**江汉大学关于进一步加强网络与信息安全管理的通知**

各部门、各单位：

为贯彻落实习近平总书记关于网信工作的重要讲话精神和中央、省、市领导关于网络与信息安全工作的指示，按照武汉市教育局《关于进一步加强全市教育系统网络与信息安全工作的通知》（武教办[2018]8号）的要求，现就进一步加强我校网络与信息安全工作的有关要求通知如下。

**一、健全组织与责任体系**

学校成立了网络安全与信息化领导小组，校党政主要负责人任组长，副校长任副组长，各职能部门和有关单位、学院负责人为成员。领导小组下设办公室，该办公室设在网络信息与教学设备管理中心，是负责网络安全和信息化建设工作的常设机构，校内各单位应配合网络信息中心做好网安工作。

按照"谁主管谁负责、谁运维谁负责、谁使用谁负责"的原则，校党委宣传部、保卫处负责网络安全教育和综治网安工作，并负责网上信息安全审查；网络信息中心负责提供技术支持。

 各单位须明确主要负责人为网络信息安全第一责任人，分管网络安全工作负责人为主要责任人，部门网络管理员为直接责任人，具体负责本单位计算机网络信息安全等管理、保障和维护工作，对本单位网络与信息安全承担责任。

**二、制定完善规划和管理制度**

(一)加强规划建设

各单位要按照国家有关政策要求，结合自身实际，制定网络与信息安全总体规划。网络安全与信息化建设要同步规划、同步建设、同步使用，切实将网络与信息安全作为单位信息化建设工作摆在重要位置。

(二)建立完善管理制度

各单位要参照国家有关标准规范，加强安全管理策略研究，建立并完善网络与信息安全管理的各项规章制度，包括人员管理、账号管理、计算机软硬件管理、信息系统建设与运维管理、信息发布管理、机房管理、数据安全及使用管理、数据备份、应急预案、应急演练等，并认真落实。

**三、建立工作机制**

(一)建立常态化核查机制

各单位对上级管理部门要求的网络与信息安全重要调查数据，各单位要根据实际情况如实填写，不得弄虚作假。

各单位要不定期对重要信息系统(网站)进行现场核查，了解网络与信息安全管理工作落实情况，工作不到位的单位按要求进行整改。

要按网络安全管理规范，定期对自有信息系统(网站)进行自查，及时修复漏洞、完善防护策略。

(二)建立预警与通报机制

要建立联系预警网络及联动机制，及时转发预警信息，跟踪、监督整改情况，适时上报整改报告。

建立学校网络安全通报机制，对教育部、省教育厅、市网信办等主管部门下发的网站漏洞信息及时通报，敦促及时整改。按照上级和学校的要求整改完成后，各单位要填写**《江汉大学网站（信息系统）风险整改报告》**，递交网络中心。

(三)健全应急处置机制

各单位要制定网络安全应急处置预案，细化网络安全应急工作流程，定期组织演练并做好演练记录。

存在网络安全漏洞或风险的单位，要结合实际情况，迅速进行整改，在规定的时限内无法整改到位的，必须关停信息系统(网站)，进行线下修复。

加强网络安全值守，重要信息系统(网站)要建立7×24小时值班制度，明确值班值守职责任务，保持通讯联络通畅。

发生网络入侵攻击、控制破坏、篡改窃密等网络安全事件，要确保能立即采取阻断网络攻击或暂停系统运行等措施，降低损害程度，防止事件扩大，保存相关记录，立即向主管部门和属地公安机关报告。做到应急处置迅速，上报及时。

(四)建立责任追究机制

对存在下列行为的，一经发现，将责令限期改正，行为严重的将通报批评一是未按规定备案、审批的；二是未按规定落实安全管理制度、措施的；三是未按规定开展系统安全状况检查的四是未按规定开展信息安全等级评定的；五是接到上级网络安全整改通知拒不按规定整改的；六是在网络安全数据调查中蓄意弄虚作假的。

因管理不善、未落实网络与信息安全管理相关规定，致使发生重大网络与信息安全事件的单位，将按有关规定严肃追究主管领导和相关责任人的责任，情节特别严重的报公安机关依法追究法律责任。

**四、强化防护措施**

(一)严格按要求办理互联网接入及信息服务备案手续

《计算机信息网络国际联网安全保护管理办法》(公安部第33号令)规定，凡接入互联网的服务器应当办理备案手续，备案信息是进行网络与信息安全监管的重要依据。

各单位在建设信息系统(网站)时，必须办理相关备案手续。单位主体信息发生变更时，必须及时办理更正手续。当信息系统(网站)关闭不再使用时，必须及时办理备案注销手续，关闭服务以防出现网络安全风险。凡属单位的信息系统(网站)，必须上线前履行备案手续，严禁忽视备案以脱离监管。

(二)强化技术防护

各单位要结合本单位实际，研究制定网络与信息完全防护方案，落实互联网安全保护技术措施，建立多层次网络与信息安全技术防护体系。按需配备防火墙、网页防篡改系统、安全网关、入侵防御系统、网络安全准入管理及访问控制系统、网络及数据安全审计系统等网络与信息安全防护设备和软件，实现安全防护、监测预警、灾难恢复、安全认证等安全保障功能，构建可信、可控、可查的网络与信息安全技术防护环境。没有采用安全防范措施的信息系统(网站)严禁接入互联网。

(三)全面推进等级保护工作

各单位要将信息系统安全等级保护作为一项长期任务，按照《教育部办公厅关于印发<教育行业信息系统安全等级保护定级工作指南(试行)〉的通知》(教技厅函[2014)74号)、《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》（教技[2015] 2号)等文件要求，积极开展信息系统定级、备案、测评、整改等工作，确保重要信息系统的安全稳定运行。未定级或定级不准的信息系统要进行准确定级和备案；已定级的信息系统要按照所定级别进行等级测评和整改新建信息系统要在系统规划设计阶段同步确定信息安全保护等级，实施阶段同步建设安全防护措施。

(四)强化数据信息安全管理

各单位在工作中收集、使用个人电子信息时，应当遵循合法、正当、必要的原则，明确收集或使用信息的目的、方式和范围，建立信息收集、处理及应用的工作流程和管理制度。对掌握的个人电子信息应严格保密，不得泄露、篡改、毁损、出售或者非法向他人提供。学生、教师等个人电子信息对外提供时应严格履行审批手续。在各类信息系统中使用的账户和密码应妥善保管、严格保密，密码必须满足一定的复杂性要求，不得向任何其它单位和个人提供。

(五)加强网络与信息安全经费投入

各单位要建立稳定的网络安全经费投入机制，将网络安全工作经费纳入年度预算。有条件的单位可设立专项经费，重点支持信息安全等级保护、安全防护能力提升、信息安全服务等工作。

(六)加强队伍建设和人员培训

各单位应选派具有网络和信息系统管理经验和专业技能的人员从事网络与信息安全管理工作，有条件的单位应建立网络与信息安全管理专职队伍和技术支撑专业队伍，落实岗位责任和考核机制。要制定网络与信息安全的培训规划，开展面向全员的普及性培训，加强管理和技术人员的专业培训，逐步实行管理和技术人员持证上岗。

网络信息与教学设备管理中心

2019年1月9日