中共安徽理工大学委员会文件

校发〔2018〕112号

关于印发《安徽理工大学网络信息安全管理办法（试行）》的通知

纪委，党委各部门，各基层党委、党总支、直属党支部，校工会、校团委，各行政部门、各学院（部）、各直属单位:

《安徽理工大学网络信息安全管理办法（试行）》已经校党委常委会会议研究通过，现予印发，请认真遵照执行。

中共安徽理工大学委员会

2018年12月28日

安徽理工大学网络信息安全管理办法（试行）

第一章　总则

第一条　为贯彻落实《中华人民共和国网络安全法》，保障学校网络与信息化工作的健康发展，制定本办法。

第二条　网络信息安全是指网络基础设施、网站、信息系统及数据内容等受到保护，保证网络、信息及内容的安全性、完整性、可用性、可控性。

第三条　网络信息安全管理的基本原则是“谁主管、谁负责，谁运营、谁负责”，明确责任、突出重点、保障安全。

第四条　网络信息安全管理的总体方针是以国家标准《信息系统安全等级保护基本要求》（GB/T 22239-2008）为指导，预防为主、综合防范。

第五条　网络信息安全管理的目标是建立健全网络信息安全保障体系，提高安全防护能力，确保学校网络信息安全工作规范有序开展，保障学校信息化可持续发展。

第二章　组织架构

第六条　学校网络与信息安全领导小组负责制定学校网络信息安全相关政策，研究处理重大网络信息安全事件，定期召开网络信息安全工作会议，统筹指导学校网络信息安全建设。

第七条　学校网络与信息安全领导小组办公室设在现代教育技术中心（以下简称“现教中心”），负责学校网络信息安全的日常工作。

第八条 学校各单位负责本单位网站及信息系统的建设、管理及安全运维。各单位主要负责人是本单位网络信息安全工作的第一责任人，同时，各单位须设置网络信息管理员，负责本单位网络信息安全具体工作。

第三章 网络信息安全建设

第九条 各单位在制作网站或信息系统的项目预算时，须包含网络信息安全的专项经费，用于该网站或信息系统的安全建设及运维。

第十条 各单位须明确网站或信息系统是否需要对校外开放，对校外开放的网站或信息系统，须满足国家标准《信息系统安全等级保护基本要求》规定的二级（或以上）安全等级要求，各单位明确其网络及信息安全需求，提供安全策略，由现教中心进行防火墙设置。

第十一条 各单位信息系统在上线前，须开展安全自查工作，提供安全自查报告，并填写《安徽理工大学非涉密信息系统基本情况备案表》(见附件)，由本单位主要负责人签字确认并加盖公章，报现教中心备案。

第十二条 现教中心采用专业技术手段对网站或信息系统进行安全检测。检测未通过的须进行安全整改，直至检测通过方可上线运行。

第四章 运行管理

第十三条 各单位须定期对本单位自己建设的网站（不在

学校网站群平台中）及信息系统（自行采购、管理、运行的系统）开展安全巡检，并做好巡检记录，同时必须自行做好系统与数据的备份工作。对校外开放的网站或信息系统，要求每周巡检一次，只对校内开放的网站或信息系统，要求每月巡检一次。

第十四条 各单位须定期对网站及信息系统进行漏洞修补，包括：操作系统漏洞、应用系统漏洞、中间件漏洞、数据库漏洞等。

第十五条 学校将定期对全校的网站及信息系统开展安全检查。对检查不合格的网站或信息系统，视其安全隐患级别，分别采取限期整改、暂停其外网访问、关闭网站或信息系统等方式处理，同时通知责任单位。责任单位完成整改后，将整改报告提交现教中心，经安全复查合格后，方可恢复该网站或信息系统的正常访问。

第十六条 特殊时期，各单位须加强网站及信息系统的安全监管工作，安排专人值守，加强安全巡检，做好安全整改。

第十七条 信息系统注销，由备案单位提出书面申请，主要负责人签字并加盖单位公章，报现教中心备案，并办理相关手续。

第五章 安全事件应急响应

第十八条 安全事件分为紧急事件和普通事件。

第十九条 紧急事件是指：

1.可由校外访问的页面发生篡改或被替换成非法信息的事件，尤其是发生在主页、新闻网站、招生信息网等访问量高的

系统或网站的事件。

2.影响学校系统正常运转的攻击事件，如：办公自动化系统、教务系统、财务系统、一卡通系统等相关的攻击事件。

3.可能造成师生隐私信息被窃取、丢失、损坏的漏洞。

4.其它可能对社会公共安全或学校造成危害或不良影响的事件或漏洞。

第二十条 普通事件是指:

1.对校内开放系统或网站的页面发生无害篡改或有隐藏漏洞。

2.影响不大的攻击事件或可能造成中低隐患的漏洞。

3.其他不构成公共危害或社会不良影响的安全事件或漏洞。

第二十一条 网络信息安全事件应急响应流程如下:

1.现教中心接到安全事件通报，通过沟通协调，结合技术手段，获取事件截图等相关证据。

2.现教中心核实事件类别，发起处理流程。

3.若事件为紧急事件，现教中心第一时间关闭相关网站或信息系统的访问权限，以降低不良影响，同时向分管校领导汇报并通报责任单位相关情况及事件证据。若事件为普通事件，则此环节略过。

4.现教中心指导分析事件原因，并提供整改建议。

5.责任单位对网站或信息系统进行安全修复，并提交整改报告。

6.现教中心对修复后的网站或信息系统进行安全复查，复查通过后恢复其访问权限。

第二十二条 各单位须制定本单位的网站及信息系统安全应急预案，并定期进行安全应急演练。

第六章 附则

第二十三条 涉密网络信息系统的安全保护遵循国家相关规定，不适用本管理办法。

第二十四条 本办法自发布之日起施行，由现代教育技术中心负责解释。

安徽理工大学党政办公室 2018年12月28日印发