附件1

**浙江省人民医院毕节医院2025年23个业务系统评级定级采购项目报名登记表**

报价单位名称：

单位地址：

联系人： ; 联系电话：

我单位已认真阅读并理解贵方发布的浙江省人民医院毕节医院2025年23个业务系统评级定级采购项目的询价要求，满足贵方“供应商资格要求”的所有内容。我方报名参加本次公开询价活动，并郑重承诺所提供的报价内容真实有效。

单位名称（盖章）：

日期：2025年 月 日

附件2：采购需求

一、项目概况

因评级政策调整，我院除HIS、PACS、LIS三个系统为三级等级保护，其余的23个系统需要有资质的评测机构进行评级定级才能满足整改的相关要求，现申请立项对我院23个业务系统的评级定级项目进行采购。

1. 项目目标

1.梳理信息系统信息，明确现有信息系统清单。

2.完成医院现有信息系统（含一级系统）的等级保护定级，确保定级结果准确、合理。

3.保证定级工作严格符合《网络安全法》及等保国标的要求，具备合规性。

4.对定级系统中涉及用户数据的信息系统开展数据安全评估。

三、商务要求

| **序号** | **评审因素** | **评审标准** | **备注** |
| --- | --- | --- | --- |
| 1 | 授权书 | 提供法定代表人（单位负责人）身份证明或授权委托书（法定代表人（单位负责人）授权文件应包含法定代表人（单位负责人）章或签字授权委托书及响应供应商为被授权人缴纳的2024年6月至今任意3个月社保证明材料） |  |
| 2 | 营业执照或身份证明 | 提供法人或其他组织的营业执照等证明文件或自然人身份证明 | 响应供应商按采购文件要求提供复印件并加盖公章 |
| 3 | 财务要求 | 提供2023年度或2024年度经第三方审计机构出具的完整财务审计报告（内容须包含审计报告意见、资产负债表、利润表、现金流量表、会计师事务所营业执照、会计师事务所执业许可证、财务审计报告应盖有会计师事务所单位章和注册会计师的执业专用章）；成立不足一年的出具开户银行的资信证明 | 响应供应商按采购文件要求提供复印件并加盖公章 |
| 4 | 未列入失信被执行人名单 | 响应供应商不得为“信用中国”网站（www.creditchina.gov.cn）中列入失信被执行人和重大税收违法失信主体的供应商（查询窗口为“信用服务”中《重点领域严重失信主体名单查询》下“失信被执行人”和“重大税收违法失信主体”）。提供信用信息查询截止时间为公告时间段内的网页截图或自行承诺（承诺函格式自拟） | 截图加盖公章 |
| 5 | 依法缴纳税收和社会保障 | 提供依法缴纳税收（2024年6月至今任意三个月的纳税证明）和社会保障资金（2024年6月至今任意三个月的社保缴纳证明）的相关材料 | 提供复印件并加盖公章 |
| 6 | 经营活动中没有重大违法犯罪记录的书面声明 | 参加采购活动前3年内，在经营活动中没有重大违法记录（重大违法记录是指投标人因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款（≥200万元）等行政处罚）。投标人近3年内在招标人组织的采购活动中不存在因违约或违法行为或失信行为取消其投标资格的。（自行声明，加盖公章）； | 提供声明原件 |
| 7 | 业绩 | 响应供应商自2022年1月1日以来具有类似项目业绩，每提供1个有效业绩得3分，满分12分。  注：提供合同首页、合同关键页及其签字盖章页的合同复印件并加盖响应供应商公章，未按要求提供或未提供不得分。 |  |
| 8 | 实施要求 | 项目要求在签订合同后10个日历日内完成系统的梳理、定级和专家评审工作，提供供应商承诺函 |  |

# 四、技术要求

1.投标人需组建专项调研团队，团队成员需包含至少 2 名具备 5 年以上医疗行业数据安全服务经验的高级工程师，且熟悉医疗信息系统架构（如 HIS、LIS、PACS 系统数据流转逻辑）。​

2.需采用 “系统梳理 + 业务访谈” 相结合的方式，完成医院所有信息系统的摸底：​

3.系统梳理：逐一排查医院在用信息系统，明确各系统的功能定位（如诊疗服务、运营管理、科研支持）、数据资产类型（参考医院 “核心数据 / 重要数据 / 一般数据” 分类）、服务对象（患者、医护人员、管理人员）及业务依赖关系（如电子病历系统与 HIS 系统的数据交互）。​

4.业务访谈：覆盖医院信息科、医务处、护理部、科研处等至少 8 个核心部门，每个部门访谈对象不少于 2 人（部门负责人 + 业务骨干），需形成访谈记录并由受访人签字确认，重点明确各系统的业务重要性、数据敏感程度及安全需求。​

5.需依据《网络安全等级保护基本要求》中 “信息系统安全等级保护定级指南”，结合医疗行业特性，按 “自主定级 - 专家论证 - 主管部门确认” 三步完成定级：​

6.自主定级：针对每个系统，从 “业务信息安全” 和 “系统服务安全” 两个维度打分，业务信息安全维度重点考虑数据泄露、篡改对患者权益、医院运营的影响（如核心数据泄露影响程度为 “严重”），系统服务安全维度重点考虑系统中断对诊疗业务的影响（如电子病历系统中断影响 “关键业务”），综合确定定级结果（二级 / 三级 / 四级）。

7.专家论证：组织专家论证会，论证内容需涵盖定级依据、打分逻辑、行业适配性，形成《定级论证报告》并由专家签字。​

8.需编制《信息系统安全等级定级报告》，每个系统单独成册，内容需包含系统基本信息、定级依据、打分明细、论证意见、最终等级，且需附 “系统拓扑图”“数据资产清单”“访谈记录摘要” 等支撑材料，格式需符合主管部门备案材料规范。​

9.材料完整性与合规性​

需按主管部门要求，编制全套备案材料，至少包含《网络安全等级保护备案表》（系统单独填写，三级及以上系统需填写详细表，二级系统填写简易表）、《定级报告》《网络安全管理制度清单》《技术防护方案摘要》等，材料需满足：​

（1）完整性：无缺项漏项，如备案表中 “系统边界”“安全保护等级”“主要安全需求” 等字段需填写准确，不得留白；管理制度清单需包含数据全生命周期管理、人员安全、应急响应等至少 15 项核心制度（参考《医疗卫生机构网络安全管理办法》要求）。​

（2）合规性：材料引用法规标准需最新（如引用 GB/T 22239-2019 而非旧版标准），数据分类分级需与医院现有体系一致，技术防护方案需体现与定级等级匹配的措施（如三级系统需包含入侵防御、安全审计、异地备份等措施）。

针对三级及以上系统，需额外编制《安全建设整改方案》（若未达到等保要求），方案需明确整改目标（如 “6 个月内完成入侵防御系统部署”）、整改内容（技术措施 + 管理措施）、责任分工（投标人协助医院信息科实施）、时间节点（分阶段推进，每个阶段有可验证成果）及预算估算（需列出主要设备 / 服务的单价、数量），确保方案具备可落地性。

10.材料审核与优化投标人需建立 “三级审核” 机制，对备案材料进行内部审核：​

一级审核（专员审核）：由项目组专员逐一核对材料完整性、字段准确性，如检查备案表中系统名称与实际系统是否一致，定级报告中打分逻辑是否连贯。​

二级审核（技术负责人审核）：由项目技术负责人（需具备等保高级测评师资质）审核材料的技术合规性，如技术防护方案是否满足对应等级的等保要求，整改方案的技术可行性。​

三级审核（合规负责人审核）：由项目合规负责人（需具备法律职业资格或医疗数据合规认证）审核材料的法规适配性，如是否符合《数据安全法》中 “重要数据保护” 要求，是否规避备案流程中的合规风险。​

1. 需协助医院将备案材料提交主管部门进行预审，根据预审反馈在 3个工作日内完成材料修改，如补充某系统的 “业务连续性预案”、调整某系统的定级打分依据。

# 五、服务内容

## 1.信息系统识别与分析

对现有信息系统资产进行梳理，明确系统资产内容（包含信息资产和数据资产）、系统重要性、被攻击产生的影响范围及侵害程度。

### 2.拟定级系统

| **序号** | **等保定级** | **系统名称** | **包含子系统** | **定级依据** |
| --- | --- | --- | --- | --- |
| 1. 1 | 二级 | 病案系统 | 病案系统 | 存储患者全周期病案（手术记录、病理报告），是医保结算、医疗纠纷鉴定核心依据；数据丢失致医院无法应对审计，符合二级 “对单位合法权益严重损害” 标准。 |
| 1. 2 | 二级 | 数据中心 | 数据中心 | 为 HIS、LIS、PACS 等核心系统提供数据调用接口 |
| 1. 3 | 二级 | 集成平台 | 集成平台 | 负责核心系统间数据交互（如 HIS 与 LIS 同步），无独立业务逻辑；仅传输数据不存储，故障可人工导入 / 导出替代，超 8 小时仅影响效率，符合二级标准。 |
| 1. 4 | 二级 | 重症系统 | 重症系统 | 记录 ICU 患者生命体征、治疗方案；仅影响 ICU 科室，故障可人工记录，超 2 小时仅降低 ICU 效率，符合二级标准。 |
| 1. 5 | 二级 | 虚拟资源池 | 虚拟资源池 | 承载医院内部信息系统运行 |
| 1. 6 | 一级 | 输血系统 | 输血系统 | 管理输血申请、配血结果，关联患者用血安全；仅波及输血科 + 外科，故障可人工核对配血单，超 4 小时影响局部患者，符合一级标准。 |
| 1. 7 | 一级 | 手麻系统 | 手麻系统 | 管理手术室麻醉记录、麻醉药品使用；仅影响手术室，故障可人工记录，超 2 小时影响手术排期，符一级标准。 |
| 1. 8 | 一级 | 心电系统 | 心电系统 | 存储心内科心电报告 + 波形；仅影响心内科门诊，故障可打印纸质报告，超 8 小时影响门诊量，符合一级标准。 |
| 1. 9 | 一级 | 病理系统 | 病理系统 | 存储病理诊断报告 + 切片数据；仅影响病理科 + 肿瘤科，故障可人工出具报告，超 4 小时影响诊断效率，符合一级标准。 |
| 1. 10 | 一级 | 血液透析系统 | 血液透析系统 | 记录肾内科透析参数；仅影响肾内科，故障可本地设备记录，超 4 小时影响透析排期，符合一级标准。 |
| 1. 11 | 一级 | 生殖系统 | 生殖系统 | 管理生殖科辅助生殖治疗数据；仅影响生殖科，故障可人工记录，超 8 小时影响治疗进度，符合一级标准。 |
| 1. 12 | 一级 | 门诊辅助服务系统 | 自助挂号系统、银医系统、排队叫号系统 | 提供挂号、缴费、叫号、物流等辅助功能；无敏感数据存储，故障可人工完全替代，无诊疗影响，符合一级标准。 |
| 1. 13 | 一级 | 微信公众号 | 微信公众号 | 辅助服务入口，核心数据存于医院后台，故障后无诊疗影响。 |
| 1. 14 | 一级 | 合理用药系统 | 合理用药系统 | 用药辅助提醒，核心决策依赖医生 / 药师，故障后仅增加人工审核量，不影响用药安全。 |
| 1. 15 | 一级 | 医护办公辅助系统 | hi 医生系统 HI 护士系统、CDSS 系统 | 记录护理过程、辅助医生决策 / 办公；不影响核心诊疗操作，故障仅增加人工量，符合一级标准。 |
| 1. 16 | 一级 | 护理文书 | 护理文书 | 记录护理过程信息（如输液时间、生命体征记录），故障后可通过纸质临时记录，恢复后补录，不影响医嘱执行、检验检查等核心环节，无高敏感数据。 |
| 1. 17 | 一级 | 行政运营管理系统 | 对账平台 SPD 系统 HRP 系统 绩效管理系统 人事管理系统 | 负责财务对账、供应链、人员管理、办公自动化；无诊疗数据，故障可人工台账 / 纸质办公替代，符合一级标准。 |
| 1. 18 | 一级 | OA系统 | OA系统 | 办公自动化，故障后纸质办公可替代，不影响核心业务。 |
| 1. 19 | 一级 | 监测上报系统 | 院感系统 传染病系统 食源性上报系统 HQMS 系统 | 承担监测、上报、运维功能；无核心数据，故障可延迟处理 / 人工统计，符合一级标准。 |
| 1. 20 | 一级 | 医保智能审核系统 | 医保智能审核系统 | 报销审核辅助，故障后人工审核可替代，不影响患者报销。 |
| 1. 21 | 一级 | 医疗辅助系统 | 追溯系统 DIP 系统 蓝蜻蜒系统 | 提供供应链追溯、医保辅助、体检等功能；无敏感数据，故障无诊疗影响，符合一级标准。 |
| 1. 22 | 一级 | 血糖监测系统 | 血糖监测系统 | 血糖记录，故障后血糖仪直接读取数据，不影响治疗决策。 |
| 1. 23 | 一级 | 体检系统 | 体检系统 | 体检业务管理，非诊疗核心数据，故障后纸质报告可替代。 |

## 3.系统定级

（1）针对新建或改扩建等需定级的信息系统，开展信息系统业务梳理及资产识别，组织信息安全领域专家完成评审（含一级系统），依据《信息安全技术 网络安全等级保护定级指南》（GB/T 22240）等标准以及行业要求，确定信息系统安全保护等级（含一级系统），并形成输出定级备案表、定级报告、专家签字的定级评审意见等材料；

（2）如涉及系统需提交公安备案，则协助客户在市公安局网安部门完成备案工作。准备备案材料，包括定级报告、备案表等。

## 4.数据安全评估

依据相关法律法规和国家标准、行业标准对具有用户数据的信息系统开展数据安全风险评估，并出具符合相关要求的评估报告。

### 5.评估范围

涵盖医院信息系统内所有数据，包括但不限于患者电子病历（含诊断记录、检验检查报告、用药信息等）、医护人员信息、医院财务数据、医疗设备运行数据、科研项目数据，以及数据产生、采集、存储、传输、使用、共享、销毁全生命周期涉及的信息系统、网络设施、人员操作等环节。

### 5.评估目标

（1）全面梳理医院数据资产，明确数据分布、类型与敏感程度。

（2）依据法规与行业标准，评估数据安全管理现状，识别潜在风险点。

（3）提出针对性整改建议，助力医院构建完善数据安全防护体系，确保数据合规、安全、有效利用。

### 6.评估内容

#### （1）数据资产梳理与分类分级

数据资产梳理：经全面梳理，医院数据资产主要包括：

患者医疗数据：电子病历（门诊病历、住院病历）、影像检查数据（X 光、CT、MRI 等影像资料）、检验检查报告、患者健康档案等。

人员数据：医护人员基本信息（姓名、身份证号、职称、联系方式）、员工绩效考核数据、培训记录等；患者家属信息（在涉及患者紧急联络等场景下收集）。

医院运营数据：财务数据（收支明细、医保结算数据）、物资管理数据（药品库存、医疗器械采购与使用数据）、医院行政管理数据（会议纪要、文件通知、排班信息）等。

科研数据：临床科研项目数据（实验数据、研究报告、病例对照数据）、医学科研论文数据、科研设备运行数据等。

数据分类分级：依据《卫生健康行业数据分类分级指南（试行）》，将医院数据分为核心数据、重要数据和一般数据三个级别：

核心数据：涉及患者个人敏感信息且一旦泄露、篡改或丢失可能对患者生命健康、人身财产安全造成严重损害的数据，如患者基因检测数据、重大疾病诊断与治疗方案、涉及患者隐私的罕见病病历；医院核心财务数据（年度财务报表、资金往来关键记录）；高价值科研项目的关键实验数据等。

重要数据：患者一般医疗信息（普通疾病诊断、常规检验检查结果）、医护人员敏感信息（如薪酬数据、职业资格证书信息）、医院运营关键数据（如药品与医疗器械采购价格数据、医保结算总体数据）等。

一般数据：医院一般性行政管理数据（如内部通知、会议安排）、不涉及个人敏感信息的患者统计数据（如疾病发病率统计、就诊人次统计）、医院后勤管理数据（如食堂食材采购数据、保洁排班数据）等，对医院运营与患者权益影响相对较小。

#### （2）数据安全风险识别

a.技术风险

网络安全风险：医院网络边界防护薄弱，防火墙规则配置不合理，可能导致外部黑客入侵，窃取或篡改数据。

系统漏洞风险：信息系统未及时更新安全补丁，存在已知安全漏洞，如 Windows 操作系统漏洞、医院自研业务系统代码漏洞等，可能被攻击者利用，获取系统权限，进而访问敏感数据。

数据存储风险：数据存储介质老化、损坏，未建立有效的数据备份与恢复机制，可能导致数据丢失。

b.管理风险

制度不完善风险：医院数据安全管理制度不健全，缺乏数据全生命周期各环节（采集、存储、传输、使用、共享、销毁）的详细操作规范与安全要求。

人员管理风险：员工数据安全意识淡薄，存在随意泄露患者信息、违规操作数据等行为。

c.物理风险

自然灾害风险：医院数据中心所在区域面临地震、洪水、火灾等自然灾害威胁，若未建立异地灾备中心，一旦发生重大自然灾害，数据中心设施受损，将导致数据丢失且难以恢复。

设备故障风险：数据中心服务器、存储设备、网络设备等硬件故障，如服务器主板损坏、硬盘故障、网络交换机死机等，可能影响数据的正常访问与存储，造成业务中断。

物理访问风险：数据中心物理访问控制不严格，无关人员可随意进入，存在数据存储设备被盗、被破坏风险。

# 六、其他要求

**1.服务期**

项目要求在签订合同后10个日历日内完成系统的梳理、定级和专家评审工作，要求供应商提供承诺函。

**2.考核验收方式**

（1）项目验收：服务完成后，经成交供应商内部自查通过，即可按照项目进度配合采购人进行验收，所有服务成果符合采购文件要求。同时成交供应商须提供软件文档（包括但不限于《定级系统清单》《系统定级报告》《专家评审意见表》《网络数据安全评估报告》等，验收通过后出具验收报告。

（2）验收范围：以采购文件、响应文件规定有利于采购人的建设（服务）内容及要求、提交的服务文档等成果资料。

（3）验收内容主要以国家、行业相关技术标准规范、采购/响应文件确认建设（服务）内容为依据，对相关建设（服务）内容进行逐一核查。

（4）成交供应商须为验收提供必需的一切条件及相关费用。

**3.付款方式**

完成服务并经招标方验收合格后，招标方收到中标方提供的正规发票和相关验收材料后60个日历日内支付全部款项。

**4.违约责任**

（1）中标方未按约定期限提供相关服务或拒绝签订合同的，除了要赔偿招标方和采购代理机构在本次招标活动中产生的一切费用外，还将报请政府采购监督管理部门按相关法律法规规定对中标方追究相应的经济和法律责任。

（2）合同任意一方单方面原因导致合同无法履行的，需向另一方支付合同总金额20%的违约金。

（3）在招标过程中或服务期内，中标方提供虚假材料的，经查实后招标方有权终止合同，中标方须退还已支付的全部款项，并支付合同总金额20%的违约金。

附件3

**（公司名称）报价单**

|  |  |  |
| --- | --- | --- |
| **项目名称** | **总价(元）** | **备注** |
| 浙江省人民医院毕节医院2025年23个业务系统评级定级采购项目 |  |  |

注：1.该公开询价并非采购行为，各单位提供的相关服务信息仅用于提高本单位对该服务的认知，不作为本单位采购行为的任何承诺。

2.供应商参与报价时，需考虑代理服务等成本。

公司名称（盖章）：

联系电话：

日期：