

信息化建设管理办法（试行）

第一章 总 则

第一条 为加强学院信息化建设的统筹规划与规范管理，避免无序建设、重复建设造成的资源浪费，有效实现全校信息资源的有机集成和共享，提升管理效能，不断发挥信息化平台在学院教学、科研及管理方面的保障支撑作用，推进智慧校园建设，根据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术个人信息安全规范》（GB/T35273-2020）、教育部等七部门《关于加强教育系统数据安全工作的通知》（教科信函〔2021〕20号）以及其他相关法律法规和标准，结合学院实际，制定本办法。

第二条 学院信息化建设遵循“统筹规划、分工负责，统一标准、服务师生”的原则，以服务为导向，以促进信息技术与教育教学深度融合为核心，逐步实现高度业务协作和资源整合，提升学院信息化建设质量与技术水平，促进信息资源交换与共享，保证网络及信息安全，为学院的建设与发展提供保障。

第三条 本办法中的信息化建设内容包括：信息化基础设施建设（包括网络工程、服务器、计算机、存储、通用软件等），信息化软件系统建设（包括面向全校业务范围的应用系统、中间件和数据库的采购、开发和集成，以

及后期的维护升级），信息安全建设和信息系统运行维护等。

第四条 信息化建设管理是指对信息化项目调研、申报、立项、招标、建设、验收、运维和结束使用等的全过程管理。

第二章 组织管理

第五条 学院网络综合治理、网络安全和信息化工作领导小组是全面推进学院信息化建设的管理与决策机构。主要职责如下：

- （一）负责审议学院信息化建设发展战略和总体规划；
- （二）负责审议学院信息化建设实施方案和规章制度；
- （三）负责审定学院信息化建设进程中各部门的责任分工、资源分配以及考核机制；
- （四）负责审议信息化建设项目的计划立项、经费预算；
- （五）对学院信息化建设中的重大问题和政策性问题进行决策。

第六条 网络综合治理、网络安全和信息化领导小组办公室是学院信息化建设技术支持部门。其主要职责是：

- （一）负责学院信息化建设的发展规划、规章制度与相关标准体系制定并组织实施，协调校内外信息化建设相关事务；
- （二）负责统筹学院信息化相关项目，对各部门的信息化建设项目进行审批、建设监管和组织验收；指导各部门信息化建设工作；

（三）负责学院网络及基础设施建设，负责校园网络整体安全管理和技术防护；负责校级软件和应用平台建设，保证硬件设备和软件平台的正常运行；负责多媒体教室仪器设备及软件系统的维保管理；

（四）负责学院信息化数据资产治理体系建设，推进学院信息数据资源融合共享和应用；

（五）负责学院通信基站、室外设施及电信固话线路设备的管理；

（六）负责学院数据中心的建设与管理，为学院管理提供决策支撑；

（七）负责学院信息化基础培训和相关系统推广工作，负责开展现代教育的各类技术培训和技術辅导；

（八）承担学院信息化领导小组办公室工作职责。

第七条 学院各职能部门及各系、部承担本部门信息化项目建设和使用管理责任。其主要职责如下：

（一）明确本部门负责信息化工作的领导与网络信息员，并上报学院备案；

（二）负责本部门信息化建设规划与项目申报，并将信息化工作列入部门年度工作计划；

（三）负责本部门信息化项目的建设实施、应用推广和信息安全工作；

（四）负责本部门信息化应用系统上线后的维护与管理工作；

（五）负责推动信息技术在教育教学和日常管理中的应用，主动宣传培训，提升师生信息素养，鼓励教师利用信息技术创新教育教学模式。

第八条 学院按照一定的投资强度将信息化建设及运维管理经费常规化，由学院网络综合治理、网络安全和信息化工作领导小组按照建设规划统筹安排学院信息化建设的先后顺序和进度。学院每年定期组织开展信息化建设项目申报工作，各职能部门及各系（部）根据部门实际需要申报。网络综合治理、网络安全和信息化领导小组办公室负责项目技术方案审定，财务科负责项目经费管理，总务科负责项目招投标和设备采购，网络综合治理、网络安全和信息化领导小组办公室会同使用部门对项目实施建设与验收。

第三章 信息标准和编码的管理

第九条 为实现校内各信息系统互联互通和资源共享（包括校区代码、机构代码、教职工人员编码、学生编码、教学课程、资产信息等），网络综合治理、网络安全和信息化领导小组办公室负责组织制定学院信息系统数据共享标准和集成规范，对标准和规范的编制过程实施统一管理，并协调相关编制代码部门对编码之间的冲突进行修改。

第十条 学院各单位须保持学院编码的唯一性和一致性，严格执行统一的信息编码，不得随意增加、删除编码。如需修改，须报网络综合治理、网络安全和信息化领导小组办公室审核后统一修订。

第十一条 学院各类信息系统的建设或升级须符合信息编码标准和集成规范，严格遵守教育部公布的《全国职业教育智慧大脑院校中台中职数据标准及接口规范》并接入学院融合门户，不符合标准的信息系统，将不予验收，不予接入校园网。

第十二条 本办法发布之前已验收上线的信息系统，若包含信息编码规则与学院统一的信息编码规则不一致，可暂时通过代码转换接入使用，待系统升级改造时执行学院统一编码标准。

第四章 项目申报与立项

第十三条 项目申报。学院各部门根据学院信息化建设规划和本部门业务需要，按照学院每年预算编制要求启动下一年度的信息化建设项目的申报工作，提出拟建信息化项目需求和立项申请。对于有专项规定的信息化建设项目，按照专项规定的办法实施。

学院信息化建设项目申报类别一般包括信息化基础设施建设项目、信息系统建设项目、信息安全建设项目和信息系统运行维护项目等。

（一）信息化基础设施建设项目主要包括校园网络各种交换路由设备、网关设备、服务器（不含各单位计算机购置）、存储设备、综合布线系统，机房建设及公共信息服务支撑平台等新建、更新、维护和升级的项目，教学环境信息化建设项目，通用软件建设项目等。

（二）信息系统建设项目主要包括学院各类公共服务平台、各业务系统（包括网站）的建设或升级改造类项目。

（三）信息安全建设项目主要包括对学院信息系统软硬件平台、信息化应用系统等的信息安全进行安全评估咨询、等级保护和安全保障类项目。

（四）信息系统运行维护项目主要包括对各类信息化应用系统日常的技术维护、功能完善、接口开发等保障系统稳定运行类项目。

（五）信息化计算机及系统建设项目评分指标应按照财政部信息化设备采购标准进行设置，包括《便携式计算机政府采购需求标准（2023 年版）》《操作系统政府采购需求标准（2023 年版）》《工作站政府采购需求标准（2023 年版）》《数据库政府采购需求标准（2023 年版）》《台式计算机政府采购需求标准（2023 年版）》《通用服务器政府采购需求标准（2023 版）》《一体式计算机政府采购需求标准（2023 年版）》规范要求。同时配件需要满足中国信息安全测评中心实时公布的测评公告中《安全可靠测评结果》（3 年有效期）相关配件进行选配。若部门在信息化计算机及系统建设过程中，若必须采购非国产信息化设备或系统，可由建设部门在专家论证前签订《非国产信息化计算机及系统采购申请单》（见附件 1），报分管院领导审批并交网络综合治理、网络安全和信息化领导小组办公室备案。

（六）信息化教学软硬件的安全性和国产化审核应作为采购和招投标的重要考量因素。

第十四条 技术审查。网络综合治理、网络安全和信息化领导小组办公室组织开展申报项目的技术审查工作，具体审查项目的技术路线、功能及性能设计、应用接口设计、安全设计、运行环境需求、标准规范等，还包括：

（一）是否为重复性建设项目；

（二）是否明确了遵守学院信息化编码标准相关要求；

（二）是否明确了与学院公共数据平台和学院统一身份认证系统等应用系统对接相关要求；

（三）是否明确了项目在网络安全、数据安全方面的相关要求；

（四）是否存在其他不符合学院信息化建设规范的内容。

第十五条 专家论证。技术审查通过的项目，项目建设部门在网络综合治理、网络安全和信息化领导小组办公室的协助下组织专家进行论证。

第十六条 审批立项。网络综合治理、网络安全和信息化领导小组办公室根据专家论证情况，编制信息化建设项目年度实施计划及预算，由学院根据年度总体预算情况进行统一审批。审批立项的项目所需经费，纳入学院预算统一管理。

第十七条 学院各部门可以采用自行研发、合作开发、公司承建等多种方式完成信息系统项目建设，但必须通过

技术审查和论证。未经技术审查和批准的信息化建设项目，不予立项、招标和报销。

第五章 项目招标与建设管理

第十八条 信息化项目申请部门负责项目的市场调研、采购需求编制，采购招标申请等相关工作。信息化项目招标工作按照国家及上级政府部门相关法规政策规定执行。

第十九条 信息化项目申请部门全程负责项目的建设，确保项目进度和质量。建设时必须遵循统一的规范和标准，建立与全校数据中心的数据同步机制，提供标准化的交互接口，实现各信息系统的用户认证和数据交换共享，共享数据同步至公共数据库，保证全校数据的唯一性、一致性、完整性、时效性和业务协同。网络综合治理、网络安全和信息化领导小组办公室对信息化建设项目执行情况进行定期检查，对未能按照项目计划执行或难以履行的建设项目进行通报和督促整改。

第二十条 信息化项目申请部门应加强项目管理，控制项目建设中可能发生的对项目进度、质量、费用等方面的影响风险，尽量避免项目建设期间的任何变更，并针对各类变更与风险处理，严格按照学院有关规定和程序执行。

第二十一条 项目申请部门因故终止项目时，应及时总结项目执行情况，并按照学院相关规定清理账目与资产，编制资金决算及资产清单，形成项目终止报告，经分管校领导同意后，报学院综合治理、网络安全和信息化工作领

导小组审议，审议通过后，携带已批示的报告至总务科办理相关政府采购计划终止手续。

第六章 项目验收

第二十二条 学院信息化建设项目验收前需包括功能测试、性能测试、安全测试，确保系统符合设计要求和相关标准。通过安全检测方可对校内局域网提供服务并达到国家一级安全等级保护要求；重要信息化软件系统需对接到互联网上的，需达到国家二级及以上的安全等级保护要求。

第二十三条 信息化项目建设完成后，按照学院有关规定组织验收。项目验收包括部门验收和学院验收两个步骤。

部门验收由项目建设部门自行按照招标文件技术要求、中标单位投标文件、技术协议、商务合同以及其他商议的内容逐项进行验收，并对存在的问题进行整改。

学院验收由项目建设部门联动总务科、财务科、网络综合治理、网络安全和信息化领导小组办公室等相关部门进行验收。经部门验收通过后，项目建设部门方可向学院提出验收申请，并提交项目相关资料：（1）项目申报书；（2）招标文件；（3）投标文件；（4）中标通知书；（5）采购合同与技术协议；（6）《贵州交通技师学院数据保密协议》（见附件2）（注：甲乙双方签订、甲方与乙方技术支持和系统维护开发人员签订）、《贵州交通技师学院网络与信息系统安全责任协议》（见附件3）（注：甲乙双方签订）；

(7) 派出所出具的乙方技术人员或系统维护开发人员近三个月内无犯罪证明；(8) 使用手册；(9) 功能确认单；(10) 部门内部验收单等。以上资料齐全后，学院组织项目验收，并给出验收结论。

第二十四条 项目验收合格后，项目建设部门按照学院规定进行固定资产办理和财务报账。并交一份归档项目验收时的各项资料到网络综合治理、网络安全与信息化建设办公室保存。

第七章 项目应用推广与运行维护

第二十五条 项目建设部门对业务系统的应用推广负责，有义务对使用部门开放相关功能，并对使用人员进行培训，采取灵活多样的宣传方式，加强业务系统的宣传推广，力求受益面最大化。

第二十六条 信息化项目建设部门负责项目的日常运行维护。网络综合治理、网络安全和信息化领导小组办公室协助项目建设部门开展信息化项目的后期运行和维护，根据项目情况，提供运行环境和硬件资源、网络 IP、域名解析以及智慧校园基础平台对接等技术支持。

第八章 网络信息安全管理

第二十七条 各部门应遵守国家网络信息安全保密的有关规定，严格审核，确保提供的上网信息的真实性。发布交换共享的数据时，必须经过数据来源部门的审核认可。各业务部门应密切关注所建设信息化项目的安全性，发现

问题及时解决并报网络综合治理、网络安全和信息化领导小组办公室。

第二十八条 学院网络信息安全管理按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则进行。网络综合治理、网络安全和信息化领导小组办公室负责网络和系统的技防安全，负责对校园网络基础设施进行维护管理，负责学院数据中心运行管理，负责中心数据库容灾备份，负责定期对学院中心机房中信息系统和网站进行系统安全检测并对有安全隐患的进行督促整改，负责保障校园网的畅通运行。各部门负责其管理信息系统和网站系统的数据维护以及必要的数据备份和归档工作。

第九章 附 则

第二十九条 涉密信息化建设项目的建设实施按照国家及学院有关保密规定执行。

第三十条 本办法由网络综合治理、网络安全和信息化领导小组办公室负责解释。

第三十一条 本办法自发布之日起，原有相关规定与本办法不符的，以本办法为准。

附件 1：非国产信息化计算机及系统采购申请单

非国产信息化计算机及系统采购申请单

注：本申请单实行一台设备（一套系统）一张申请单原则

采购原因	注：写明必须使用该非国产产品的原因，说明是否有国产产品可以替代（写明替代的性价比）						
违反条款	例如：第四章 第十三条（五）《便携式计算机政府采购需求标准（2023 年版）》中，未按照要求设置评分点 第四章 第十三条（五）中国信息安全测评中心实时公布的测评公告中《安全可靠测评结果》未有该产品						
产品基础信息	设备或软件名称	规格型号		特殊功能描述		市场价格（元）	
采购人签字	签字： 年 月 日	部门领导审批	签字： 年 月 日	院领导审批	签字： 年 月 日	网信小组备案	签字： 年 月 日

附件 2：贵州交通技师学院数据保密协议

贵州交通技师学院数据保密协议

项目名称：_____

甲方：_____贵州交通技师学院（网络综合治理、网络安全和信息化领导小组办公室）_____

乙方：_____

本协议适用于：

- （1）学院（网络综合治理、网络安全和信息化领导小组）与校内各部门及部门相关个人；
- （2）学院各部门与部门内相关个人；
- （3）学院或院内各部门与校外信息服务提供方。

第一条 乙方必须严格遵守贵州交通技师学院相关管理规定，合理、规范、安全地使用计算机、网络、数据和信息资源。乙方承诺在管理、开发、实施项目的过程中，视所接触到的资料、数据和项目信息为保密内容，承担保密责任。

第二条 来源于贵州交通技师学院的所有资料、数据和项目信息，包括但不限于教职工、学生个人身份信息、贵州交通技师学院组织架构信息、教学、科研、管理、服务等相

关业务信息，以及项目建设内部文件、建设规划和建设方案等资料。

第三条 乙方未经允许，不得访问、删除、修改、增加、复制、备份、摄录、摘抄、打印数据和资料，不得擅自传播保密信息。

第四条 乙方保存数据、资料的存储介质（云盘、U 盘、终端存储等）不可交由其他人使用，或作其他用途，必须妥善保管，严防丢失。

第五条 乙方未经允许，不得进行影响系统运行的操作，如关闭主机（设备）、关闭关键服务、大量数据查询、修改数据库、修改系统配置等。

第六条 乙方对自己使用及管理的账号，要做到指定专人负责使用，且必须加强密码管理，要求管理员账号使用字符、数字、符号组合的复杂密码，长度不小于 8 位，口令定期更换。

第七条 存有保密信息的介质（硬盘、U 盘、磁盘、闪存、光盘等）如需送到学院外维修时，要经过学院保密办审批通过，将涉密资料备份后，对介质进行技术处理（如低级格式化、写零处理等），以防泄密。

第八条 乙方在承担项目工作完成以后，不得保留保密信息的副本，一切关于保密信息的资料销毁或返还信息提供部门，保证信息不会外流；乙方承诺若中途不再从事项目有

关工作，仍对保密信息承担保密责任。

第九条 若违反本承诺书内容，一经发现，学校可视行为严重程度进行行政处分或经济处罚。后果严重者，学校将通过法律途径向乙方索赔，或向司法机关报案处理。

第十条 乙方的保密义务自本协议盖章之日起开始生效，至保密信息公开或被公众知悉时止。乙方的保密义务并不因双方合作关系的解除而免除。

第十一条 凡与贵州交通技师学院发生的相关涉及数据安全的业务，均须签订本责任书。

第十二条 本协议一式三份，甲方（学院网络综合治理、网络安全和信息化领导小组办公室）、乙方（系统承建方）、学院主办（使用）部门各执一份，经签字确认后生效。乙方若违反本协议，愿意承担贵州交通技师学院因此而产生的一切法律责任及损失。

甲方责任部门（盖章）：

乙 方（盖章）：

责任部门负责人（签字）：

乙方负责人及身份

证号：

日 期：

日 期：

附件 3：贵州交通技师学院网络与信息系统安全责任协议

贵州交通技师学院网络与信息系统 安全责任协议

项目名称：_____

甲方：____贵州交通技师学院（网络综合治理、网络安全和信息化领导小组办公室）_____

乙方：_____

按照《中华人民共和国网络安全法》“谁主办，谁负责，谁使用，谁负责”及其他相关法律法规的相关原则，本协议适用于：

（1）学院（网络综合治理、网络安全和信息化领导小组）与学院各部门（主办（使用）部门）

（2）学院各部门（主办（使用）部门）与网络信息服务提供方（承建方）

凡与贵州交通技师学院发生的信息化相关业务，均须签订本责任书。

乙方应严格遵守信息系统备案制度，按要求完成信息系统的域名、主机布置方式、主机布置位置，未经批准，严禁将包含学校标志、标识、LOGO、学校名称的信息系统或 App

部署到校外的 IP、服务器、虚拟主机、IaaS、PaaS、SaaS、DasS 等平台上。未经备案开设信息系统，学校追究主办部门责任并由相关主办部门承担全部安全责任。

乙方必须严格遵守贵州交通技师学院信息与网络安全管理规定和管理办法，合理、规范、安全地使用计算机、网络、数据和信息资源。乙方承诺在管理、开发、实施、维护维修项目的过程中，承担如下安全责任：

第一条 乙方对提供系统的硬件、操作系统、网络承担安全责任。包括但不限于：

- (1) 保障硬件系统的安全稳定运行状态；
- (2) 对操作系统进行漏洞修补、安全更新；
- (3) 对系统所需的各类网络协议与服务端口进行安全设置；
- (4) 对数据进行备份和加密；
- (5) 对病毒、木马程序及网络上出现的各类攻击手段进行事前防范、应急响应、事后处置等工作。

最大限度地保障系统所用软硬件环境的安全。

第二条 乙方对所提供的信息系统及相关辅助软件（如数据库、Web 容器、第三方组件等）承担安全责任。包括但不限于：

- (1) 符合学院信息安全技术要求，对学院信息与网络安全环境和其他系统不造成负面影响；

(2) 对系统进行严格的安全检测、并对安全事件和隐患进行处置;

(3) 负责落实甲方对系统提出的安全工作要求。

第三条 乙方应对乙方工作人员进行网络安全教育, 对其技术行为承担安全责任。包括但不限于:

(1) 在对系统进行建设、开发、安装、维护等各类必要的工作过程中, 不得在服务器上安装各类与建设维护内容无关的软件(如 QQ、微信、支付宝、各类游戏等);

(2) 不得在服务器上进行与建设维护内容无关的各类操作(如打游戏、查询股票等);

(3) 必须按照甲方提供的登录方式进行工作, 不得擅自安装远程登录访问软件, 不得擅自开启任何后门程序进入;

(4) 在系统上线之后进行维护操作对系统访问产生影响的, 应知会甲方, 为甲方提供合理的业务处置时间;

(5) 做好账号管理工作, 防止账号泄露、侵入等事件的发生;

(6) 履行甲方的安全责任有关要求。

第四条 乙方对安全检测、应急响应和安全事件处置承担。包括但不限于:

(1) 对系统进行经常性的安全检测和监控(每季度不少于一次), 并将结果以书面形式报告给甲方;

(2) 系统被检测出或发生安全问题时, 乙方必须在 1

小时内做出响应，48 小时内完成应急处置，有效防止损失的进一步扩大。

第五条 乙方无法在规定时间内响应和完成相关安全工作时，甲方可自行组织开展相关工作，由乙方承担相关费用。

第六条 本协议一式三份，甲方（学院网络综合治理、网络安全和信息化领导小组办公室）、乙方（系统承建方）、学院主办（使用）部门各执一份，经签字确认后生效。乙方若违反本协议，愿意承担贵州交通技师学院因此而产生的一切法律责任及损失。

甲 方（盖章）:

乙 方（盖章）:

部门负责人（签字）:

乙方负责人（签字）:

日 期:

日 期: