桂 林 学 院 文 件

桂院政办〔2023〕39号

关于印发《桂林学院网络与信息系统安全管理办法》的通知

各二级学院，各部门：

《桂林学院网络与信息系统安全管理办法》已经2023年秋季学期第9次校长办公会议审议通过，现予以印发，请认真组织学习并遵照执行。

桂林学院学校办公室

2023年12月7日

桂林学院网络与信息系统安全管理办法

第一章　总则

第一条 为保障学校网络与信息系统安全稳定运行，规范校园网络与信息系统安全管理工作，确保学校网络与信息系统安全，根据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》《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》等相关法律法规，结合学校实际，制定本办法。

第二条 学校坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第三条 本办法适用于学校所有的网络与信息系统。

第四条 本办法所称网络与信息系统安全工作是指通过采取必要管理措施或技术手段，防范学校网络和信息系统受到攻击、侵入、干扰和非法使用等，保障网络相关基础设施、信息系统及数据的完整性、保密性和可用性，使学校网络和信息系统处于稳定可靠的运行状态。

第五条 学校所有单位及个人均须按照国家有关法律法规要求，合法使用校园网络及信息系统，不得有危害校园网络和信息系统的行为，不得利用校园网络和信息系统侵犯国家、社会、集

体利益及个人合法权益、从事违法犯罪活动、从事以营利为目的的商业活动。

第六条 网络与信息系统安全必须贯穿学校网络信息化建设始终，做到同步规划、同步建设和同步运行。

第二章　组织领导及责任分工

第七条 学校网络安全和信息化工作领导小组是学校网络与信息系统安全管理的领导机构，全面指导学校网络与信息安全工作。

第八条 图文信息中心负责学校网络与信息系统安全防护体系的建设、管理与运行维护，对各单位进行网络和信息系统技术指导、安全监督和应急处置工作。相关职能部门工作职责为：

（一）学校办公室负责与上级部门的沟通协调、网络安全管理政策发文、学校重大突发网络安全事件的统筹协调等工作。

（二）党委工作部负责网络意识形态阵地的舆情监管，负责对校园网络信息内容的编排、维护、语言使用规范等进行指导和监督，负责对学校网络安全保密工作落实情况进行监督、指导和检查。

（三）后勤保卫处负责协助重大网络安全事件的调查处理，负责网络安全相关的安全保卫工作。

第九条 各单位按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，负责本单位建设、运维、使用的各类网络和信息系统的安全工作。

第十条 各单位党政主要负责人为本单位网络与信息系统安全管理第一责任人并负领导责任，各单位应明确本单位网络与信息系统的分管领导及运行维护具体责任人，具体管理本单位的网络与信息系统安全工作。

各单位应将分管领导及系统维护人员信息及系统信息报备至图文信息中心，人员或信息系统有变动时应及时更新并报备。

第十一条 网络与信息系统通过外包服务方式进行维护的，相应的安全监管责任主体仍为系统使用单位，使用单位负责督促外包服务单位做好安全运维工作。

第十二条 广大师生作为校园网的使用者、信息化建设的参与者，有责任和义务遵守国家及学校网络与信息系统安全相关规定。

第三章　保障及机制

第十三条 网络与信息系统安全工作是学校信息化建设的重要工作，学校在人员、资金、技术、设备等方面提供充足的支持与保障。

学校在经费安排上切实保障网络安全等级保护测评、网络安全监测和检测评估、信息系统安全升级和防护加固、网络安全攻防演练、网络安全教育培训、网络安全事件处置和安全运维等网络安全常规工作预算。

第十四条 按照国家相关法律法规要求，学校及时开展校内网络安全等级保护（以下简称等保）工作。图文信息中心负责校

内等保工作的组织协调、等保定级、等保测评、等保整改，确保学校等保工作按照国家法律法规要求正常开展；各单位应积极配合。

第十五条 按照国家相关法律法规要求，学校制定网络与信息安全应急预案，明确应急处置流程和工作职责，落实应急处置技术支撑队伍，开展安全应急演练，提高网络与信息安全应急处置能力。

第十六条 学校积极提高校内相关人员的网络安全工作能力，增强广大师生的网络安全意识，各单位应做好本单位的网络与信息安全宣传推广工作。

第四章　校园网安全建设与管理

第十七条 校园网及相关基础设施由学校网络安全和信息化工作领导小组统一规划、建设，图文信息中心负责管理并提供统一网络出口，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，保障学校网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。各单位及个人不得擅自建设、更改、损毁、挪用校园网及相关基础设施，不得私接外网出口。

第十八条 校园网入网实行实名制和备案制，未经登记不得以任何方式私接校园网，严禁账号共享、私自发展校外用户、盗用其他用户上网账号使用校园网。

第十九条 校园网用户应文明上网，规范网络行为，并做好

个人网络安全维护及校园网个人资源相关网络安全管理维护。校园网用户的上网行为不得危害到学校网络安全和正常秩序，严禁利用校园网从事任何无授权的探测、破坏、信息窃取等互联网攻击活动。

第二十条 信息系统接入校园网使用 IP 地址及域名的，须经图文信息中心审批备案，严禁私自占用网络资源。

第二十一条 违反上述规定的，经查实，图文信息中心可暂停违规用户的一切网络与信息化服务，并根据学校相关规定进行追责处理。

第五章　信息系统安全建设与管理

第二十二条 学校信息化项目建设应遵循校内外网络安全相关制度、技术规范及标准流程，信息化项目全生命周期内各环节均需完成相关网络安全建设工作。各信息化项目上线、验收前必须通过必要的网络安全检测，未通过检测擅自上线或验收的，一切网络安全责任由项目主管单位承担。

第二十三条 各单位原则上应依托校园网开展信息系统建设。涉及学校基础数据、师生员工个人信息或敏感信息的信息系统，不得部署在校外。对于必须使用校外运营服务器、云服务建设的信息化项目，需在采购文件和合同中明确要求由运营单位、云服务供应商负责项目的网络安全建设，由校内项目主管单位及运营单位、云服务供应商共同承担网络安全责任。

对涉及学校基础数据、师生员工个人信息或敏感信息的信息

系统，相关主管单位、运营单位的具体责任人应签订安全保密协议，明确安全和保密义务与权力。

第二十四条 为保证学校信息化建设项目网络安全建设工作及安全运维工作正常开展，应采用安全规范、质量优良的软硬件产品和售后服务优良的供应商，不得由自然人承担信息化项目建设任务。对拒不履行网络安全责任和义务的供应商，列入学校供应商黑名单；触犯相关法律法规的，学校依法配合公安、网信等主管部门进行处理。

第二十五条 学校网络与信息系统实行审批备案制。学校所有信息化项目，均需到图文信息中心办理相关备案手续，完成安全检测、项目验收后方可上线运行。

第二十六条 图文信息中心通过技术手段对校园网络与信息系统进行入侵防护、安全检测并及时通报、处置相关安全事件，相关责任单位应积极响应、主动处理，整改通过后方可继续运行。

第二十七条 信息系统原则上不直接通过学校公网 IP 地址对外提供访问。如需开放至外网、使用域名访问方式的，相关单位应按照信息系统名称的拼音或英文缩写简写设置子域名并提出开放外网申请，经 OA 审批同意后方可使用。

第二十八条 学校杜绝出现并持续清理“双非”系统（网站），即与学校业务相关但未使用学校 IP 或学校域名（gxljc.edu.cn）的信息系统（网站），如使用校外 IP 及校外域名，使用校内 IP 但域名为校外域名等。

第二十九条 面向在校师生提供公共服务及其他业务信息服务系统的账号需落实实名制，确保账号对应到个人。管理员账号、用户账号应妥善保管，不能与他人共用；对无人负责的账号、测试账号应及时采取停用、删除等措施，避免此类账号被非法利用造成网络安全事件。

第三十条 各单位须加强信息系统的密码管理，杜绝弱密码、默认密码和通用密码的使用。密码应使用由数字、大小写字母、特殊字符的组合，长度在 8 位及以上，且密码中不应包含用户名、个人信息及登录页面上出现的信息。尤其是高权限用户密码、管理员密码，至少每 90 天更换一次密码，以增强信息系统的安全防护能力。

第三十一条 对所建设和管理的信息系统，各单位应建立安全管理制度，定期开展网络与信息系统安全自查；采取必要的安全措施，及时修补漏洞、打补丁、升级防病毒软件、检查并留存系统日志，对重要数据备份、加密处理，确保信息系统及数据安全。

第三十二条 信息化建设中所涉及到的个人信息，必须按照国家相关法律法规及学校相关管理规定进行严格保护，任何单位及个人不得违法违规采集、存储、使用和处理校内各类个人信息。

（一）收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用的规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

（二）不得泄露、篡改、毁损收集的个人信息。

（三）不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第三十三条 各单位应加强信息系统生命周期管理，在确定信息系统退出运维和服务周期后及时报告图文信息中心关停相应服务回收计算资源，办理撤销备案手续。

第三十四条 对于不符合网络与信息系统安全要求的各类信息系统必须先进行整改，整改完成后方可继续进行建设或继续提供服务。

第六章　安全检测与安全事件处置

第三十五条 图文信息中心负责对学校各类网络、信息系统和其他相关设备开展安全检测工作，检测结果认定为网络安全事件的，按照《桂林学院网络安全事件应急预案》进行处置，同时按照规定留存相关的网络日志不少于六个月。

第三十六条 图文信息中心建立定期与不定期相结合的安全检测制度。对检查中发现的安全漏洞和隐患，各单位应积极配合整改；对于不积极配合整改的单位或个人，图文信息中心有权直接对相关的网络及信息系统进行暂时断网、暂停服务等应急处理，直至修复漏洞和排除隐患。

第三十七条 图文信息中心按照《桂林学院网络安全事件应急预案》，负责组织实施校内网络安全事件的分级、分类处理。安全事件相关单位及人员应积极配合，认真落实网络安全事件处

置相关工作。为避免安全事件不良影响扩大，图文信息中心应根据学校网络安全事件应急预案进行应急处理。

第三十八条 图文信息中心建立全天候网络安全监测体系，各单位应根据本单位信息化建设情况制定相应的监控制度，重要时期应做好巡检和安全保障工作，发现网络安全问题应及时向图文信息中心报告并进行应急处置。

第三十九条 图文信息中心负责组织校内网络安全事件处置应急演练，各单位应积极参与，通过演练提高校内网络安全事件处置能力。

第七章　奖励与责任追究

第四十条 学校对网络与信息系统存在的安全隐患、漏洞等提供了相关证据和可实施指导方案的单位或个人给予奖励。

第四十一条 对于违反法律、法规，造成国家、学校和个人权益损失的，学校将依法配合公安、网信等主管部门进行处理，并依照国家法律、法规及学校相关规定进行追究责任。

第八章　附则

第四十二条 本办法由学校网络安全和信息化工作领导小组负责解释。

第四十三条 本办法自发布之日起施行，原广西师范大学漓江学院网络运行安全管理暂行办法（漓院政办〔2017〕27号）同时废止。学校原有规定与本办法不一致的，以本办法为准。

桂林学院学校办公室　　2023年12月11日印发