党发〔2023〕39号

沧州师范学院信息系统安全管理办法

第一章 总则

第一条 为保障沧州师范学院校园信息系统安全稳定运行，规范校园信息系统安全管理工作，确保学校信息系统安全，根据《中华人民共和国网络安全法》等相关法律法规要求，结合我校实际，特制定本办法。

第二条 本办法适用于所有学校规划建设的非涉密信息系统，以及构建在校园网上的网站和信息系统。涉及国家机密的信息系统安全管理办法，由学校相关单位另行制定。

第三条 本办法所称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，防范对信息系统的攻击、侵入、干扰和非法使用等破坏，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，使学校信息系统处于稳定可靠的运行状态。

第四条 学校任何单位及个人均应按照国家有关法律法规要求，合法使用校园信息系统，不得有危害校园网络、信息系统及利用校园网络、信息系统侵犯国家与集体利益以及个人合法权益的行为，不得从事违法犯罪活动，不得从事以营利为目的的商业活动。

第五条 信息系统安全必须贯穿学校信息化建设始终，

做到同步规划、同步建设和同步运行。

第二章　组织机构及责任分工

第六条 学校网络安全和信息化工作领导小组是学校信息系统网络安全管理的领导机构，全面指导学校信息安全工作。

第七条 现代教育技术中心负责信息系统安全防护体系的建设以及校级信息系统的运行维护，对各单位进行网络安全技术指导、服务支持、技术监督和考核评估，定期向领导小组报告信息系统安全态势。

第八条 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，分别负责本单位建设、运维、使用的各类信息系统的安全工作。各单位主要领导为本单位信息系统安全管理责任人，并明确指定归属本单位信息系统的运行维护具体责任人，名单报备至网络安全和信息化工作领导小组，人员变动时应及时更新。各单位要建立本单位的网络安全管理制度和应急处置预案。

第九条 广大师生作为校园网的使用者、信息化建设的参与者，同时也是信息系统安全工作的参与者，有责任和义务遵守学校信息系统安全的相关规定，积极参与信息系统安全的建设和管理。

第三章　保障及机制

第十条 信息系统安全工作是学校信息化建设的重要工作，各相关单位应通力合作，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。

第十一条 按照国家相关法律法规要求，学校应及时开展校内网络安全等级保护（以下简称等保）工作。现代教育技术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。

第十二条 按照国家相关法律法规要求，学校应积极开展关键信息基础设施保护工作。现代教育技术中心负责组织关键信息基础设施的认定、网络安全评估及网络安全建设工作。

第四章　校园网安全建设与管理

第十三条 校园网及相关基础设施由现代教育技术中心统一规划、建设、管理，并提供统一网络出口，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。

第十四条 校园网入网实行实名制，校园网用户必须通

过学校统一身份认证接入校园网，未经登记不得以任何方式私接校园网，严禁盗用其他用户上网账号使用校园网。具体要求参照《沧州师范学院校园计算机网络与信息安全管理办法》要求。

第十五条 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。

第十六条 各类信息系统原则上应依托于学校数据中心建设，使用学校 IP 地址及域名，并经现代教育技术中心审批备案。未经许可不得提供网络服务，如确有特殊需求，需经学校网络安全和信息化工作领导小组审批同意，并由申请人员及所在单位承担网络安全主体责任。

第十七条 对于违反上述规定的用户，经现代教育技术中心查实，可对违规用户暂停一切信息化服务，并可根据本办法进行追责处理。

第五章　信息系统安全建设与管理

第十八条 对于不符合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。具体要求参照《沧州师范学院信息系统技术安全漏洞整改流程》和《沧州师范学院信息系统软件项目建设通用

性技术要求》。

第十九条 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、标准流程开展，信息化项目全生命周期内各环节均需要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。

第二十条 对于必须使用校外云服务建设的信息化项目，需按照学校信息化项目建设要求完成审批等流程，在采购文件和合同中应明确要求由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云服务供应商共同承担网络安全责任。

未按要求建设的此类系统，不得使用学校资金建设，不得使用校名、校徽、域名等学校标识，一切网络安全责任由相关单位及参与人员承担。

第二十一条 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。

第二十二条 学校信息系统实行审批备案制。学校所有信息化项目，均需到现代教育技术中心办理审批备案手续，审批通过后加入学校信息系统白名单，方可上线运行。

第二十三条 学校信息系统实行年审制。现代教育技术

中心每年年底对学校所有信息化项目进行年审，审核通过后方可继续运行。

第二十四条 信息系统不允许对外直接提供IP地址。各单位按信息系统名称的拼音或英文缩写简写设置域名并提出申请，经审批同意后方可使用。未经许可，任何单位或个人不得以冠有“沧州师范学院”或“沧州师院”中文及其对应外文字样的名义开通信息系统。

第二十五条 学校应杜绝出现并持续清理以下类型的“双非系统”，包括：

1.使用校外IP地址，但采用caztc.edu.cn域名后缀；

2.使用校内IP地址，但没有采用caztc.edu.cn域名后缀；

3.使用校外IP地址，且没有采用caztc.edu.cn域名后缀，但主要内容与“沧州师范学院”或“沧州师院”中文及其对应外文有关，且没有经过学校备案。各单位应主动持续清理“双非系统”。

第二十六条 面向在校师生提供公共服务的信息系统必须使用学校统一身份认证，不得单独建立用户认证系统。

第二十七条 各单位应针对所建设和管理的信息系统建立安全管理制度，定期开展信息系统安全自查，及时修补漏洞、打补丁、升级防病毒软件、查看系统日志，确保系统安全。

第二十八条 各单位应针对所建设和管理的信息系统按

照学校信息化数据资源相关管理规定，采取必要的安全措施，确保数据安全。

第二十九条 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个人信息保护相关规定进行严格保护，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。

第三十条 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三个月内办理撤销备案和报废手续。

第六章　安全检测与安全事件处置

第三十一条 现代教育技术中心作为学校信息系统安全管理单位，代表学校对各类网络、信息系统和其他相关设备开展安全检测工作，并根据检测结果启动校内信息系统安全事件处置流程或发布安全预警或通报。

第三十二条 现代教育技术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，现代教育技术中心有权直接对相关的网络及信息系统进行断网、停止服务等应急处理。

第七章　奖励与追责

第三十三条 学校对信息系统实行网络安全检查制度，

将网络安全检查结果作为各单位年度信息化业绩考核的重要依据，并对网络安全建设先进单位及个人进行评选和表彰。

第三十四条 对于违反法律、法规，造成国家和学校利益，以及个人权益损失的，学校将依法配合公安、网信等主管部门进行处理。

第八章　附则

第三十五条 本办法由网络安全和信息化工作领导小组负责解释。

第三十六条 本办法自印发之日起执行。