桂林电子科技大学文件

桂电网信〔2022〕1号

关于印发《桂林电子科技大学网络安全管理办法》的通知

各单位、各部门：

现将《桂林电子科技大学网络安全管理办法》印发给你们，请认真遵照执行。

桂林电子科技大学

2022年7月21日

桂林电子科技大学网络安全管理办法

第一章 总 则

第一条 为规范学校网络安全管理，提高防护能力和水平，保障学校各项事业健康有序发展，根据《中华人民共和国网络安全法》、《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》等文件要求，结合学校实际，特制定本办法。

第二条 本办法所称网络安全工作是指为保障学校建设、运行、维护或管理的校园网基础设施、数据中心、信息系统、移动互联网应用程序、网站、数据等信息资产的机密性、完整性、可用性而开展的相关管理和技术工作。

第二章 组织机构及职责

第三条 学校党委对学校网络安全工作负主体责任。学校网络与信息安全工作领导小组是学校网络安全管理的议事决策机构，负责学校网络安全工作的顶层设计、重大决策和指导监督。

第四条 网络与信息技术中心是学校网络安全工作的管理监督、统筹协调和组织实施部门，负责学校网络安全总体规划、统筹推进及检查考核，协调网络安全事件的处理，对学校信息化基础设施和公共服务平台进行整体防护。

第五条 网络与信息技术中心配合保卫处负责对网络违规行为进行调查、取证和处理，根据相关证据及事态影响或破坏程度，对违规者按照有关规定进行处理，或移送公安机关处理。

第六条 各单位各部门应根据本部门信息化建设情况，建立本部门内部的网络安全管理制度，组织和实施本部门的网络安全工作，遵循学校的管理规范和技术标准，负责本部门建设、运维、使用的信息系统及内部网络的安全工作。

第七条 各单位各部门领导班子主要负责人是本单位本部门网络安全第一责任人；各部门主管网络安全的领导班子成员是直接责任人。信息化项目建设部门或牵头部门负责该项目网络安全工作的具体落实；通过外包服务方式进行服务运维的，建设部门负责督促外包服务单位做好安全运维工作，网络安全监管责任主体为建设部门。

第八条 学校教职工和学生作为校园网络的使用者，有责任和义务遵守学校网络安全相关规定，积极参与网络安全的建设和管理。

第三章 校园网运行中的网络安全建设与管理

第九条 校园网及相关基础设施由网络与信息技术中心统一规划、建设、管理和防护，并提供统一网络出口。各单位各部门及个人不得擅自建设、更改、损毁和挪用校园网设施，不得私自接入其他网络的出口，不得私自提供给校外人员使用。

第十条 校园网接入实行登记备案制，使用网络实行实名制

（统一身份认证），不得以其他任何方式私自接入校园网，严禁盗用其他用户账号信息使用校园网。

第十一条 校园网络主要用于学校教学、科研、管理和服务等各项业务，严禁任何部门和个人利用校园网络及相关基础设施开展未经许可的其他活动。

第十二条 业务专网（自建业务网,如保卫处监控网络、各学院自建门禁系统等）中的任何设备不得接入校园网、互联网，校园网的任何设备不得私自接入业务专网。

第十三条 网络与信息技术中心负责统筹学校关键信息基础设施安全保护工作，组织开展关键信息基础设施识别认定、检测评估等工作。

第十四条 校园网 IP 地址未经许可不得对校园网以外提供互联网服务，如在教学、科研上确有特殊需求，需要 IP 地址对外开放服务（限于非信息发布类服务），应经网络与信息技术中心、党委宣传部审批后方可开放，建设部门承担全部网络安全责任。

第十五条 各单位各部门负责本单位本部门安装使用的网络打印机、LED 电子显示屏等物联终端及其控制系统的安全防护，应掌握使用情况、落实防范措施、加强安全监管、确保运行安全，并向网络与信息技术中心备案。

第十六条 终端计算机使用人应做好终端计算机的安全防范，终端计算机上安装、运行的软件须为正版软件，使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第十七条 各部门和教职工、学生使用学校电子邮箱应遵守学校电子邮箱管理等相关规章制度，并对使用其电子邮箱账号开展的所有活动负责，禁止使用电子邮箱传播恶意程序和不良信息，禁止使用电子邮箱存储、处理、传输涉密信息和工作敏感信息。

第十八条 各部门应指定在岗在编的专职人员担任信网工作专员，并向网络与信息技术中心备案；关键岗位的信息系统使用和管理人员应签订网络安全保密协议；离岗、离职人员的访问权限应及时终止。

第十九条 网络与信息技术中心负责组织开展学校网络安全宣传、教育和培训工作，各部门应积极参与，并做好在本部门的宣传推广工作。

第二十条 校园网络用户应文明上网，规范网络行为，并做好个人网络安全防护和隐私信息保护。校园网络用户的上网行为不得危害到学校、集体的整体网络安全，严禁利用校园网络从事任何无授权的探测、破坏、信息窃取等网络攻击活动。

第四章　信息化建设中的网络安全建设与管理

第二十一条 学校信息化建设实行网络安全一票否决制。对于不符合网络安全要求的信息化项目必须先进行整改，整改完成后方可继续建设或提供服务。

第二十二条 各部门对于新建、改建、扩建的信息系统，应遵循学校网络安全相关制度和标准规范，并在规划、设计和建设

阶段同步建设网络安全保障措施，落实网络安全等级保护要求。信息系统投入试运行前，由建设部门初步验收，出具网络安全测评报告、代码安全审计报告和项目初验报告。信息系统投入正式运行前，必须通过必要的网络安全测评，由网信办组织项目终验。对于安全等级第二级以上（含第二级）的信息系统，由网信办统一组织系统备案和网络安全等级保护测评。

第二十三条 学校应在网络安全等保测评、升级加固、评估监测、事件处置、宣传培训和安全运维等方面提供充足的经费保障。

第二十四条 网络与信息技术中心负责学校数据中心的物理安全、网络安全和数据存储安全，各部门应遵循数据中心的管理制度和技术标准，按需申请、有序使用，确保本部门业务系统的应用安全和数据安全，不利用数据中心资源从事任何与申请项目无关或危害网络安全的活动。

第二十五条 各部门的信息系统应部署在学校的数据中心、使用学校 IP 地址及域名并进行审批备案；涉及学校基础数据、教职工和学生个人信息或敏感信息的信息系统，不得部署在校外；未经批准，严禁使用境外数据中心。

第二十六条 与学校教学、科研、管理和服务等各项业务无关或未经信审核备案的信息系统不属于学校信息资产，不得使用学校资金、数据中心、域名、IP 地址建设，不得使用校名、校标等学校标识，一切网络安全责任由系统建设、使用部门和建设、使用人员承担。

第二十七条 对于特殊用途使用非学校域名或在非校园网环境建设的各类信息系统，需经网络与信息技术中心审核后单独备案，原则上不得使用学校资金建设，不得使用校名、校标、域名等学校标识，一切网络安全责任由校内相关部门（包括系统建设部门、使用部门、资金提供部门、宣传推广部门等）及所有参与人员承担。

第二十八条 各部门的信息系统必须使用统一身份认证平台进行身份认证，不得单独建立用户认证系统。

第二十九条 信息系统建设部门是信息系统网络安全等级保护及测评整改的责任主体，应全力配合等保测评工作，并按照要求进行整改加固。网络与信息技术中心负责统筹学校信息系统网络安全等级保护工作，组织各部门开展信息系统定级、备案和等保测评。

第三十条 各部门应采用安全规范、质量和售后服务优良的软硬件产品并选择服务优质、资质和信誉良好的服务厂商承建信息化项目，不得由自然人承担信息化项目的建设任务。

第三十一条 信息化数据资源是学校的公共资源和战略资源，各部门应按照学校信息化数据资源相关管理规定，将业务系统与学校中心数据库对接，加强信息系统的数据安全，对重要数据做好定期完整备份和实时增量备份，确保重要数据资源不被破坏、篡改和泄露。

第三十二条 各部门的网站应基于学校网站群平台进行建设。

网络与信息技术中心负责网站群平台的建设、管理、运行和维护，提供建站的技术支持，各部门负责本部门网站的规范运行和内容安全。

第三十三条 各部门的移动互联网应用程序应基于学校统一的移动平台和入口进行建设、运行和服务。移动互联网应用程序应按照教育部、公安部有关要求履行备案程序，并进行等保测评。

第三十四条 各部门应按照国家有关法律法规的规定严格保护学校师生个人信息，不得违规采集、存储、使用和处理校内各类个人信息，不得通过各类即时社交平台（如微信、QQ 等）和 U 盘传输个人信息。

第三十五条 各单位各部门要加强账户安全管理，杜绝使用弱密码、默认密码和通用密码。

第五章　网络安全监测预警与应急处置

第三十六条 学校授权网络与信息技术中心对校内各类信息系统、网络和其他相关设备开展网络安全检测工作。网络与信息技术中心可根据检测结果启动校内网络安全事件处置流程或发布安全预警。

第三十七条 网络与信息技术中心负责学校网络安全相关的各类安全情报搜集和分析，并结合校内信息化建设实际情况对校内开展网络安全预警。相关部门及人员应根据预警信息，认真落实网络安全自查及问题修复，避免预警相关安全问题的发生。

第三十八条 校内网络安全事件的处理由网络与信息技术中

心负责协调实施。安全事件相关部门及人员应认真落实网络安全事件处置相关工作。为避免扩大安全事件的不良影响，网络与信息技术中心可直接对安全事件相关的网络及信息系统进行断网、停止服务等应急处理。

第三十九条 网络与信息技术中心负责组织校内网络安全事件处置应急演练，相关部门应全力配合，通过演练提高校内网络安全事件处置能力。

第四十条 各部门应根据本部门信息化建设情况制定相应的监控与值守制度和网络安全事件报告流程，发现网络安全问题应及时向网络与信息技术中心报告并进行必要的应急处置，不得在未授权情况下对外公布、测试或利用所发现的安全漏洞或安全隐患。

第四十一条 各部门应对所属信息系统（网站）进行安全监测，安排专人定时巡检和备份数据，留存网络状态、安全事件等相关日志六个月以上，并采取必要的安全措施，严防黑客入侵、数据被篡改、信息泄露等事件发生。

第四十二条 各部门应制定本部门的网络安全应急预案，并报网络与信息技术中心备案；应定期开展网络安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第六章　网络安全奖励与追责

第四十三条 学校将网络安全工作纳入学校发展考核指标体系，将网络安全责任制落实情况作为对各部门、部门领导班子和

领导干部综合考核评价的重要内容，考核结果应与部门绩效奖励和领导干部提职、晋级挂钩。

第四十四条 学校每年组织网络安全先进单位及个人评选，对获奖单位和个人进行表彰奖励。

第四十五条 各部门在收到网络安全整改通知书后，应按要求限期整改，整改不力的，给予通报批评并责令改正；瞒报、缓报网络安全事件的，对相关部门责任人进行约谈并通报批评；玩忽职守、失职渎职造成严重后果的，严肃追究相关人员的责任。

第四十六条 对于违反上述规定的部门和个人，经网络与信息技术中心查实，可对其暂停或终止一切网络与信息化服务。

第四十七条 对于违反法律、法规，造成国家、学校和个人损失的，学校将依法配合公安、网信等主管部门进行处理。

第七章 附 则

第四十八条 本办法下列用语的含义：

（一）校园网，是指校园范围内连接各种信息系统及信息终端的计算机网络，包括校园有线网络、无线网络、物联网和各种虚拟专网，也涵盖与校园网络提供类似服务的运营商网络。

（二）数据中心，主要包括支撑学校信息系统的物理环境（含机房）、软硬件设备、云计算平台、学校中心数据库（含基础数据库）、学校数据公共服务平台（含数据共享与交换平台）、统一身份认证平台及统一信息门户、统一移动门户等信息化基础设施和公共服务平台。

（三）数据，是指学校各类信息系统收集、存储、传输、处理、使用和产生的各种电子数据，包括但不限于网站内容、业务数据、网络课程、图书资源、档案资料、日志记录等。

（四）移动互联网应用程序，是指教育行政部门和学校引入的，用于支撑学校教学、科研、管理、服务的校园移动互联网应用程序，是学校信息系统的重要组成部分，包括但不限于基于移动设备操作系统的原生应用、微信企业号、QQ 校园号、具有业务交互功能的微信小程序、微信公众号、QQ 小程序、支付宝小程序、钉钉企业应用。

（五）终端计算机，是指由学校教职工和学生使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括台式电脑、笔记本电脑及其他移动终端。

第四十九条 本办法所指网络安全不涉及信息内容安全、网络舆情安全、涉密信息系统安全等，其管理由学校相关部门另行规定。

第五十条 各部门应参照本办法制订本部门的实施细则。

第五十一条 本办法由网络与信息技术中心负责解释，自公布之日起施行。

（三）数据，是指学校各类信息系统收集、存储、传输、处理、使用和产生的各种电子数据，包括但不限于网站内容、业务数据、网络课程、图书资源、档案资料、日志记录等。

（四）移动互联网应用程序，是指教育行政部门和学校引入的，用于支撑学校教学、科研、管理、服务的校园移动互联网应用程序，是学校信息系统的重要组成部分，包括但不限于基于移动设备操作系统的原生应用、微信企业号、QQ 校园号、具有业务交互功能的微信小程序、微信公众号、QQ 小程序、支付宝小程序、钉钉企业应用。

（五）终端计算机，是指由学校教职工和学生使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括台式电脑、笔记本电脑及其他移动终端。

第四十九条 本办法所指网络安全不涉及信息内容安全、网络舆情安全、涉密信息系统安全等，其管理由学校相关部门另行规定。

第五十条 各部门应参照本办法制订本部门的实施细则。

第五十一条 本办法由网络与信息技术中心负责解释，自公布之日起施行。