中共金陵科技学院委员会
金 陵 科 技 学 院 文件

金委字〔2019〕3号
金院字〔2019〕1号

关于印发《金陵科技学院网络信息系统安全管理办法》的通知

各有关党委、党总支部、直属党支部，各单位、部门:

《金陵科技学院网络信息系统安全管理办法》已经校党委常委会审定通过，现印发给你们，请认真贯彻执行。

中共金陵科技学院委员会　　金陵科技学院

2019年1月4日

金陵科技学院网络信息系统安全管理办法

第一章　总　　则

第一条　为了保障金陵科技学院校园网络及信息系统的安全稳定、确保学校网络信息安全工作规范有序开展、促进学校信息化健康可持续发展，根据《中华人民共和国网络安全法》等国家相关法律法规并结合我校实际情况，特制定本管理办法。

第二条　信息系统是指我校各单位在校园网内或经学校备案在公有云上构建的网站、系统及数据内容等，保证网络、系统及内容的安全性、完整性、可用性、可控性。

第三条　依据“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，逐级落实信息系统安全责任，实现明确责任、突出重点、自主防护、保障安全的目标。

第四条　任何单位及个人不得利用学校网络和信息系统泄露国家或学校秘密、危害国家或学校安全，不得侵犯国家、集体和个人的合法权益，不得从事违法犯罪活动。

第二章　组织架构

第五条　网络安全与信息化工作领导小组是学校网络安全和信息化工作的领导机构，负责研究学校网络信息安全相关政策，指导学校网络信息安全建设，定期召开网络信息安全工作会议，研究处理重大网络信息安全事件。

第六条 信息化建设与管理中心（以下简称信息中心）为学校网络安全与信息化工作领导小组办公室单位，负责学校网络信息安全工作的统筹规划、建设、管理，以及技术支持、保障与培训等日常工作，党委办公室负责重大网络安全问题处理的统筹协调工作，党委宣传部负责信息发布和媒体联络工作。

第七条 学校各单位负责本单位（含本单位的组织及个人）网站及应用系统的建设、运维以及内容管理。各单位主要负责人为本单位网络信息安全工作的第一责任人，同时，各单位需明确分管网络信息安全的领导，并设置网络信息安全管理员，负责本单位网络信息安全具体工作，并负责与信息中心对接。人员发生变动时，需及时报送信息中心备案。

第三章 系统安全

第八条 各单位在建设网站或信息系统时，须同步建立网络信息安全体系，在技术方案、经费预算及运行维护等方面予以落实，以确保安全，并报送信息中心备案。

第九条 各单位需明确本单位的网站或信息系统是否需要对外网开放，如需要对外网开放，则需按照《信息系统安全等级保护基本要求》（GB/T 22239-2008）规定的二级（或以上）安全等级要求进行建设及管理。

第十条 各单位网站或信息系统上线前，需开展安全自查工作，并填写相关登记表与安全责任承诺书，由本单位网络信息安全分管领导签字确认后，提交信息中心备案。信息中心负

责上线前的专业安全检测，检测未通过的网站或信息系统需进行安全整改，检测通过后方可上线运行。

第十一条 各单位应定期对本单位的网站及信息系统开展安全巡检、漏洞修补。对校外开放的网站或信息系统，每月巡检一次；对校内开放的网站或信息系统，每季度巡检一次。

第十二条 信息中心定期对全校的网站及信息系统开展安全检查，检查不合格的网站或信息系统，视其漏洞级别暂停其外网访问，同时通知责任单位限期整改并提交整改报告。整改完成并经复查合格后，方可恢复正常访问。

第十三条 切实加强网站及信息系统的安全管理工作。信息化处加强整体安全监管，做好整体技术防范；各单位加强本单位网站及信息系统的安全巡检工作，做好系统防护、安全整改等工作。

第四章 数据安全

第十四条 本办法所涉及的数据是指各类信息系统所覆盖的相关业务数据，包括但不限于：智慧校园门户、人事系统、OA 系统、学工系统、教务系统以及其他各类信息系统产生的数据。

第十五条 金陵科技学院数据管理部门包括数据统筹管理部门、数据生产部门、数据使用部门三部分。

第十六条 信息中心是学校数据资产的统筹管理部门，负

责主数据中心、数据仓库平台、数据共享平台的安全管理，并规范数据服务流程，确保数据流向清晰，实现数据可控、可管、可查。

第十七条 数据生产部门为权威数据的单一来源部门，负责数据收集、维护、使用、备份、归档等全程安全，需遵循学校信息标准规范及数据服务规范。

第十八条 数据使用部门根据实际需求向信息中心和数据生产部门提出申请，获得批准后方可使用。数据使用部门有义务和责任保护所获得数据的安全，未经允许，不得将数据用于其他用途。

第十九条 未经批准，任何单位或个人不得擅自提供信息系统产生的内部数据。对于非法泄露或擅自提供数据的单位或个人，依照相关法律法规予以处理。

第五章 内容安全

第二十条 任何单位和个人必须遵守《中华人民共和国计算机信息网络国际互联网络管理暂行规定》、国家有关法律法规和学校的有关管理规定，严格执行信息安全保密制度，并对所提供和发布的信息负责。

第二十一条 任何单位和个人不得利用校园网及经学校备案的公有云系统制作、复制、传播下列信息:

(一)煽动抗拒、破坏宪法和法律、法规实施的;

(二)煽动颠覆国家政权，推翻社会主义制度的;

(三)煽动分裂国家、破坏国家统一的;

(四)煽动民族仇恨、民族歧视，破坏民族团结的;

(五)煽动非法集会、结社、游行、示威、聚众扰乱社会秩序的;

(六)捏造或者歪曲事实，散布谣言，扰乱社会秩序的;

(七)宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的;

(八)公然侮辱他人或者捏造事实诽谤他人的;

(九)损害国家荣誉和利益的;

(十)以非法民间组织名义组织活动的;

(十一)其他违反宪法和法律、行政法规的。

第二十二条 需严格遵循内容审核机制，规范信息发布审批流程，加强信息安全监控，防止出现内容篡改等安全事故。

第二十三条 宣传部负责网站内容审查及监管，信息中心负责技术支持和保障。

第六章 应急响应

第二十四条 网络信息安全事件分为紧急事件和普通事件。

第二十五条 紧急事件是指:

(一)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。

(二)影响学校系统正常运转的攻击事件，如与服务门户、教务系统、财务系统、办公自动化系统等相关的攻击事件。

(三)可能造成师生隐私信息被窃取、丢失、损坏的漏洞。

(四)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。

第二十六条 普通事件是指:

(一)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。

(二)影响不大的攻击事件或可能造成中低隐患的漏洞。

(三)其他不构成公共危害或社会不良影响的安全事件或漏洞。

第二十七条 网络信息安全事件应急响应如下:

(一)信息中心接到安全事件的通报后，通过沟通协调，结合技术手段，获取事件截图等相关证据。

(二)信息中心核实事件类别，发起处理流程。

(三)若事件为紧急事件，信息中心第一时间向相关校领导汇报，同时通报责任单位相关情况及事件证据，并关闭相关网站或信息系统的访问权限，以降低不良影响。

(四)信息中心指导分析事件原因，并提供整改建议。

(五)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。

(六)信息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。

第二十八条 学校制定“金陵科技学院网络与信息系统安全应急处置预案”和“金陵科技学院安全工作责任制考核指标”（见附件内容），各单位负责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。

第七章 附 则

第二十九条 依据《中华人民共和国网络安全法》第六章“法律责任”的规定，因网络信息安全导致的事故，由网站或信息系统所属单位和责任人承担相应的经济处罚、民事责任、治安管理处罚或刑事责任。

第三十条 网络信息失泄密事件按照国家和学校相关法律法规和规章制度处理。

第三十一条 本管理办法自发布之日起施行。

第三十二条 本办法由信息化建设与管理中心负责解释。

附件：1. 金陵科技学院网络与信息系统安全应急处置预案

2. 金陵科技学院二级单位网络安全工作责任制考核指标

附件 1

金陵科技学院网络
与信息系统安全应急处置预案

一、总则

(一)指导思想：减轻和消除网络安全突发时间造成的危害和影响，维护学校的安全和稳定，“统一领导、统一指挥、各司其职、整体作战、发挥优势、保障安全”

(二)适用范围：金陵科技学院校园网络与信息系统

(三)处置原则：快速、有效

二、组织指挥和职责任务

(一)组织指挥

由学校网络安全与信息化领导小组组织指挥。

(二)职责任务

一般事件（详见《金陵科技学院网络信息系统安全管理办法》第二十六条）及时向学校网络安全与信息化领导小组办公室汇报，紧急事件（详见《金陵科技学院网络信息系统安全管理办法》第二十五条）应直接向学校网络安全与信息化领导小组组长汇报。

党委办公室、党委宣传部和信息中心分工协作，共同组织做好部门协调、事件处置、信息发布和媒体联络等相关工作。

各学院、处、所网络信息员应配合信息中心技术人员进行

技术处理，无法处理的应尽可能完整地保护现场并及时通知公安部门。

三、处置措施和处置程序

(一)发现情况

信息中心严格落实安全责任制度，做好校园网信息系统安全的日常巡查及其每周访问记录的备份和访问日志保存工作，以保障及时发现并处置灾害及突发性事件。

(二)预案启动

一旦事件发生，立即启动应急预案，进入应急预案的处置程序。

(三)应急处置方法

在事件发生时，首先应区分事件发生是否为自然灾害与人为破坏两种情况，根据这两种情况把应急处置方法分为两个流程。

流程一：当发生的事件为自然灾害时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

流程二：当人为或病毒破坏的灾害发生时，具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的信息网络设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏

来源的 IP 或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照灾害发生的性质分别采用以下方案:

1.病毒传播：针对这种现象，要及时断开传播源，判断病毒的性质、采用的端口，然后关闭相应的端口，在网上公布病毒攻击信息以及防御方法。

2．入侵：对于网络入侵，首先要判断入侵的来源，区分外网与内网。入侵来自外网的，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵地 IP 地址的访问，在无法制止的情况下可以采用断开网络连接的方法。入侵来自内网的，查清入侵来源，如 IP 地址、上网帐号等信息，同时断开对应的交换机端口。然后针对入侵方法建设或更新入侵检测设备。

3．信息被篡改：这种情况，要求一经发现马上断开相应的信息上网链接，并尽快恢复。

4．网络故障：一旦发现，可根据相应工作流程尽快排除。

5．其它没有列出的不确定因素造成的灾害，可根据总的安全原则，结合具体的情况，做出相应的处理。不能处理的可以请示相关的专业人员。

(四)情况报告

事件发生时，一方面按照应急处置方法进行处置，同时判定事件的性质，紧急事件应直接向学校网络安全与信息化领导小组组长汇报，同时向市委网信办报告。一般事件向学校网络安全与信息化领导小组汇报，并及时报告处置工作进展情况，

直至处置工作结束。

情况报告内容包括：事件发生的时间、地点，事件的级别，事件造成的后果，应急处置的过程、结果，灾害结束的时间，以及如何防范类似灾害发生的建议与方案等。

(五)发布预警

事件发生时，可根据事件的危害程度适当地发布预警，特别是一些在其它地方已经出现，或在安全相关网站发布了预警而学校信息网络还没有出现相应的安全事件，除了在技术上进行防范以外，还应当向用户发布预警，直至安全事件警报解除。

(六)预案终止

灾害险情或安全事件已消除，或者得到有效控制后，由学校网络安全与信息化领导小组宣布险情或事件应急期结束，并予以公告，同时预案终止。

四、保障措施

(一)人员保障

敏感期间，安排 24 小时专人值班、联系。各单位安排网络安全员 24 小时监控网页的互动栏目等。

(二)技术保障

已配备防火墙系统、网页内容过滤器、网络防病毒系统；网管人员可通过远程网管环境及时反应；已购买网络安全产品厂家的远程技术支持。网页的互动栏目尽量采用先审后发机制。

（三）训练和演练

通过校内各种宣传形式对师生员工进行正面引导、宣传并落实我院关于网络安全的各项规章制度。各学院、处、所安排人员参加网络安全培训。敏感时期之前，在学校网络安全与信息化领导小组统一部署下，安排全校范围演练。

五、工作要求

所有相关单位工作人员必须坚持在岗、保证通讯畅通、工作认真负责。

附件 2

金陵科技学院二级单位网络安全工作责任制考核指标

序号	考　　核　　项	分值
1	认真落实上级部门及学校关于信息化建设、意识形态工作等的政策文件、工作方案或实施办法	20
2	根据学校相关要求，签订《金陵科技学院网络与信息安全承诺书》，落实责任人和工作联系人，认真做好本部门的网络安全工作计划和实施，落实相关网络和信息系统安全保障措施	10
3	做好本部门网络及信息系统安全监测、重要信息的备份、用户弱密码检测、隐私信息是否脱敏；针对发现问题及时加固落实预警信息的查验、反馈	10
4	严格文件发布和审批制度，网站页面能正常访问，各栏目及其子栏目内容及时更新，网站链接经过审核把关，不存在错链和断链，网站提供的各项服务正常	10
5	网站所属单位职责明确，信息发布审核和保密审查机制健全，发布的信息不存在错漏、表述不准确、数据不严谨、错误政治倾向等情况	15
6	网站安全防范工作到位，管理员账号密码专人保管，采取了防攻击、防篡改、防病毒等安全防护措施；切实抓好内网、外网、网站的安全；确保“涉密计算机不上网，上网计算机不涉密”，严格按照保密要求处理光盘、硬盘、优盘、移动硬盘等管理、维修和销毁工作。	10
7	网站和信息系统安全运行无上级主管部门和电信运行部门等相关单位通报漏洞及网络安全事件发生	15

8	采用多种形式对网络安全法进行宣传，并组织培训，根据工作内容结合实际，以多种形式开展网络安全宣传教育活动，如举办在线学习、讲座、展览、组织培训、竞赛、制作宣传片等组织开展相关宣传活动	10
合计		100

金陵科技学院 党委办公室 院长办公室 2019 年 1 月 4 日印发