ICS 91.040.01
CCS Q 00

T/CS

中 国 商 品 学 会 团 体 标 准

T/CS 481—2026

建筑工程智能投标文件编制技术应用规范

Application specification for the preparation of intelligent bidding documents of construction engineering

2026-09-11 发布　　2026-09-11 实施

中国商品学会　发 布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 系统操作流程 1
4.1 投标策划处理 1
4.2 招标文件解析 1
4.3 投标方案生成 2
4.4 文件排版填充 2
4.5 合规性自查比对 2
5 数据要求 3
5.1 数据标准格式 3
5.2 数据质量要求 3
6 接口要求 3
6.1 接口协议规范 3
6.2 与招投标平台交互 4
6.3 与电子评标系统交互 4
7 质量控制要求 4
7.1 准确性控制 4
7.2 完整性 5
7.3 错误检验 5
7.4 人工复核程序 5
7.5 合规管理要求 6
8 安全要求 6
8.1 商业秘密保护 6
8.2 存储传输安全 6
8.3 用户权限管理 7

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由杭州筑龙信息技术股份有限公司提出。

本文件由中国商品学会归口。

本文件起草单位：杭州筑龙信息技术股份有限公司、五洲工程顾问集团有限公司、绍兴市上虞区标准化研究院、宁波汇泰通信科技有限公司、四川国投建设有限责任公司、祥昇建工有限公司。

本文件主要起草人：吴许杰、方必清、焦尧、贾海峰、费慧慧、许铁峰、陶治、倪文娅、周安迪、项庆辉、董永贤、董硕、顾大正、蒋承杰、杨轮、陈应庚。

建筑工程智能投标文件编制技术应用规范

1 范围

本文件规定了建筑工程智能投标文件编制技术的系统操作流程、数据要求、接口要求、质量控制要求和安全要求。

本文件适用于建筑工程智能投标文件编制技术的应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20275 信息安全技术网络入侵检测系统技术要求和测试评价方法

GB/T 20281 信息安全技术防火墙安全技术要求和测试评价方法

GB/T 20988 网络安全技术信息系统灾难恢复规范

GB/T 22239 信息安全技术网络安全等级保护基本要求

GB/T 36344 信息技术数据质量评价指标

GB/T 43711 电子采购交易规范非招标方式

GB/T 45393.5 信息技术建筑信息模型（BIM）软件第5部分：数据接口

GB/T 50500 建设工程工程量清单计价标准

GB/T 51212 建筑信息模型应用统一标准

DA/T 103 招标投标电子文件归档规范

GM/T 0002 SM4分组密码算法

GM/T 0031 安全电子签章密码技术规范

GM/T 0095 电子招投标密码应用技术要求

JGJ/T 393 房屋建筑和市政工程项目电子招标投标系统技术标准

3 术语和定义

GB/T 51212、JGJ/T 393、DA/T 103界定的术语和定义适用于本文件。

4 系统操作流程

4.1 投标策划处理

4.1.1 获取建筑工程招标公告及招标文件，提取关键要素并生成招标需求图谱。

4.1.2 根据投标人条件和能力，辅助评估项目竞争经济性，筛选并推送匹配的项目信息。

4.1.3 结合历史项目数据，辅助进行投标可行性评估及风险预判，对废标条款、资格条件、技术偏离、报价策略等风险分类提示并提供规避建议。

4.2 招标文件解析

4.2.1 从招标文件中提取关键要素，生成招标要求。提取要素应至少包括但不限于：

a) 项目基本信息；
b) 投标人资格要求；
c) 技术规范；
d) 商务条件；
e) 评标办法和合同条款。

4.2.2 识别并标注招标文件中的废标条款和强制性要求的内容，标注范围应至少包括：

a) 投标有效期；
b) 投标保证金要求；
c) 资格条件底线要求；
d) 技术参数不可偏离项；
e) 报价限制条件。

4.2.3 识别解析补遗文件和澄清文件，实现变更条款与原条款的差异比对，按版本保留差异标记并更新招标需求图谱。

4.3 投标方案生成

4.3.1 解析招标需求，结合投标人输入的信息，辅助确定技术方案和技术保障措施。

4.3.2 基于历史项目和同类案例数据，智能推荐适合本项目特点和规模的技术方案，并支持方案的经济技术比选。

4.3.3 结合工程量清单和成本测算模型，辅助确定合理报价区间并提供策略建议。对超低报价等重大报价风险应实施监测预警。

4.3.4 编制施工组织设计、工期排布、资源配置等施工方案应符合GB/T 51235的规定，与BIM模型保持一致。应用BIM技术的建设工程，投标方案应包含BIM技术应用范围、深度和交付标准等要求。

4.3.5 系统生成的投标方案应符合招标文件规定的格式要求和技术深度。

4.4 文件排版填充

4.4.1 按照招标文件规定的格式要求进行自动排版，统一字体、字号、页边距、行距、页码等格式要素。

4.4.2 将投标人基础信息库中的数据自动填充至投标文件的固定模块。固定模块至少包括以下要素：

a) 投标人基本情况表；
b) 法定代表人身份证明；
c) 授权委托书；
d) 财务状况表；
e) 类似项目业绩表；
f) 拟投入人员情况表；
g) 拟投入设备表。

4.4.3 将方案内容按模块化结构填充至相应章节，设定逻辑关联，对无法识别的内容应进行标准化重构。

4.4.4 系统应支持暗标格式编排和敏感信息脱敏处理，自动清除投标人名称、企业标识等可识别信息及文档元数据，并对脱敏结果进行自动校验和人工确认。

4.5 合规性自查比对

4.5.1 解析招标文件要求，从资格条件响应、技术参数响应、商务条款响应等方面对投标人编制的投标文件进行比对。

4.5.2 识别和提示投标文件中的问题包括以下内容：

a) 资格条件：投标人资质等级、类似项目业绩、财务状况、信用记录等；
b) 技术规范：技术参数、技术路线、施工方案、质量措施等；
c) 废标条款：结合已建立的废标条款响应映射关系，对触发废标条件的内容进行专项预警；
d) 时效性要求：投标有效期、工期承诺、财务报表有效期、人员资质有效期、业绩证明时间范围等。

4.5.3 检测投标文件中的错误缺漏、语义歧义、前后矛盾、格式偏差等问题，并标注问题位置和修改建议。

4.5.4 对可能低于成本价的投标进行风险提示。

4.5.5 自查完成后应出具合规自查报告，报告内容应包括：

a) 逐条响应性比对结果；
b) 问题项列表及严重程度等级；
c) 问题定位标注；
d) 修改建议；
e) 综合评估结论；
f) 风险提示等级。

5 数据要求

5.1 数据标准格式

5.1.1 统一结构化数据规范，明确企业资信、人员资质、项目业绩、工程量清单、投标报价等核心数据的字段定义、数据类型、编码规则和命名规范。

5.1.2 结构化数据交换应采用XML通用接口格式，兼容招投标交易平台、电子评标系统、造价软件、BIM模型数据的导入导出规则。

5.1.3 BIM数据格式应符合GB/T 45393.5的规定，宜兼容IFC开放标准。

5.1.4 结构化数据应支持跨系统自动识别、关联匹配与批量同步。

5.1.5 文本类、表单类、证照类附件数据应统一存储格式和命名规则，符合DA/T 103的规定。

5.2 数据质量要求

5.2.1 基础数据、资质证照、业绩合同、人员信息等应真实有效，不应虚构、篡改或使用虚假数据。

5.2.2 数据录入及同步前应设置自动校验规则。

5.2.3 按招标文件要求完整归集必填数据项，关键字段和佐证附件不应缺失，缺项应自动预警。

5.2.4 企业名称、资质等级、人员证书、项目规模等信息在投标文件中应保持前后一致。

5.2.5 建立基础数据库常态化更新机制，定期清理过期资质、注销人员、失效业绩。

6 接口要求

6.1 接口协议规范

6.1.1 接口应采用HTTP/HTTPS标准通信协议，统一数据交换的文件格式、字符编码、报文结构和访问控制规则。

6.1.2 接口管理应满足以下要求：

a) 信息交换方式应符合XML数据交换标准；
b) 交互操作服务接口应符合WebServices标准；
c) 系统交互模式支持同步与异步方式，交互数据应支持各种数据类型。

6.1.3 接口应支持结构化数据、版式文件及附件的批量导入导出，具备兼容性和可扩展性。

6.1.4 系统接口应开放合规标准通信协议，不应设置技术壁垒，不应限制、排斥符合规范要求的第三方工具软件、造价软件、BIM软件接入对接。

6.1.5 接口技术实现方式应当保持中立性，不绑定特定软硬件平台，符合GB/T 43711的规定。

6.1.6 接口应具备安全校验机制，对请求和数据进行合法性校验和身份鉴别。

6.2 与招投标平台交互

6.2.1 与招投标交易平台的数据交互应按照JGJ/T 393的规定执行，建立标准化双向数据流转机制。

6.2.2 通过标准接口从招标投标平台抓取、同步招投标平台发布的招标公告、招标文件、答疑补遗、项目基础信息等源数据。

6.2.3 投标文件完成校验和签章后，应通过标准接口向平台加密上传，并提供明确的提交状态反馈。

6.2.4 系统应具备断点续传和上传重试机制。

6.2.5 数据传输和操作记录应全程留痕。

6.3 与电子评标系统交互

6.3.1 系统与电子评标系统之间的数据传输应采用加密传输和完整性校验机制。

6.3.2 投标文件应支持被电子评标系统识别、解析和自动评审。

6.3.3 投标文件各组成部分应按照统一的结构化标识体系进行标注。

6.3.4 涉及评审的关键数据项应独立提取并形成结构化数据包。

6.3.5 评标结束后应支持评标数据的合规调取和分项读取。

7 质量控制要求

7.1 准确性控制

7.1.1 招标文件关键要素提取和解析应准确，关键要素提取准确率不应低于95%，评审关键条款解析准确率不应低于90%。准确率按公式（1）计算。

$$A = \frac{N_c}{N_t} \times 100\% \qquad \text{公式（1）}$$

式中：

A——准确率；

N_c——经人工复核确认提取或解析正确的关键要素数量；

N_t——应提取或解析的关键要素总数。

7.1.2 投标方案应与招标文件需求相匹配，核心技术和不可偏离条款应全部响应。

7.1.3 生成报价方案应工程量准确、计价合规，符合GB/T 50500的规定。报价数据应与投标人预设的策略和价格区间一致，最终报价需经投标人审批。

7.1.4 输出结论应提供依据，标注置信度标识，具体要求可参照GB/T 36344。

7.1.5 应通过定期测试和反馈机制验证系统准确性，测试周期不宜超过一个季度，测试结果应存档备查。对不达标项应及时优化。

7.2 完整性保障

7.2.1 检查投标文件是否涵盖招标文件要求的所有内容和响应点，校验结果应与评标办法的缺项预警一致。

7.2.2 投标文件的每一组成部分均应有明确的编制状态标识，辅助用户规范填写内容，并采用颜色标识区分不同操作阶段。

7.2.3 检查各类附件是否齐全并与正文一致，符合DA/T 103的规定。

7.2.4 对缺失内容应生成修正清单，标注缺漏类别和对应的招标文件条款依据。

7.2.5 提交前应进行完整性校核并出具确认报告，对未完成项设置预警提醒，在规定时限内完整提交。

7.3 错误检验

7.3.1 投标文件错误检验应包括以下方面：

a) 语义歧义；
b) 前后矛盾；
c) 格式错误；
d) 格式排版瑕疵；
e) 逻辑不通。

7.3.2 投标文件中的文字表述的规范性错误包括以下内容：

a) 错别字；
b) 数值错误；
c) 文件标识错误；
d) 单位错误；
e) 引用错误。

7.3.3 对关键时间节点的合规性进行监测，时间节点应包括：

a) 投标有效期；
b) 计划工期；
c) 开标日期；
d) 提交截止日期。

7.3.4 检测出的问题应在文件正文中以高亮、批注等形式标记位置，提供修正建议，并按严重等级以问题清单形式输出。

7.3.5 系统应支持二次自动校验。未完成整改的错误应拒绝通过并提示，校验通过后方可生成正式文件。

7.4 人工复核程序

7.4.1 系统输出结果应设置人工复核程序，由具备相应专业能力的人员进行审核确认。

7.4.2 人工复核的重点应包括以下内容：

a) 技术方案可行性：是否符合项目需求和投标人技术能力，BIM模型与施工方案是否匹配；
b) 报价合理性：是否符合成本测算和定价策略，计价合规性是否符合内部审批程序；

c） 资质业绩信息准确性：资质、业绩、人员信息是否在有效期内，是否满足招标文件实质性要求。

7.4.3 系统对人工复核过程中发现的问题应支持在线修订，并记录复核意见和修订人基本信息。

7.4.4 人工复核完成后应形成复核记录留档，复核记录应包括以下内容：

a） 复核人姓名；
b） 复核时间；
c） 复核内容范围；
d） 复核发现及处理结果。

7.4.5 系统应利用人工复核数据持续优化算法模型。对人工复核过程中发现的系统误判、漏判等问题进行分类汇总和分析，定期通过增量学习手段优化模型的算法精度和差错拦截能力。

7.5 合规管理要求

7.5.1 算法模型应具备可解释性。具体包括下列要求：

a） 决策依据可追溯：数据来源标注、推理过程展示、引用条款定位；
b） 输出结果可验证：关键计算过程可查、比对结果可复核、方案推荐可比较；
c） 模型版本与变更可追溯：版本记录、变更影响评估、历史版本可查；
d） 置信度与不确定性标注：置信度等级、不确定性说明、置信度标注方法；
e） 不可解释情形的处理：主动标注、降级处理、人工接管。

7.5.2 投标人对系统生成的投标文件承担最终责任，输出结果须经审查确认后方可使用。

7.5.3 输出结果的模型版本、数据来源和处理过程应可追溯。

8 安全要求

8.1 商业秘密保护

8.1.1 建立数据分类分级管理机制，对不同级别的数据实施相应的访问控制和加密措施。

8.1.2 涉密数据应存储于经授权的设备和系统中，不应存储于非授权设备或网络空间。核心数据应采用加密方式存储。

8.1.3 实施最小权限原则，限制数据访问范围，留存操作审计记录。

8.1.4 编制过程中的中间数据和版本历史应妥善保管，不应在系统外泄露。应自动保存版本快照，废弃文件应及时清除。

8.1.5 建立数据泄露预警和应急响应机制。

8.2 存储传输安全

8.2.1 存储加密应符合GM/T 0095的规定。

8.2.2 敏感数据应实施加密存储，加密算法应符合GM/T 0002的规定。

8.2.3 数据传输应采用不低于TLS 1.2的加密协议。

8.2.4 数字证书管理应符合GM/T 0031的规定。

8.2.5 入侵检测系统的安全技术要求和测试评价方法应符合GB/T 20275的规定，防范常见的网络攻击，部署入侵检测、恶意代码防范等安全措施。防火墙安全技术要求和测试评价方法应符合GB/T 20281的规定，信息系统还应符合GB/T 22239的规定。

8.2.6 系统应具备完整的数据备份和容灾能力，符合GB/T 20988的规定。

8.3 用户权限管理

8.3.1 用户访问管理和访问控制应符合GB/T 22081的规定。

8.3.2 访问控制管理满足以下要求：

a) 应具备用户功能使用、数据访问的权限及其时限控制功能；
b) 应识别非授权访问，不应同一账号多处同时登录；
c) 权限设置应遵循最小化原则，系统开发权、管理权和业务权应相互分离；
d) 对重要信息资源设置敏感。

8.3.3 系统用户身份识别与认证应采用CA数字证书认证、CA扫码人脸等方式完成身份认证和登录验证。

8.3.4 记录所有用户的操作行为，用户行为日志应包括以下内容：

a) 操作用户信息；
b) 操作时间；
c) 操作对象；
d) 操作内容；
e) 操作结果。

8.3.5 对员工及第三方人员的权限定期进行复审，对离职、离岗人员的账号和权限应立即终止。