管理制度》规定，建立健全校园网络信息发布制度，明确审核审查程序，确定专人负责审核审查工作，建立审核审查记录台帐，确保信息内容的准确性、真实性和严肃性。如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进行整改。

（二）堵塞安全漏洞，增强防护能力

1. 全面监测网络安全威胁。信息与网络中心配合相关部门对校内的信息系统（网站）开展常态化监测，若发现漏洞、后门、暗链、弱口令等安全威胁的信息系统（网站），应及时采取措施进行修复，尽快消除安全隐患。新建立的站点、信息系统必须通过学校信息与网络中心或国家网络管理部门进行安全检测，检测合格后方可上线运行。

2. 加强和规范学校网络信息数据管理。加快推进对重要数据的加密存储、传输和容灾备份，防止数据丢失、泄密事件发生。

3.加强关键信息基础设备的建设与规划管理。做好网站站群系统的采购与应用，于2017年9月前将校内所有网站迁入站群系统。

4. 加快推进教育实名制上网工作。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。

5.加强对校内教工邮箱（以@hynu.edu.cn为后缀的邮箱）的管理。信息与网络中心于6月30日之前对校内非在职人员的教工邮箱账号予以注销，对使用简单密码的用户采取有效措施要求其更换，并建立定期更新密码的制度。

（三）严格开展等保工作，履行安全保护义务

1. 加快完成已有信息系统（网站）的梳理与定级。根据《网络安全法》、教育部《教育行业信息系统安全等级保护定级工作指南（试行）》和湖南省教育厅、公安厅《关于全面推进湖南省教育行业信息安全等级保护工作的通知》要求，建立信息系统（网站）安全等级保护制度和程序，组织开展对正在运行的信息系统（网站）等级保护定级工作。等级保护工作预计8月底完成。

2. 规范新上线应用系统的定级与安全管理。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。

（四）落实网络安全应急响应机制，有效预防安全事件

1. 落实网络安全应急响应机制。根据《衡阳师范学院网络安全应急处理预案》，建立安全事件分级响应、多部门协同处置的工作机制，加强应急处置队伍建设，落实24小时值守制度，并定期开展安全演练，提高信息系统（网站）应急处置水平。

2.加强舆情监控。第一时间对涉及学校的网络舆情进行预报、及时通报相关部门处置舆情和做好解释疏导与跟踪分析工作，由事后处置转为事前疏导和防范。

（五）加强培训教育，不断提高网络安全意识

1.强化技术培训。由信息与网络中心牵头，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，全面提高网络安全管理水平和防护能力。

2.加强宣传教育。由宣传统战部牵头，制订《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和形势政策课、讲座、报告会等方式，广泛开展《网络安全法》宣传教育，充分利用校报、官方微信平台等方式加大网络安全知识的宣传密度和广度，提高师生网络安全意识和素养。

四、工作要求

（一）提高思想认识，强化主体责任。各部门要认真学习、领会习近平总书记关于网络安全的系列重要讲话精神，学习、贯彻国家《网络安全法》，充分认识开展网络安全综合治理行动的重要性和紧迫性，将其作为2017年重点工作予以部署，确保各项工作落到实处。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，确保学校和各部门网络安全管理工作规范化、常态化。

（二）加强协调配合，形成工作合力。网络安全问题不仅仅是信息化建设的问题，更是学校推进“双一流”建设和学校建设地方高水平应用型大学奋斗目标的战略问题。各部门要在信息共享、技术支持、教育培训等方面加强合作，凝聚网络安全力量，共同建设校园网络良好生态，推进学校信息化健康发展。

（三）加强监督检查，完善通报机制。学校将网络安全工作纳入校园治安综合治理工作考核评价体系和各部门目标管理考核体系。信息与网络中心负责牵头制订学校年度网络安全检查工作方案，定期开展网络安全检查，并将检查结果予以通报。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机制。