湖北大学文件

校信建管字〔2018〕2号

关于印发《湖北大学网络与信息安全工作责任制暂行规定》的通知

学校各单位：

为进一步加强和规范学校网络与信息安全工作，经校党委常委会研究审定，现将《湖北大学网络与信息安全工作责任制暂行规定》予以印发，请认真学习并遵照执行。

湖北大学

2018年1月8日

湖北大学网络与信息安全工作责任制暂行规定

第一条 为进一步加强和改进学校网络与信息安全工作，促进学校各单位、部门及各级领导干部进一步增强网络与信息安全观念，切实履行网络与信息安全工作职责，提高防护能力和水平，根据《中华人民共和国网络安全法》(中华人民共和国主席令 第五十三号)、《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》、《教育部关于加强教育行业网络与信息安全工作的指导意见》(教技〔2014〕4 号)、《教育行业信息系统安全等级保护定级工作指南（试行)》等文件精神和省教育厅维护安全稳定工作有关部署和规定，结合学校实际，制订本规定。

第二条 网络与信息安全工作应遵循以下原则：

1. 分级管理、层层负责。根据“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各单位、部门主要负责人对本单位、部门网络与信息安全（包含且不限于单位、部门应用系统和二级网站）负总的领导责任和管理责任,同时需明确一名分管领导负直接领导责任，指派一名工作人员负责本单位、部门网络与信息安全的日常管理。

2. 自主防护、明确责任。加强领导，认真实行校园网络与信息安全工作责任制和责任追究制，各单位、部门应建立“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。

3. 统筹规划、遵循标准。各单位、部门对网络与信息安全工作要归口管理，做好统筹规划；要严格执行国家网络与信息安全法律法规、政策和标准规范，遵循省教育厅制订发布的各类教育

信息化管理制度和网络与信息安全标准规范，在管理、技术、人员岗位和操作实施等各个方面符合要求。

第三条 信息化建设与管理处、党委宣传部和保卫部（处）统筹负责学校网络与信息安全工作的部署与监督检查。信息化建设与管理处负责全校网络和信息系统（网站）的宏观监控、漏洞扫描、督促整改、统筹管理与综合评估；负责学校信息化公共基础设施建设和提供技术支撑；负责对学校网络和信息系统（网站）安全管理人员进行业务和安全知识培训。党委宣传部负责规范校内网站、校园网络媒体平台（含新媒体）管理，负责督促各单位加强网站、校园网络媒体平台（含新媒体）安全管理，加强网站内容审核管理，并负责网络舆情管理及网络突发事件的预防和处理。保卫部（处）负责与公安机关、国家安全机关等部门的联络沟通，并协助相关单位进行网络与信息系统（网站）安全事件的查处。

第四条 在接到上级部门通报时，网络或信息系统（含网站、新媒体等）涉及到发布内容方面的问题由党委宣传部负责处理；涉及到技术方面的问题由信息化建设与管理处负责处理。

第五条 学校网络安全与信息化管理部门在进行安全扫描和监测时发现网络、信息系统（含网站、新媒体等）或信息内容存在安全漏洞、安全隐患时，有权先行对网络或信息系统（含网站、新媒体等）进行关闭、暂停或限制访问，并向相关单位、部门下达整改通知。相关单位、部门在接到通知后应在第一时间对有关问题进行整改，在整改到位且通过安全检测后方可恢复服务。

第六条 各单位、部门及个人应履行以下职责：

1. 自觉遵守国家法律、法规和学校其他有关规定、条例和协议。不得从事国家法律法规和学校禁止的一切危害网络和信息安全的活动。

2. 各单位、部门负责本单位、部门的网络与信息安全工作，在研究部署本单位、部门业务工作时，应强调网络与信息安全工作要求，切实采取扎实有效的措施，推动维护本单位、部门网络与信息安全各项措施的落实。

3. 各单位、部门须指定政治可靠、业务能力强、有责任心的在编在岗职工负责本单位、部门的网络与信息安全日常管理工作。各单位、部门应积极建立有效的网络与信息安全管理和响应机制，采取相关技术保障措施，并应定期组织本单位、部门工作人员进行网络与信息安全教育培训，同时有责任和义务接受与配合上级网络与信息安全相关管理职能部门和学校信息化建设与管理处、党委宣传部、保卫部（处）、保密办公室等部门的网络与信息安全保密监督和检查。

4. 各单位、部门对本单位、部门的网络和应用系统（含网站、新媒体等）负有管理职责， 应采取必要手段对其接入的各项内容（包含且不限于发布的信息内容、链接地址、视频、工具软件、设备等）进行全面检查和审核。

5. 各单位、部门及个人如因所使用的网络和应用系统（含网站、新媒体等）或发布的信息内容不当所引起的各种政治责任、法律责任、经济纠纷，应自行承担相应责任。

6. 各单位、部门应做好：重要数据异地备份；日志信息留存；服务器、虚拟机安全升级（包括及时安装和升级系统、网络

程序和应用软件补丁，安装杀毒软件并及时更新)；妥善保管相关密码并不定期修改密码（密码应由数字、字母和特殊字符组成且长度应大于 10 位)；防止服务器、虚拟机被人为攻击、利用。如因此引发网络与信息安全事件，各单位、部门应承担相关责任。

7. 对使用独立 IP 地址或拥有独立服务器主机的单位、部门，其负责人和相关工作人员应对独立 IP 地址或独立服务器主机的安全运行和使用负网络与信息安全方面的全部责任。

8. 各单位、部门的主要负责人、分管负责人、相关工作人员、网络、信息系统（含网站、新媒体等）发生变更，应第一时间以书面形式通知信息化建设与管理处和党委宣传部，并在信息化建设与管理处办理重新备案或进行备案登记变更。

9. 各单位、部门应定期组织人员参加学校组织的网络与信息安全相关专业技术教育培训。

第七条 各单位、部门领导班子网络与信息安全工作履职情况应纳入领导干部考核指标体系,作为领导干部综合考察的重要依据之一。

第八条 凡未履行职责和落实责任或因工作疏忽而发生不安全或不稳定事件、有下列情形之一的，应逐级倒查，追究当事人、分管负责人、主要负责人责任。监管不力的，还应当追究监管部门负责人责任。

1. 单位、部门网站、关键信息系统等基础设施遭受攻击篡改，导致不良信息或者谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；

2. 发生国家秘密泄露、大面积个人信息泄露的；

3. 封锁、瞒报网络安全事件情况，拒不配合相关管理部门依法开展调查、处置工作，或者对相关管理部门通报的问题和风险隐患不及时整改并造成严重后果的；

4. 发生其他严重危害网络安全行为的。

对领导班子、领导干部进行问责，由纪委监察部门依据有关规定实施。

第九条 网络意识形态工作责任制和涉密网络、涉密信息系统、涉密计算机相关管理按照学校有关规定执行。

第十条 本办法由网络安全与信息化领导小组办公室负责解释，自印发之日起施行。

湖北大学学校办公室　　2018 年 1 月 8 日印发

校对:孙　倩